OS/390
Integrated Cryptographic Service Facility

Application Programmer's Guide

SC23-3976-07

OS/390
Integrated Cryptographic Service Facility

IBM

Application Programmer’s Guide

SC23-3976-07

Note!

Before using this information and the product it supports, be sure to read the general information in the "Appendix N. Notices" on page 429.

Eighth Edition (September 2000)

This is a major revision of SC23-3976-06.

This edition applies to Version 2 Release 10 of the Integrated Cryptographic Service Facility, 5647-A01, and to all subsequent releases and modifications until otherwise indicated in new editions.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address below.

IBM welcomes your comments. A form for readers' comments may be provided at the back of this publication, or you may address your comments to the following address:

International Business Machines Corporation
Department 55JA, Mail Station P384
2455 South Road
Poughkeepsie, NY 12601-5400
United States of America

FAX (United States & Canada): 1+845+432-9405
FAX (Other Countries):
Your International Access Code +1+845+432-9405

IBMLink (United States customers only): IBMUSM10(MHVRCFS)
IBM Mail Exchange: USIB6TC9 at IBMMAIL
Internet e-mail: mhvrcfs@us.ibm.com
World Wide Web: http://www.ibm.com/s390/os390/webqs.html

If you would like a reply, be sure to include your name, address, telephone number, or FAX number.

Make sure to include the following in your comment or note:
- Title and order number of this book
- Page number or topic related to your comment

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 1997, 2000. All rights reserved.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures . . . xv

Tables . . . xvii

About This Book . . . xxi
Who Should Use This Book . . . xxi
How To Use This Book . . . xxi
Where To Find More Information . . . xxiii
  Related Publications . . . xxiii
Do You Have Problems, Comments, or Suggestions? . . . xxiv

Summary of Changes . . . xxvii

Part 1. Data Encryption Standard (DES) Cryptography . . . 1

Chapter 1. Introducing ICSF and DES Cryptography . . . 3
Functions of the DES Cryptographic Keys . . . 3
  Key Separation . . . 3
  Master Key Variant . . . 4
  Transport Key Variant . . . 4
  Key Forms . . . 5
  Control Vector. . . . 5
  Types of Keys. . . . 5
  Special Secure Mode . . . 9
Generating and Managing DES Keys. . . . 10
  Key Generator Utility Program . . . 10
  Common Cryptographic Architecture DES Key Management Services. . . . 10
  Dynamic CKDS Update Callable Services . . . 12
  System Encryption Algorithm . . . 13
  ANSI X9.17 Key Management Services . . . 14
Enciphering and Deciphering Data. . . . 16
Encoding and Decoding Data . . . 16
Generating Random Numbers . . . 16
Translating Ciphertext . . . 16
Managing Data Integrity and Message Authentication . . . 16
  Message Authentication Code Processing . . . 17
  Hashing Functions . . . 18
  Verifying Credit Card Data. . . . 19
Managing Personal Authentication . . . 19
  Clear PIN Generate Callable Service . . . 20
| Encrypted PIN Generate Callable Service . . . 20
| Clear PIN Encrypt Callable Service . . . 20
  Clear PIN Generate Alternate Callable Service . . . 20
  Encrypted PIN Verify Callable Service . . . 20
  Encrypted PIN Translate Callable Service . . . 20
Trusted Key Entry (TKE) Support . . . 21
Utilities . . . 21
  Key Token Build Callable Service . . . 21
| Cryptographic Variable Encipher Callable Service . . . 21
| Control Vector Generate Callable Service . . . 21
| Control Vector Translate Callable Service . . . 21
  Code Conversion Callable Services . . . 21
  Character/Nibble Conversion Callable Services . . . 22

© Copyright IBM Corp. 1997, 2000

X9.9 Data Editing Callable Service 22

Chapter 2. Programming Considerations 23
Callable Service Syntax 23
Callable Services with ALET Parameters 24
Rules for Defining Parameters and Attributes 24
Parameter Definitions 26
Invocation Requirements 29
Security Considerations. 29
Performance Considerations 29
Summary of the DES Callable Services 30

Chapter 3. Using the Callable Services 35
Understanding Key Form and Key Flow 35
Key Form 35
DES Key Flow 36
Creating Keys 36
Generating an Operational Key 37
Generating an Importable Key 37
Generating an Exportable Key 38
Linking a Program with the ICSF Callable Services 38
Typical Sequences of ICSF Callable Services 38
Key Forms and Types Used in the Key Generate Callable Service 40
Purpose of Single and Double-Length Keys in One Form Only 40
Purpose of OPIM, OPOP, and IMIM Single- and Double-Length Keys in Two Forms 40
Purpose of OPEX Single- and Double-Length Keys in Two Forms 41
Purpose of IMEX Single- and Double-Length Keys in Two Forms 43
Purpose of EXEX Single- and Double-Length Keys in Two Forms 43
Generating AKEKs 44
Using the Ciphertext Translate Callable Service 44
When the Call Succeeds 45
When the Call Does Not Succeed 46

Chapter 4. Managing Cryptographic Keys 47
The Key Generator Utility Program 47
The Key Generate Callable Service 48
The Key Import and Key Export Callable Services 48
Prohibiting Export 48
Generating a Verification Pattern and Verifying a Key 48
The Dynamic CKDS Update Callable Services 48
Changing a CDMF DATA Key to a Transformed Shortened DES DATA Key. . . 48
Generating a User-Derived Key 49
Clear Key Import (CSNBCKI). 49
Format 49
Parameters 49
Usage Note 50
Multiple Clear Key Import (CSNBCKM) 50
Format 51
Parameters 51
Usage Note 52
| Data Key Import (CSNBDKM) 53
| Format 53
| Parameters 53
| Restriction 54
| Usage Notes. 54

Data Key Export (CSNBDKX) 54
Format 55
Parameters 55
Usage Note 56
Key Export (CSNBKEX) 56
Format 57
Parameters 57
Usage Notes. 60
| Prohibit Export (CSNBPEX) 60
| Format 61
| Parameters 61
| Restriction 61
| Usage Note 61
Prohibit Export Extended (CSNBPEXX) 62
Format 62
Parameters 62
Key Generate (CSNBKGN) 63
Format 63
Parameters 63
Restriction 71
Usage Notes. 71
| Key Translate (CSNBKTR) 73
| Format 73
| Parameters 73
| Restriction 74
| Usage Note 74
Key Import (CSNBKIM) 74
Format 75
Parameters 75
Usage Notes. 78
Key Part Import (CSNBKPI) 79
Format 79
Parameters 79
Restriction 81
Usage Note 81
Related Information 81
Secure Key Import (CSNBSKI) 81
Format 82
Parameters 82
Multiple Secure Key Import (CSNBSKM) 84
Format 85
Parameters 85
Usage Notes. 88
Key Test (CSNBKYT and CSNBKYTX) 88
Format 89
Parameters 89
Usage Notes. 91
Key Record Create (CSNBKRC) 92
Format 92
Parameters 92
Restrictions 93
Usage Notes. 93
Key Record Delete (CSNBKRD) 93
Format 93
Parameters 93
Restrictions 94

Key Record Read (CSNBKRR) 95
Format 95
Parameters 95
Restrictions 96
Key Record Write (CSNBKRW) 96
Format 96
Parameters 96
Restrictions 97
Related Information 97
Transform CDMF Key (CSNBTCK) 97
Format 98
Parameters 98
Restrictions 99
Usage Notes. 99
User Derived Key (CSFUDK). 99
Format 100
Parameters. 100
Usage Note 102

Chapter 5. Managing Keys According to the ANSI X9.17 Standard 103
ANSI X9.17 EDC Generate (CSNAEGN) 103
Format 103
Parameters. 103
Usage Notes 105
ANSI X9.17 Key Export (CSNAKEX) 105
Format 106
Parameters. 106
Usage Note. 110
ANSI X9.17 Key Import (CSNAKIM). 110
Format 110
Parameters. 110
Usage Note. 114
ANSI X9.17 Key Translate (CSNAKTR) 114
Format 115
Parameters. 115
Usage Note. 118
ANSI X9.17 Transport Key Partial Notarize (CSNATKN) 119
Format 119
Parameters. 119
Usage Note 120

Chapter 6. Protecting Data 121
Modes of Operation. 121
Cipher Block Chaining (CBC) Mode 121
Electronic Code Book (ECB) Mode 121
Triple DES Encryption 121
Processing Rules 122
Encipher (CSNBENC and CSNBENC1) 123
Choosing between CSNBENC and CSNBENC1 124
Format 125
Parameters. 125
Restrictions. 129
Related Information. 129
Decipher (CSNBDEC and CSNBDEC1) 130
Choosing Between CSNBDEC and CSNBDEC1 131
Format 131

Parameters . . . 132
Restrictions . . . 135
Usage Note . . . 135
Related Information . . . 135
Encode (CSNBECO) . . . 135
Considerations . . . 136
Format . . . 136
Parameters . . . 136
Restriction . . . 137
Decode (CSNBDCO) . . . 137
Considerations . . . 137
Format . . . 137
Parameters . . . 137
Restriction . . . 138

Chapter 7. Generating Random Numbers . . . 139
Random Number Generate (CSNBRNG) . . . 139
Format . . . 139
Parameters . . . 139

Chapter 8. Translating Ciphertext . . . 141
Ciphertext Translate (CSNBCTT and CSNBCTT1) . . . 141
Choosing Between CSNBCTT and CSNBCTT1 . . . 141
Format . . . 141
Parameters . . . 142
Restrictions . . . 144
Usage Note . . . 144

Chapter 9. Verifying Data Integrity and Authenticating Messages . . . 145
How MACs are Used . . . 145
How Hashing Functions Are Used . . . 146
How MDCs Are Used . . . 146
How VISA Card Verification Values Are Used . . . 147
MAC Generation (CSNBMGN and CSNBMGN1) . . . 147
Choosing Between CSNBMGN and CSNBMGN1 . . . 148
Format . . . 148
Parameters . . . 148
Restrictions . . . 151
Usage Notes . . . 151
Related Information . . . 151
MAC Verification (CSNBMVR and CSNBMVR1) . . . 152
Choosing Between CSNBMVR and CSNBMVR1 . . . 152
Format . . . 152
Parameters . . . 153
Restrictions . . . 156
Usage Notes . . . 156
Related Information . . . 156
MDC Generation (CSNBMDG and CSNBMDG1) . . . 156
Choosing Between CSNBMDG and CSNBMDG1 . . . 156
Format . . . 157
Parameters . . . 157
Usage Notes . . . 160
Related Information . . . 160
One-Way Hash Generate (CSNBOWH and CSNBOWH1) . . . 160
Format . . . 160
Parameters . . . 161

Usage Note . . . 163
VISA CVV Service Generate (CSNBCSG) . . . 163
Format . . . 164
Parameters . . . 164
Restriction . . . 166
VISA CVV Service Verify (CSNBCSV) . . . 166
Format . . . 167
Parameters . . . 167
Restrictions . . . 169

Chapter 10. Managing Personal Identification Numbers . . . 171
How Personal Identification Numbers (PINs) are Used . . . 171
Translating Data and PINs in Networks . . . 171
PIN Callable Services . . . 171
Generating a PIN . . . 171
| Encrypting a PIN . . . 172
Generating a PIN Validation Value from an Encrypted PIN Block . . . 172
Verifying a PIN . . . 172
Translating a PIN . . . 172
Algorithms for Generating and Verifying a PIN . . . 172
Using PINs on Different Systems . . . 172
PIN-Encrypting Keys . . . 173
| The PIN Profile . . . 173
| PIN Block Format . . . 173
| Format Control . . . 174
| Pad Digit . . . 174
| Recommendations for the Pad Digit . . . 175
Clear PIN Generate (CSNBPGN) . . . 175
Format . . . 176
Parameters . . . 176
| Restriction . . . 178
Usage Note . . . 179
Related Information . . . 179
| Encrypted PIN Generate (CSNBEPG) . . . 179
| Format . . . 179
| Parameters . . . 179
| Restrictions . . . 183
| Usage Note . . . 183
| Clear PIN Encrypt (CSNBCPE) . . . 183
| Format . . . 183
| Parameters . . . 183
| Restrictions . . . 185
| Usage Note . . . 186
Clear PIN Generate Alternate (CSNBCPA) . . . 186
Format . . . 186
Parameters . . . 186
Restriction . . . 190
Usage Notes . . . 190
Encrypted PIN Verification (CSNBPVR) . . . 191
Format . . . 191
Parameters . . . 191
Restrictions . . . 196
Usage Notes . . . 196
Related Information . . . 197
Encrypted PIN Translation (CSNBPTR) . . . 197
Format . . . 197

Parameters . . . 198
| Restriction . . . 202
Usage Notes . . . 202

Chapter 11. DES Utilities . . . 203
Key Token Build (CSNBKTB) . . . 203
Format . . . 203
Parameters . . . 203
Usage Notes . . . 209
Related Information . . . 211
| Cryptographic Variable Encipher (CSNBCVE) . . . 211
| Format . . . 212
| Parameters . . . 212
| Restrictions . . . 213
| Usage Note . . . 213
| Control Vector Generate (CSNBCVG) . . . 213
| Format . . . 213
| Parameters . . . 214
| Usage Notes . . . 215
| Control Vector Translate (CSNBCVT) . . . 215
| Format . . . 216
| Parameters . . . 216
| Restriction . . . 218
| Usage Notes . . . 218
Code Conversion (CSNBXEA and CSNBXAE) . . . 218
Format . . . 219
Parameters . . . 219
Usage Notes . . . 220
Character/Nibble Conversion (CSNBXBC and CSNBXCB) . . . 220
Format . . . 220
Parameters . . . 221
Usage Notes . . . 222
X9.9 Data Editing (CSNB9ED) . . . 222
Format . . . 223
Parameters . . . 223
Usage Notes . . . 224

Chapter 12. Trusted Key Entry Workstation Interfaces . . . 225
PCI Interface Callable Service (CSFPCI) . . . 225
Format . . . 225
Parameters . . . 225
Restriction . . . 228
Usage Note . . . 228
PKSC Interface Callable Service (CSFPKSC) . . . 229
Format . . . 229
Parameters . . . 229
Restrictions . . . 230

Part 2. Public Key Cryptography . . . 231

Chapter 13. Introducing PKA Support . . . 233
PKA Key Algorithms . . . 233
The RSA Algorithm . . . 233
Digital Signature Standard (DSS) . . . 233
PKA Master Keys . . . 233
PKA Callable Services . . . 234

Callable Services Supporting Digital Signatures 235
Callable Services for PKA Key Management 235
Callable Services to Update The Public Key Data Set (PKDS) 236
Callable Services for Working with Retained Private Keys. 236
Callable Services for Distributing CDMF and DES DATA Keys 237
Callable Services for SET Secure Electronic Transaction 237
Callable Services that Support Secure Sockets Layer (SSL) 238
PKA Utility 238

Chapter 14. Programming Considerations for PKA 241
PKA Key Tokens 241
PKA Key Management 242
Invocation Requirements 243
Exits 243
Security and Integrity of the Token 243
Key Identifier for PKA Key Token 243
Key Label 244
Key Token 244
The Transaction Security System and ICSF Portability 245
Summary of the PKA Callable Services 245

Chapter 15. Using Digital Signatures 247
Digital Signature Generate (CSNDDSG) 247
Format 248
Parameters 248
Restrictions 250
Usage Notes 250
Digital Signature Verify (CSNDDSV) 251
Format 251
Parameters 251
Restrictions 253
Usage Note 253

Chapter 16. Key Distribution 255
Symmetric Key Generate (CSNDSYG) 255
Format 255
Parameters 255
Restrictions 258
Usage Notes 258
Symmetric Key Import (CSNDSYI) 259
Format 259
Parameters 260
Restrictions 262
Usage Notes 262
Symmetric Key Export (CSNDSYX) 262
Format 263
Parameters 263
Restrictions 265
Usage Notes 265

Chapter 17. SET Secure Electronic Transaction 267
SET Block Compose (CSNDSBC) 267
Format 268
Parameters 268
Restrictions 272
Usage Notes 272

SET Block Decompose (CSNDSBD) 272
Format 273
Parameters. 273
Restrictions. 277
Usage Notes 277

Chapter 18. Secure Sockets Layer (SSL) 279
PKA Encrypt (CSNDPKE) 279
Format 280
Parameters. 280
Restrictions. 282
Usage Notes 282
PKA_Decrypt (CSNDPKD) 282
Format 283
Parameters. 283
Restrictions. 285
Usage Notes 285

Chapter 19. PKA Utility 287
PKA Key Token Build (CSNDPKB) 287
Format 287
Parameters. 288
Usage Note 295

Chapter 20. PKA Key Management 297
PKA Key Generate (CSNDPKG) 297
Format 298
Parameters. 298
Restriction 300
Usage Note 300
PKA Key Import (CSNDPKI) 300
Format 301
Parameters. 301
Restrictions. 303
Usage Notes 303
PKA Public Key Extract (CSNDPKX) 303
Format 303
Parameters. 303
Usage Note 305
PKDS Record Create (CSNDKRC) 305
Format 305
Parameters. 305
Restriction 306
Usage Note 306
PKDS Record Write (CSNDKRW) 306
Format 307
Parameters. 307
Restrictions. 308
Usage Note 308
PKDS Record Read (CSNDKRR) 308
Format 309
Parameters. 309
Restriction 310
Usage Note 310
PKDS Record Delete (CSNDKRD) 310
Format 310

Parameters . . . 310
Restrictions . . . 312
Usage Note . . . 312
Retained Key List (CSNDRKL) . . . 312
Format . . . 312
Parameters . . . 312
Restriction . . . 314
Usage Notes . . . 314
Retained Key Delete (CSNDRKD) . . . 314
Format . . . 315
Parameters . . . 315
Restriction . . . 316
Usage Notes . . . 316

Part 3. Appendixes . . . 317

Appendix A. ICSF and TSS Return and Reason Codes . . . 319
ICSF Return Codes and Reason Codes . . . 319
Return Codes . . . 319
ICSF Reason Codes for Return Code 0 (0) . . . 320
ICSF Reason Codes for Return Code 4 (4) . . . 320
ICSF Reason Codes for Return Code 8 (8) . . . 321
ICSF Reason Codes for Return Code C (12) . . . 332
ICSF Reason Codes for Return Code 10 (16) . . . 335
Transaction Security System Return Codes and Reason Codes . . . 335
TSS Reason Codes for Return Code 0 (0) . . . 336
TSS Reason Codes for Return Code 4 (4) . . . 336
Reason Codes for Return Code 8 (8) . . . 337
TSS Reason Codes for Return Code C (12). . . . 341
TSS Reason Codes for Return Code 10 (16) . . . 342

Appendix B. Coding Examples . . . 343
C . . . 343
COBOL . . . 345
Assembler H . . . 347
PL/1 . . . 349

Appendix C. Cipher Processing Rules . . . 355
CBC and ANSI X3.106 . . . 355
ANSI X9.23 and IBM 4700 . . . 355
Segmenting . . . 356
Cipher Last-Block Rules . . . 356
CUSP Considerations . . . 356
The Information Protection System (IPS) . . . 357

Appendix D. PIN Formats and Algorithms . . . 359
PIN Notation . . . 359
PIN Block Formats . . . 359
ANSI X9.8 . . . 359
ISO Format 1 . . . 360
| ISO Format 2 . . . 360
VISA Format 2 . . . 360
VISA Format 3 . . . 360
IBM 4700 Encrypting PINPAD Format . . . 360
IBM 3624 Format . . . 360
IBM 3621 Format . . . 360

ECI Format 2 361
ECI Format 3 361
PIN Extraction Rules 361
Encrypted PIN Verify Callable Service 361
| Clear PIN Generate Alternate Callable Service. 361
Encrypted PIN Translate Callable Service 362
IBM PIN Algorithms. 362
3624 PIN Generation Algorithm 362
German Banking Pool PIN Generation Algorithm 363
PIN Offset Generation Algorithm 364
3624 PIN Verification Algorithm 365
German Banking Pool PIN Verification Algorithm 367
VISA PIN Algorithms 370
PVV Generation Algorithm 370
PVV Verification Algorithm 371
Interbank PIN Generation Algorithm. 371

Appendix E. Transform CDMF Key Algorithm 373

Appendix F. Multiple Decipherment and Encipherment 375
Multiple Encipherment of Single-length Keys 376
Multiple Decipherment of Single-length Keys 376
Multiple Encipherment of Double-length Keys 377
Multiple Decipherment of Double-length Keys 378
Multiple Encipherment of Triple-length Keys. 379
Multiple Decipherment of Triple-length Keys. 380

Appendix G. ANSI X9.17 Partial Notarization Method 383
Partial Notarization 383
Notations Used in the Calculations 383
Partial Notarization Calculation for a Double-Length AKEK 384
Partial Notarization Calculation for a Single-Length AKEK. 384

Appendix H. Key Token Formats 385
Format of the DES Internal Key Token. 385
Token Validation Value 386
DES External Key Token 386
DES Null Key Token 387
Format of the RSA Public Key Token 388
Format of the DSS Public Key Token 389
Format of RSA Private External Key Tokens. 389
RSA Private Key Token, 1024-bit Modulus-Exponent External Form 390
RSA Private Key Token, 2048-bit Chinese Remainder Theorem External Form 391
Format of the DSS Private External Key Token 393
Format of the RSA Private Internal Key Token 394
RSA Private Key Token, 1024-bit Modulus-Exponent Internal Form for Cryptographic Coprocessor Feature 396
RSA Private Key Token, 1024-bit Modulus-Exponent Internal Form for PCI Cryptographic Coprocessor 397
RSA Private Key Token, 2048-bit Chinese Remainder Theorem Internal Form 398
Format of the DSS Private Internal Key Token 399
PKA Null Key Token 401

Appendix I. EBCDIC and ASCII Default Conversion Tables 403

Appendix J. Using BSAFE Applications to Access ICSF Services 405
Some BSAFE Basics 405
Computing Message Digests and Hashes 405
Generating Random Numbers 405
Encrypting and Decrypting with DES 406
Generating and Verifying RSA Digital Signatures 406
| Encrypting and Decrypting with RSA 407
Using the New Function Calls in Your BSAFE Application. 407
Using the BSAFE KI_TOKEN 409
ICSF Triple DES via BSAFE 409
Retrieving ICSF Error Information 410

Appendix K. Control Vector Table. 413
| Specifying a Control-Vector-Base Value 418

| **Appendix L. PKA92 Key Format and Encryption Process 421**

| **Appendix M. Changing Control Vectors with the Control Vector Translate**
| **Callable Service 423**
| Providing the Control Information for Testing the Control Vectors 423
| Mask Array Preparation 423
| Selecting the Key-Half Processing Mode 425
| When the Target Key-Token CV Is Null 427
| Control Vector Translate Example 427

Appendix N. Notices 429
Programming Interface Information 430
Trademarks. 430

Glossary 433

Index 441

Figures

1. The ICSF/MVS Library . . . xxv
2. PKA Key Management . . . 242
3. 3624 PIN Generation Algorithm . . . 363
4. GBP PIN Generation Algorithm . . . 364
5. PIN-Offset Generation Algorithm. . . 365
6. PIN Verification Algorithm . . . 367
7. GBP PIN Verification Algorithm . . . 369
8. PVV Generation Algorithm . . . 371
9. The CDMF Key Transformation Algorithm . . . 373
10. Multiple Encipherment of Single-length Keys . . . 376
11. Multiple Decipherment of Single-length Keys . . . 377
12. Multiple Encipherment of Double-length Keys . . . 378
13. Multiple Decipherment of Double-length Keys . . . 379
14. Multiple Encipherment of Triple-length Keys . . . 380
15. Multiple Decipherment of Triple-length Keys . . . 381
16. Control Vector Base Bit Map (Common Bits and Key-Encrypting Keys) . . . 415
17. Control Vector Base Bit Map (Data Operation Keys) . . . 416
18. Control Vector Base Bit Map (PIN Processing Keys and Cryptographic Variable-Encrypting Keys) 417
| 19. Control Vector Translate Callable Service Mask_Array Processing . . . 425
| 20. Control Vector Translate Callable Service. . . 426

Tables

1. Descriptions of Key Types . . . 7
2. Summary of Data Encryption Standard Bits . . . 14
3. Standard Return Code Values From ICSF Callable Services . . . 26
4. Summary of ICSF DES Callable Services . . . 30
5. Combinations of the Callable Services . . . 39
6. Keywords for Multiple Clear Key Import Rule Array Control Information . . . 52
| 7. Key Type Values for the Key Export Callable Service . . . 58
8. Key Form Values for the Key Generate Callable Service . . . 64
9. Key Length Values for the Key Generate Callable Service . . . 66
10. Key Type Values for the Key Generate Callable Service . . . 67
11. Key Generate Valid Key Types and Key Forms for a Single Key . . . 71
12. Key Generate Valid Key Types and Key Forms for a Key Pair . . . 71
| 13. Key Type Values for the Key Import Callable Service . . . 76
14. Keywords for Key Part Import Control Information . . . 80
15. Key Type Values for the Secure Key Import Callable Service . . . 83
16. Keywords for Multiple Secure Key Import Rule Array Control Information . . . 86
17. Key Type Values for the Multiple Secure Key Import Callable Service . . . 87
18. Keywords for Key Test and Key Test Extended Control Information . . . 90
19. Keywords for User Derived Key Control Information . . . 101
20. Keywords for ANSI X9.17 Key Export Rule Array . . . 107
21. Keywords for ANSI X9.17 Key Import Rule Array . . . 111
22. Keywords for ANSI X9.17 Key Translate Rule Array . . . 116
23. Keywords for the Encipher Rule Array Control Information . . . 127
24. Keywords for the Decipher Rule Array Control Information . . . 133
25. Keywords for the Form Parameter . . . 140
26. Keywords for MAC Generation Control Information . . . 150
27. Keywords for MAC Verification Control Information . . . 154
28. Keywords for MDC Generation Control Information . . . 159
29. Keywords for One-Way Hash Generate Rule Array Control Information . . . 162
30. CVV_Generate rule_array Keywords . . . 165
31. CVV_Verify rule_array Keywords . . . 168
| 32. Format of a PIN Profile . . . 173
| 33. Format Values of PIN Blocks . . . 173
| 34. Format of a Pad Digit . . . 174
| 35. Pad Digits for PIN Block Formats . . . 175
36. Process Rules for the Clear PIN Generate Callable Service . . . 177
37. Array Elements for the Clear PIN Generate Callable Service . . . 178
38. Array Elements Required by the Process Rule . . . 178
| 39. Process Rules for the Encrypted PIN Generate Callable Service . . . 181
| 40. Array Elements for the Encrypted PIN Generate Callable Service . . . 181
| 41. Array Elements Required by the Process Rule . . . 182
| 42. Process Rules for the Clear PIN Encryption Callable Service . . . 184
| 43. Rule Array Elements for the Clear PIN Generate Alternate Service . . . 188
| 44. Rule Array Keywords (first element) for the Clear PIN Generate Alternate Service . . . 188
| 45. PIN Extraction Method Keywords . . . 188
| 46. Data Array Elements for the Clear PIN Generate Alternate Service (IBM-PINO) . . . 189
47. Data Array Elements for the Clear PIN Generate Alternate Service (VISA-PVV) . . . 190
48. PIN Block Variant Constants (PBVCs) . . . 190
| 49. Rule Array Elements for the Encrypted PIN Verification Service . . . 193
50. Calculation methods for the PIN Verification Process . . . 193
| 51. PIN Verification Rule Array Keywords (Second Element) . . . 194
52. Array Elements for the Encrypted PIN Verification Callable Service . . . 195
53. Array Elements Required by the Process Rule . . . 196

© Copyright IBM Corp. 1997, 2000

54. PIN Block Variant Constants (PBVCs) . . . 197
| 55. Rule Array Elements for the Encrypted PIN Translation Service . . . 199
56. Modes for the Encrypted PIN Translation Callable Service . . . 200
| 57. Encrypted PIN Translate Rule Array Keywords (Second Element) . . . 200
58. Additional Names for PIN Formats . . . 202
59. PIN Block Variant Constants (PBVCs) . . . 202
60. Key Type Values for the Key Token Build Callable Service . . . 204
61. Keywords for Key Token Build Control Information . . . 206
| 62. Control Vector Generate and Key Token Build Control Vector Keyword Combinations . . . 210
| 63. Keywords for Control Vector Translate . . . 218
64. Keywords for PCI Interface Callable Service . . . 226
65. Summary of PKA Key Token Sections . . . 241
66. Internal and External Private RSA Key Token Section Identifiers . . . 244
67. Summary of PKA Callable Services . . . 245
68. Keywords for Digital Signature Generate Control Information. . . . 249
69. Keywords for Digital Signature Verify Control Information . . . 252
70. Keywords for Symmetric Key Generate Control Information. . . . 256
71. Keywords for Symmetric Key Import Control Information . . . 260
72. Keywords for Symmetric Key Export Control Information . . . 264
73. Keywords for SET Block Compose Control Information . . . 269
74. Keywords for SET Block Compose Control Information . . . 274
75. Keywords for PKA Encrypt . . . 281
76. Keywords for PKA Decrypt . . . 284
77. Keywords for PKA Key Token Build Control Information . . . 288
78. Key Value Structure Length Maximum Values for Key Types . . . 289
79. Key Value Structure Elements for PKA Key Token Build . . . 290
80. Keyword for PKA Key Generate Rule Array. . . . 299
81. Keywords for PKDS Record Write . . . 308
82. Keywords for PKDS Record Delete. . . . 311
83. ICSF Return Codes . . . 319
84. ICSF Reason Codes for Return Code 0 (0). . . . 320
85. ICSF Reason Codes for Return Code 4 (4). . . . 320
86. ICSF Reason Codes for Return Code 8 (8). . . . 322
87. ICSF Reason Codes for Return Code C (12) . . . 332
88. ICSF Reason Codes for Return Code 10 (16). . . . 335
89. TSS Reason Codes for Return Code 0 (0) . . . 336
90. TSS Reason Codes for Return Code 4 (4) . . . 336
91. TSS Reason Codes for Return Code 8 (8) . . . 337
92. TSS Reason Codes for Return Code C (12) . . . 342
93. TSS Reason Codes for Return Code 10 (16) . . . 342
94. Internal Key Token Format . . . 385
95. Format of External Key Tokens . . . 387
96. Format of Null Key Tokens . . . 388
97. RSA Public Key Token . . . 388
98. DSS Public Key Token . . . 389
99. RSA Private External Key Token Basic Record Format . . . 390
100. RSA Private Key Token, 1024-bit Modulus-Exponent External Format . . . 390
101. RSA Private Key Token, 2048-bit Chinese Remainder Theorem External Format . . . 391
102. DSS Private External Key Token . . . 393
103. RSA Private Internal Key Token Basic Record Format. . . . 394
104. RSA Private Internal Key Token, 1024-bit ME Form for Cryptographic Coprocessor Feature 396
105. RSA Private Internal Key Token, 1024-bit ME Form for PCI Cryptographic Coprocessor . . . 397
106. RSA Private Internal Key Token, 2048-bit Chinese Remainder Theorem External Format 398
107. DSS Private Internal Key Token . . . 399
108. Format of PKA Null Key Tokens . . . 401
109. EBCDIC to ASCII Default Conversion Table . . . 403

110. ASCII to EBCDIC Default Conversion Table 403
111. Control Vector Table 413
| 112. PKA96 Clear DES Key Record 421

About This Book

This book describes how to use the callable services provided by the Integrated Cryptographic Service Facility, which is part of the OS/390 Cryptographic Services. The OS/390 Cryptographic Services includes these components:

- Integrated Cryptographic Service Facility
- OS/390 Open Cryptographic Services Facility (OCSF)

ICSF is a software element of OS/390 that works with the hardware cryptographic feature and the OS/390 Security Server (RACF) to provide secure, high-speed cryptographic services. ICSF provides the application programming interfaces by which applications request the cryptographic services.

Who Should Use This Book

This book is intended for application programmers who:

- Are responsible for writing application programs that use the security application programming interface (API) to access cryptographic functions.
- Want to use ICSF callable services in high-level languages such as C, COBOL, FORTRAN, and PL/I, as well as in assembler.

How To Use This Book

ICSF includes both Data Encryption Standard (DES) and public key cryptography. These are two very different cryptographic systems. Accordingly, this book is divided into two parts that focus on these different processes. In addition, there are several appendixes.

Part 1 focuses on DES cryptography. It includes the following chapters:

- Chapter 1. Introducing ICSF and DES Cryptography gives an overview of the DES cryptographic services.
- Chapter 2. Programming Considerations describes the programming considerations for using the ICSF DES callable services. It also explains the syntax and parameter definitions used in callable services.
- Chapter 3. Using the Callable Services provides general guidance information on how the DES callable services use different key types and key forms. It also discusses how to write your own callable services called installation-defined callable services and provides suggestions on what to do if there is a problem.
- Chapter 4. Managing Cryptographic Keys describes the callable services for generating and maintaining cryptographic keys.
- Chapter 5. Managing Keys According to the ANSI X9.17 Standard describes the callable services that support the ANSI X9.17 key management standard[1], which defines a process for protecting and exchanging DES keys.
- Chapter 6. Protecting Data describes the callable services for enciphering and deciphering data with encrypted keys and encoding and decoding data with clear keys.
- Chapter 7. Generating Random Numbers describes the random number generate callable service, which generates 8-byte random numbers.

1. ANSI X9.17-1985: Financial Institution Key Management (Wholesale)

© Copyright IBM Corp. 1997, 2000

- Chapter 8. Translating Ciphertext describes the callable service for deciphering ciphertext from one key and enciphering it under another key.
- Chapter 9. Verifying Data Integrity and Authenticating Messages describes the callable services for generating and verifying message authentication codes (MACs), generating modification detection codes (MDCs), and generating and verifying VISA card verification values.
- Chapter 10. Managing Personal Identification Numbers describes the callable services for generating, verifying, and translating personal identification numbers (PINs).
- Chapter 11. DES Utilities presents utilities to build DES tokens, generate and translate conrol vectors, convert data between EBCDIC and ASCII format, convert between binary strings and character strings, and edit text strings according to ANSI X9.9-4 editing rules.
- Chapter 12. Trusted Key Entry Workstation Interfaces describes the PCI interface (PCI) and the Public Key Secure Cable (PKSC) interface that supports Trusted Key Entry (TKE), an optional feature available with ICSF.

Part 2 focuses on public key cryptography and includes the following chapters:
- Chapter 13. Introducing PKA Support introduces Public Key Algorithm (PKA) support.
- Chapter 14. Programming Considerations for PKA describes programming considerations for using the ICSF PKA callable services, such as the PKA key token structure and key management.
- Chapter 15. Using Digital Signatures describes the PKA callable services that support using digital signatures to authenticate messages.
- Chapter 16. Key Distribution describes the PKA callable services that support DES key distribution.
- Chapter 17. SET Secure Electronic Transaction describes the callable services that support the Secure Electronic Transaction (SET) protocol.
- Chapter 18. Secure Sockets Layer (SSL) describes the callable services that support Secure Sockets Layer (SSL) security protocol.
- Chapter 19. PKA Utility presents the PKA key token build utility.
- Chapter 20. PKA Key Management describes the PKA callable services that support exchanging PKA keys.

The appendixes include the following information:
- Appendix A. ICSF and TSS Return and Reason Codes explains the return and reason codes returned by the callable services.
- Appendix B. Coding Examples provides examples for COBOL, assembler, and PL/1.
- Appendix C. Cipher Processing Rules describes the cipher processing and segmenting rules.
- Appendix D. PIN Formats and Algorithms describes the PIN formats and algorithms.
- Appendix E. Transform CDMF Key Algorithm describes the algorithm for transforming a Commercial Data Masking Facility (CDMF) key.
- Appendix F. Multiple Decipherment and Encipherment describes multiple encipherment and decipherment and their equations.
- Appendix G. ANSI X9.17 Partial Notarization Method describes the steps of the partial notarization of an ANSI key-encrypting key (AKEK).

- Appendix H. Key Token Formats describes the formats for DES internal, external, and null key tokens and for PKA public, private external, and private internal key tokens containing either Rivest-Shamir-Adleman (RSA) or Digital Signature Standard (DSS) information. This appendix also describes the PKA null key token.
- Appendix I. EBCDIC and ASCII Default Conversion Tables presents EBCDIC to ASCII and ASCII to EBCDIC conversion tables.
- Appendix J. Using BSAFE Applications to Access ICSF Services explains how to access ICSF services from applications written using RSA's BSAFE cryptographic toolkit.
- Appendix K. Control Vector Table contains a table of the default control vector values that are associated with each key type.
- Appendix L. PKA92 Key Format and Encryption Process describes the PKA92 encryption process.
- Appendix M. Changing Control Vectors with the Control Vector Translate Callable Service describes the control information for testing control vectors, mask array preparation, selecting the key-half processing mode, and an example of Control Vector Translate.
- Appendix N. Notices contains notices, programming interface information, and trademarks.
- The Glossary defines terms used in this publication.

Where To Find More Information

For information about the referenced ICSF books, see Figure 1 on page xxv.

Other books referenced in this book are:

- *IBM Common Cryptographic Architecture: Cryptographic Application Programming Interface Reference*, SC40-1675
- *OS/390 MVS Programming: Callable Services for HLL*, GC28-1768
- *OS/390 MVS Programming: Authorized Assembler Services Reference LLA-SDU*, GC28-1766
- *S/390 Support Element Operations Guide*, GC38-3118
- *BSAFE User's Manual*
- *BSAFE Library Reference Manual*

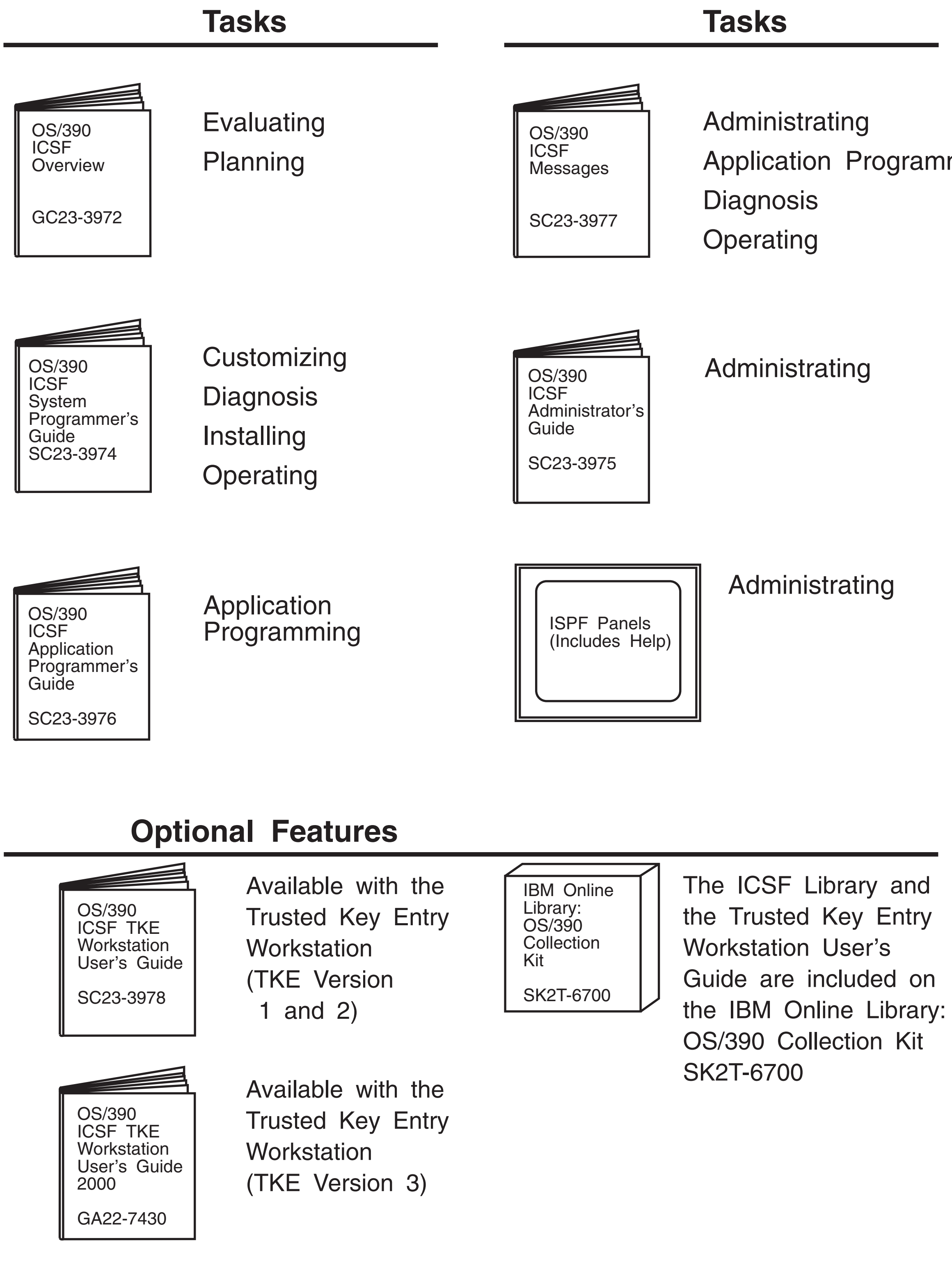
Related Publications

- *OS/390 ICSF TKE Workstation User's Guide 2000*, GA22-7430
- *OS/390 ICSF TKE Workstation User's Guide*, SC23-3978
- *MVS Planning: Security*, GC28-1439
- *IBM ES/9000 ES/3090 Integrated Cryptographic Feature User's Guide*, GA22-7142-05
- *IBM Transaction Security System: General Information Manual and Planning Guide*, GA34-2137
- *IBM Transaction Security System: Concepts and Programming Guide: Volume I, Access Controls and DES Cryptography*, GC31-3937
- *IBM Transaction Security System: Basic CCA Cryptographic Services*, SA34-2362
- *IBM Transaction Security System: Concepts and Programming Guide: Volume II, Public-Key Cryptography*, GC31-2889

- *IBM Distributed Key Management System, Installation and Customization Guide*, GG24-4406

Do You Have Problems, Comments, or Suggestions?

Your suggestions and ideas can contribute to the quality and the usability of this book. If you have problems using this book, or if you have suggestions for improving it, complete and mail the Reader's Comment Form found at the back of the book.



Tasks

OS/390 ICSF Overview GC23-3972 — Evaluating, Planning

OS/390 ICSF System Programmer's Guide SC23-3974 — Customizing, Diagnosis, Installing, Operating

OS/390 ICSF Application Programmer's Guide SC23-3976 — Application Programming

Tasks

OS/390 ICSF Messages SC23-3977 — Administrating, Application Programming, Diagnosis, Operating

OS/390 ICSF Administrator's Guide SC23-3975 — Administrating

ISPF Panels (Includes Help) — Administrating

Optional Features

OS/390 ICSF TKE Workstation User's Guide SC23-3978 — Available with the Trusted Key Entry Workstation (TKE Version 1 and 2)

OS/390 ICSF TKE Workstation User's Guide 2000 GA22-7430 — Available with the Trusted Key Entry Workstation (TKE Version 3)

IBM Online Library: OS/390 Collection Kit SK2T-6700 — The ICSF Library and the Trusted Key Entry Workstation User's Guide are included on the IBM Online Library: OS/390 Collection Kit SK2T-6700

Figure 1. The ICSF/MVS Library

Summary of Changes

Summary of Changes
for SC23-3976-07
OS/390 Version 2 Release 10

New Information:

The following new callable services have been added:

- Clear PIN Encrypt (CSNBCPE)
- Control Vector Generate (CSNBCVG)
- Control Vector Translate (CSNBCVT)
- Cryptographic Variable Encipher (CSNBCVE)
- Data Key Import (CSNBDKM)
- Encrypted PIN Generate (CSNBEPG)
- Key Translate (CSNBKTR)
- Prohibit Export (CSNBPEX)

ISO-2 PIN block format support has been added.

User Defined Extensions (UDX) capabilities are now supported by OS/390 ICSF and the PCI Cryptographic Coprocessor. A new option, UDX(UDX-id,service-number,load-module name,'comment_text',FAIL(fail-option)) has been added to the Installation Options data set.

A new option, WAITLIST(data_set_name), has been added to the Installation Options data set. The WAITLIST parameter points to a modifiable data set which contains the names of services that are placed in the CICS Wait List. If this option is not specified, the default ICSF CICS Wait List will be utilized by ICSF when a CICS application invokes an ICSF callable service.

Additional control vector support was added for the following key types: CIPHER, ENCIPHER, DECIPHER, DATAC, CVARDEC, CVARENC, CVARPINE, CVARXCVL, CVARXCVR, IKEYXLAT, OKEYXLAT

Changed Information: The following services have changed:

- Clear PIN Generate (CSNBPGN) - enhanced to support additional control vectors for the *PIN_generating_key_identifier*
- Clear PIN Generate Alternate (CSNBCPA) - enhanced to support the IBM-PINO rule array keyword, the ISO-2 PIN block format and the specification of a PIN extraction method for 3624 and 3621 PIN block formats
- Data Key Export (CSNBDKX) - enhanced to support additional control vectors for the exporter key
- Encrypted PIN Translate (CSNBPTR) - enhanced to support additional control vectors, the ISO-2 PIN block format, and the specification of a PIN extraction method for the 3624 and 3621 PIN block formats
- Encrypted PIN Verify (CSNBPVR) - enhanced to support additional control vectors, the ISO-2 PIN block format, and the specification of a PIN extraction method for the 3624 and 3621 PIN block formats
- Key Export (CSNBKEX) - enhanced to support additional key type values
- Key Generate (CSNBKGN)

© Copyright IBM Corp. 1997, 2000

  - New keywords (OPOP, IMIM) for the *key_form* parameter
  - New *key_length* value SINGLE-R
  - Enhanced to support additional key type values
- Key Import (CSNBKIM) - enhanced to support additional key type values
- Key Part Import (CSNBKPI) - support extended to all key types and all 4758 supported control vectors
- Key Record Write (CSNBKRW) - support now provided to write a record to the CKDS which contains a key token with a control vector that is not supported by the Cryptographic Coprocessor Feature.
- Key Test (CSNBKYT and CSNBKYTX) - CSNBKYT is now routed to a PCI Cryptographic Coprocessor for processing if ANSI enablement keys are not installed on the CKDS. CSNBKYT is also enhanced to support the VISA verification algorithm (keyword ENC-ZERO). CSNBKYTX must execute on the Cryptographic Coprocessor Feature
- Key Token Build (CSNBKTB) - enhanced to support additional key types, internal and external key tokens, and optional CV Status keywords CV and NO-CV
- Multiple Secure Key Import (CSNBSKM) - enhanced to support additional key types and control vectors
- Retained Key Delete (CSNDRKD) - enhanced to delete a retained key from the PKDS even if the PCI Cryptographic Coprocessor holding the retained key is not online, as long as the FORCE keyword is specified on the invocation of the service
- Secure Key Import (CSNBSKI) - enhanced to support additional key types and control vectors
- SET Block Decompose (CSNDSBD) - new *rule_array* keyword PINBLOCK and support for the output of an encrypted PIN block
- Symmetric Key Generate (CSNDSYG) - new *rule_array* keywords: PKA92, SINGLE, DOUBLE, SINGLE-R
- Symmetric Key Import (CSNDSYI) - new *rule_array* keyword PKA92
- VISA CVV Service Generate (CSNBCSG) - enhanced to support additional control vectors for DATA keys. This services also supports the specification of a MAC key type for key-A and key-B
- VISA CVV Service Verify (CSNBCSV) - enhanced to support additional control vectors for DATA keys. This service also supports the specification of a MAC or MACVER key type for key-A and key-B

Deleted Information: Beginning with OS/390 V2 R10, ICSF will no longer support water cooled processors with ICRF (Integrated Cryptographic Feature).

This book includes terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change.

Summary of Changes for SC23-3976-06 OS/390 Version 2 Release 9

New Information: The following new callable services support the PCI Cryptographic Coprocessor.

- Retained Key List (CSNDRKL)
- Retained Key Delete (CSNDRKD)

- PCI Interface (CSFPCI)

This version introduces support for the 2048-bit Optimized Chinese Remainder Theorem format RSA key.

Changed Information: The following callable services have been changed to support the PCI Cryptographic Coprocessor.

- PKA Key Token Build (CSNDPKB)
- PKA Key Generate (CSNDPKG)
- PKA Key Import (CSNDPKI)
- PKA Key Extract (CSNDPKX)
- Symmetric Key Generate (CSNDSYG)
- Symmetric Key Import (CSNDSYI)
- Symmetric Key Export (CSNDSYX)
- Digital Signature Generate (CSNDDSG)
- Digital Signature Verify (CSNDDSV)
- SET Block Compose (CSNDSBC)
- SET Block Decompose (CSNDSBD)
- PKA Key Encrypt (CSNDPKE)
- PKA Key Decrypt (CSNDPKD)

This book includes terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change.

Summary of Changes for SC23-3976-05 OS/390 Version 2 Release 6 with APAR OW37791

This revision includes support for new key types (DATAM and DATAMV) for the compatibility double-length MAC keys, and withdrawal of support for double-length versions of MAC and MACVER keys.

Summary of Changes for SC23-3976-04 OS/390 Version 2 Release 6

This book includes terminology, maintenance, and editorial changes.

Summary of Changes for SC23-3976-03 OS/390 Version 2 Release 6

This revision includes support for the following enhancements:

- Support for Secure Sockets Layer (SSL)
- Expanded Support for Double-key MAC

Part 1. Data Encryption Standard (DES) Cryptography

This part of the book introduces DES cryptography and its programming considerations. It explains how to use DES callable services.

© Copyright IBM Corp. 1997, 2000

Chapter 1. Introducing ICSF and DES Cryptography

The Integrated Cryptographic Service Facility protects data from unauthorized disclosure or modification. ICSF protects data stored within a system, stored in a file off a system on magnetic tape, and sent between systems. ICSF also authenticates the identity of customers in the financial industry and authenticates messages from originator to receiver. It uses cryptography to accomplish these functions.

ICSF provides access to cryptographic functions through callable services. A callable service is a routine that receives control using a CALL statement in an application language. Each callable service performs one or more cryptographic functions, including:

- Generating and managing cryptographic keys
- Enciphering and deciphering data with encrypted keys using either the U.S. National Institute of Standards and Technology (NIST) Data Encryption Standard (DES), or the Commercial Data Masking Facility (CDMF)
- Transforming a CDMF DATA key to a transformed shortened DES key
- Reenciphering text from encryption under one key to encryption under another key
- Encoding and decoding data with clear keys
- Generating random numbers
- Ensuring data integrity and verifying message authentication
- Generating, verifying, and translating personal identification numbers (PINs) that identify a customer on a financial system

Note: For information about PKA functions, see page 234.

This chapter provides an overview of the DES cryptographic functions provided in ICSF, explains the functions of the cryptographic keys, and introduces the topic of building key tokens.

Functions of the DES Cryptographic Keys

ICSF provides functions to create, import, and export DES keys. This section gives an overview of these cryptographic keys. Detailed information about how ICSF organizes and protects keys is in *OS/390 ICSF Administrator's Guide*.

Key Separation

The cryptographic feature controls the use of keys by separating them into unique types, allowing you to use a specific type of key only for its intended purpose. For example, a key used to protect data cannot be used to protect a key.

The type of cryptographic feature on your system depends on your server or processor.

The Cryptographic Coprocessor Feature is available on the following servers:

- IBM S/390 Parallel Enterprise Server - Generation 3 with feature 0800 plus one of the following feature codes (0801, 0802, 0803, 0804, 0805)
- IBM S/390 Multiprise 2000 with feature 0800 plus one of the following feature codes (0801, 0802, 0803, 0804, 0805)

© Copyright IBM Corp. 1997, 2000

- S/390 G4 Enterprise Server with feature code 0800 plus one of the following feature codes (0811, 0812, 0813, 0814, 0815, 0832, 0833, 0834, 0835)
- S/390 G5 Enterprise Server with feature code 0800 plus one of the following feature codes (0811, 0812, 0813, 0814, 0815, 0832, 0833, 0834, 0835)
- S/390 G6 Enterprise Server with feature code 0800 plus one of the following feature codes (0811, 0812, 0813, 0814, 0815, 0832, 0833, 0834, 0835)

The PCI Cryptographic Coprocessor is available on the following servers:

| - S/390 G5 Enterprise Server field upgrade or S/390 G6 Enterprise Server with
| feature codes 0864 or 0865. Feature code 0860 is needed for each PCI
| Cryptographic Coprocessor.

An ICSF system has only one DES master key. (For information about PKA master keys, see “PKA Master Keys” on page 233.) However, to provide for key separation, the cryptographic feature automatically encrypts each type of key under a unique variation of the master key. Each variation of the master key encrypts a different type of key. Although you enter only one master key, you have a unique master key to encrypt all other keys of a certain type.

Note: In CUSP/PCF, key separation applies only to keys enciphered under the master key (keys in operational form). In ICSF, key separation also applies to keys enciphered under transport keys (keys in importable or exportable form). This allows the creator of a key to transmit the key to another system and to enforce its use at the other system.

Master Key Variant

Whenever the master key is used to encipher a key, the cryptographic coprocessor produces a variation of the master key according to the type of key the master key will encipher. These variations are called *master key variants*. The cryptographic coprocessor creates a master key variant by exclusive ORing a fixed pattern, called a *control vector*, onto the master key. A unique control vector is associated with each type of key. For example, all the different types of data-encrypting, PIN, MAC, and transport keys are each exclusive ORed with a unique control vector. The different key types are described in “Types of Keys” on page 5.

Each master key variant protects a different type of key. It is similar to having a unique master key protect all the keys of a certain type.

The master key, in the form of master key variants, protects keys operating on the system. A key can be used in a cryptographic function only when it is enciphered under a master key. When systems want to share keys, transport keys are used to protect keys sent outside of systems. When a key is enciphered under a transport key, the key cannot be used in a cryptographic function. It must first be brought on to a system and enciphered under the system’s master key, or exported to another system where it will then be enciphered under that system’s master key.

Transport Key Variant

Like the master key, ICSF creates variations of a transport key to encrypt a key according to its type. This allows for key separation when a key is transported off the system. A *transport key variant*, also called *key-encrypting key variant*, is created the same way a master key variant is created. The transport key’s clear value is exclusive ORed with a control vector associated with the key type of the key it protects.

Note: To exchange keys with systems that do not recognize transport key variants, ICSF allows you to encrypt selected keys under a transport key itself, not under the transport key variant.

Key Forms

A key that is protected under the master key is in *operational form*, which means ICSF can use it in cryptographic functions on the system.

When you store a key with a file or send it to another system, the key is enciphered under a transport key rather than the master key because, for security reasons, the key should no longer be active on the system. When ICSF enciphers a key under a transport key, the key is not in operational form and cannot be used to perform cryptographic functions.

When a key is enciphered under a transport key, the sending system considers the key in *exportable form*. The receiving system considers the key in *importable form*. When a key is reenciphered from under a transport key to under a system’s master key, it is in operational form again.

Control Vector

A unique control vector exists for each type of key the master key enciphers. The cryptographic feature exclusive ORs the master key with the control vector associated with the type of key the master key will encipher. The control vector ensures that an operational key is only used in cryptographic functions for which it is intended. For example, the control vector for an input PIN-encrypting key ensures that such a key can be used only in the Encrypted PIN translate and Encrypted PIN verify functions.

Types of Keys

The cryptographic keys are grouped into the following categories based on the functions they perform.

- **DES master key.** The DES master key is a double-length (128 bits) key used only to encrypt other keys. (See “PKA Master Keys” on page 233 for information about PKA master keys.) The ICSF administrator installs and changes the DES master key (see *OS/390 ICSF Administrator’s Guide* for details). On S/390 G3, or higher, Enterprise Servers and S/390 Multiprise Servers, the administrator does this by using the Clear Master Key Entry panels or the Trusted Key Entry (TKE) workstation.

  The master key always remains in a secure area in the cryptographic facility.

  It is used only to encipher and decipher keys. Other keys also encipher and decipher keys and are mostly used to protect cryptographic keys you transmit on external links. These keys, while on the system, are also encrypted under the master key.
- **SYM-MK master key.** The SYM-MK master key is a double-length (128-bit) key that is used only to encrypt other DES keys on the PCI Cryptographic Coprocessor. The ICSF administrator installs and changes the SYM-MK master key using either the ICSF panels or the optional Trusted Key Entry (TKE) workstation. The master key always remains within the secure boundary of the PCI Cryptographic Coprocessor. As with the DES master key, the SYM-MK master key is used only to encipher and decipher keys that are in operational form.
- **Data-encrypting keys.** The data-encrypting keys are single-length (64-bit), double-length (128-bit), or triple-length (192-bit) keys that protect data privacy.

Single-length data-encrypting keys can also be used to encode and decode data and authenticate data sent in messages. If you intend to use a data-encrypting key for an extended period, you can store it in the CKDS so that it will be reenciphered if the master key is changed.

You can use single-length data-encrypting keys in the encipher, decipher, encode, and decode callable services to manage data and also in the MAC generation and MAC verification callable services. Double-length and triple-length data-encrypting keys can be used in the encipher and decipher callable services for more secure data privacy.

Single-length data-encrypting keys can be exported and imported using the ANSI X9.17 key management callable services.

- **Data-translation keys.** The data-translation keys are single-length (64 bits) keys used for the ciphertext translate callable service as either the input or the output data-transport key.
- **MAC keys.** The MAC keys are single-length (64 bits) and double-length (128 bits) keys used for the MAC generation and MAC verification callable services.
- **PIN keys.** The personal identification number (PIN) is a basis for verifying the identity of a customer across financial industry networks. PIN keys are used in cryptographic functions to generate, translate, and verify PINs, and protect PIN blocks. They are all double-length (128 bits) keys. PIN keys are used in the Clear PIN generate, Encrypted PIN verify, and Encrypted PIN translate callable services.

  For installations that do not support double-length 128-bit keys, effective single-length keys are provided. For a single-length key, the left key half of the key equals the right key half.

  "Managing Personal Authentication" on page 19 gives an overview of the PIN algorithms you need to know to write your own application programs.
- **Transport keys (or key-encrypting keys).** Transport keys are also known as key-encrypting keys. They are double-length (128 bits) keys used to protect keys when you distribute them from one system to another.

  There are four types of transport keys:
  - *Exporter or OKEYXLAT key-encrypting key* protects keys of any type that are sent from your system to another system. The exporter key at the originator is the same key as the importer key of the receiver.
  - *Importer or IKEYXLAT key-encrypting key* protects keys of any type that are sent from another system to your system. It also protects keys that you store externally in a file that you can import to your system later. The importer key at the receiver is the same key as the exporter key at the originator.

  Note: Transport keys replace local, remote, and cross keys used by CUSP/PCF.

  You use key-encrypting keys to protect keys that are transported using any of the following services: data key export, key export, key import, clear key import, multiple clear key import, secure key import, multiple secure key import, key generate, and key translate. See "PKA Key Import (CSNDPKI)" on page 300 for information about using the public key import callable service to import RSA and DSS keys enciphered under transport keys.

  For installations that do not support double-length key-encrypting keys, effective single-length keys are provided. For an effective single-length key, the clear key value of the left key half equals the clear key value of the right key half.
- **ANSI X9.17 key-encrypting keys.** These bidirectional key-encrypting keys are used exclusively in ANSI X9.17 key management. They are either single-length

(64 bits) or double-length (128 bits) keys used to protect keys when you distribute them from one system to another according to the ANSI X9.17 protocol.

Other Considerations

The following are considerations for keys held in the cryptographic key data set (CKDS) or by applications.

Note: PKA keys are stored in a separate VSAM data set, the PKA key data set (PKDS). See “Chapter 14. Programming Considerations for PKA” on page 241 for more information.

- ICSF ensures that keys held in the CKDS are reenciphered during the master key change. Keys with a long life span (more than one master key change) should be stored in the CKDS.
- Keys enciphered under the host DES master key and held by applications are automatically reenciphered under a new master key as they are used. Keys with a short life span (for example, VTAM SLE data keys) do not need to be stored in the CKDS. However, if you have keys with a long life span and you do not store them in the CKDS, they should be enciphered under the importer key-encrypting key. The importer key-encrypting key itself should be stored in the CKDS.

| Table 1 describes the key types. You can build, generate, import, or export key
| types DECIPHER, ENCIPHER, CIPHER, CVARDEC, and CVARPINE, but they will
| not be usable by ICSF in other services since they are not supported by the
| Cryptographic Coprocessor Feature.

Table 1. Descriptions of Key Types

Key Type	**Meaning**
DATA	Single-length, double-length, and triple-length data-encrypting keys used in the encipher and decipher callable services. Single-length data-encrypting keys used in the MAC generation, and MAC verification callable services.
DATAXLAT	Single-length data-translation key used for the ciphertext translate callable service as either the input or the output data-transport key.
MAC	Single-length key for the MAC generation and MAC verification callable services. MAC keys may also be used in the VISA CVV generate and VISA CVV verify services.
MACVER	Single-length key for the MAC verification callable service. MACVER keys may also be used in the VISA CVV verify service.
DATAM	Double-length key for MAC generation and MAC verification callable services.
DATAMV	Double-length key for the MAC verification callable service.
PINGEN	Double-length PIN generation key for the Clear PIN generate callable service.
PINVER	Double-length PIN verification key for the Encrypted PIN verify callable service.

Table 1. Descriptions of Key Types (continued)

Key Type	Meaning
IPINENC	Double-length input PIN-encrypting key. PIN blocks received from other nodes or automatic teller machine (ATM) terminals are encrypted under this type of key. These encrypted PIN blocks are the input to the Encrypted PIN translate, Encrypted PIN verify, and Clear PIN Generate Alternate services. If an encrypted PIN block is contained in the output of the SET Block Decompose service, it may be encrypted by an IPINENC key.
OPINENC	Double-length output PIN-encrypting key. The output PIN blocks from the Encrypted PIN translate, Encrypted PIN generate, and Clear PIN generate alternate callable services are encrypted under this type of key. If an encrypted PIN block is contained in the output of the SET Block Decompose service, it may be encrypted by an OPINENC key.
EXPORTER	Double-length exporter key-encrypting key used for the key export, key generate, and data key export callable services.
IMPORTER	Double-length importer key-encrypting key used for the key import, key generate, and secure key import callable services.
AKEK	Single-length or double-length, bidirectional key-encrypting key used for the ANSI X9.17 key management callable services.
IMP-PKA	Double-length limited-authority importer key used to encrypt PKA private key values in PKA external tokens.
DECIPHER	Used only to decrypt data.
ENCIPHER	Used only to encrypt data.
IKEYXLAT	Used to decrypt an input key in the Key Translate callable service.
OKEYXLAT	Used to encrypt an output key in the Key Translate callable service.
CIPHER	Used only to encrypt or decrypt data.
DATAC	Used to specify a DATA-class key that will perform in the Encipher and Decipher callable services, but not in the MAC Generate or MAC Verify callable services.
CVARDEC	The TSS Cryptographic variable decipher verb uses a CVARDEC key to decrypt plaintext by using the Cipher Block Chaining (CBC) method.
CVARENC	Cryptographic variable encipher service uses a CVARENC key to encrypt plaintext by using the Cipher Block Chaining (CBC) method.
CVARPINE	Used to encrypt a PIN value for decryption in a PIN-printing application.
CVARXCVL	Used to encrypt special control values in DES key management.
CVARXCVR	Used to encrypt special control values in DES key management.

Clear Keys

A clear key is the base value of a key, and is not encrypted under another key. Encrypted keys are keys whose base value has been encrypted under another key.

There are four callable services you can use to convert a clear key to an encrypted key:

- To convert a clear key to an encrypted *data* key in operational form, use either the clear key import callable service or the multiple clear key import callable service.
- To convert a clear key to an encrypted key of any type, in operational or importable form, use either the secure key import callable service or the multiple secure key import callable service.

Notes:

1. The secure key import and multiple secure key import callable services can only execute in special secure mode.
2. To create external PKA tokens, see “PKA Key Token Build (CSNDPKB)” on page 287.

Special Secure Mode

Special secure mode is a special processing mode in which:

- The secure key import and multiple secure key import callable services, which works with clear keys, can be used.
- The Clear PIN Generate and Clear PIN Generate Alternate callable services, which works with clear PINs, can be used.
- The Symmetric Key Generate callable service with the ″IM″ keyword (the DES enciphered key is enciphered by an IMPORTER key) can be used.
- The key generator utility program (KGUP) can be used to enter clear keys into the CKDS.

To use special secure mode, several conditions must be met.

- The installation options data set must specify YES for the SSM installation option.

  For information about specifying installation options, see *OS/390 ICSF System Programmer’s Guide*.
- The environmental control mask (ECM) must be configured to permit special secure mode.

  The ECM is a 32-bit mask defined for each crypto domain during hardware installation. The second bit in this mask must have been turned on to enable special secure mode.
- If you are running in LPAR mode, special secure mode must be enabled.

  On an S/390 G3, or higher, Enterprise Servers and S/390 Multiprise Servers you enable special secure mode during activation using the Crypto page of the Customize Activation Profiles task. After activation, you can enable or disable special secure mode on the Change LPAR Crypto task. Both of these tasks can be accessed from the Hardware Master Console.

For S/390 G3, or higher, Enterprise Servers and S/390 Multiprise Servers with TKE, TKE enables special secure mode. For more information about entering clear keys, see *OS/390 ICSF Administrator’s Guide*.

Generating and Managing DES Keys

Using ICSF, you can generate keys using either the *key generator utility program* or the *key generate callable service*. The dynamic CKDS update callable services allow applications to directly manipulate the CKDS. ICSF provides callable services that support DES key management as defined by the IBM Common Cryptographic Architecture (CCA) and by the ANSI X9.17 standard. CDMF also supports such DES key management.

The next few sections describe the key generating and management options ICSF provides. (See “PKA Key Management” on page 242 for information about managing PKA keys.)

Key Generator Utility Program

The key generator utility program generates data, data-translation, MAC, PIN, and key-encrypting keys, and enciphers each type of key under a specific master key variant. After the KGUP generates a key, it stores it in the cryptographic key data set (CKDS). For more information about KGUP, refer to the *OS/390 ICSF Administrator’s Guide*.

Common Cryptographic Architecture DES Key Management Services

ICSF provides callable services that support CCA key management for DES keys. (For information about PKA key management, see “Callable Services for Distributing CDMF and DES DATA Keys” on page 237.)

Key Generate Callable Service

The key generate callable service generates data, data-translation, MAC, PIN, and key-encrypting keys. It generates a single key or a pair of keys. Unlike the key generator utility program, the key generate service does not store the keys in the CKDS where they can be saved and maintained. The key generate callable service returns the key to the application program that called it. The application program can then use a dynamic CKDS update service to store the key in the CKDS.

When you call the key generate callable service, include parameters specifying information about the key you want generated. Because the form of the key restricts its use, you need to choose the form you want the generated key to have. You can use the *key_form* parameter to specify the form. The possible forms are:

- **Operational,** if the key is used for cryptographic operations on the local system. Operational keys are protected by master key variants and can be stored in the CKDS or held by applications in internal key tokens.
- **Importable,** if the key is stored with a file or sent to another system. Importable keys are protected by importer key-encrypting keys.
- **Exportable,** if the key is transported or exported to another system and imported there for use. Exportable keys are protected by exporter key-encrypting keys and cannot be used by ICSF callable service.

Importable and exportable keys are contained in external key tokens. For more information on key tokens, refer to “Key Token” on page 28.

| ### Key Translate Callable Service

| This service uses one key-encrypting key to decipher an input key and then
| enciphers this key using another key-encrypting key within the secure environment.
| Use of this service requires the optional PCI Cryptographic Coprocessor.

Clear Key Import Callable Service

This service imports a clear DATA key that is used to encipher or decipher data. It accepts a clear key and enciphers the key under the host master key, returning an encrypted DATA key in operational form in an internal key token.

Multiple Clear Key Import Callable Service

This service imports a single-, double-, or triple-length clear DATA key that is used to encipher or decipher data. It accepts a clear key and enciphers the key under the host master key, returning an encrypted DATA key in operational form in an internal key token.

Data Key Import Callable Service

This service imports an encrypted source DES single-length or double-length DATA key and creates or updates a target internal key token with the master key enciphered source key. Use of this service requires the optional PCI Cryptographic Coprocessor.

Data Key Export Callable Service

This service reenciphers a DATA key from encryption under the master key to encryption under an exporter key-encrypting key, making it suitable for export to another system.

Prohibit Export Callable Service

This service modifies an operational key so that it cannot be exported. This callable service does not support NOCV key-encrypting keys, DATA, MAC, or MACVER keys with standard control vectors (for example, control vectors supported by the Cryptographic Coprocessor Feature). Use of this service requires the optional PCI Cryptographic Coprocessor.

Prohibit Export Extended Callable Service

This service updates the control vector in the external token of a key in exportable form so that the receiver node can import the key but not export it. When the key import callable service imports such a token, it marks the token as non-exportable. The key export callable service does not allow export of this token.

Key Export Callable Service

This service reenciphers any type of key (except an AKEK or IMP-PKA key) from encryption under a master key variant to encryption under the same variant of an exporter key-encrypting key, making it suitable for export to another system.

Key Import Callable Service

This service reenciphers a key (except an AKEK) from encryption under an importer key-encrypting key to encryption under the master key. The reenciphered key is in the operational form.

Key Part Import Callable Service

This service combines clear key of any key type and returns the combined key value either in an internal token or as an update to the CKDS. The PCI Cryptographic Coprocessor is required for all keys types except AKEK.

Secure Key Import Callable Service

This service enciphers a clear key under the host master key or under an importer key-encrypting key. The clear key can then be imported as any of the possible key types. This service can be used only when ICSF is in special secure mode and does not allow the import of an AKEK.

Note: The symmetric key generate, symmetric key import, and symmetric key export callable services (see “Symmetric Key Generate Callable Service” on page 237) provide a way of distributing DES DATA keys protected under a PKA key.

Multiple Secure Key Import Callable Service

This service enciphers a single-, double-, or triple-length clear key under the host master key or under an importer key-encrypting key. The clear key can then be imported as any of the possible key types. Triple-length keys can only be imported as DATA keys. This service can be used only when ICSF is in special secure mode and does not allow the import of an AKEK.

Key Test Callable Service

This service generates or verifies a secure cryptographic verification pattern for keys. A parameter indicates the action you want to perform.

The key to test can be in the clear or encrypted under a master key. The key test extended callable service works on keys encrypted under a KEK.

For generating a verification pattern, the service creates and returns a random number with the verification pattern. For verifying a pattern, you supply the random number from the call to the service that generated the pattern.

User Derived Key Callable Service

This service generates a single-length or double-length MAC key, or updates an existing user-derived key. A single-length MAC key can be used to compute a Message Authentication Code (MAC) following the ANSI X9.9, ANSI X9.19, or the Europay, MasterCard, Visa (EMV) Specification MAC processing rules. A double-length MAC key can be used to compute a MAC following the ANSI X9.19 optional double MAC processing rule or the EMV rules.

Dynamic CKDS Update Callable Services

ICSF provides additional key management capabilities through the dynamic CKDS update callable services. These services allow applications to directly manipulate both the in-storage copy and the DASD copy of the CKDS. These callable services have the identical syntax as the IBM Transaction Security System verbs of the same name. Key management applications that use these common callable services or verbs can be executed on either system without change.

Key Record Create Callable Service

This service accepts a key label and creates a null key record in both the DASD copy and in-storage copy of the CKDS. The record contains a key token set to binary zeros and is identified by the key label passed in the call statement. The key label must be unique. Callers must be in task mode and cannot be in cross memory mode.

Before you can update a key record using either the dynamic CKDS update services or KGUP, that record must already exist in the CKDS. You can use either the key record create service, KGUP, or your key entry hardware to create the initial record in the CKDS.

Key Record Write Callable Service

This service accepts an internal key token and a label and writes the key token to the CKDS record identified by the key label. The key label must be unique. Application calls to this service write the key token to both the DASD copy and in-storage copy of the CKDS, so the record must already exist in both copies of the CKDS. Callers must be in task mode and cannot be in cross memory mode.

Key Record Read Callable Service

This service copies an internal key token from the in-storage CKDS to the application storage, where it may be used directly in other cryptographic services. Key labels specified with this service must be unique.

Key Record Delete Callable Service

This service accepts a unique key label and deletes the associated key record from both the in-storage and DASD copies of the CKDS. This service deletes the entire record, including the key label from the CKDS. Callers must be in task mode and cannot be in cross memory mode to execute this service.

System Encryption Algorithm

ICSF uses either the DES algorithm or the Commercial Data Masking Facility (CDMF) to encipher and decipher data. The CDMF defines a scrambling technique for data confidentiality. It is intended to be a substitute for DES for those customers who have been previously prohibited from receiving IBM products that support DES data confidentiality services. The CDMF data confidentiality algorithm is composed of two processes: a key shortening process and a standard DES process to encipher and decipher data.

Your system can be one of the following:
- DES
- CDMF
- DES-CDMF

A DES system protects data using a single-, double-, or triple-length DES data-encrypting key and the DES algorithm.

A CDMF system protects data using a single-length DES data-encrypting key and the CDMF. You input a standard single-length data-encrypting key to the encipher (CSNBENC) and decipher (CSNBDEC) callable services. The single-length data-encrypting key that is intended to be passed to the CDMF is called a CDMF key. Cryptographically, it is indistinguishable from a DES data-encrypting key. Before the key is used to encipher or decipher data, however, the Cryptographic Coprocessor Feature hardware cryptographically shortens the key as part of the CDMF process. This transformed, shortened data-encrypting key can be used only in the DES. (It must never be used in the CDMF; this would result in a double shortening of the key.) When used with the DES, a transformed, shortened data-encrypting key produces results identical to those that the CDMF would produce using the original single-length key.

A DES-CDMF system protects data using either the DES or the CDMF. The default is DES.

ICSF provides functions to mark internal IMPORTER, EXPORTER, and DATA key tokens with **data encryption algorithm bits.** IMPORTER and EXPORTER KEKs are marked when they are installed in operational form in ICSF. Your cryptographic key administrator does this. (See *OS/390 ICSF Administrator’s Guide* for details.) Whenever a DATA key is imported or generated in concert with a marked KEK, this marking is transferred to the DATA key token, unless the token copying function of the callable service is used to override the KEK marking with the marking of the key token passed. These data encryption algorithm bits internally drive the DES or CDMF for the ICSF encryption services. External key tokens are not marked with these data encryption algorithm bits.

IMPORTER and EXPORTER KEKs can have data encryption algorithm bit markings of CDMF (X'80'), DES (X'40'), or SYS-ENC (X'00'). DATA keys generated or imported with marked KEKs will also be marked. A CDMF-marked KEK will transfer a data encryption algorithm bit marking of CDMF (X'80') to the DATA key token. A DES-marked KEK will transfer a data encryption algorithm bit marking of DES (X'00') to the DATA key token. A SYS-ENC-marked KEK will transfer a CDMF (X'80') marking to the DATA key token on a CDMF system, and a DES (X'00') marking to the DATA key token on DES-CDMF and DES systems.

Notes:

1. For the multiple secure key import callable service the token markings on the KEK are ignored. In this case, the algorithm choice specified in the rule array determines the markings on the DATA key.
2. Propagation of data encryption algorithm bits and token copying are only performed when the ICSF callable service is performed on the Cryptographic Coprocessor Feature. The PCI Cryptographic Coprocessor does not perform these functions.

Table 2 summarizes the data encryption algorithm bits by key type, and the algorithm they drive in the ICSF encryption services.

Table 2. Summary of Data Encryption Standard Bits

Algorithm	**Key Type**	**Bits**
CDMF	DATA	X'80'
	KEK	X'80'
DES	DATA	X'00'
	KEK	X'40'
System Default Algorithm	KEK	X'00'

For CUSP/PCF users, your system programmer specifies a default encryption mode of DES or CDMF when installing ICSF. (See *OS/390 ICSF System Programmer's Guide* for details.)

Transform CDMF Key Callable Service

This service is available for S/390 G3, or higher, Enterprise Servers and S/390 Multiprise Servers only. It changes a CDMF DATA key in an internal or external token to a transformed shortened DES key. It ignores the input internal DES token markings and marks the output internal token for use in the DES. You need to use this service only if you have a CDMF or DES-CDMF system that needs to send CDMF-encrypted data to a DES-only system. The CDMF or DES-CDMF system must generate the key, shorten it, and pass it to the DES-only system.

If the input DATA key is in an external token, the operational KEK must be marked as DES or SYS-ENC. The service fails for an external DATA key encrypted under a KEK that is marked as CDMF.

ANSI X9.17 Key Management Services

The ANSI X9.17 key management standard defines a process for protecting and exchanging DES keys. The ANSI X9.17 standard defines methods for generating, exchanging, using, storing, and destroying these keys. ANSI X9.17 keys are protected by the processes of *notarization* and *offsetting*, instead of control vectors. In addition to providing services to support these processes, ICSF also defines and uses an optional process of *partial notarization*.

Offsetting involves exclusive-ORing a key-encrypting key with a counter. The counter, a 56-bit binary number that is associated with a key-encrypting key and contained in certain ANSI X9.17 messages, prevents either a replay or an out-of-sequence transmission of a message. When the associated AKEK is first used, the application initializes the counter. With each additional use, the application increments the counter.

Notarization associates the identities of a pair of communicating parties with a cryptographic key. The notarization process cryptographically combines a key with two 16-byte quantities, the origin identifier and the destination identifier, to produce a notarized key. The notarization process is completed by offsetting the AKEK with a counter.

ICSF makes it possible to divide the AKEK notarization process into two steps. In the first step, partial notarization, the AKEK is cryptographically combined with the origin and destination identifiers and returned in a form that can be stored in the CKDS or application storage. In the second step, the partially notarized AKEK is exclusive OR-ed with a binary counter to complete the notarization process. Partial notarization improves performance when you use an AKEK for many cryptographic service messages, each with a different counter. For details of the partial notarization calculations, refer to “Appendix G. ANSI X9.17 Partial Notarization Method” on page 383.

ICSF provides the following callable services to support the ANSI X9.17 key management standard. Except where noted, these callable services have the identical syntax as the Transaction Security System verbs of the same name. With few exceptions, key management applications that use these common callable services, or verbs, can be executed on either system without change. Internal tokens cannot be interchanged; external tokens can be. (See “The Transaction Security System and ICSF Portability” on page 245 for PKA information.)

Key Generate Callable Service Used to Generate an AKEK

The key generate callable service, described in “Key Generate Callable Service” on page 10, can also be used to generate an AKEK in the operational form. It generates either an 8-byte or 16-byte AKEK and places it in a skeleton key token created by the key token build callable service. The length of the AKEK is determined by the key length keyword specified when building the key token.

ANSI X9.17 EDC Generate Callable Service

This service generates an ANSI X9.17 error detection code on an arbitrary length string.

ANSI X9.17 Key Export Callable Service

This service uses the ANSI X9.17 protocol to export a DATA key or a pair of DATA keys, with or without an AKEK. It also provides the ability to convert a single supplied DATA key or combine two supplied DATA keys into a MAC key.

ANSI X9.17 Key Import Callable Service

This service uses the ANSI X9.17 protocol to import a DATA key or a pair of DATA keys, with or without an AKEK. It also provides the ability to convert a single supplied DATA key or combine two supplied DATA keys into a MAC key. The syntax is identical to the Transaction Security System verb, with the following exceptions:

- Keys cannot be imported directly into the CKDS.

ANSI X9.17 Key Translate Callable Service

This service translates one or two DATA keys or an AKEK from encryption under one AKEK to encryption under another AKEK, using the ANSI X9.17 protocol.

ANSI X9.17 Transport Key Partial Notarize Callable Service

This service preprocesses or partially notarizes an AKEK with origin and destination identifiers. The partially notarized key is supplied to the ANSI X9.17 key export, ANSI X9.17 key import, or ANSI X9.17 key translate callable service to complete the notarization process. The syntax is identical to the Transaction Security System verb except that:

- The callable service does not update the CKDS.

Enciphering and Deciphering Data

The encipher and decipher callable services protect data off the host. ICSF protects sensitive data from disclosure to people who do not have authority to access it. Using algorithms that make it difficult and expensive for an unauthorized user to derive the original clear data within a practical time period assures privacy.

To protect data, ICSF can use the Data Encryption Standard (DES) algorithm to encipher or decipher data or keys. The algorithm is documented in the *Federal Information Processing Standard #46*. You can use the encipher and decipher callable services to encipher and decipher data with encrypted keys. ICSF also supports the CDMF encryption mode. See “System Encryption Algorithm” on page 13 for more information.

Encoding and Decoding Data

The encode and decode callable services perform functions with clear keys. Encode enciphers 8 bytes of data using the electronic code book (ECB) mode of the DES and a clear key. Decode does the inverse of the encode service. These services are available only on a DES-capable system. (See “System Encryption Algorithm” on page 13 for more information.)

Generating Random Numbers

| The random number generate callable service creates a random number value to
| use in generating a key. The callable service uses cryptographic hardware to
| generate a random number for use in encryption.

Translating Ciphertext

ICSF also provides a ciphertext translate callable service. This service is available only on a DES-capable system. (See “System Encryption Algorithm” on page 13 for more information.) It deciphers encrypted data (ciphertext) under one encryption key and reenciphers it under another key without having the data appear in the clear outside the cryptographic feature. Such a function is useful in a multiple node network, where sensitive data is passed through multiple nodes before it reaches its final destination. Different nodes use different keys in the process. For more information about different nodes, see “Using the Ciphertext Translate Callable Service” on page 44.

The keys cannot be used for the encipher and decipher callable services.

Managing Data Integrity and Message Authentication

To ensure the integrity of transmitted messages and stored data, ICSF provides:
- Message authentication code (MAC)

- Several hashing functions, including modification detection code (MDC), SHA-1, and MD5

(See “Chapter 15. Using Digital Signatures” on page 247 for an alternate method of message authentication using digital signatures.)

The choice of callable service depends on the security requirements of the environment in which you are operating. If you need to ensure the authenticity of the sender and also the integrity of the data, consider message authentication code processing. If you need to ensure the integrity of transmitted data in an environment where it is not possible for the sender and the receiver to share a secret cryptographic key, consider hashing functions, such as the modification detection code process.

Message Authentication Code Processing

The process of verifying the integrity and authenticity of transmitted messages is called *message authentication*. Message authentication code (MAC) processing allows you to verify that a message was not altered or a message was not fraudulently introduced onto the system. You can check that a message you have received is the same one sent by the message originator. The message itself may be in clear or encrypted form. The comparison is performed within the cryptographic feature. Since both the sender and receiver share a secret cryptographic key used in the MAC calculation, the MAC comparison also ensures the authenticity of the message.

In a similar manner, MACs can be used to ensure the integrity of data stored on the system or on removable media, such as tape.

ICSF provides support for both single-length and double-length MAC generation and MAC verification keys. With the ANSI X9.9-1 single key algorithm, use the single-length MAC and MACVER keys. With the ANSI X9.19 optional double key algorithm, use the double-length DATAM and DATAMV keys available with APAR OW37791.

ICSF provides support for the use of data-encrypting keys in the MAC generation and verification callable services, and also the use of a MAC generation key in the MAC verification callable service. This support permits ICSF MAC services to interface more smoothly with non-CCA key distribution system, including those implementing the ANSI X9.17 protocol.

MAC Generation Callable Service

When a message is sent, an application program can generate an authentication code for it using the MAC generation callable service. The callable service computes the message authentication code using one of the following methods:

- Using the ANSI X9.9-1 single key algorithm, a single-length MAC generation key or data-encrypting key, and the message text.
- Using the ANSI X9.19 optional double key algorithm, a double-length MAC generation key and the message text.
- Using the Europay, MasterCard and Visa (EMV) padding rules.

ICSF allows a MAC to be the leftmost 32 or 48 bits of the last block of the ciphertext or the entire last block (64 bits) of the ciphertext. The originator of the message sends the message authentication code with the message text.

MAC Verification Callable Service

When the receiver gets the message, an application program calls the MAC verification callable service. The callable service verifies a MAC by generating another MAC and comparing it with the MAC received with the message. If the two codes are the same, the message sent was the same one received. A return code indicates whether the MACs are the same.

The MAC verification callable service can use either of the following methods to generate the MAC for authentication:

- The ANSI X9.9-1 single key algorithm, a single-length MAC verification or MAC generation key (or a data-encrypting key), and the message text.
- The ANSI X9.19 optional double key algorithm, a double-length MAC verification or MAC generation key and the message text.
- Using the Europay, MasterCard and Visa (EMV) padding rules.

The method used to verify the MAC should correspond with the method used to generate the MAC.

Hashing Functions

Hashing functions include one-way hash generation and modification detection code (MDC) processing.

One-Way Hash Generate Callable Service

This service hashes a supplied message. Supported hashing methods include:
- SHA-1[2]
- MD5

Also supported, through the MDC generation callable service are:
- MDC-2
- MDC-4
- PADMDC-2
- PADMDC-4

MDC Generation Callable Service

The modification detection code (MDC) provides a form of support for data integrity. The MDC allows you to verify that data was not altered during transmission or while in storage. The originator of the data ensures that the MDC is transmitted with integrity to the intended receiver of the data. For instance, the MDC could be published in a reliable source of public information. When the receiver gets the data, an application program can generate an MDC, and compare it with the original MDC value. If the MDC values are equal, the data is accepted as unaltered. If the MDC values differ the data is assumed to be bogus.

In a similar manner, MDCs can be used to ensure the integrity of data stored on the system or on removable media, such as tape.

When data is sent, an application program can generate a modification detection code for it using the MDC generation callable service. The callable service computes the modification detection code by encrypting the data using a

2. The Secure Hash Algorithm (SHA) is also called the Secure Hash Standard (SHS), which Federal Information Processing Standard (FIPS) Publication 180 defines.

publicly-known cryptographic one-way function. The MDC is a 128-bit value that is easy to compute for specific data, yet it is hard to find data that will result in a given MDC.

Once an MDC has been established for a file, the MDC generate service can be run at any later time on the file. The resulting MDC can then be compared with the previously established MDC to detect deliberate or inadvertent modification.

Verifying Credit Card Data

The Visa International Service Association (VISA) and MasterCard International, Incorporated have specified a cryptographic method to calculate a value that relates to the personal account number (PAN), the card expiration date, and the service code. The VISA card-verification value (CVV) and the MasterCard card-verification code (CVC) can be encoded on either track 1 or track 2 of a magnetic striped card and are used to detect forged cards. Because most online transactions use track-2, the ICSF callable services generate and verify the CVV[3] by the track-2 method.

The VISA CVV service generate callable service calculates a 1- to 5-byte value through the DES-encryption of the PAN, the card expiration date, and the service code using two data-encrypting keys or two MAC keys. The VISA CVV service verify callable service calculates the CVV by the same method, compares it to the CVV supplied by the application (which reads the credit card's magnetic stripe) in the *CVV_value*, and issues a return code that indicates whether the card is authentic.

Managing Personal Authentication

The process of validating personal identities in a financial transaction system is called *personal authentication*. The personal identification number (PIN) is the basis for verifying the identity of a customer across the financial industry networks. ICSF checks a customer-supplied PIN by verifying it using an algorithm. The financial industry needs functions to generate, translate, and verify PINs. These functions prevent unauthorized disclosures when organizations handle personal identification numbers.

ICSF supports the following algorithms for generating and verifying personal identification numbers:
- IBM 3624
- IBM 3624 PIN offset
- IBM German Bank Pool
- IBM German Bank Pool PIN Offset (GBP-PINO)
- VISA PIN validation value
- Interbank

Note: Interbank is available only on S/390 G3, or higher, Enterprise Servers and S/390 Multiprise Servers.

With ICSF, you can translate PIN blocks from one format to another. ICSF supports the following formats:
- ANSI X9.8
- ISO formats 0, 1, 2
- VISA formats 1, 2, 3, 4
- IBM 4704 Encrypting PINPAD format

3. The VISA CVV and the MasterCard CVC refer to the same value. CVV is used here to mean both CVV and CVC.

- IBM 3624 formats
- IBM 3621 formats
- ECI formats 1, 2, 3

With the capability to translate personal identification numbers into different PIN block formats, you can use personal identification numbers on different systems.

Clear PIN Generate Callable Service

To generate personal identification numbers, call the Clear PIN generate callable service. Using a PIN generation algorithm, data used in the algorithm, and the PIN generation key, the callable service generates a clear PIN, a PIN verification value, or an offset. The callable service can only execute in special secure mode, which is described in “Special Secure Mode” on page 9.

Encrypted PIN Generate Callable Service

To generate personal identification numbers, call the Encrypted PIN generation callable service. Using a PIN generation algorithm, data used in the algorithm, and the PIN generation key, the callable service generates a PIN and using a PIN block format and the PIN encrypting key, formats and encrypts the PIN. Use of this service requires the optional PCI Cryptographic Coprocessor.

Clear PIN Encrypt Callable Service

To format a PIN into a PIN block format and encrypt the results, use the Clear PIN Encrypt callable service. You can also use this service to create an encrypted PIN block for transmission. With the RANDOM keyword, you can have the service generate random PIN numbers. Use of this service requires the optional PCI Cryptographic Coprocessor.

Clear PIN Generate Alternate Callable Service

To generate a clear VISA PIN validation value from an encrypted PIN block, call the clear PIN generate alternate callable service. This service also supports the IBM-PINO algorithm to produce a 3624 offset from a customer selected encrypted PIN.

Note: The PIN block must be encrypted under either an input PIN-encrypting key (IPINENC) or output PIN-encrypting key (OPINENC). Using an IPINENC key requires NOCV keys to be enabled in the CKDS. Functions other than VISA PIN validation value generation require the optional PCI Cryptographic Coprocessor.

Encrypted PIN Verify Callable Service

To verify a supplied PIN, call the Encrypted PIN verify callable service. You need to specify the supplied enciphered PIN, the PIN-encrypting key that enciphers it, and other relevant data. You must also specify the PIN verification key and PIN verification algorithm. It compares the two personal identification numbers; if they are the same, it verifies the supplied PIN.

Encrypted PIN Translate Callable Service

To translate a PIN from one PIN-encrypting key to another or from one PIN block format to another or both, call the Encrypted PIN translation callable service. You must identify the input PIN-encrypting key that originally enciphers the PIN. You also need to specify the output PIN-encrypting key that you want the callable service to use to encipher the PIN. If you want to change the PIN block format, specify a different output PIN block format from the input PIN block format.

Trusted Key Entry (TKE) Support

The Trusted Key Entry (TKE) workstation is an optional feature. It offers an alternative to clear key entry. You can use the TKE workstation to load:

- DES master keys, PKA master keys (see "PKA Master Keys" on page 233), and operational TRANSPORT and PIN keys in a *secure* way.
- SYM-MK and ASYM-MK master keys on the PCI Cryptographic Coprocessor.

You can load keys remotely and for multiple Cryptographic Coprocessor Features and PCI Cryptographic Coprocessors. The TKE workstation eases the administration for using one Cryptographic Coprocessor Feature as a production machine and as a test machine at the same time, while maintaining security and reliability.

For complete details about the TKE workstation (Versions 1 and 2), see *OS/390 ICSF TKE Workstation User's Guide*. For complete details about the TKE workstation (Version 3), see *OS/390 ICSF TKE Workstation User's Guide 2000*.

Utilities

ICSF provides the following utilities.

Key Token Build Callable Service

The key token build callable service is a utility you can use to create skeleton key tokens for AKEKs as input to the key generate or key part import callable service. You can also use this service to build CCA key tokens for all key types ICSF supports or to update the data encryption standard bits in a supplied DATA, IMPORTER, or EXPORTER token.

Cryptographic Variable Encipher Callable Service

The cryptographic variable encipher callable service uses a CVARENC key to encrypt plaintext by using the Cipher Block Chaining (CBC) method. You can use this service to prepare a mask array for the control vector translate service. The plaintext must be a multiple of eight bytes in length. Use of this service requires the optional PCI Cryptographic Coprocessor.

Control Vector Generate Callable Service

The control vector generate callable service builds a control vector from keywords specified by the *key_type* and *rule_array* parameters.

Control Vector Translate Callable Service

The control vector translate callable service changes the control vector used to encipher an external key. Use of this service requires the optional PCI Cryptographic Coprocessor.

Code Conversion Callable Services

The code conversion callable services are utilities that convert EBCDIC data to ASCII data and vice versa.

Character/Nibble Conversion Callable Services

The character/nibble conversion callable services are utilities that convert a binary string to a character string and vice versa.

X9.9 Data Editing Callable Service

The data editing callable service is a utility that edits an ASCII text string according to the editing rules of ANSI X9.9-4.

Chapter 2. Programming Considerations

ICSF provides access to cryptographic functions through callable services, which are also known as verbs. A callable service is a routine that receives control using a CALL statement in an application language.

Before invoking callable services in an application program, you must link them into the application program. See "Linking a Program with the ICSF Callable Services" on page 38.

To invoke the callable service, the application program must include a procedure call statement that has the entry point name and parameters for the callable service. The parameters that are associated with a callable service provide the only communication between the application program and ICSF.

Callable Service Syntax

This book uses a general call format to show the name of the ICSF callable service and its parameters. An example of that format is shown below:

```
CALL CSNBxxxx(return_code,
              reason_code,
              exit_data_length,
              exit_data,
              parameter_5,
              parameter_6,
              .
              .
              .
              parameter_N)
```

where CSNBxxxx is the name of the callable service. CSFXXX corresponds to CSNBxxx. (The ANSI services start with CSNAxxx and have corresponding CSFAxxx names. For the PKA services, which start with CSNDxxx and have corresponding CSFxxx names, see "Summary of the PKA Callable Services" on page 245.) The return code, reason code, exit data length, exit data, parameter 5 through parameter *N* represent the parameter list. The call generates a fixed length parameter list. You must supply the parameters in the order shown in the syntax diagrams. "Parameter Definitions" on page 26 describes the parameters in more detail.

ICSF callable services can be called from application programs written in a number of high-level languages as well as assembler. The high-level languages are:
- C
- COBOL
- FORTRAN
- PL/I

The ICSF callable services comply with the IBM Common Cryptographic Architecture: Cryptographic Application Programming Interface. The services can be invoked using the generic format, CSNBxxxx. Use the generic format if you want your application to work with more than one cryptographic product. Otherwise, use the **CSFxxxx** format.

Specific formats for the languages that can invoke ICSF callable services are as follows:

C

```
CSNBxxxx (return_code,reason_code,exit_data_length,exit_data,
parameter_5,...parameter_N)
```

COBOL

```
CALL 'CSNBxxxx' USING return_code,reason_code,exit_data_length,
exit_data,parameter_5,...parameter_N
```

FORTRAN

```
CALL CSNBxxxx (return_code,reason_code,exit_data_length,exit_data,
parameter_5,...parameter_N)
```

PL/I

```
DCL CSNBxxxx ENTRY OPTIONS(ASM);
CALL CSNBxxxx return_code,reason_code,exit_data_length,exit_data,
parameter_5,...parameter_N;
```

Assembler language programs must use standard linkage conventions when invoking ICSF callable services. An example of how an assembler language program can invoke a callable service is shown as follows:

```
CALL CSNBxxxx,(return_code,reason_code,exit_data_length,exit_data,
parameter_5,...parameter_N)
```

Coding examples using the high-level languages are shown in Appendix B. Coding Examples.

Callable Services with ALET Parameters

Some callable services have an alternate entry point (with ALET parameters—for data that resides in data spaces). They are in the format of *CSNBxxx1*:

Verb	Callable Service without ALET	Callable Service with ALET
Decipher	CSNBDEC	CSNBDEC1
Encipher	CSNBENC	CSNBENC1
Ciphertext translate	CSNBCTT	CSNBCTT1
MAC generation	CSNBMGN	CSNBMGN1
MAC verification	CSNBMVR	CSNBMVR1
MDC generation	CSNBMDG	CSNBMDG1
One way hash generate	CSNBOWH	CSNBOWH1

When choosing which service to use, consider the following:

- Callable services that do not have an ALET parameter require data to reside in the caller's primary address space. A program using these services adheres to the IBM Common Cryptographic Architecture: Cryptographic Application Programming Interface.
- Callable services that have an ALET parameter allow data to reside either in the caller's primary address space or in a data space. This can allow you to encipher more data with one call. However, a program using these services does not adhere to the IBM Common Cryptographic Architecture: Cryptographic Application Programming Interface, and may need to be modified before it can run with other cryptographic products that follow this programming interface.

Rules for Defining Parameters and Attributes

The following rules apply to the callable services:

- Parameters are required and positional.
- Each parameter list has a fixed number of parameters.

- Each parameter is defined as an integer or a character string.
- Keywords passed to the callable services, such as TOKEN, CUSP, and FIRST can be in lower, upper, or mixed case. The callable services fold them to uppercase before using them.

Each callable service defines its own list of parameters. The entire list must be supplied on every call. If you do not use a specific parameter, you must supply that parameter with hexadecimal zeros or binary zeros.

Parameters are passed to the callable service. All information that is exchanged between the application program and the callable service is through parameters passed on the call.

Each parameter definition begins with the direction that the data flows and the attributes that the parameter must possess (called "type"). The following describes the direction.

Direction	Meaning
Input	The application sends (*supplies*) the parameter to the callable service. The callable service does not change the value of the parameter.
Output	The callable service *returns* the parameter to the application program. The callable service may have changed the value of the parameter on return.
Input/Output	The application sends (*supplies*) the parameter to the callable service. The callable service may have changed the value of the parameter on return.

The following describes the attributes or type.

Type	Meaning
Integer (I)	A 4-byte (32-bit), twos complement, binary number that has sign significance.
String	A series of bytes where the sequence of the bytes must be maintained. Each byte can take on any bit configuration. The string consists only of data bytes. No string terminators, field-length values, or type-casting parameters are included. The maximum size of a string is X'7FFFFFFF' or 2 gigabytes. In some of the callable services, the length of some string data has an upper bound defined by the installation.

Alphanumeric character string
A string of bytes in which each byte represents characters from the following set:

Character	EBCDIC Value	Character	EBCDIC Value	Character	EBCDIC Value
A-Z		(	X'4D'	/	X'61'
a-z		)	X'5D'	,	X'6B'
0-9		+	X'4E'	%	X'6C'
Blank	X'40'	&	X'50'	?	X'6F'
*	X'5C'	.	X'4B'	:	X'7A'
<	X'4C'	;	X'5E'	=	X'7E'
>	X'6E'	-	X'60'	'	X'7D'

Parameter Definitions

This section describes the following parameters, which are used by most of the callable services:

- *Return_code*
- *Reason_code*
- *Exit_data_length*
- *Exit_data*
- *Key_identifier*

Note: The *return_code* parameter, the *reason_code* parameter, the *exit_data_length* parameter, and the *exit_data* parameter are used with every callable service.

Return and Reason Codes

Return_code and *reason_code* parameters return integer values upon completion of the call.

Return_code

The return code parameter contains the general results of processing as an integer.

Table 3 shows the standard return code values that the callable services return. A complete list of return codes is shown in Appendix A. ICSF and TSS Return and Reason Codes.

Table 3. Standard Return Code Values From ICSF Callable Services

Value Hex (Decimal)	Meaning
00 (00)	Successful. Normal return.
04 (04)	A warning. Execution was completed with a minor, unusual event encountered.
08 (08)	An application error occurred. The callable service was stopped due to an error in the parameters. Or, another condition was encountered that needs to be investigated.
0C (12)	Error. ICSF is not active or an environment error was detected.
10 (16)	System error. The callable service was stopped due to a processing error within the software or hardware.

Generally, CUSP and PCF macros will receive identical error return codes if they execute on CUSP/PCF or on ICSF. A single exception has been noted: if a key is installed on the ICSF CKDS with the correct label but with the wrong key type, CUSP/PCF issues a return code of 8, indicating that the key type was incorrect. ICSF issues a return code of 12, indicating that the key could not be found.

Reason_code

The reason code parameter contains the results of processing as an integer. You can specify which set of reason codes (ICSF or TSS) are returned from callable services. The default value is ICSF. For more information about the REASONCODES installation option, see *OS/390 ICSF System Programmer's Guide*. Different results are assigned to unique reason code values under a return code.

A list of reason codes is shown in Appendix A. ICSF and TSS Return and Reason Codes.

Exit Data Length and Exit Data

The following describes the *exit_data_length* and *exit_data* parameters. The parameters are input to all callable services. (Although all services require these parameters, several services ignore them. Installation exits are not enabled for the following callable services: code conversion, character/nibble conversion, X9.9 data editing, and some PKA callable services. See “Exits” on page 243 for more information about PKA services.) ICSF provides two installation exits for each callable service. The preprocessing exit is invoked when an application program calls a callable service, but before the callable service starts processing. For example, this exit is used to check or change parameters passed on the call or to stop the call. It can also be used to perform additional security checks.

The post-processing exit is invoked when the callable service has completed processing, but before the callable service returns control to the application program. For example, this exit can be used to check and change return codes from the callable service or perform clean-up processing.

For more information about the exits, see *OS/390 ICSF System Programmer’s Guide*.

Exit_data_length
The integer that has the string length of the data passed to the exit. The data is identified in the following *exit_data* parameter.

Exit_data
The installation exit data string that is passed to the callable service’s preprocessing exit. The installation exit can use the data for its own processing.

Key Identifier for DES Key Token

A *key identifier* for a DES key token is a 64-byte area that contains one of the following:

- **Key label** identifies keys that are in the CKDS. Ask your ICSF administrator for the key labels that you can use.
- **Key token** can be either an internal key token, an external key token, or a null key token. (See “PKA Key Tokens” on page 241 for information about PKA key tokens.) Key tokens are generated by an application (for example, using the key generate callable service), or received from another system that can produce external key tokens.

  An **internal key token** can be used only on ICSF, because the master key encrypts the key value. Internal key tokens contain keys in operational form only.

  An **external key token** can be exchanged with other systems, because a transport key that is shared with the other system encrypts the key value. External key tokens contain keys in either exportable or importable form.

  A **null key token** can be used to import a key from a system that cannot produce external key tokens. A null key token contains a key encrypted under an importer key-encrypting key, but does not contain the other information present in an external key token.

The term *key identifier* is used when a parameter could be one of the above items and to indicate that different inputs are possible. For example, you may want to specify a specific parameter as either an internal key token or a key label. The key label is, in effect, an indirect reference to a stored internal key token.

Key Label: If the first byte of the key identifier is greater than X'40', the field is considered to be holding a **key label**. The contents of a key label are interpreted as a pointer to a cryptographic key data set (CKDS) key entry. The key label is an indirect reference to an internal key token.

A key label is specified on callable services with the *key_identifier* parameter as a 64-byte character string, left-justified, and padded on the right with blanks. In most cases, the callable service does not check the syntax of the key label beyond the first byte. One exception is the key record create callable service which enforces the KGUP rules for key labels unless syntax checking is bypassed by a preprocessing exit.

A key label has the following form:

Offset	Length	Data
00-63	64	Key label name

Key Token: A key token is a 64-byte field composed of a key value and control information. The control information is assigned to the key when ICSF creates the key. The key token can be either an internal key token, an external key token, or a null key token. (See page 241 for information about PKA key tokens.) Through the use of key tokens, ICSF can do the following:
- Support continuous operation across a master key change
- Control use of keys in cryptographic services

If the first byte of the key identifier is X'01', the key identifier is interpreted as an **internal key token**. An internal key token is a token that can be used only on the ICSF system that created it (or another ICSF system with the same host master key). It contains a key that is encrypted under the master key.

An application obtains an internal key token by using one of the callable services such as those listed below. The callable services are described in detail in Chapter 4. Managing Cryptographic Keys.
- Key generate
- Key import
- Secure key import
- Multiple secure key import
- Clear key import
- Multiple clear key import
- Key record read
- Key token build
- | Data Key Import

The master key may be dynamically changed between the time that you invoke a service, such as the key import callable service to obtain a key token, and the time that you pass the key token to the encipher callable service. When a change to the master key occurs, ICSF reenciphers the caller’s key from under the old master key to under the new master key. A Return Code of 0 with a reason code of 10000 notifies you that ICSF reenciphered the key. For information on reenciphering the CKDS, see *OS/390 ICSF Administrator’s Guide*.

Attention: If an internal key token held in user storage is not used while the master key is changed twice, the internal key token is no longer usable. (See “Other Considerations” on page 7 for additional information.)

For debugging information, see Appendix H. Key Token Formats for the format of an internal key token.

If the first byte of the key identifier is X'02', the key identifier is interpreted as an **external key token**. By using the external key token, you can exchange keys between systems. It contains a key that is encrypted under a key-encrypting key.

An external key token contains an encrypted key and control information to allow compatible cryptographic systems to:
- Have a standard method of exchanging keys
- Control the use of keys through the control vector
- Merge the key with other information needed to use the key

An application obtains the external key token by using one of the callable services such as those listed below. They are described in detail in Chapter 4. Managing Cryptographic Keys.
- Key generate
- Key export
- Data key export

For debugging information, see Appendix H. Key Token Formats for the format of an external key token.

If the first byte of the key identifier is X'00', the key identifier is interpreted as a **null key token**. Use the null key token to import a key from a system that cannot produce external key tokens. That is, if you have an 8- to 16-byte key that has been encrypted under an importer key, but is not imbedded within a token, place the encrypted key in a null key token and then invoke the key import callable service to get the key in operational form.

For debugging information, see Appendix H. Key Token Formats for the format of a null key token.

Invocation Requirements

Applications that use ICSF callable services must meet the following invocation requirements:
- Data can be located above or below 16Mb but must be 31-bit addressable
- Problem or supervisor state
- Any PSW key
- Task mode or Service Request Block (SRB) mode
- No mode restrictions
- Enabled for interrupts

Note: The dynamic CKDS update services have two additional restrictions.
- The caller must be in task mode, not SRB mode.
- The caller must not be in cross-memory mode.

Security Considerations

Your installation can use the OS/390 Security Server (RACF) or an equivalent product to control who can use ICSF callable services or key labels. Before using an ICSF callable service or a key label, ask your security administrator to ensure that you have the necessary authorization.

Performance Considerations

In most cases, the OS/390 operating system Dispatcher provides optimum performance. However, if your application makes extensive use of ICSF functions, you should consider using one or both of the following:

- If your application runs in SRB mode, you should consider scheduling an SRB to run on a processor with cryptographic feature installed (using the FEATURE=CRYPTO keyword on the SCHEDULE macro). For more information on the SCHEDULE macro, refer to *OS/390 MVS Programming: Authorized Assembler Services Reference LLA-SDU*.
- Use the IEAAFFN callable service (processor affinity) to avoid system overhead in selecting which processor your program (specifically, a particular TCB in the application) runs in. Note that you do **not** have to use the IEAAFFN service to ensure that the system runs a program on a processor with a cryptographic feature; the system ensures that automatically. However, you can avoid some of the system overhead involved in the selection process by using the IEAAFFN service, thus improving the program's performance. For more information on using the IEAAFFN callable service, refer to *OS/390 MVS Programming: Callable Services for HLL*.

IBM recommends that you run applications first without using these options. Consider these options when you are tuning your application for performance. Use these options only if they improve the performance of your application. For more information on the Cryptographic Coprocessor Feature, see *S/390 Support Element Operations Guide*.

Summary of the DES Callable Services

Table 4 lists the DES callable services described in this book, and their corresponding verbs. The figure also references the chapter that describes the callable service.

Table 4. Summary of ICSF DES Callable Services

Verb	Service Name	Function
Chapter 4. Managing Cryptographic Keys		
CSNBCKI	Clear key import	Imports an 8-byte clear DATA key, enciphers it under the master key, and places the result into an internal key token. CSNBCKI converts the clear key into operational form as a DATA key.
CSNBCKM	Multiple clear key import	Imports a single-, double-, or triple-length clear DATA key, enciphers it under the master key, and places the result into an internal key token. CSNBCKM converts the clear key into operational form as a DATA key.
| CSNBDKM	Data key import	Imports an encrypted source DES single- or double-length DATA key and creates or updates a target internal key token with the master key enciphered source key.
CSNBDKX	Data key export	Converts a DATA key from operational form into exportable form.
CSNBKEX	Key export	Converts any key from operational form into exportable form. (However, this service does not export a key that was marked non-exportable when it was imported.)
| CSNBPEX	Prohibit export	Modifies an operational key so that it cannot be exported.
CSNBPEXX	Prohibit export extended	Changes the external token of a key in exportable form so that it can be imported at the receiver node but not exported from that node.

Table 4. Summary of ICSF DES Callable Services (continued)

Verb	Service Name	Function
CSNBKGN	Key generate	Generates a 64-bit, 128-bit, or 192-bit odd parity key, or a pair of keys; and returns them in encrypted forms (operational, exportable, or importable). CSNBKGN does not produce keys in plaintext.
CSNBKTR	Key translate	Uses one key-encrypting key to decipher an input key and then enciphers this key using another key-encrypting key within the secure environment.
CSNBKIM	Key import	Converts any key from importable form into operational form.
CSNBKPI	Key part import	Combines the clear key parts of any key type and returns the combined key value in an internal key token or an update to the CKDS.
CSNBSKI	Secure key import	Enciphers a clear key under the master key, and places the result into an internal or external key token as any key type. CSNBSKI executes only in special secure mode.
CSNBSKM	Multiple secure key import	Enciphers a single-, double-, or triple-length clear key under the master key or an input importer key, and places the result into an internal or external key token as any key type. Triple-length keys can only be imported as DATA keys. CSNBSKM executes only in special secure mode.
CSNBKRC	Key record create	Adds a key record containing a key token set to binary zeros to both the in-storage and DASD copies of the CKDS.
CSNBKRD	Key record delete	Deletes a key record from both the in-storage and DASD copies of the CKDS.
CSNBKRR	Key record read	Copies an internal key token from the in-storage copy of the CKDS to application storage.
CSNBKRW	Key record write	Writes an internal key token to the CKDS record specified in the key label parameter. Updates both the in-storage and DASD copies of the CKDS currently in use.
CSNBKYT or CSNBKYTX	Key test service	Generates or verifies (depending on keywords in the rule array) a secure verification pattern for keys. CSNBKYT requires the tested key to be in the clear or encrypted under the master key. CSNBKYTX also allows the tested key to be encrypted under a key-encrypting key.
CSNBTCK	Transform CDMF key	Changes a CDMF DATA key in an internal or external token to a transformed shortened DES key.
CSFUDK	User Derived Key	Generates single-length or double-length MAC keys, or updates an existing user derived key.
Chapter 5. Managing Keys According to the ANSI X9.17 Standard		
CSNAEGN	ANSI X9.17 EDC generate	Generates an ANSI X9.17 error detection code on an arbitrary length string using the special MAC key (x'0123456789ABCDEF').
CSNAKEX	ANSI X9.17 key export	Uses the ANSI X9.17 protocol to export a DATA key or a pair of DATA keys with or without an AKEK. Supports the export of a CCA IMPORTER or EXPORTER KEK. Converts a single DATA key or combines two DATA keys into a single MAC key.

Table 4. Summary of ICSF DES Callable Services (continued)

Verb	Service Name	Function
CSNAKIM	ANSI X9.17 key import	Uses the ANSI X9.17 protocol to import a DATA key or a pair of DATA keys with or without an AKEK. Supports the import of a CCA IMPORTER or EXPORTER KEK. Converts a single DATA key or combines two DATA keys into a single MAC key.
CSNAKTR	ANSI X9.17 key translate	Uses the ANSI X9.17 protocol to translate, in a single service call, either one or two DATA keys or a single KEK from encryption under one AKEK to encryption under another AKEK. Converts a single DATA key or combines two DATA keys into a single MAC key.
CSNATKN	ANSI X9.17 transport key partial notarize	Permits the preprocessing of an AKEK with origin and destination identifiers to create a partially notarized AKEK.
Chapter 6. Protecting Data		
CSNBENC or CSNBENC1	Encipher	Enciphers data using either the CDMF or the cipher block chaining mode of the DES. (The method depends on the token marking or keyword specification.) The result is called ciphertext. CSNBENC requires the plaintext and ciphertext to reside in the caller's primary address space. CSNBENC1 allows the plaintext and ciphertext to reside in the caller's primary address space or in an OS/390 MVS data space.
CSNBDEC or CSNBDEC1	Decipher	Deciphers data using either the CDMF or the cipher block chaining mode of the DES. (The method depends on the token marking or keyword specification.) The result is called plaintext. CSNBDEC requires the plaintext and ciphertext to reside in the caller's primary address space. CSNBDEC1 allows the plaintext and ciphertext to reside in the caller's primary address space or in an OS/390 MVS data space.
CSNBECO	Encode	Encodes an 8-byte string of data using the electronic code book mode of the DES. (This is for DES encryption only.)
CSNBDCO	Decode	Decodes an 8-byte string of data using the electronic code book mode of the DES. (This is for DES encryption only.)
Chapter 7. Generating Random Numbers		
CSNBRNG	Random number generate	Generates an 8-byte random number. The output can be specified in three forms of parity: RANDOM, ODD, and EVEN.
Chapter 8. Translating Ciphertext		
CSNBCTT or CSNBCTT1	Ciphertext translate	Translates the user-supplied ciphertext from one key and enciphers the ciphertext to another key. (This is for DES encryption only.) CSNBCTT requires the ciphertext to reside in the caller's primary address space. CSNBCTT1 allows the ciphertext to reside in the caller's primary address space or in an OS/390 MVS data space.
Chapter 9. Verifying Data Integrity and Authenticating Messages		

Table 4. Summary of ICSF DES Callable Services (continued)

Verb	Service Name	Function
CSNBMGN or CSNBMGN1	MAC generation	Generates a 4-, 6-, or 8-byte message authentication code (MAC) for a text string that the application program supplies. The MAC is computed using either the ANSI X9.9-1 algorithm or the ANSI X9.19 optional double key algorithm. CSNBMGN requires data to reside in the caller's primary address space. CSNBMGN1 allows data to reside in the caller's primary address space or in an OS/390 MVS data space.
CSNBMVR or CSNBMVR1	MAC verification	Verifies a 4-, 6-, or 8-byte message authentication code (MAC) for a text string that the application program supplies. The MAC is computed using either the ANSI X9.9-1 algorithm or the ANSI X9.19 optional double key algorithm and is compared with a user-supplied MAC. CSNBMVR requires data to reside in the caller's primary address space. CSNBMVR1 allows data to reside in the caller's primary address space or in an OS/390 MVS data space.
CSNBMDG or CSNBMDG1	MDC generation	Generates a 128-bit modification detection code (MDC) for a text string that the application program supplies. CSNBMDG requires data to reside in the caller's primary address space. CSNBMDG1 allows data to reside in the caller's primary address space or in an OS/390 MVS data space.
CSNBOWH or CSNBOWH1	One way hash generate	Generates a one-way hash on specified text.
CSNBCSG	VISA CVV service generate	Generates a VISA Card Verification Value (CVV) or a MasterCard Card Verification Code (CVC).
CSNBCSV	VISA CVV service verify	Verifies a VISA Card Verification Value (CVV) or a MasterCard Card Verification Code (CVC).
Chapter 10. Managing Personal Identification Numbers		
CSNBPGN	Clear PIN generate	Generates a clear personal identification number (PIN), a PIN verification value (PVV), or an offset using one of the following algorithms: IBM 3624 (IBM-PIN or IBM-PINO) IBM German Bank Pool (GBP-PIN or GBP-PINO) VISA PIN validation value (VISA-PVV) Interbank PIN (INBK-PIN) CSNBPGN executes only in special secure mode.
| CSNBEPG	Encrypted PIN generate	Generates and formats a PIN and encrypts the PIN block.
| CSNBCPE	Clear PIN encrypt	Formats a PIN into a PIN block format and encrypts the results.
| CSNBCPA	Clear PIN generate alternate	Generates a clear VISA PIN validation value (PVV) from an input encrypted PIN block. The PIN block may have been encrypted under either an input or output PIN encrypting key. The IBM-PINO algorithm is supported to produce a 3624 offset from a customer selected encrypted PIN.

Table 4. Summary of ICSF DES Callable Services (continued)

Verb	Service Name	Function
CSNBPVR	Encrypted PIN verify	Verifies a supplied PIN using one of the following algorithms: IBM 3624 (IBM-PIN or IBM-PINO) IBM German Bank Pool (GBP-PIN or GBP-PINO) VISA PIN validation value (VISA-PVV) Interbank PIN (INBK-PIN)
CSNBPTR	Encrypted PIN translate	Reenciphers a PIN block from one PIN-encrypting key to another and, optionally, changes the PIN block format.
Chapter 11. DES Utilities		
CSNBKTB	Key token build	Builds an internal or external token from the supplied parameters. You can use this callable service to build an internal token for an AKEK for input to the key generate and key part import callable services. You can also use this service to build CCA key tokens for all key types ICSF supports or to update the DES, CDMF, or SYS-ENC markings in a supplied DATA, IMPORTER, or EXPORTER token.
CSNBCVE	Cryptographic variable encipher	Uses a CVARENC key to encrypt plaintext by using the Cipher Block Chaining (CBC) method. The plaintext must be a multiple of eight bytes in length.
CSNBCVG	Control vector generate	Builds a control vector from keywords specified by the *key_type* and *rule_array* parameters.
CSNBCVT	Control vector translate	Changes the control vector used to encipher an external key.
CSNBXEA or CSNBXAE	Code conversion	Converts EBCDIC data to ASCII data or vice versa.
CSNBXBC or CSNBXCB	Character/nibble conversion	Converts a binary string to a character string or vice versa.
CSNB9ED	X9.9 data editing	Edits an ASCII text string according to the editing rules of ANSI X9.9–4.
Chapter 12. Trusted Key Entry Workstation Interfaces		
CSFPCI	PCI interface	Puts a request to a specific PCI Cryptographic Coprocessor queue and removes the corresponding response when complete. Only the Trusted Key Entry (TKE) workstation uses this service.
CSFPKSC	PKSC interface	Puts a request to a specific cryptographic module and removes the corresponding response when complete. Only the Trusted Key Entry (TKE) workstation uses this service.

Chapter 3. Using the Callable Services

This chapter discusses how ICSF callable services use the different key types and key forms. It also provides suggestions on what to do if there is a problem.

ICSF provides callable services that perform cryptographic functions. You call and pass parameters to a callable service from an application program. Besides the callable services ICSF provides, you can write your own callable services called *installation-defined callable services*. **Note that only an experienced system programmer should attempt to write an installation-defined callable service**.

To write an installation-defined callable service, you must first write the callable service and link-edit it into a load module. Then define the service in the installation options data set.

You must also write a service stub. To execute an installation-defined callable service, you call a service stub from your application program. In the service stub, you specify the service number that identifies the callable service.

For more information about installation-defined callable services, see *OS/390 ICSF System Programmer's Guide*.

For reference, you may want to review the discussion of key types in "Types of Keys" on page 5.

For a summary of the DES callable services, see Table 4 on page 30.

Understanding Key Form and Key Flow

This section discusses the forms of enciphered keys and explains the key flow for converting one key to another.

Key Form

Enciphered keys appear in three forms. The form you need depends on how and when you use a key.

- **Operational** key form is used at the local system. Many callable services can *use* an operational key form.

  The key token build, key generate, key import, data key import, clear key import, multiple clear key import, secure key import, and multiple secure key import callable services can *create* an operational key form.
- **Exportable** key form is transported to another cryptographic system. It can only be passed to another system. The ICSF callable services cannot use it for cryptographic functions. The key generate, data key export, and key export callable services produce the exportable key form.
- **Importable** key form can be transformed into operational form on the local system. The key import callable service (CSNBKIM) and the Data Key Import callable service (CSNBDKM) can *use* an importable key form. Only the key generate callable service (CSNBKGN) can *create* an importable key form. The secure key import (CSNBSKI) and multiple secure key import (CSNBSKM) callable services can convert a clear key into an importable key form.

© Copyright IBM Corp. 1997, 2000

For more information about the key types, see either “Functions of the DES Cryptographic Keys” on page 3 or the *OS/390 ICSF Administrator’s Guide*. See “Key Forms and Types Used in the Key Generate Callable Service” on page 40 for more information about key form.

DES Key Flow

The conversion from one key to another key is considered to be a one-way flow. An operational key form cannot be turned back into an importable key form. An exportable key form cannot be turned back into an operational or importable key form. The flow of ICSF key forms can only be in one direction:

```
IMPORTABLE —to→ OPERATIONAL —to→ EXPORTABLE
```

Creating Keys

This section discusses generating an operational, importable, or exportable key.

For the following callable services, you do **not** need an ICSF generated key:
- Character/nibble Conversion (CSNBXBC and CSNBXCB)
- Code Conversion (CSNBXAE and CSNBXEA)
- Decode (CSNBDCO)
- Encode (CSNBECO)
- Key Record Create (CSNBKRC)
- Key Record Delete (CSNBKRD)
- Key Record Read (CSNBKRR)
- Key Token Build (CSNBKTB)
- MDC Generation (CSNBMDG and CSNBMDG1)
- Random Number Generate (CSNBRNG)
- X9.9 data editing (CSNB9ED)
- Control Vector Generate (CSNBCVG)

For those services, call them directly with your chosen parameters.

The following callable services require a key in operational form. It can either be supplied as an encrypted key in an internal key token, or be pointed to by a CKDS key label:
- Ciphertext translate (CSNBCTT or CSNBCTT1)
- Clear PIN Encrypt (CSNBCPE)
- Clear PIN generate alternate (CSNBCPA)
- Control Vector Translate (CSNBCVT)
- Cryptographic Variable Encipher (CSNBCVE)
- Data Key Export (CSNBDKX)
- Data Key Import (CSNBDKM)
- Decipher (CSNBDEC or CSNBDEC1)
- Encipher (CSNBENC or CSNBENC1)
- Encrypted PIN Generate (CSNBEPG)
- Key Export (CSNBKEX)
- Key Generate (CSNBKGN)
- Key Import (CSNBKIM)
- Key Part Import (CSNBKPI)
- Key Record Write (CSNBKRW)
- Key Translate (CSNBKTR)
- MAC Generation (CSNBMGN or CSNBMGN1)
- MAC Verification (CSNBMVR or CSNBMVR1)
- Multiple Secure Key Import (CSNBSKM)

- Clear PIN Generate (CSNBPGN)
- Encrypted PIN Verify (CSNBPVR)
- Encrypted PIN Translate (CSNBPTR)
- Prohibit Export (CSNBPEX)
- Prohibit Export Extended (CSNBPEXX)
- Secure Key Import (CSNBSKI)
- Symmetric Key Export (CSNDSYI)
- Transform CDMF Key (CSNBTCK)
- User Derived Key (CSFUDK)
- VISA CVV Service Generate (CSNBCSG)
- VISA CVV Service Verify (CSNBCSV)

There are two considerations when you are using the above services:

- If you want to use the key only once and do not want to use it later, generate the operational key form.
- If you want to use the same key later, generate the operational form and store it in the CKDS using the key record write callable service (CSNBKRW). If you want to use the key on different systems that have a shared IMPORTER KEK, an alternative to storing the key in the CKDS is to generate the importable key form and use the key import callable service (CSNBKIM) to obtain the operational key.

Generating an Operational Key

To generate an operational key, choose one of the following methods:

- **For operational keys,** call the key generate callable service (CSNBKGN). Table 11 on page 71 and Table 12 on page 71 show the key type and key form combinations for a single key and for a key pair.
- **For operational keys,** call the random number generate callable service (CSNBRNG) and specify the *form* parameter as RANDOM. Specify ODD parity for a random number you intend to use as a key. Then pass the generated value to the secure key import callable service (CSNBSKI) with a required key type. The required key type is now in operational form.

  This method requires a cryptographic unit to be in special secure mode. For more information about special secure mode, see “Special Secure Mode” on page 9.
- **For data-encrypting keys,** call the random number generate callable service (CSNBRNG) and specify the *form* parameter as ODD. Then pass the generated value to the clear key import callable service (CSNBCKI) or the multiple clear key import callable service (CSNBCKM). The DATA key type is now in operational form.

You cannot generate a PIN verification (PINVER) key in operational form because the originator of the PIN generation (PINGEN) key generates the PINVER key in exportable form, which is sent to you to be imported.

Generating an Importable Key

To generate an importable key form, call the key generate callable service (CSNBKGN).

If you want a DATA, MAC, PINGEN, DATAM, or DATAC key type in importable form, obtain it directly by generating a single key. If you want any other key type in importable form, request a key pair where either the first or second key type is importable (IM). Discard the generated key form that you do not need.

Generating an Exportable Key

To generate an exportable key form, call the key generate callable service (CSNBKGN).

| If you want a DATA, MAC, PINGEN, DATAM, or DATAC key type in exportable
| form, obtain it directly by generating a single key. If you want any other key type in
| exportable form, request a key pair where either the first or second key type is
| exportable (EX). Discard the generated key form that you do not need.

Linking a Program with the ICSF Callable Services

To link the ICSF callable services into an application program, you can use the following sample JCL statements.In the SYSLIB concatenation, include the CSF.SCSFMOD0 module in the link edit step.

```
//LKEDENC  JOB
//*------------------------------------------------------------------*
//*                                                                  *
//*  The JCL links the ICSF encipher callable service, CSNBENC,   *
//*  into an application called ENCIPHER.                            *
//*                                                                  *
//*------------------------------------------------------------------*
//LINK     EXEC PGM=IEWL,
//   PARM='XREF,LIST,LET'
//SYSUT1   DD   UNIT=SYSDA,SPACE=(CYL,(10,10))
//SYSPRINT DD SYSOUT=*
//SYSLIB   DD DSN=CSF.SCSFMOD0,DISP=SHR        * SERVICES ARE IN HERE
//SYSLMOD  DD DSN=MYAPPL.LOAD,DISP=SHR         * MY APPLICATION LIBRARY
//SYSLIN   DD DSN=MYAPPL.ENCIPHER.OBJ,DISP=SHR * MY ENCIPHER PROGRAM
//         DD *
      ENTRY ENCIPHER
  NAME ENCIPHER(R)
/*
```

Typical Sequences of ICSF Callable Services

Sample sequences in which the ICSF callable services might be called are shown in Table 5 on page 39.

Table 5. Combinations of the Callable Services

```
   Combination A (DATA keys only)     Combination B

 1. Random number generate         1. Random number generate
 2. Clear key import or            2. Secure key import or
    multiple clear key import         multiple secure key import
 3. Encipher/decipher              3. Any service
 4. Data key export or key export  4. Data key export for DATA keys, or
     (optional step)                  key export in the general case
                                       (optional step)

   Combination C                      Combination D

 1. Key generate (OP form only)    1. Key generate (OPEX form)
 2. Any service                    2. Any service
 3. Key export (optional)

   Combination E                      Combination F

 1. Key generate (IM form only)    1. Key generate (IMEX form)
 2. Key import                     2. Key import
 3. Any service                    3. Any service
 4. Key export (optional)

   Combination G                      Combination H

 1. Key generate                   1. Key import
 2. Key record create              2. Key record create
 3. Key record write               3. Key record write
 4. Any service (passing label     4. Any service (passing label
    of the key just generated)        of the key just generated)

   Combination I

 1. Key token build to create
    key token skeleton
 2. Key generate to OP form of
    AKEK using key token skeleton
 3. Use AKEK in any ANSI X9.17
    service
```

Notes:

1. "Any service" means any of the following services:
   - CSNBENC
   - CSNBENC1
   - CSNBDEC
   - CSNBDEC1
   - CSNBCTT
   - CSNBCTT1
   - CSNBMGN
   - CSNBMGN1
   - CSNBMVR
   - CSNBMVR1
   - CSNBPGN
   - CSNBPTR
   - CSNBPVR
2. These combinations exclude services that can be used on their own; for example, key export or encode, or using key generate to generate an exportable key.
3. These combinations do not show key communication, or the transmission of any output from an ICSF callable service.

The key forms are described in "Key Generate (CSNBKGN)" on page 63.

Key Forms and Types Used in the Key Generate Callable Service

The key generate callable service is the most complex of all the ICSF callable services. This section provides a list of the key forms and key types used in the key generate callable service.

Purpose of Single and Double-Length Keys in One Form Only

The following provides a list of the single and double-length keys in one form.

```
 Key    Key Type
 Form      1

  OP      DATA
  OP      MAC
  OP      PINGEN
  OP      DATAC*
  OP      DATAM
  IM      DATA
  IM      MAC
  IM      PINGEN
  IM      DATAC*
  IM      DATAM
  EX      DATA
  EX      MAC
  EX      PINGEN
  EX      DATAC*
  EX      DATAM

Note: Keywords marked with an "*" must be requested through the specification of
      a proper control vector in a key token and the use of the TOKEN keyword.

Examples:

  OP DATA -   Encipher or decipher data. Use data key export or key export
              to send encrypted key to another cryptograpic partner. Then
              communicate the ciphertext.
  OP MAC -    MAC generate. Because no MACVER key exists, there is no secure
              communication of the MAC with another cryptographic partner.
  IM DATA -   Key Import, and then encipher or decipher. Then key export to
              communicate ciphertext and key with another cryptographic partner.
  EX DATA -   You can send this key to a cryptographic partner, but you can do
              nothing with it directly. Use it for the key distribution service.
              The partner could then use key import to get it in operational
              form, and use it as in OP DATA above.
```

Purpose of OPIM, OPOP, and IMIM Single- and Double-Length Keys in Two Forms

The following provides a list of key pairs; one key is operational, and the other is imported to the local system.

The first two letters of the key form indicate the form that key type 1 parameter is in, and the second two letters indicate the form that key type 2 parameter is in.

```
 Key    Key Type    Key Type
 Form      1           2

 OPIM     DATA       DATA
 OPIM     MAC        MAC
 OPIM     MAC        MACVER
 OPIM     DATAC*     DATAC*
 OPIM     DATAM      DATAM
 OPIM     DATAM      DATAMV
 OPIM     CIPHER     CIPHER
 OPIM     CIPHER     DECIPHER
 OPIM     CIPHER     ENCIPHER
 OPIM     DECIPHER   CIPHER
 OPIM     DECIPHER   ENCIPHER
 OPIM     ENCIPHER   CIPHER
 OPIM     ENCIPHER   DECIPHER
 OPIM     OPINENC    IPINENC
 OPIM     IPINENC    OPINENC
 OPIM     OPINENC    OPINENC
 OPOP     DATA       DATA
 OPOP     MAC        MAC
 OPOP     MAC        MACVER
 OPOP     DATAC*     DATAC*
 OPOP     DATAM      DATAM
 OPOP     DATAM      DATAMV
 OPOP     CIPHER     CIPHER
 OPOP     CIPHER     DECIPHER
 OPOP     CIPHER     ENCIPHER
 OPOP     DECIPHER   CIPHER
 OPOP     DECIPHER   ENCIPHER
 OPOP     ENCIPHER   CIPHER
 OPOP     ENCIPHER   DECIPHER
 OPOP     OPINENC    IPINENC
 OPOP     IPINENC    OPINENC
 OPOP     OPINENC    OPINENC
 IMIM     DATA       DATA
 IMIM     MAC        MAC
 IMIM     MAC        MACVER
 IMIM     DATAC*     DATAC*
 IMIM     DATAM      DATAM
 IMIM     DATAM      DATAMV
 IMIM     CIPHER     CIPHER
 IMIM     CIPHER     DECIPHER
 IMIM     CIPHER     ENCIPHER
 IMIM     DECIPHER   CIPHER
 IMIM     DECIPHER   ENCIPHER
 IMIM     ENCIPHER   CIPHER
 IMIM     ENCIPHER   DECIPHER
 IMIM     OPINENC    IPINENC
 IMIM     IPINENC    OPINENC
 IMIM     OPINENC    OPINENC

Note: Keywords marked with an "*" must be requested through the specification of
      a proper control vector in a key token and the use of the TOKEN keyword.

Examples:

OPIM  DATA DATA   Use the OP form in encipher. Use key export with the
                  OP form to communicate ciphertext and key with
                  another cryptographic partner. Use key import at a
                  later time to use encipher or decipher with the same
                  key again.
 OPIM  MAC  MAC   Single-length MAC generation key. Use the OP form in
                  MAC generation. You have no corresponding MACVER key,
                  but you can call the MAC verification service with
                  the MAC key directly. Use the key import callable
                  service and then compute the MAC again using the MAC
                  verification callable service, which comapres the MAC
                  it generates with the MAC supplied with the message
                  and issues a return code indicating whether they
                  compare.
```

Purpose of OPEX Single- and Double-Length Keys in Two Forms

The following provides a list of key pairs; one key is operational and the other is exported from the system.

Key Form	Key Type 1	Key Type 2
OPEX	DATA	DATA
OPEX	MAC	MAC
OPEX	MAC	MACVER
OPEX	DATAC*	DATAC*
OPEX	DATAM	DATAM
OPEX	DATAM	DATAMV
OPEX	CIPHER	CIPHER
OPEX	CIPHER	DECIPHER
OPEX	CIPHER	ENCIPHER
OPEX	DECIPHER	CIPHER
OPEX	DECIPHER	ENCIPHER
OPEX	ENCIPHER	CIPHER
OPEX	ENCIPHER	DECIPHER
OPEX	EXPORTER	IMPORTER
OPEX	IMPORTER	EXPORTER
OPEX	EXPORTER	IKEYXLAT
OPEX	IKEYXLAT	EXPORTER
OPEX	IKEYXLAT	OKEYXLAT
OPEX	IMPORTER	OKEYXLAT
OPEX	OKEYXLAT	IMPORTER
OPEX	OKEYXLAT	IKEYXLAT
OPEX	PINGEN	PINVER
OPEX	PINVER	PINGEN
OPEX	DATA	DATAXLAT
OPEX	DATAXLAT	DATAXLAT
OPEX	OPINENC	IPINENC
OPEX	IPINENC	OPINENC
OPEX	CVARDEC*	CVARENC*
OPEX	CVARENC*	CVARDEC*
OPEX	CVARENC*	CVARXCVL*
OPEX	CVARENC*	CVARXCVR*
OPEX	CVARXCVL*	CVARENC*
OPEX	CVARXCVR*	CVARENC*
OPEX	CVARDEC*	CVARPINE*
OPEX	CVARPINE*	CVARDEC*

Note: Keywords marked with an "*" must be requested through the specification of a proper control vector in a key token and the use of the TOKEN keyword.

Examples:

OPEX DATA DATA	Use the OP form in encipher. Send the EX form and the ciphertext to another cryptographic partner.
OPEX MAC MAC	Single-length MAC generation key. Use the OP form in both MAC generation and MAC verification. Send the EX form to a cryptographic partner to be used in the MAC generation or MAC verification services.
OPEX MAC MACVER	Single-length MAC generation and MAC verification keys. Use the OP form in MAC generation. Send the EX form to a cryptographic partner where it will be put into key import, and then MAC verification, with the message and MAC that you have also transmitted.
OPEX PINGEN PINVER	Use the OP form in Clear PIN generate. Send the EX form to a cryptographic partner where it is put into key import, and then Encrypted PIN verify, along with an IPINENC key.
OPEX IMPORTER EXPORTER	Use the OP form in key import, key generate, or secure key import. Send the EX form to a cryptographic partner where it is used in key export, data key export, or key generate, or put in the CKDS.
OPEX EXPORTER IMPORTER	Use the OP form in key export, data key export, or key generate. Send the EX form to a cryptographic partner where it is put into the CKDS or used in key import, key generate or secure key import.

When you and your partner have the OPEX IMPORTER EXPORTER, OPEX EXPORTER IMPORTER pairs of keys in “Purpose of OPEX Single- and Double-Length Keys in Two Forms” on page 41 installed, you can start key and data exchange.

Purpose of IMEX Single- and Double-Length Keys in Two Forms

The following provides a list of key pairs; one key is imported locally and the other key is sent elsewhere.

Key Form	Key Type 1	Key Type 2	Purpose
IMEX	DATA	DATA	All these key forms correspond to
IMEX	DATA	DATAXLAT	the OPEX forms. The difference between using IMEX
IMEX	DATAXLAT	DATAXLAT	forms instead of OPEX is that IM must be transformed
IMEX	MAC	MAC	into oprerational form by using the key import
IMEX	MAC	MACVER	callable service.
IMEX	DATAM	DATAM	
IMEX	DATAM	DATAMV	
IMEX	DATAC*	DATAC*	
IMEX	CIPHER	CIPHER	
IMEX	CIPHER	DECIPHER	
IMEX	CIPHER	ENCIPHER	
IMEX	DECIPHER	CIPHER	
IMEX	DECIPHER	ENCIPHER	
IMEX	ENCIPHER	CIPHER	
IMEX	ENCIPHER	DECIPHER	
IMEX	EXPORTER	IMPORTER	
IMEX	IMPORTER	EXPORTER	
IMEX	EXPORTER	IKEYXLAT	
IMEX	IKEYXLAT	EXPORTER	
IMEX	IKEYXLAT	OKEYXLAT	
IMEX	IMPORTER	OKEYXLAT	
IMEX	OKEYXLAT	IMPORTER	
IMEX	OKEYXLAT	IKEYXLAT	
IMEX	PINGEN	PINVER	
IMEX	PINVER	PINGEN	
IMEX	OPINENC	IPINENC	
IMEX	IPINENC	OPINENC	
IMEX	CVARDEC*	CVARENC*	
IMEX	CVARENC*	CVARDEC*	
IMEX	CVARENC*	CVARXCVL*	
IMEX	CVARENC*	CVARXCVR*	
IMEX	CVARXCVL*	CVARENC*	
IMEX	CVARXCVR*	CVARENC*	
IMEX	CVARDEC*	CVARPINE*	
IMEX	CVARPINE*	CVARDEC*	

Note: Keywords marked with an "*" must be requested through the specification of a proper control vector in a key token and the use of the TOKEN keyword.

Purpose of EXEX Single- and Double-Length Keys in Two Forms

For the keys shown in the following list, you are providing key distribution services for other nodes in your network, or other cryptographic partners. Neither key type can be used in your installation.

Key Form	Key Type 1	Key Type 2
EXEX	DATA	DATA
EXEX	DATA	DATAXLAT
EXEX	DATAXLAT	DATAXLAT
EXEX	MAC	MAC
EXEX	MAC	MACVER
EXEX	DATAM	DATAM

```
|                     EXEX   DATAM      DATAMV
|                     EXEX   DATAC*     DATAC*
|                     EXEX   CIPHER     CIPHER
|                     EXEX   CIPHER     DECIPHER
|                     EXEX   CIPHER     ENCIPHER
|                     EXEX   DECIPHER   CIPHER
|                     EXEX   DECIPHER   ENCIPHER
|                     EXEX   ENCIPHER   CIPHER
|                     EXEX   ENCIPHER   DECIPHER
|                     EXEX   EXPORTER   IMPORTER
|                     EXEX   IMPORTER   EXPORTER
|                     EXEX   EXPORTER   IKEYXLAT
|                     EXEX   IKEYXLAT   EXPORTER
|                     EXEX   IKEYXLAT   OKEYXLAT
|                     EXEX   IMPORTER   OKEYXLAT
|                     EXEX   OKEYXLAT   IMPORTER
|                     EXEX   OKEYXLAT   IKEYXLAT
|                     EXEX   PINGEN     PINVER
|                     EXEX   PINVER     PINGEN
|                     EXEX   OPINENC    IPINENC
|                     EXEX   IPINENC    OPINENC
|
|                   Note: Keywords marked with an "*" must be requested through the specification of
|                         a proper control vector in a key token and the use of the TOKEN keyword.
```

Generating AKEKs

AKEKs are bidirectional and are OP-form-only keys that can be used in both import and export. Before using the key generate callable service to create an AKEK, you need to use the key token build callable service to create a key token for receiving the AKEK. The steps involved in this process are presented below.

1. Use the key token build callable service with the following parameter values:

Parameter	**Value**
Key_type	AKEK
Rule_array	INTERNAL NO-KEY {SINGLE or DOUBLE-O}

2. Use the key generate callable service with the following parameter values:

Parameter	**Value**
Key_form	OP
Key_type_1	TOKEN
Generated_key_identifier_1	The skeleton key token created in step 1

Using the Ciphertext Translate Callable Service

Note: The ciphertext translate callable service does not work in CDMF-only systems (see “System Encryption Algorithm” on page 13).

This section describes a scenario using the encipher, ciphertext translate, and decipher callable services with four network nodes: A, B, C, and D. You want to send data from your network node A to a destination node D. You cannot communicate directly with node D, and nodes B and C are situated between you. You do not want nodes B and C to decipher your data.

At node A, you use the encipher callable service (CSNBENC or CSNBENC1). Node D uses the decipher callable service (CSNBDEC or CSNBDEC1).

Node B and C will use the ciphertext translate callable service. Consider the keys that are needed to support this process:

1. At your node, generate one key in two forms: OPEX DATA DATAXLAT
2. Send the exportable DATAXLAT key to node B.
3. Node B and C need to share a DATAXLAT key, so generate **a different key** in two forms: EXEX DATAXLAT DATAXLAT.
4. Send the first exportable DATAXLAT key to node B.
5. Send the second exportable DATAXLAT key to node C.
6. Node C and node D need to share a DATAXLAT key and a DATA key. Node D can generate one key in two forms: OPEX DATA DATAXLAT.
7. Node D sends the exportable DATAXLAT key to node C.

The communication process is shown as:

```
Node:       A             B                    C                D

Callable
Service: Encipher  Ciphertext Translate  Ciphertext Translate   Decipher

Keys:     DATA      DATAXLAT  DATAXLAT    DATAXLAT  DATAXLAT     DATA

Key Pairs: |____ = ____|         |____ = ____|         |____ = ____|
```

Therefore, you need three keys, each in two different forms. You can generate two of the keys at node A, and node D can generate the third key. Note that the key used in the decipher callable service at node D is **not** the same key used in the encipher callable service at node A.

When the Call Succeeds

If the return code is **0**, ICSF has successfully completed the call. If a reason code other than 0 is included, refer to "Appendix A. ICSF and TSS Return and Reason Codes" on page 319, for additional information. For instance, reason code 10000 indicates the key in the key identifier (or more than one key identifier, for services that use two internal key identifiers) has been reenciphered from encipherment under the old master key to encipherment under the current master key. Keys in external tokens are not affected by this processing because they contain keys enciphered under keys other than the host master key. If you manage your key identifiers on disk, then reason code 10000 should be a "trigger" to store these updated key identifiers back on disk.

Your program can now continue providing its function, but you may want to communicate the key that you used to another enterprise. This process is exporting a key.

If you want to communicate the key that you are using to a cryptographic partner, there are several methods to use:

- For DATA keys only, call the data key export callable service. You now have a DATA key type in exportable form.
- Call the key export callable service. You now have the key type in exportable form.
- When you use the key generate callable service to create your operational or importable key form, you can create an exportable form, **at the same time**, and you now have the key type, in exportable form, at the same time as you get the operational or importable form.

When the Call Does Not Succeed

Now you have planned your use of the ICSF callable services, made the call, but the service has completed with a return and reason codes other than zero.

If the return code is **4**, there was a minor problem. For example, reason code 8004 indicates the trial MAC that was supplied does not match the message text provided.

If the return code is **8**, there was a problem with one of your parameters. Check the meaning of the reason code value, correct the parameter, and call the service again. You may go through this process several times before you succeed.

If the return code is **12**, ICSF is not active, or has no access to cryptographic units, or has an environmental problem. Check with your ICSF administrator.

If the return code is **16**, the service has a serious problem that needs the help of your system programmer.

There are several reason codes that can occur **after** you have fully debugged and tested your program. For example:

- Reason code 10004 indicates that you provided a key identifier that holds a key enciphered under a host master key. The host master key is not installed in the cryptographic unit. If this happens, you have to go back and import your importable key form again and call the service again. You need to build this flow into your program logic.
- Reason code 10012 indicates a key corresponding to the label that you specified is not in the CKDS or PKDS. Check with your ICSF administrator to see if the label is correct.

Return and reason codes are described in "Appendix A. ICSF and TSS Return and Reason Codes" on page 319.

Chapter 4. Managing Cryptographic Keys

This chapter describes the callable services that generate and maintain cryptographic keys.

Using ICSF, you can generate keys using either the key generator utility program or the key generate callable service. ICSF provides a number of callable services to assist you in managing and distributing keys and maintaining the cryptographic key data set (CKDS).

This chapter describes the following callable services:

- “Clear Key Import (CSNBCKI)” on page 49
- “Multiple Clear Key Import (CSNBCKM)” on page 50
- | “Data Key Import (CSNBDKM)” on page 53
- “Data Key Export (CSNBDKX)” on page 54
- “Key Export (CSNBKEX)” on page 56
- | “Prohibit Export (CSNBPEX)” on page 60
- “Prohibit Export Extended (CSNBPEXX)” on page 62
- “Key Generate (CSNBKGN)” on page 63
- | “Key Translate (CSNBKTR)” on page 73
- “Key Import (CSNBKIM)” on page 74
- “Key Part Import (CSNBKPI)” on page 79
- “Secure Key Import (CSNBSKI)” on page 81
- “Multiple Secure Key Import (CSNBSKM)” on page 84
- “Key Test (CSNBKYT and CSNBKYTX)” on page 88
- “Key Record Create (CSNBKRC)” on page 92
- “Key Record Delete (CSNBKRD)” on page 93
- “Key Record Read (CSNBKRR)” on page 95
- “Key Record Write (CSNBKRW)” on page 96
- “Transform CDMF Key (CSNBTCK)” on page 97
- “User Derived Key (CSFUDK)” on page 99

See also “Key Token Build (CSNBKTB)” on page 203 for a description of the key token build callable service.

The Key Generator Utility Program

The key generator utility program uses the key generate callable service to generate all types of keys. A master key variant enciphers each key that the key generator utility program creates. After the key generator utility program generates a key, it stores the key in the CKDS.

Note: If you specify CLEAR, KGUP uses the random number generate and secure key import callable services rather than the key generate service.

You can access KGUP using ICSF panels. The KGUP path of these panels helps you create the JCL control statements to control the key generator utility program. When you want to generate a key, you can enter the ADD control statement and information, such as the key type on the panels. For a detailed description of the key generator utility program and how to use it to generate keys, see *OS/390 ICSF Administrator’s Guide*.

© Copyright IBM Corp. 1997, 2000

The Key Generate Callable Service

The key generate callable service creates all types of keys. It generates a single key or a pair of keys. Unlike the key generator utility program, the key generate callable service does not store the keys in the CKDS where they can be saved and maintained. The key generate callable service merely returns the key to the application program that called it.

The Key Import and Key Export Callable Services

The key import and key export callable services are used to import keys, prepare keys for export, and change key forms. These services support key distribution and management activities.

Prohibiting Export

The prohibit export extended service updates the control vector in the external token of a key in exportable form so that the receiver node can import the key but not export it. This service differs from the prohibit export service, which changes only an internal token. The key export callable service does not allow export of this token.

Generating a Verification Pattern and Verifying a Key

The key test service generates or verifies a secure cryptographic verification pattern for keys. The key to test can be in the clear or encrypted under a master key. The key test extended callable service works on keys encrypted under a KEK.

The Dynamic CKDS Update Callable Services

ICSF provides the dynamic CKDS update services that allow applications to directly manipulate both the DASD copy and in-storage copy of the current CKDS.

Note: Applications using the dynamic CKDS update callable services can run concurrently with other operations that affect the CKDS, such as KGUP, CKDS conversion, REFRESH, and dynamic master key change. An operation can fail if it needs exclusive or shared access to the same DASD copy of the CKDS that is held shared or exclusive by another operation. ICSF provides serialization to prevent data loss from attempts at concurrent access, but your installation is responsible for the effective management of concurrent use of competing operations. Consult your system administrator or system programmer for your installation guidelines.

The syntax of the key record create, key record read, and key record write services is identical with the same services provided by the Transaction Security System security application programming interface. Key management applications that use these common interface verbs can run on both systems without change.

Changing a CDMF DATA Key to a Transformed Shortened DES DATA Key

The transform CDMF key callable service changes a CDMF DATA key in an internal or external token to a transformed shortened DES key. This callable service is implemented on all S/390 G3, or higher, Enterprise Servers and S/390 Multiprise Servers. Using this service is optional. It is for CDMF or DES-CDMF systems that need to send CDMF-encrypted data to DES-only systems. The CDMF or DES-CDMF system must generate the key, shorten it, and pass it to the DES-only system.

Generating a User-Derived Key

The user derived key callable service generates a single-length or double-length MAC key. The single-length MAC key can be used in the ANSI X9.9-1 or ANSI X9.19 basic MAC procedures. The double-length MAC key can be used in the ANSI X9.19 optional double key MAC procedure. The user derived key is generated according to the Europay, MasterCard and Visa (EMV) specification algorithm. In addition to generating a user derived key, this service can also be used to update an existing user derived key.

Clear Key Import (CSNBCKI)

Use the clear key import callable service to import a clear DATA key that is to be used to encipher or decipher data. This callable service can import only DATA keys. Clear key import accepts an 8-byte clear DATA key, enciphers it under the master key, and returns the encrypted DATA key in operational form in an internal key token. This service marks this internal key token CDMF or DES, according to the system's default encryption algorithm, unless token copying overrides this.

If the clear key value does not have odd parity in the low-order bit of each byte, the service returns a warning value in the *reason_code* parameter. The callable service does not adjust the parity of the key.

Note: To import 16-byte or 24-byte DATA keys, use the multiple clear key import callable service that is described in "Multiple Clear Key Import (CSNBCKM)" on page 50.

Format

```
CALL CSNBCKI(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             clear_key,
             key_identifier )
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that are assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

clear_key

Direction: Input	Type: String

The *clear_key* specifies the 8-byte clear key value to import.

key_identifier

Direction: Input/Output	Type: String

A 64-byte string that is to receive the internal key token. “Key Identifier for DES Key Token” on page 27 describes the internal key token. If this parameter contains a valid internal key token for a DATA key, clear key import propagates the data encryption algorithm bits to the imported key token. Otherwise, this callable service marks the key token according to the system's default algorithm.

Usage Note

| This service produces an internal DATA token with a control vector which is usable
| on the Cryptographic Coprocessor Feature. If a valid internal token is supplied as
| input to the service in the *key_identifier* field, that token’s control vector will not be
| used in the encryption of the clear key value.

Multiple Clear Key Import (CSNBCKM)

This callable service encrypts a single-, double-, or triple-length DATA key under the system master key.

Format

```
CALL CSNBCKM(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            clear_key_length,
            clear_key,
            key_identifier_length,
            key_identifier )
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that are assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you are supplying in the *rule_array* parameter. The *rule_array_count* parameter must be 0 or 1.

rule_array

Direction: Input	Type: String

Zero or one keyword that supplies control information to the callable service. The keyword must be in 8 bytes of contiguous storage, left-justified and padded on the right with blanks. Refer to Table 6 for a list of keywords.

The keyword specifies the cryptographic algorithm. If no algorithm is specified, the system default algorithm is used unless a double- or triple-length DATA key is specified on a CDMF system. In this case, the resulting DATA token is marked DES.

Table 6. Keywords for Multiple Clear Key Import Rule Array Control Information

Keyword	Meaning
Algorithm (optional)	
DES	The output key identifier is to be a DES token.
CDMF	The output key identifier is to be a CDMF token. For a DATA key of length 16 or 24, you may not specify CDMF.

clear_key_length

Direction: Input Type: Integer

The *clear_key_length* specifies the length of the clear key value to import. This length must be 8, 16, or 24.

clear_key

Direction: Input Type: String

The *clear_key* specifies the clear key value to import.

key_identifier_length

Direction: Input/Output Type: Integer

The byte length of the *key_identifier* parameter. This must be at least 64 bytes.

key_identifier

Direction: Output Type: String

A 64-byte string that is to receive the internal key token. “Appendix H. Key Token Formats” on page 385 describes the key tokens.

Usage Note

| This service produces an internal DATA token with a control vector which is usable
| on the Cryptographic Coprocessor Feature. If a valid internal token is supplied as
| input to the service in the *key_identifier* field, that token’s control vector will not be
| used in the encryption of the clear key value.

Data Key Import (CSNBDKM)

Use the data key import callable service to import an encrypted source DES single-length or double-length DATA key and create or update a target internal key token with the master key enciphered source key. ICSF routes the Data Key Import request to a PCI Cryptographic Coprocessor for processing. If no PCI Cryptographic Coprocessor is online, the request fails.

Format

```
CALL CSNBDKM(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             source_key_token,
             importer_key_identifier,
             target_key_identifier)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

source_key_token

Direction: Input	Type: String

A 64-byte string variable containing the source key to be imported. The source key must be an external key. The external key token must indicate that a control vector is present; however, the control vector is usually valued at zero. A double-length key that should result in a default DATA control vector must be specified in a version X'01' external key token. Otherwise, both single and double-length keys are presented in a version X'00' key token. Alternatively, the encrypted data key can be provided at offset 16 in an otherwise all X'00' key token. The service will process this token format as a DATA key encrypted by the importer key and a null (all zero) control vector.

importer_key_identifier

Direction: Input/Output	Type: String

A 64-byte string variable containing the (IMPORTER) transport key or key label of the transport key used to decipher the source key.

target_key_identifier

Direction: Output	Type: String

A 64-byte string variable containing a null key token or an internal key token. The key token receives the imported key.

Restriction

The caller must be in task mode, not in SRB mode.

Usage Notes

SAF will be invoked to check authorization to use the Data Key Import service and the label of the *importer_key_identifier*.

This service does not adjust the key parity of the source key.

CDMF/DES token markings will be ignored.

Data Key Export (CSNBDKX)

Use the data key export callable service to reencipher a data-encrypting key (key type of DATA only) from encryption under the master key to encryption under an exporter key-encrypting key. The reenciphered key is in a form suitable for export to another system.

ICSF examines the data encryption algorithm bits on the exporter key-encrypting key and DATA key for consistency. It does not export a CDMF key under a DES-marked key-encrypting key or a DES key under a CDMF-marked key-encrypting key. These checks are not enforced when the service is executed on a PCI Cryptographic Coprocessor. ICSF does not propagate the data encryption marking on the operational key to the external token.

The data key export service generates a key token with the same key length as the input token's key.

| ICSF routes the Data Key Export request to a PCI Cryptographic Coprocessor if the
| control vector of the *exporter_key_identifier* cannot be processed on the
| Cryptographic Coprocessor Feature. If no PCI Cryptographic Coprocessor is online
| in this case, the request fails.

Format

```
CALL CSNBDKX(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            source_key_identifier,
            exporter_key_identifier,
            target_key_identifier )
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

source_key_identifier

Direction: Input/Output	Type: String

A 64-byte string for an internal key token or label that contains a data-encrypting key to be reenciphered. The data-encrypting key is encrypted under the master key.

exporter_key_identifier

Direction: Input/Output	Type: String

A 64-byte string for an internal key token or key label that contains the exporter *key_encrypting* key. The data-encrypting key above will be encrypted under this exporter *key_encrypting* key.

target_key_identifier

Direction: Input/Output	Type: String

A 64-byte field that is to receive the external key token, which contains the reenciphered key that has been exported. The reenciphered key can now be exchanged with another cryptographic system.

Usage Note

You cannot export a CDMF key under a DES-marked KEK or a DES key under a CDMF-marked KEK. The service fails with a return code of 8 and reason code of 10120. These checks are not enforced when the service is executed on a PCI Cryptographic Coprocessor.

Key Export (CSNBKEX)

Use the key export callable service to reencipher any type of key (except an AKEK or an IMP-PKA) from encryption under a master key variant to encryption under the same variant of an exporter key-encrypting key. The reenciphered key can be exported to another system.

ICSF examines the data encryption algorithm bits on the exporter key-encrypting key and the key being exported for consistency. It does not export a CDMF key under a DES-marked key-encrypting key or a DES key under a CDMF-marked key-encrypting key. These checks are not enforced when the service is executed on a PCI Cryptographic Coprocessor. ICSF does not propagate the data encryption marking on the operational key to the external token.

If the key to be exported is a DATA key, the key export service generates a key token with the same key length as the input token's key.

This service supports the no-export bit that the key import service sets in the internal token.

ICSF routes the Key Export request to a PCI Cryptographic Coprocessor if the control vector of the *exporter_key_identifier* cannot be processed on the Cryptographic Coprocessor Feature. The service will also be routed to a PCI Cryptographic Coprocessor if the key type specified is one of the following: DECIPHER, ENCIPHER, IKEYXLAT, OKEYXLAT or CIPHER. If no PCI Cryptographic Coprocessor is online in this case, the request fails. If the key type is MACD, the key export service will be processed on a Cryptographic Coprocessor Feature.

Format

```
CALL CSNBKEX(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            key_type,
            source_key_identifier,
            exporter_key_identifier,
            target_key_identifier )
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

key_type

Direction: Input	Type: Character string

The parameter is an 8-byte field that contains either a key type value or the keyword TOKEN. The keyword is left-justified and padded on the right with blanks. The key types you can specify are listed in Table 7 on page 58.

For a double-length MAC key with a key type of DATAM, the service uses the data compatibility control vector to create an external token. For a double-length MAC key with a key type of MACD, the service uses the single-length control vector for both the left and right half of the key to create an external token (MAC ‖ MAC). For a table of control vectors, refer to “Appendix K. Control Vector Table” on page 413.

To export a double-length MAC generation key, use a key type of either DATAM or TOKEN. To export a double-length MAC verification key, use a key type of either DATAMV or TOKEN.

If the key type is TOKEN, ICSF determines the key type from the control vector (CV) field in the internal key token provided in the *source_key_identifier* parameter. If the control vector is invalid on the Cryptographic Coprocessor Feature, the key export request will be routed to the PCI Cryptographic Coprocessor.

Table 7. Key Type Values for the Key Export Callable Service

Key Type	**Meaning**
DATA	Data-encrypting key. Use this single-, double-, or triple-length key to encipher and decipher data.
DATAXLAT	Data translation key. Use this single-length key to reencipher text from one DATA key to another.
MAC	MAC generation key. Use this single-length key to generate a message authentication code.
MACVER	MAC verification key. Use this single-length key to verify a message authentication code.
DATAM	MAC generation key. Use this double-length key to generate a message authentication code.
DATAMV	MAC verification key. Use this double-length key to verify a message authentication code.
MACD	Double-length MAC generation and verification key. ICSF continues to support this key type for compatibility with ICSF Version 2 Release 1.
PINGEN	PIN generation key. Use this double-length key to generate PINs.
PINVER	PIN verification key. Use this double-length key to verify PINs.
IPINENC	Input PIN-encrypting key. Use this double-length input key to translate PINs. PIN blocks received from other nodes or automatic teller machine (ATM) terminals are encrypted under this type of key. These encrypted PIN blocks are the input to the Encrypted PIN translate and Encrypted PIN verify callable services.
OPINENC	Output PIN-encrypting key. Use this double-length output key to translate PINs. The output PIN blocks from the Encrypted PIN translate callable service are encrypted under this type of key.
EXPORTER	Exporter key-encrypting key. Use this double-length key to convert any key (including a DATA key) from operational form into exportable form.
IMPORTER	Importer key-encrypting key. Use this double-length key to convert a key from importable form into operational form.
DECIPHER	Used only to decrypt data.

Table 7. Key Type Values for the Key Export Callable Service (continued)

Key Type	Meaning
ENCIPHER	Used only to encrypt data.
IKEYXLAT	Used to decrypt an input key in the Key Translate callable service.
OKEYXLAT	Used to encrypt an output key in the Key Translate callable service.
CIPHER	Used only to encrypt or decrypt data.
DATAC	Used to specify a DATA-class key that will perform in the Encipher and Decipher callable services, but not in the MAC Generate or MAC Verify callable services.

source_key_identifier

Direction: Input Type: String

A 64-byte string of the internal key token or key label that contains the key to be reenciphered. This parameter must identify an internal key token in application storage, or a label of an existing key in the cryptographic key data set.

If you supply TOKEN for the *key_type* parameter, ICSF looks at the control vector in the internal key token and determines the key type from this information. Therefore, if you supply a key label in the *source_key_identifier* parameter, the keyword TOKEN cannot be used in the *key_type* parameter.

exporter_key_identifier

Direction: Input/Output Type: String

A 64-byte string of the internal key token or key label that contains the exporter key-encrypting key. This parameter must identify an internal key token in application storage, or a label of an existing key in the cryptographic key data set.

If the NOCV bit is on in the internal key token containing the key-encrypting key, the key-encrypting key itself (not the key-encrypting key variant) is used to encipher the generated key. For example, the key has been installed in the cryptographic key data set through the key generator utility program or the key entry hardware using the NOCV parameter; or you are passing the key-encrypting key in the internal key token with the NOCV bit on and your program is running in supervisor state or in key 0-7.

Control vectors are explained in “Control Vector” on page 5 and the NOCV bit is shown in Table 94 on page 385.

target_key_identifier

Direction: Input/Output Type: String

The 64-byte field external key token that contains the reenciphered key. The reenciphered key can be exchanged with another cryptographic system.

Usage Notes

You cannot export a CDMF key under a DES-marked KEK or a DES key under a CDMF-marked KEK. The service fails with a return code of 8 and reason code of 10120. These checks are not enforced when the service is executed on a PCI Cryptographic Coprocessor.

This service supports the no-export bit that the key import service sets in the internal token. (A return code of 8 and reason code of 10124 indicates a key cannot be exported.)

For key export, you can use the following combinations of parameters:

- A valid key type in the *key_type* parameter and an internal key token in the *source_key_identifier* parameter. The key type must be equivalent to the control vector specified in the internal key token.
- A *key_type* parameter of TOKEN and an internal key token in the *source_key_identifier* parameter. The key type is extracted from the control vector contained in the internal key token.
- A valid key type in the *key_type* parameter, and a label in the *source_key_identifier* parameter.

If internal key tokens are supplied in the *source_key_identifier* or *exporter_key_identifier* parameters, the key in one or both tokens can be reenciphered. This occurs if the master key was changed since the internal key token was last used. The return and reason codes that indicate this do *not* indicate which key was reenciphered. Therefore, assume both keys have been reenciphered.

This service cannot be used to export AKEKs. Refer to “ANSI X9.17 Key Export (CSNAKEX)” on page 105 for information on exporting AKEKs.

To use NOCV key-encrypting keys or to export double-length MAC and MACVER keys, the NOCV-enablement keys must be installed in the CKDS.

Key Export operations which specify a NOCV key-encrypting key as the exporter key and also specify a source or key-encrypting key which contains a control vector not supported by the Cryptographic Coprocessor Feature will fail.

If the key type is MACD, the control vectors of the input keys must be the standard control vectors supported by the Cryptographic Coprocessor Feature, since the key export service will be processed on the Cryptographic Coprocessor Feature in this case.

Prohibit Export (CSNBPEX)

The Prohibit Export service modifies an operational key so that it cannot be exported. The Prohibit Export service does not support NOCV key-encrypting keys, or DATA, MAC, or MACVER keys with standard control vectors (for example, control vectors supported by the Cryptographic Coprocessor Feature).

ICSF routes the Prohibit Export request to a PCI Cryptographic Coprocessor for processing. If no PCI Cryptographic Coprocessor is online, the request fails.

Format

```
CALL CSNBPEX(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             key_identifier)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

key_identifier

Direction: Input/Output	Type: String

A 64-byte string variable containing the internal key token to be modified.

Restriction

The caller must be in task mode, not in SRB mode.

Usage Note

SAF will be invoked to check authorization to use the Prohibit Export service.

Prohibit Export Extended (CSNBPEXX)

Use the prohibit export extended callable service to change the external token of a cryptographic key in exportable form so that it can be imported at the receiver node and is non-exportable from that node. You cannot prohibit export of DATA keys.

The inputs are an external token of the key to change in the *source_key_token* parameter and the label or internal token of the exporter key-encrypting key in the *kek_key_identifier* parameter.

| CSNBPEXX is a variation of the prohibit export service, which supports only
| changing an *internal* token.

Format

```
CALL CSNBPEXX(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            source_key_token,
            kek_key_identifier)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

source_key_token

Direction: Input/Output　　　　Type: String

A 64-byte string of an external token of a key to change. It is in exportable form.

kek_key_identifier

Direction: Input/Output　　　　Type: Integer

A 64-byte string of an internal token or label of the exporter KEK used to encrypt the key contained in the external token specified in the previous parameter.

Key Generate (CSNBKGN)

Use the key generate callable service to generate either one or two odd parity DES keys of *any* type.The keys can be single-length (8 bytes), double-length (16 bytes), or, in the case of DATA keys, triple-length (24 bytes). The callable service does not produce keys in clear form and all keys are returned in encrypted form. When two keys are generated, each key has the same clear value, although this clear value is not exposed outside the secure cryptographic feature.

| ICSF routes the Key Generate request to a PCI Cryptographic Coprocessor if the
| key type specified in *key_type_1* or *key_type_2* is not valid for the Cryptographic
| Coprocessor Feature or if the control vector in a supplied token cannot be
| processed on the Cryptographic Coprocessor Feature. The Key Generate request is
| also routed to a PCI Cryptographic Coprocessor. is a key length of SINGLE-R is
| specified, or if a key form of OPOP or IMIM is specified. If no PCI Cryptographic
| Coprocessor is online in this case, the request fails.

Format

```
CALL CSNBKGN(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             key_form,
             key_length,
             key_type_1,
             key_type_2,
             kek_key_identifier_1,
             kek_key_identifier_2,
             generated_key_identifier_1,
             generated_key_identifier_2 )
```

Parameters

return_code

Direction: Output　　　　Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output Type: String

The data that is passed to the installation exit.

key_form

Direction: Input Type: Character string

A 4-byte keyword that defines the type of key(s) you want generated. This parameter also specifies if each key should be returned for either operational, importable, or exportable use. The keyword must be in a 4-byte field, left-justified, and padded with blanks.

The first two characters refer to *key_type_1*. The next two characters refer to *key_type_2*.

| The following keywords are allowed: OP, IM, EX, OPIM, OPEX, IMEX, EXEX,
| OPOP, and IMIM. See Table 8 for their meanings.

Table 8. Key Form Values for the Key Generate Callable Service

Keyword	Meaning
OP	One operational key. The key is returned to the caller in the key token format. Specify the OP key form when generating AKEKs.
IM	One key that can be locally imported. The key can later be imported onto this system to make it operational.
EX	One key that can be sent to another system.
OPIM	A key pair; one key that is operational and one key to be imported to the local system. Both keys have the same clear value. On the other system, the external key token can be imported to make it operational.
OPEX	A key pair; one key that is operational and one key to be sent from this system. Both keys have the same clear value.
IMEX	A key pair to be imported; one key to be imported locally and one key to be sent elsewhere. Both keys have the same clear value.

Table 8. Key Form Values for the Key Generate Callable Service (continued)

Keyword	Meaning
EXEX	A key pair; both keys to be sent elsewhere, possibly for exporting to two different systems. The key pair has the same clear value.
OPOP	A key pair; normally with different control vector values.
IMIM	A key pair to be imported; both keys to be imported locally at a later time.

The key forms are defined as follows:

Operational (OP)
The key value is enciphered under a master key. The result is placed into an internal key token. The key is then operational at the local system. For AKEKs, the result is placed in a skeleton token created by the key token build callable service.

Importable (IM)
The key value is enciphered under an importer key-encrypting key. The result is placed into an external key token.

Exportable (EX)
The key value is enciphered under an exporter key-encrypting key. The result is placed into an external key token. The key can then be transported or exported to another system and imported there for use. This key form cannot be used by any ICSF callable service.

The keys are placed into tokens that the *generated_key_identifier_1* and *generated_key_identifier_2* parameters identify.

If this service is generating only the OP form for a DATA key, it marks the DATA key with the data encryption algorithm according to the system default encryption algorithm unless token copying overrides this. If this service is generating only the OP form for an IMPORTER, it marks the IMPORTER with the SYS-ENC (X'00') data encryption algorithm bits, unless token copying overrides this. Marking of data encryption algorithm bits and token copying are performed only if the service is processed on the Cryptographic Coprocessor Feature. See the *generated_key_identifier_1* parameter for more information on token copying.

Valid key type combinations depend on the key form. See Table 12 for valid key combinations.

key_length

Direction: Input	Type: Character string

An 8-byte value that defines the setting of each part of a double-length or triple-length key. The keyword must be left-justified and padded on the right with blanks. You must supply one of the key length values from Table 9 in the *key_length* parameter.

To generate a single-length key, specify *key_length* as SINGLE or KEYLN8.

Use SINGLE if you want to create a transport key that you would use to exchange DATA keys with a PCF system. Because PCF does not use double-length transport keys, specify SINGLE so that the effects of multiple encipherment are nullified.

| The SINGLE-R keyword (″single replicated″) specifies a double-length key
| where both halves of the key are identical. This key performs as though the key
| were single length.

Double-length (16-byte) keys have an 8-byte left half and an 8-byte right half. Both halves can have identical clear values or not. If you want the same value to be used in both key halves, specify *key_length* as SINGLE or KEYLN8. If you want different values to be the basis of each key half, specify *key_length* as DOUBLE or KEYLN16.

Triple-length (24-byte) keys have three 8-byte key parts. This key length is valid for DATA keys only. To generate a triple-length DATA key with three different values to be the basis of each key part, specify *key_length* as KEYLN24.

When generating an AKEK, the *key_length* parameter is ignored. The AKEK key length (8-byte or 16-byte) is determined by the skeleton token created by the key token build callable service and provided in the *generated_key_identifier_1* parameter.

Table 9. Key Length Values for the Key Generate Callable Service

Keyword	Meaning
SINGLE	Valid for all key types except DATAM and DATAMV. For 8-byte keys (DATAXLAT, MAC, and MACVER) this is the only valid value for the *key_length* parameter. For DATA keys, SINGLE generates a standard token containing a single-length key. For 16-byte keys (IMPORTER, EXPORTER, PINGEN, PINVER, IPINENC, OPINENC), SINGLE generates effective single-length for those key types. Therefore, each half of the 16-byte key has the same clear value. Note that the following restrictions exist when you specify SINGLE for 16-byte keys. • If you specify *key_length* as SINGLE and key_type_1 or *key_type_2* as any of the double-length keys (IMPORTER, EXPORTER, IPINENC, OPINENC, PINGEN and PINVER) and you specify the parameter *key_form* as IMEX, parameter *kek_key_identifier_1 must* contain a NOCV IMPORTER key-encrypting key, either as a key label or an internal key token. • If you specify SINGLE for any double-length keys, the CKDS must contain NOCV enablement keys.
| SINGLE-R	A double-length key with equal valued halves.
DOUBLE	A 16-byte key with independent 8-byte parts. Valid for IMPORTER, EXPORTER, PINGEN, PINVER, IPINENC, OPINENC, DATAM, and DATAMV key types. For DATA keys, DOUBLE generates a standard token containing two separate 8-byte DATA keys.
KEYLN8	Synonymous with SINGLE.

Table 9. Key Length Values for the Key Generate Callable Service (continued)

Keyword	Meaning
KEYLN16	Valid for all key types except DATAXLAT, MAC, and MACVER. Synonymous with DOUBLE.
KEYLN24	Valid for DATA key type only. Generates a standard token containing three separate 8-byte DATA keys.

key_type_1

Direction: Input Type: Character string

An 8-byte keyword from the list shown in Table 10 or the keyword TOKEN. Use the *key_type_1* parameter for the first, or only key, that you want generated. The keyword must be left-justified and padded with blanks. Valid type combinations depend on the key form.

If *key_type_1* is TOKEN, ICSF examines the control vector (CV) field in the *generated_key_identifier_1* parameter to derive the key type. The *generated_key_identifier_1* parameter must be a key token, not a key label. When *key_type_1* is TOKEN, ICSF does not check for the length of the key for DATA keys. Instead, ICSF uses the *key_length* parameter to determine the length of the key.

To generate an AKEK, specify a *key_type_1* of TOKEN. The *generated_key_identifier_1* parameter must be a skeleton token of an AKEK created by the key token build (CSNBKTB) callable service. The token cannot be a partially notarized AKEK or an AKEK key part.

See Table 11 and Table 12 for valid key type and key form combinations.

key_type_2

Direction: Input Type: Character string

An 8-byte keyword from the list shown in Table 10 or the word TOKEN. Use the *key_type_2* parameter for a key pair, which is shown in Table 12 on page 71. The keyword must be left-justified and padded with blanks. Valid type combinations depend on the key form.

If *key_type_2* is TOKEN, ICSF examines the control vector (CV) field in the *generated_key_identifier_2* parameter to derive the key type. When *key_type_2* is TOKEN, ICSF does not check for the length of the key for DATA keys. Instead, ICSF uses the *key_length* parameter to determine the length of the key.

If you want only one key to be generated, specify the *key_type_2* and *KEK_key_identifier_2* as binary zeros.

Table 10. Key Type Values for the Key Generate Callable Service

Key Type	Meaning
DATA	Data-encrypting key. Use this single-length, double-length, or triple-length key to encipher and decipher data.

Table 10. Key Type Values for the Key Generate Callable Service (continued)

Key Type	Meaning
DATAXLAT	Data translation key. Use this single-length key to reencipher text from one DATA key to another.
MAC	MAC generation key. Use this single-length key to generate a message authentication code.
MACVER	MAC verification key. Use this single-length key to verify a message authentication code.
DATAM	MAC generation key. May be specified explicitly as a key type or through the TOKEN keyword.
DATAMV	MAC verification key. May be specified explicitly as a key type or through the TOKEN keyword.
PINGEN	PIN generation key. Use this double-length key to generate PINs.
PINVER	PIN verification key. Use this double-length key to verify PINs.
IPINENC	Input PIN-encrypting key. Use this double-length input key to translate PINs. PIN blocks received from other nodes or automatic teller machine (ATM) terminals are encrypted under this type of key. These encrypted PIN blocks are the input to the Encrypted PIN translate and Encrypted PIN verify callable services.
OPINENC	Output PIN-encrypting key. Use this double-length output key to translate PINs. The output PIN blocks from the Encrypted PIN translate callable service is encrypted under this type of key.
EXPORTER	Exporter key-encrypting key. Use this double-length key to convert any key (including a DATA key) from operational form into exportable form.
IMPORTER	Importer key-encrypting key. Use this double-length key to convert a key from importable form into operational form.
DECIPHER	Used only to decrypt data.
ENCIPHER	Used only to encrypt data.
IKEYXLAT	Used to decrypt an input key in the Key Translate callable service.
OKEYXLAT	Used to encrypt an output key in the Key Translate callable service.
CIPHER	Used only to encrypt or decrypt data.
DATAC	Used to specify a DATA-class key that will perform in the Encipher and Decipher callable services, but not in the MAC Generate or MAC Verify callable services.
CVARDEC	The TSS Cryptographic variable decipher verb uses a CVARDEC key to decrypt plaintext by using the Cipher Block Chaining (CBC) method.
CVARENC	Cryptographic variable encipher service uses a CVARENC key to encrypt plaintext by using the Cipher Block Chaining (CBC) method.
CVARPINE	Used to encrypt a PIN value for decryption in a PIN-printing application.

Table 10. Key Type Values for the Key Generate Callable Service (continued)

Key Type	Meaning
CVARXCVL	Used to encrypt special control values in DES key management.
CVARXCVR	Used to encrypt special control values in DES key management.

See Table 11 on page 71 and Table 12 on page 71 for valid key type and key form combinations.

KEK_key_identifier_1

Direction: Input/Output Type: String

A 64-byte string of an internal key token containing the importer or exporter key-encrypting key, or a key label. If you supply a key label that is less than 64-bytes, it must be left-justified and padded with blanks. *KEK_key_identifier_1* is required for a *key_form* of IM, EX, IMEX, EXEX, or IMIM.

If the *key_form* is OP, OPEX, OPIM, or OPOP, the *KEK_key_identifier_1* is null.

If the NOCV bit is on in the internal key token containing the key-encrypting key, the key-encrypting key itself (not the key-encrypting key variant) is used to encipher the generated key. For example, the key has been installed in the cryptographic key data set through the key generator utility program or the key entry hardware using the NOCV parameter; or you are passing the key-encrypting key in the internal key token with the NOCV bit on and your program is running in supervisor state or key 0-7.

Control vectors are explained in "Control Vector" on page 5 and the NOCV bit is shown in Table 94 on page 385.

KEK_key_identifier_2

Direction: Input/Output Type: String

A 64-byte string of an internal key token containing the importer or exporter key-encrypting key, or a key label of an internal token. If you supply a key label that is less than 64-bytes, it must be left-justified and padded with blanks. *KEK_key_identifier_2* is required for a *key_form* of OPIM, OPEX, IMEX, IMIM, or EXEX. This field is ignored for *key_form* keywords OP, IM and EX.

For DATA and KEK (importer and exporter) types, the key generate service propagates the data encryption algorithm bits from the KEK you supply to the key it generates, unless overridden by token copying. In generating an IMPORTER or EXPORTER OP KEK, this service marks the key CDMF, DES, or SYS-ENC, corresponding to *kek_key_identifier_2*. In generating an OP DATA key, if the *kek_key_identifier_2* is SYS-ENC, this service marks the key according to the system default encryption algorithm. Otherwise, it marks the key CDMF or DES, corresponding to the *kek_key_identifier_2*. Propagation of token markings is only relevant when this service is processed on the Cryptographic Coprocessor Feature. For more information on token copying, see the *generated_key_identifier_1* parameter.

If the NOCV bit is on in the internal key token containing the key-encrypting key, the key-encrypting key itself (not the key-encrypting key variant) is used to encipher the generated key. For example, the key has been installed in the cryptographic key data set through the key generator utility program or the key entry hardware using the NOCV parameter; or you are passing the key-encrypting key in the internal key token with the NOCV bit on and your program is running in supervisor state or in key 0-7.

Control vectors are explained in “Control Vector” on page 5 and the NOCV bit is shown in Table 94 on page 385.

generated_key_identifier_1

Direction: Input/Output	Type: String

This parameter specifies either a generated:

- Internal key token for an operational key form, or
- External key token containing a key enciphered under the *kek_key_identifier_1* parameter.

If you specify a *key_type_1* of TOKEN, then this field contains a valid token of the key type you want to generate. See Table 10 on page 67 for a list of valid *key_type_1* key types.

If you specify a *key_type_1* of IMPORTER or EXPORTER and a *key_form* of OPEX, and if the *generated_key_identifier_1* parameter contains a valid internal token of the SAME type, the NOCV bit, if on, is propagated to the generated key token.

Note: Propagation of the NOCV bit is performed only if the service is processed on the Cryptographic Coprocessor Feature.

If you specify a *key_type_1* of DATA or IMPORTER, and a *key_form* of OP, and the *generated_key_identifier_1* parameter contains a valid internal token of the same type, the data encryption algorithm bits are copied to the generated key token. This overrides any markings on the *kek_key_identifier_2*. If you specify a *key_type_1* of DATA, IMPORTER, or EXPORTER and a *key_form* of OPIM or OPEX and the *generated_key_identifier_1* parameter contains a valid internal token of the same type, the data encryption algorithm bits are copied to the generated key token. This overrides any data encryption algorithm bit markings on the *kek_key_identifier_2*.

Note: Marking of data encryption algorithm bits and token copying are performed only if the service is processed on the Cryptographic Coprocessor Feature.

When generating an AKEK, specify the skeleton key token created by the key token build callable service (CSNBKTB) as input for this parameter.

generated_key_identifier_2

Direction: Input/Output	Type: String

This parameter specifies a generated external key token containing a key enciphered under the *kek_key_identifier_2* parameter.

If you specify a *key_type_2* of TOKEN, then this field contains a valid token of the key type you want to generate. See Table 10 on page 67 for a list of the valid *key_type_2* key types. The token can be an internal or external token.

Restriction

The caller must be in task mode, not in SRB mode.

Usage Notes

No external tokens that this service generates contain data encryption algorithm bit markings.

It is possible to generate an operational DES-marked DATA key on a CDMF-only system or a CDMF-marked DATA key on a DES-only system. However, the encipher (CSNBENC) and decipher (CSNBDEC) callable services fail when you use these keys on the systems where they were generated unless overridden by keyword.

Double-length MAC keys (DATAM and DATAMV) can be generated in the same key forms as single-length MAC keys.

Table 11 shows the valid key type and key form combinations for a single key. Key types marked with an "*" must be requested through the specification of a proper control vector in a key token and through the use of the TOKEN keyword.

Table 11. Key Generate Valid Key Types and Key Forms for a Single Key

Key Type 1	Key Type 2	OP	IM	EX
MAC	Not applicable	X	X	X
DATA	Not applicable	X	X	X
PINGEN	Not applicable	X	X	X
DATAC*	Not applicable	X	X	X
DATAM	Not applicable	X	X	X

Table 12 shows the valid key type and key form combinations for a key pair. Key types marked with an "*" must be requested through the specification of a proper control vector in a key token and through the use of the TOKEN keyword.

Table 12. Key Generate Valid Key Types and Key Forms for a Key Pair

Key Type 1	Key Type 2	OPEX	EXEX	OPIM, OPOP, IMIM	IMEX
DATA	DATA	X	X	X	X
MAC	MAC	X	X	X	X
MAC	MACVER	X	X	X	X
DATAC*	DATAC*	X	X	X	X
DATAM	DATAM	X	X	X	X
DATAM	DATAMV	X	X	X	X
CIPHER	CIPHER	X	X	X	X
CIPHER	DECIPHER	X	X	X	X
CIPHER	ENCIPHER	X	X	X	X

Table 12. Key Generate Valid Key Types and Key Forms for a Key Pair (continued)

Key Type 1	Key Type 2	OPEX	EXEX	OPIM, OPOP, IMIM	IMEX
DECIPHER	CIPHER	X	X	X	X
DECIPHER	ENCIPHER	X	X	X	X
ENCIPHER	CIPHER	X	X	X	X
ENCIPHER	DECIPHER	X	X	X	X
EXPORTER	IMPORTER	X	X		X
IMPORTER	EXPORTER	X	X		X
EXPORTER	IKEYXLAT	X	X		X
IKEYXLAT	EXPORTER	X	X		X
IKEYXLAT	OKEYXLAT	X	X		X
IMPORTER	OKEYXLAT	X	X		X
OKEYXLAT	IMPORTER	X	X		X
OKEYXLAT	IKEYXLAT	X	X		X
PINGEN	PINVER	X	X		X
PINVER	PINGEN	X	X		X
DATA	DATAXLAT	X	X		X
DATAXLAT	DATAXLAT	X	X		X
OPINENC	IPINENC	X	X	X	X
IPINENC	OPINENC	X	X	X	X
OPINENC	OPINENC			X	
CVARDEC*	CVARENC*	X			X
CVARENC*	CVARDEC*	X			X
CVARENC*	CVARXCVL*	X			X
CVARENC*	CVARXCVR*	X			X
CVARXCVL*	CVARENC*	X			X
CVARXCVR*	CVARENC*	X			X
CVARDEC*	CVARPINE*	X			X
CVARPINE*	CVARDEC*	X			X

Note: If the *key_form* is IMEX, the *key_length* is SINGLE, and *key_type_1* is IPINENC, OPINENC, PINGEN, IMPORTER, or EXPORTER, you must specify the *kek_key_identifier_1* parameter as NOCV IMPORTER.

To use NOCV key-encrypting keys, NOCV-enablement keys must be installed in the CKDS.

To generate DATAM and DATAMV keys in the importable form, the ANSI system keys must be installed in the CKDS.

Key Translate (CSNBKTR)

The Key Translate callable service uses one key-encrypting key to decipher an input key and then enciphers this key using another key-encrypting key within the secure environment.

ICSF routes the Key Translate request to a PCI Cryptographic Coprocessor for processing. If no PCI Cryptographic Coprocessor is online, the request fails.

Format

```
CALL CSNBKTR(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            input_key_token,
            input_KEK_key_identifier,
            output_KEK_key_identifier,
            output_key_token )
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

input_key_token

Direction: Input	Type: String

A 64-byte string variable containing an external key token. The external key token contains the key to be re-enciphered (translated).

input_KEK_key_identifier

Direction: Input/Output Type: String

A 64-byte string variable containing the internal key token or the key label of an internal key token record in the CKDS. The internal key token contains the key-encrypting key used to decipher the key. The internal key token must contain a control vector that specifies an importer or IKEYXLAT key type. The control vector for an importer key must have the XLATE bit set to 1.

output_KEK_key_identifier

Direction: Input/Output Type: String

A 64-byte string variable containing the internal key token or the key label of an internal key token record in the CKDS. The internal key token contains the key-encrypting key used to encipher the key. The internal key token must contain a control vector that specifies an exporter or OKEYXLAT key type. The control vector for an exporter key must have the XLATE bit set to 1.

output_key_token

Direction: Output Type: String

A 64-byte string variable containing an external key token. The external key token contains the re-enciphered key.

Restriction

The caller must be in task mode, not in SRB mode.

Usage Note

SAF will be invoked to check authorization to use the Key Translate service and any key labels specified as input.

Key Import (CSNBKIM)

Use the key import callable service to reencipher a key (except an AKEK) from encryption under an importer key-encrypting key to encryption under the master key. The reenciphered key is in operational form.

This service examines the data encryption algorithm bits on the operational KEK supplied. It propagates the DES, CDMF, or SYS-ENC markings on the KEK token to the imported KEK or DATA key token unless token copying overrides this. It propagates the SYS-ENC marking to the KEK and marks the DATA key according to the system's default encryption algorithm. Propagation of token markings is only relevant when this service is processed on the Cryptographic Coprocessor Feature. See the *target_key_identifier* and *importer_key_identifier* parameters for more information.

For DATA keys, this service generates a key of the same length as that contained in the input token.

| ICSF routes the Key Import request to a PCI Cryptographic Coprocessor if the
| control vector in a supplied internal token cannot be processed on the
| Cryptographic Coprocessor Feature, or if the key type is not valid for the
| Cryptographic Coprocessor Feature. If no PCI Cryptographic Coprocessor is online
| in this case, the request fails.

Format

```
CALL CSNBKIM(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            key_type,
            source_key_identifier,
            importer_key_identifier,
            target_key_identifier )
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

key_type

Direction: Input	Type: Character string

The type of key you want to reencipher under the master key. Specify an 8-byte keyword or the keyword TOKEN. The keyword must be left-justified and padded on the right with blanks. The key types you can specify are listed in Table 13.

To import a double-length MAC generation key, use a key type of DATAM or TOKEN. To import a double-length MAC verification key, use a key type of DATAMV or TOKEN.

For a double-length MAC key with a key type of DATAM, the source key identifier must specify an external token that uses the data compatibility control vector. For a double-length MAC key with a key type of MACD, the source key identifier must specify an external token that uses the single-length control vector for both the left and right half of the key (MAC ‖ MAC). For a table of control vectors, refer to “Appendix K. Control Vector Table” on page 413.

If the key type is TOKEN, ICSF determines the key type from the control vector (CV) field in the internal key token provided in the *source_key_identifier* parameter. If the control vector is invalid on the Cryptographic Coprocessor Feature, the key import request will be routed to the PCI Cryptographic Coprocessor.

Table 13. Key Type Values for the Key Import Callable Service

Key Type	Meaning
DATA	Data-encrypting key. Use this single-, double-, or triple-length key to encipher and decipher data.
DATAXLAT	Data translation key. Use this single-length key to reencipher text from one DATA key to another.
MAC	MAC generation key. Use this single-length key to generate a message authentication code.
MACVER	MAC verification key. Use this single-length key to verify a message authentication code.
DATAM	MAC generation key. Use this double-length key to generate a message authentication code.
DATAMV	MAC verification key. Use this double-length key to verify a message authentication code.
MACD	Double MAC generation key. Use this double-length key to generate and verify a message authentication code for the double-key MAC procedure. ICSF continues to support this key type for compatibility with ICSF Version 2 Release 1.
PINGEN	PIN generation key. Use this double-length key to generate PINs.
PINVER	PIN verification key. Use this double-length key to verify PINs.
IPINENC	Input PIN-encrypting key. Use this double-length input key to translate PINs. PIN blocks received from other nodes or automatic teller machine (ATM) terminals are encrypted under this type of key. These encrypted PIN blocks are the input to the Encrypted PIN translate and Encrypted PIN verify callable services.

| *Table 13. Key Type Values for the Key Import Callable Service (continued)*

Key Type	Meaning
OPINENC	Output PIN-encrypting key. Use this double-length output key to translate PINs. The output PIN blocks from the Encrypted PIN translate callable service are encrypted under this type of key.
EXPORTER	Exporter key-encrypting key. Use this double-length key to convert any key (including a DATA key) from operational form into exportable form.
IMPORTER	Importer key-encrypting key. Use this double-length key to convert a key from importable form into operational form.
IMP-PKA	Limited authority importer key. Use this double-length key to import an encrypted RSA or DSS private key.
AKEK	ANSI X9.17 key-encrypting key. A single- or double-length key that must be ANSI notarized and offset before use as a key-encrypting key. The default is double-length.
DECIPHER	Used only to decrypt data.
ENCIPHER	Used only to encrypt data.
IKEYXLAT	Used to decrypt an input key in the Key Translate callable service.
OKEYXLAT	Used to encrypt an output key in the Key Translate callable service.
CIPHER	Used only to encrypt or decrypt data.
DATAC	Used to specify a DATA-class key that will perform in the Encipher and Decipher callable services, but not in the MAC Generate or MAC Verify callable services.

| **source_key_identifier**

Direction: Input Type: String

The key you want to reencipher under the master key. The parameter is a 64-byte field for the enciphered key to be imported containing either an external key token or a null key token. If you specify a null token, the token is all binary zeros, except for a key in bytes 16-23 or 16-31, or in bytes 16-31 and 48-55 for triple-length DATA keys. Refer to Table 96 on page 388.

This service supports the no-export function in the CV.

importer_key_identifier

Direction: Input/Output Type: String

The importer key-encrypting key that the key is currently encrypted under. The parameter is a 64-byte area containing either the key label of the key in the cryptographic key data set or the internal key token for the key. If you supply a key label that is less than 64-bytes, it must be left-justified and padded with blanks.

Key Import (CSNBKIM)

This service examines data encryption algorithm bits on the operational KEK token supplied. It propagates DES or CDMF markings on the KEK token to the imported KEK or DATA key token unless token copying overrides this. For SYS-ENC marking, this service propagates the marking to the KEK or marks the DATA key according to the default system encryption algorithm, unless token copying overrides this.

Note: If you specify a NOCV importer in the *importer_key_identifier* parameter, the key to be imported must be enciphered under the importer key itself.

target_key_identifier

Direction: Input/Output Type: String

This parameter is the generated reenciphered key. The parameter is a 64-byte area that receives the internal key token for the imported key.

If the imported key TYPE is IMPORTER or EXPORTER and the token key TYPE is the same, the *target_key_identifier* parameter changes direction to both input and output. If the application passes a valid internal key token for an IMPORTER or EXPORTER key in this parameter, the NOCV bit is propagated to the imported key token.

Note: Propagation of the NOCV bit is performed only if the service is processed on Cryptographic Coprocessor Feature.

If the *key_type* is DATA, IMPORTER, or EXPORTER and the application passes a valid internal key token for a DATA, IMPORTER, or EXPORTER key in the *target_key_identifier,* this service propagates the data encryption algorithm bits to the imported key token. Any data encryption algorithm bits supplied on *importer_key_identifier* are ignored.

Note: Marking of data encryption algorithm bits and token copying are performed only if the service is processed on the Cryptographic Coprocessor Feature.

Usage Notes

For the key import callable service, choose one of the following options:

- Specify the *key_type* parameter as TOKEN and specify the external key token in the *source_key_identifier* parameter. The key type information is determined from the control vector in the external key token.
- Specify a key type in the *key_type* parameter and specify an external key token in the *source_key_identifier* parameter. The specified key type must be compatible with the control vector in the external key token.
- Specify a valid key type in the *key_type* parameter and a null key token in the *source_key_identifier* parameter. Use the control vector that maps to the specification of the *key_type* parameter.

The key import callable service cannot be used to import ANSI key-encrypting keys. For information on importing these types of keys, refer to "ANSI X9.17 Key Import (CSNAKIM)" on page 110.

If the key type is MACD or IMP-PKA, the control vectors of supplied internal tokens must all be supported by the Cryptographic Coprocessor Feature, since processing for these key types will not be routed to a PCI Cryptographic Coprocessor.

For Source key encrypted without CVs, the length of DATA keys is determined by non-zero enciphered key values.

To use NOCV key-encrypting keys or to import DATAM or DATAMV keys, NOCV-enablement keys must be installed in the CKDS.

| Key Import operations which specify a NOCV key-encrypting key as either the importer key or the target and also specify a source or key-encrypting key which contains a control vector not supported by the Cryptographic Coprocessor Feature will fail.

Note: To import a double-length MAC generation key encrypted under a NOCV KEK, use the DATAM key type value. To import a double-length MAC verification key encrypted under a NOCV KEK, use the DATAMV key type value. In either case, do not specify a key type value of TOKEN.

Key Part Import (CSNBKPI)

| Use the key part import callable service to combine the clear key parts of any key type and return the combined key value either in an internal token or as an update to the CKDS.

Before you use the key part import service for the first key part, you must use the key token build service to create the internal key token into which the key will be imported. Subsequent key parts are combined with the first part in internal token form or as a label from the CKDS.

Key parts are specified as FIRST, MIDDLE, or LAST in the *rule_array*. Only when the LAST part has been combined can the key token be used in any other service.

| The key part import callable service can also be used to import a key without using key parts. Call the key part import service FIRST with key part value X'0000...' then call the key part import service LAST with the complete value.

Keys created via this service have odd parity. The FIRST key part is adjusted to odd parity. All subsequent key parts are adjusted to even parity before being combined.

Format

```
CALL CSNBKPI(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            key_part,
            key_identifier)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input Type: Integer

The number of keywords you supplied in the *rule_array* parameter. The value must be 1.

rule_array

Direction: Input Type: String

The keyword that provides control information to the callable service. The keywords must be 8 bytes of contiguous storage with the keyword left-justified in its 8-byte location and padded on the right with blanks.

Table 14. Keywords for Key Part Import Control Information

Keyword	Meaning
Key Part (Required)	
FIRST	This keyword specifies that an initial key part is being entered.
MIDDLE	This keyword specifies that an intermediate key part, which is neither the first key part nor the last key part, is being entered.
LAST	This keyword specifies that the last key part is being entered.

key_part

Direction: Input Type: String

A 16-byte field containing the clear key part to be entered. If the key is a single-length key, the key part must be left-justified and padded on the right with zeros.

key_identifier

Direction: Input/Output	Type: String

A 64-byte field containing an internal token or a label of an existing CKDS record. If *rule_array* is FIRST, this field is the skeleton of an internal token of a single- or double-length key with the KEY-PART marking. If *rule_array* is MIDDLE or LAST, this is an internal token or the label of a CKDS record of a partially combined key. Depending on the input format, the accumulated partial or complete key is returned as an internal token or as an updated CKDS record.

Restriction

The caller must be in task mode and must not be in cross memory mode. If a label is specified on *key_identifier*, the label must be unique. If more than one record is found, the service fails.

Usage Note

This service requires that the ANSI system keys be installed on the CKDS.

Related Information

This service is consistent with the Transaction Security System key part import verb.

Secure Key Import (CSNBSKI)

Use the secure key import callable service to encipher a single- or double-length clear key under the system master key or under an importer key-encrypting key. The clear key can then be imported as any of the possible key types. This service does not adjust key parity.

The callable service can execute only when ICSF is in special secure mode, which is described in "Special Secure Mode" on page 9.

You can import DATA keys or KEKs whose data encryption algorithm bits indicate the encryption algorithm. DATA keys can be marked CDMF or DES. This service marks the imported DATA key token according to the system's default encryption algorithm, unless token copying overrides this. KEKs can be marked CDMF DES, or SYS-ENC. They are marked SYS-ENC unless token-copying overrides this. See the *key_identifier* parameter in this service and the key token build callable service ("Key Token Build (CSNBKTB)" on page 203) for more information.

Note: Marking of data encryption algorithm bits and token copying are performed only if the service is processed on the Cryptographic Coprocessor Feature.

To import double-length and triple-length DATA keys, or double-length MAC or MACVER keys, use the multiple secure key import (CSNBSKM) callable service. See "Multiple Secure Key Import (CSNBSKM)" on page 84.

Secure Key Import (CSNBSKI)

| ICSF routes the Secure Key Import request to a PCI Cryptographic Coprocessor if
| the control vector cannot be processed on the Cryptographic Coprocessor Feature.
| If no PCI Cryptographic Coprocessor is online in this case, the request fails.

Format

```
CALL CSNBSKI(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            clear_key,
            key_type,
            key_form,
            importer_key_identifier,
            key_identifier )
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

clear_key

Direction: Input	Type: String

The clear key to be enciphered. Specify a 16-byte string (clear key value). For single-length keys, the value must be left-justified and padded with zeros. For effective single-length keys, the value of the right half must equal the value of the left half. For double-length keys, specify the left and right key values.

key_type

Direction: Input Type: Character string

| The type of key you want to encipher under the master key or an importer key.
| Specify an 8-byte field that must contain a keyword from the list shown in
| Table 15 or the keyword TOKEN. If the key type is TOKEN, ICSF determines
| the key type from the CV in the *key_identifer* parameter. If the control vector is
| invalid on the Cryptographic Coprocessor Feature, the secure key import
| request will be routed to the PCI Cryptographic Coprocessor.

Table 15. Key Type Values for the Secure Key Import Callable Service

Key Type	Meaning
DATA	Data-encrypting key. Use this single-length key to encipher and decipher data.
DATAXLAT	Data translation key. Use this single-length key to reencipher text from one DATA key to another.
MAC	MAC generation key. Use this single-length key to generate a message authentication code.
MACVER	MAC verification key. Use this single-length key to verify a message authentication code.
PINGEN	PIN generation key. Use this double-length key to generate PINs.
PINVER	PIN verification key. Use this double-length key to verify PINs.
IPINENC	Input PIN-encrypting key. Use this double-length input key to translate PINs. PIN blocks received from other nodes or automatic teller machine (ATM) terminals are encrypted under this type of key. These encrypted PIN blocks are the input to the Encrypted PIN translate and Encrypted PIN verify callable services.
OPINENC	Output PIN-encrypting key. Use this double-length output key to translate PINs. The output PIN blocks from the Encrypted PIN translate callable service are encrypted under this type of key.
EXPORTER	Exporter key-encrypting key. Use this double-length key to convert any key (including a DATA key) from operational form into exportable form.
IMPORTER	Importer key-encrypting key. Use this double-length key to convert a key from importable form into operational form.
IMP-PKA	Limited authority importer key. Use this double-length key to import an encrypted RSA or DSS private key.

key_form

Direction: Input Type: Character string

The key form you want to generate. Enter a 4-byte keyword specifying whether the key should be enciphered under the master key (OP) or the importer key-encrypting key (IM). The keyword must be left-justified and padded with blanks. Valid keyword values are OP for encryption under the master key or IM for encryption under the importer key-encrypting key. If you specify IM, you must specify an importer key-encrypting key in the *importer_key_identifier* parameter. For a *key_type* of IMP-PKA, this service supports only the OP *key_form*.

importer_key_identifier

Direction: Input/Output	Type: String

The importer key-encrypting key under which you want to encrypt the clear key. Specify either a 64-byte string of the internal key format or a key label. If you specify IM for the *key_form* parameter, the *importer_key_identifier* parameter is required.

key_identifier

Direction: Input/Output	Type: String

The generated encrypted key. The parameter is a 64-byte string. The callable service returns either an internal key token if you encrypted the clear key under the master key (*key_form* was OP); or an external key token if you encrypted the clear key under the importer key-encrypting key (*key_form* was IM).

If the imported key_type is IMPORTER or EXPORTER and the key_form is OP, the *key_identifier* parameter changes direction to both input and output. If the application passes a valid internal key token for an IMPORTER or EXPORTER key in this parameter, the NOCV bit is propagated to the imported key token.

Note: Propagation of the NOCV bit is performed only if the service is processed on the Cryptographic Coprocessor Feature.

If the *key_type* is DATA, IMPORTER, or EXPORTER and the application passes a valid internal key token for a DATA, IMPORTER, or EXPORTER key in the *key_identifier,* this service propagates the data encryption algorithm bits to the imported key token. Propagation of token markings is only relevant when this service is processed on the Cryptographic Coprocessor Feature.

The secure key import service does not adjust key parity.

Multiple Secure Key Import (CSNBSKM)

Use this service to encipher a single-, double-, or triple-length key under the system master key or an importer key-encrypting key. The clear key can then be imported as any of the possible key types.

For double-length MAC keys, the importable form of the key token uses the MAC data compatibility control vector.

Only control vectors and key types supported by the Cryptographic Coprocessor Feature will be valid when importing a triple-length key.

ICSF routes the Multiple Secure Key Import request to a PCI Cryptographic Coprocessor if the control vector of a supplied internal token cannot be processed

| on the Cryptographic Coprocessor Feature, or if the key type is not valid for the
| Cryptographic Coprocessor Feature. If no PCI Cryptographic Coprocessor is online
| in this case, the request fails.

Format

```
CALL CSNBSKM(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            clear_key_length,
            clear_key,
            key_type,
            key_form,
            key_encrypting_key_identifier,
            imported_key_identifier_length,
            imported_key_identifier )
```

Parameters

return_code

Direction: Output   Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output   Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output   Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output   Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input   Type: Integer

The number of keywords you are supplying in the *rule_array* parameter. The *rule_array_count* parameter must be 0, 1, or 2.

rule_array

Direction: Input Type: String

Zero to two keywords that supply control information to the callable service. Each keyword must be in 8 bytes of contiguous storage, left-justified and padded on the right with blanks. The keywords are shown in Table 16.

The first keyword is the algorithm. If no algorithm is specified, the system default algorithm is used. If no algorithm is specified on a CDMF only system and either a double- or triple-length DATA key is specified, the token is marked DES. The algorithm keyword applies only when the desired output token is of key form OP and key type IMPORTER, EXPORTER, or DATA. For key form IM or any other key type, specifying DES or CDMF causes an error.

The second keyword is optional and specifies that the output key token be marked as an NOCV-KEK.

Table 16. Keywords for Multiple Secure Key Import Rule Array Control Information

Keyword	Meaning
Algorithm (optional)	
DES	The output key identifier is to be a DES token.
CDMF	The output key identifier is to be a CDMF token. For a DATA key of length 16 or 24, you may not specify CDMF.
NOCV Choice (optional)	
NOCV-KEK	The output token is to be marked as an NOCV-KEK. This keyword only applies if key form is OP and key type is IMPORTER, EXPORTER or IMP-PKA. For key form IM or any other key type, specifying NOCV-KEK causes an error.

clear_key_length

Direction: Input Type: Integer

The *clear_key_length* specifies the length of the clear key value to import. The length must be 8, 16, or 24, but cannot exceed the maximum length for the specified key type.

clear_key

Direction: Input Type: String

The *clear_key* specifies the clear key value to import.

key_type

Direction: Input Type: 8 Character String

| The type of key you want to encipher under the master key or an importer key.
| Specify an 8-byte field that must contain a keyword from the list shown in

| Table 17 or the keyword TOKEN. For types with fewer than 8 characters, the
| type should be padded on the right with blanks. If the key type is TOKEN, ICSF
| determines the key type from the control vector (CV) field in the internal key
| token provided in the *imported_key_identifier* parameter. If the control vector is
| invalid on the Cryptographic Coprocessor Feature, the multiple secure key
| import request will be routed to the PCI Cryptographic Coprocessor.

Table 17. Key Type Values for the Multiple Secure Key Import Callable Service

Key Type	Meaning
DATA	Data-encrypting key. Use this single-length key to encipher and decipher data.
DATAXLAT	Data translation key. Use this single-length key to reencipher text from one DATA key to another.
MAC	MAC generation key. Use this single-length key to generate or verify a message authentication code.
MACVER	MAC verification key. Use this single-length key to verify a message authentication code.
DATAM	MAC generation key. Use this double-length key to generate a message authentication code.
DATAMV	MAC verification key. Use this double-length key to verify a message authentication code.
PINGEN	PIN generation key. Use this double-length key to generate PINs.
PINVER	PIN verification key. Use this double-length key to verify PINs.
IPINENC	Input PIN-encrypting key. Use this double-length input key to translate PINs. PIN blocks received from other nodes or automatic teller machine (ATM) terminals are encrypted under this type of key. These encrypted PIN blocks are the input to the Encrypted PIN translate and Encrypted PIN verify callable services.
OPINENC	Output PIN-encrypting key. Use this double-length output key to translate PINs. The output PIN blocks from the Encrypted PIN translate callable service are encrypted under this type of key.
EXPORTER	Exporter key-encrypting key. Use this double-length key to convert any key (including a DATA key) from operational form into exportable form.
IMPORTER	Importer key-encrypting key. Use this double-length key to convert a key from importable form into operational form.
IMP-PKA	Limited authority importer key. Use this double-length key to import an encrypted RSA or DSS private key.

key_form

Direction: Input Type: 4 Character String

The key form you want to generate. Enter a 4-byte keyword specifying whether the key should be enciphered under the master key (OP) or the importer key-encrypting key (IM). The keyword must be left-justified and padded with blanks. Valid keyword values are OP for encryption under the master key or IM for encryption under the importer key-encrypting key. If you specify IM, you must specify an importer key-encrypting key in the *importer_key_identifier* parameter. For a *key_type* of IMP-PKA, this service supports only the OP *key_form*.

key_encrypting_key_identifier

Direction: Input/Output	Type: String

A 64-byte string internal key token or key label of an importer key-encrypting key.

imported_key_identifier_length

Direction: Input/Output	Type: Integer

The byte length of the *imported_key_identifier* parameter. This must be at least 64 bytes.

imported_key_identifier

Direction: Output	Type: String

A 64-byte string that is to receive the output key token. If OP is specified in the *key_form* parameter, the service returns an internal key token. If IM is specified in the *key_form* parameter, the service returns an external key token. “Appendix H. Key Token Formats” on page 385 describes the key tokens.

Note that for a DATA key of length 16 or 24, no reference will be made to the data encryption algorithm bits or to the system's default algorithm; the token will be marked DES.

Usage Notes

To generate double-length MAC and MACVER keys in the importable form, the ANSI system keys must be installed in the CKDS.

| If the key to be imported is a triple-length key, only control vectors supported by the
| Cryptographic Coprocessor Feature are valid.

Key Test (CSNBKYT and CSNBKYTX)

Use the key test callable service to generate or verify a secure, cryptographic verification pattern for keys. The key to test can be in the clear or encrypted under the master key. The key test extended callable service also supports keys encrypted under a key-encrypting key (KEK). Keywords in the rule array specify whether the callable service generates or verifies a verification pattern.

When the service generates a verification pattern, it creates and cryptographically processes a random number. The service returns the random number with the verification pattern.

When the service tests a verification pattern against a key, you must supply the random number and the verification pattern from a previous call to key test or key test extended. The service returns the verification result in the return and reason codes.

CSNBKYT is consistent with the Transaction Security System verb of the same name. If you generate a key on the Transaction Security System, you can verify it on ICSF and vice versa.

| The key test callable service does not support triple-length DATA keys. CSNBKYT will be routed to a PCI Cryptographic Coprocessor for processing if ANSI enablement keys are not installed in the CKDS. CSNBKYTX is processed on the Cryptographic Coprocessor Feature. ENC-ZERO requests are routed to the PCI Cryptographic Coprocessor.

Format

```
CALL CSNBKYT(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             rule_array_count,
             rule_array,
             key_identifier,
             random_number,
             verification_pattern)
```

```
CALL CSNBKYTX(
              return_code,
              reason_code,
              exit_data_length,
              exit_data,
              rule_array_count,
              rule_array,
              key_identifier,
              random_number,
              verification_pattern,
              kek_key_identifier)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you supplied in the *rule_array* parameter. The value can be 2 or 3.

rule_array

Direction: Input	Type: String

Two or three keywords that provide control information to the callable service. Table 18 lists the keywords. The keywords must be in 16 or 24 bytes of contiguous storage with each of the keywords left-justified in its own 8-byte location and padded on the right with blanks.

Table 18. Keywords for Key Test and Key Test Extended Control Information

Keyword	Meaning
Key Rule (required)	
KEY-CLR	Specifies the key supplied in *key_identifier* is a single-length clear key.
KEY-CLRD	Specifies the key supplied in *key_identifier* is a double-length clear key.
KEY-ENC	Specifies the key supplied in *key_identifier* is a single-length encrypted key.
KEY-ENCD	Specifies the key supplied in *key_identifier* is a double-length encrypted key.
Process Rule (required)	
GENERATE	Generate a verification pattern for the key supplied in *key_identifier*.
VERIFY	Verify a verification pattern for the key supplied in *key_identifier*.
Parity Adjustment (optional)	
ADJUST	Adjust the parity of test key to odd before generating or verifying the verification pattern. The *key_identifier* field itself is not adjusted.
NOADJUST	Do not adjust the parity of test key to odd before generating or verifying the verification pattern. This is the default.
Verification Process Rule (optional)	

Table 18. Keywords for Key Test and Key Test Extended Control Information (continued)

Keyword	Meaning
ENC-ZERO	Specifies use of the ″encrypted zeros″ method. Use only with KEY-CLR, KEY-CLRD, KEY-ENC, or KEY-ENCD keywords.

key_identifier

Direction: Input/Output Type: String

The key for which to generate or verify the verification pattern. The parameter is a 64-byte string of an internal token, key label, or a clear key value left-justified. In the CSNBKYTX service, this parameter can also be an external token.

Note: If you supply a key label for this parameter, it must be unique on the CKDS.

random_number

Direction: Input/Output Type: String

This is an 8-byte field that contains a random number supplied as input for the test pattern verification process and returned as output with the test pattern generation process.

verification_pattern

Direction: Input/Output Type: String

This is an 8-byte field that contains a verification pattern supplied as input for the test pattern verification process and returned as output with the test pattern generation process.

kek_key_identifier

Direction: Input/Output Type: String

This parameter is for the CSNBKYTX service only. If *key_identifier* is an external token, then this is a 64-byte string of an internal token or a key label of an IMPORTER or EXPORTER used to encrypt the test key.

Note: If you supply a key label for this parameter, it must be unique on the CKDS.

Usage Notes

You can generate the verification pattern for a key when you generate the key. You can distribute the pattern with the key and it can be verified at the receiving node. In this way, users can ensure using the same key at the sending and receiving locations. You can generate and verify keys of any combination of key forms, that is, clear, operational or external.

In the Transaction Security System, KEY-ENC and KEY-ENCD both support enciphered single-length and double-length keys. They use the key-form bits in byte 5 of CV to determine the length of the key. To be consistent, in ICSF, both

KEY-ENC and KEY-ENCD handle single- and double-length keys. Both products effectively ignore the keywords, which are supplied only for compatibility reasons.

Key Record Create (CSNBKRC)

Use the key record create callable service to add a key record to the CKDS. The record contains a key token set to binary zeros and is identified by the label passed in the *key_label* parameter. This service updates both the DASD copy of the CKDS currently in use by ICSF and the in-storage copy of the CKDS.

Format

```
CALL CSNBKRC(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            key_label)
```

Parameters

return_code

Direction: Output　　　　Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output　　　　Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output　　　　Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output　　　　Type: String

The data that is passed to the installation exit.

key_label

Direction: Input　　　　Type: Character string

The 64-byte label of a record in the CKDS that is the target of this service. The created record contains a key token set to binary zeros and has a key type of NULL.

Restrictions

The caller must be in task mode and must not be in cross memory mode. The record must have a unique label. Therefore, there cannot be another record in the CKDS with the same label and a different key type.

Usage Notes

The key record create callable service checks the syntax of the label provided in the *key_label* parameter to ensure that it follows the KGUP rules. To bypass label syntax checking, use a preprocessing exit to turn on the bypass parse bit in the Exit Parameter Control Block (EXPB). For more information about preprocessing exits and the EXPB, refer to the *OS/390 ICSF System Programmer's Guide*.

You must use either the key record create callable service or KGUP to create an initial record in the CKDS before you can use the key record write service to update the record with a valid key token. Your applications perform better if you use KGUP to create the initial records and REFRESH the entire in-storage copy of the CKDS, rather than using key record create to create the initial NULL key entries. This is particularly true if you are creating a large number of key records. Key record create adds a record to a portion of the CKDS that is searched sequentially during key retrieval. Using KGUP followed by a REFRESH puts the null key records in the portion of the CKDS that is ordered in key-label/type sequence. A binary search of the key-label/type sequenced part of the CKDS is more efficient than searching the sequentially ordered section.

Key Record Delete (CSNBKRD)

Use the key record delete callable service to delete a key record from both the DASD copy of the CKDS and the in-storage copy.

Format

```
CALL CSNBKRD(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             rule_array_count,
             rule_array,
             key_label)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input	Type: Integer

The number of keywords supplied in the rule_array parameter. This number must always be 1.

rule_array

Direction: Input	Type: Character string

The 8 byte keyword that defines the action to be performed. The keyword must be LABEL-DL.

key_label

Direction: Input	Type: Character string

The 64-byte label of a record in the CKDS that is the target of this service. The record pointed to by this label is deleted.

Restrictions

The caller must be in task mode and must not be in cross memory mode. The record defined by the *key_label* must be unique. If more than one record per label is found, the service fails.

Key Record Read (CSNBKRR)

Use the key record read callable service to copy an internal key token from the in-storage CKDS to application storage. Other cryptographic services can then use the copied key token directly. The key token can also be used as input to the token copying functions of key generate, key import, or secure key import services to create additional NOCV keys.

Format

```
CALL CSNBKRR(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            key_label,
            key_token)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it indicating specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

key_label

Direction: Input	Type: Character string

The 64-byte label of a record in the in-storage CKDS. The internal key token in this record is returned to the caller.

key_token

Direction: Output   Type: String

The 64-byte internal key token retrieved from the in-storage CKDS.

Restrictions

The record defined by the *key_label* parameter must be unique and must already exist in the CKDS.

Key Record Write (CSNBKRW)

| Use the key record write callable service to write an internal key token to the CKDS record specified by the *key_label* parameter. This service supports writing a record to the CKDS which contains a key token with a control vector which is not supported by the Cryptographic Coprocessor Feature. These records will be written to the CKDS with a key type of CV, unless the key is an IMPORTER, EXPORTER, PINGEN, PINVER, IPINENC, or OPINENC type. These key types will be preserved in the CKDS record, even if the control vector is not supported by the Cryptographic Coprocessor Feature. This service updates both the DASD copy of the CKDS currently in use by ICSF and the in-storage copy. The record you are updating must be unique and must already exist in both the DASD and in-storage copies of the CKDS.

Format

```
CALL CSNBKRW(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            key_token,
            key_label)
```

Parameters

return_code

Direction: Output   Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output   Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output Type: String

The data that is passed to the installation exit.

key_token

Direction: Input/output Type: String

The 64-byte internal key token that is written to the CKDS.

key_label

Direction: Input Type: Character string

The 64-byte label of a record in the CKDS that is the target of this service. The record is updated with the internal key token supplied in the *key_token* parameter.

Restrictions

The caller must be in task mode and must not be in cross memory mode. The record defined by the *key_label* parameter must be unique and must already exist in the CKDS.

Related Information

You can use this service with the key record create callable service to write an initial record to key storage. Use it following the key import and key generate callable services to write an operational key imported or generated by these services directly to the CKDS.

Transform CDMF Key (CSNBTCK)

Use the transform CDMF key callable service to change a CDMF DATA key in an internal or external token to a transformed shortened DES key. You can also use the key label of a CKDS record as input. This callable service is implemented on S/390 G3, or higher, Enterprise Servers and S/390 Multiprise Servers. The Cryptographic Coprocessor Feature on S/390 G3, or higher, Enterprise Servers and S/390 Multiprise Servers is configured as either CDMF or DES-CDMF. This callable service ignores the input internal DATA token markings, and it marks the output internal token for use in the DES.

If the input DATA key is in an external token, the operational KEK must be marked as DES or SYS-ENC. The service fails for an external DATA key encrypted under a KEK that is marked as CDMF.

Transform CDMF Key (CSNBTCK)

Format

```
CALL CSNBTCK(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            source_key_identifier,
            kek_key_identifier,
            target_key_identifier )
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you are supplying in the *rule_array* parameter. This number must be 0.

rule_array

Direction: Input	Type: String

Currently no *rule_array* keywords are defined for this service, but you still must specify this parameter.

source_key_identifier

Direction: Input/Output	Type: String

A 64-byte string of the internal token, external token or key label that contains the DATA key to transform. Token markings on this key token are ignored.

kek_key_identifier

Direction: Input/Output	Type: String

A 64-byte string of the internal token or a key label of a key encrypting key under which the *source_key_identifier* is encrypted.

Note: If you supply a label for this parameter, the label must be unique in the CKDS.

target_key_identifier

Direction: Output	Type: String

A 64-byte string where the internal token or external token of the transformed shortened DES key is returned. The internal token is marked as DES.

Restrictions

This service is available on S/390 G3, or higher, Enterprise Servers and S/390 Multiprise Servers with Cryptographic Coprocessor Features. These systems may be configured as either CDMF or DES-CDMF.

Usage Notes

This service transforms a CDMF DATA key to a transformed shortened DES DATA key to allow interoperability to a DES-only capable system. The algorithm is described in Appendix E. Transform CDMF Key Algorithm.

User Derived Key (CSFUDK)

Use the user derived key callable service to generate a single-length or double-length MAC key or to update an existing user derived key. A single-length MAC key can be used to compute a MAC following the ANSI X9.9, ANSI X9.19, or the Europay, MasterCard and VISA (EMV) Specification MAC processing rules. A double-length MAC key can be used to compute a MAC following either the ANSI X9.19 optional double MAC processing rule or the EMV Specification MAC processing rule.

This service updates an existing user derived key by XORing it with data you supply in the *data_array* parameter. This is called SESSION MAC key generation by VISA.

This service adjusts the user derived key or SESSION MAC key to odd parity. The parity of the supplied derivation key is not tested.

Format

```
CALL CSFUDK(
          return_code,
          reason_code,
          exit_data_length,
          exit_data,
          key_type,
          rule_array_count,
          rule_array,
          derivation_key_identifier,
          source_key_identifier,
          data_array,
          generated_key_identifier)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

key_type

Direction: Input	Type: String

The 8-byte keyword of ’MAC ’ or ’MACD ’ that specifies the key type to be generated. The keyword must be left-justified and padded on the right with blanks. MAC specifies an 8-byte, single-length MAC key which is used in the ANSI X9.9-1 or the ANSI X9.19 basic MAC processing rules. MACD specifies a 16-byte, double-length internal MAC key that uses the single-length control vector for both the left and right half of the key (MAC ‖ MAC). The double-length MAC key is used in the ANSI X9.19 optional double-key MAC processing rules. The keyword ’TOKEN ’ is also accepted. If you specify TOKEN with a *rule_array* of VISA or NOFORMAT, the key type is determined by the valid internal token of the single-length or double-length MAC key in the *generated_key_identifier* parameter. If you specify TOKEN with a *rule_array* of SESS-MAC, the key type is determined by the valid internal token of the single-length or double-length MAC key in the *source_key_identifier.*

rule_array_count

Direction: Input Type: Integer

The number of keywords specified in the *rule_array* parameter. The value must be 1.

rule_array

Direction: Input Type: Character string

The process rule for the user derived key in an 8-byte field. The keywords must be in 8 bytes of contiguous storage, left-justified and padded on the right with blanks. For example,

```
'VISA    '
```

The keywords are shown in Table 19.

Table 19. Keywords for User Derived Key Control Information

Keyword	Meaning
User Derived Key Process Rules (required)	
VISA	For generating a user derived key using the VISA algorithm to format the data array input before encryption under the *derivation_key_identifier*. For guidance information refer to the VISA Integrated Circuit Card Specification, V1.3 Aug 31, 1996.
NOFORMAT	For generating a user derived key with no formatting done on the array before encryption under the *derivation_key_identifier.*
SESS-MAC	To update an existing user derived key supplied in the *source_key_ identifier* parameter with data provided in the *data_array* parameter.

derivation_key_identifier

Direction: Input/Output Type: String

For a *rule_array* value of VISA or NOFORMAT, this is a 64-byte key label or internal key token of the derivation key used to generate the user derived key. The key must be an EXPORTER key type. For any other keyword, this field must be a null token.

source_key_identifier

Direction: Input/Output Type: String

For a *rule_array* value of SESS-MAC, this is a 64-byte internal token of a single-length or double-length MAC key. For any other keyword, this field must be a null token.

data_array

Direction: Input	Type: String

Two 16-byte data elements required by the corresponding *rule_array* and *key_type* parameters. The data array consists of two 16-byte hexadecimal character fields whose specification depends on the process rule and key type. VISA requires only one 16-byte hexadecimal character input. Both NOFORMAT and SESS-MAC require one 16-byte input for a key type of MAC and two 16-byte inputs for a key type of MACD. If only one 16-byte field is required, then the rest of the data array is ignored by the callable service.

generated_key_identifier

Direction: Input/Output	Type: String

The 64-byte internal token of the generated single-length or double-length MAC key. This is an input field only if TOKEN is specified for *key_type*.

Usage Note

This service requires that the ANSI system keys be installed in the CKDS.

Chapter 5. Managing Keys According to the ANSI X9.17 Standard

This chapter describes the callable services that support the ANSI X9.17 key management standard:

- "ANSI X9.17 EDC Generate (CSNAEGN)"
- "ANSI X9.17 Key Export (CSNAKEX)" on page 105
- "ANSI X9.17 Key Import (CSNAKIM)" on page 110
- "Key Part Import (CSNBKPI)" on page 79
- "ANSI X9.17 Key Translate (CSNAKTR)" on page 114
- "ANSI X9.17 Transport Key Partial Notarize (CSNATKN)" on page 119

The following callable services, that are described in other sections of this book, also support the ANSI X9.17 key management standard:

- "Key Generate (CSNBKGN)" on page 63
- "Key Token Build (CSNBKTB)" on page 203

ANSI X9.17 EDC Generate (CSNAEGN)

Use the ANSI X9.17 EDC generate callable service to generate an error detection code (EDC) on a text string. The service calculates the EDC by by using a key value of X'0123456789ABCDEF' to generate a MAC on the specified text string, as defined by the ANSI X9.17 standard.

Format

```
CALL CSNAEGN(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             rule_array_count,
             rule_array,
             text_length,
             text,
             chaining_vector,
             EDC)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that are assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you supplied in the *rule_array* parameter. The value must be 0.

rule_array

Direction: Input	Type: String

Keywords that provide control information to the callable service. Currently there are no keywords that are defined for this variable, but you must declare the variable. To do so, declare an area of blanks of any length.

text_length

Direction: Input	Type: Integer

The length of the user-supplied *text* parameter for which the service should calculate the EDC.

text

Direction: Input	Type: String

The application-supplied text field for which the service is to generate the EDC.

chaining_vector

Direction: Input/Output	Type: String

An 18-byte string that ICSF uses as a system work area. The chaining vector permits data to be chained from one call to another. ICSF ignores the information in this field, but you must declare an 18-byte string.

EDC

Direction: Output	Type: String

A 9-byte field where the callable service returns the EDC generated as two groups of four ASCII-encoded hexadecimal characters that are separated by an ASCII space character.

Usage Notes

The ANSI X9.17 standard states that for EDC, before the service generates the MAC the caller must first edit the input text according to section 4.3 of ANSI X9.9-1982. It is the caller's responsibility to do the editing before calling the ANSI X9.17 EDC generate service. If the supplied text is not a multiple of 8, the service pads the text with X'00' up to a multiple of 8, as specified in ANSI X9.9-1.

To use this service you must have the ANSI system keys installed in the CKDS.

ANSI X9.17 Key Export (CSNAKEX)

Use the ANSI X9.17 key export callable service to export a DATA key or a pair of DATA keys, along with an ANSI key-encrypting key (AKEK), using the ANSI X9.17 protocol. This service converts a single DATA key, or combines two DATA keys, into a single MAC key. You can use the MAC key in either, or both, the MAC generation, or MAC verification service to authenticate the service message. In addition, this service also supports the export of a CCA IMPORTER or EXPORTER KEK.

If you export only DATA keys, the DATA keys are exported encrypted under the specified transport AKEK. You have the option of applying the ANSI X9.17 key offset or key notarization process to the transport AKEK.

If you export both DATA keys and an AKEK, the DATA keys are exported encrypted under the key-encrypting key that is also being exported. The AKEK is exported encrypted under the specified transport AKEK. You have the option of applying the ANSI X9.17 key offset or key notarization process to the transport AKEK. The ANSI X9.17 key offset process is applied to the source AKEK. Use the CKT keyword to specify whether to use an offset of 0 or 1. Use an offset of 0 when sending the DATA key to a key translation center along with a transport AKEK.

Note: You must create the cryptographic service message and maintain the offset counter value that is associated with the AKEK.

Format

```
CALL CSNAKEX(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            origin_identifier,
            destination_identifier,
            source_data_key_1_identifier,
            source_data_key_2_identifier,
            source_key_encrypting_key_identifier,
            transport_key_identifier,
            outbound_KEK_count,
            target_data_key_1,
            target_data_key_2,
            target_key_encrypting_key,
            MAC_key_token)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicates specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you supplied in the *rule_array* parameter. The value can be 0 to 4. If you specify 0, the callable service does not perform either notarization or offset.

rule_array

Direction: Input	Type: String

Zero to four keywords that provide control information to the callable service. See the list of keywords in Table 20. The keywords must be in 8 to 32 bytes of contiguous storage. Left-justify each keyword in its own 8-byte location and pad on the right with blanks. You must specify this parameter even if you specify no keyword.

Table 20. Keywords for ANSI X9.17 Key Export Rule Array

Keyword	Meaning
Notarization and Offset Rule (optional with no defaults)	
NOTARIZE	Perform notarization processing using the values obtained from the *origin_identifier*, *destination_identifier*, and *outbound_KEK_count* parameters.
OFFSET	Perform ANSI X9.17 key offset processing using the origin counter value obtained from the *outbound_KEK_count* parameter.
CPLT-NOT	Complete ANSI X9.17 notarization using the value obtained from the *outbound_KEK_count* parameter. The transport key that the *transport_key_identifier* specifies must be partially notarized.
Parity Rule (optional)	
ENFORCE	Stop processing if any source keys do not have odd parity. This is the default value.
IGNORE	Ignore the parity of the source key.
Source Key Rule (optional)	
1-KD	Export one DATA key. This is the default parameter.
2-KD	Export two DATA keys.
1-KD+KK	Export one DATA key and a single-length AKEK.
2-KD+KK	Export two DATA keys and a single-length AKEK.
1-KD+*KK	Export one DATA key and a double-length AKEK.
2-KD+*KK	Export two DATA keys and a double-length AKEK.
CCA-IMP	Export a CCA IMPORTER KEK. Requires NOCV keys to be enabled.
CCA-EXP	Export a CCA EXPORTER KEK. Requires NOCV keys to be enabled.
Data Key Offset Value (optional)	
CKT	Valid only when a key-encrypting key is being exported along with a DATA key. If this keyword is specified, any DATA keys being exported are encrypted under the key-encrypting key using an offset value of 0. If this keyword is not specified (this is the default), any DATA keys being exported are encrypted under the key-encrypting key using an offset value of 1. The CKT keyword is not valid with CCA-IMP or CCA-EXP keywords.

origin_identifier

Direction: Input	Type: String

This parameter is valid if the NOTARIZE keyword is specified. It specifies an area that contains a 16-byte string that contains the origin identifier that is defined in the ANSI X9.17 standard. The string must be ASCII characters, left-justified, and padded on the right by space characters. This parameter must be a minimum of four, non-space characters. ICSF ignores this parameter if you specify the OFFSET or CPLT-NOT keyword in the *rule_array* parameter.

destination_identifier

Direction: Input	Type: String

This parameter is valid if the NOTARIZE keyword is specified. It specifies an area that contains a 16-byte string. The 16-byte string contains the destination identifier that is defined in the ANSI X9.17 standard. The string must be ASCII characters, left-justified, and padded on the right by space characters. This parameter must be a minimum of four, non-space characters. ICSF ignores this parameter if you specify the OFFSET or CPLT-NOT keyword in the *rule_array* parameter.

source_data_key_1_identifier

Direction: Input/Output	Type: String

A 64-byte area that contains an internal token, or the label of a CKDS entry that contains a DATA key. ICSF ignores this field if you specify CCA-EXP or CCA-IMP in the *rule_array* parameter.

source_data_key_2_identifier

Direction: Input/Output	Type: String

A 64-byte area that contains an internal token, or the label of a CKDS entry that contains a DATA key. This parameter is valid only if you specify 2-KD, 2-KD+KK, or 2-KD+*KK as the source key rule keyword on the *rule_array* parameter. ICSF ignores this parameter if you specify other source key rule keywords, or if you specify CCA-EXP or CCA-IMP in the *rule_array* parameter.

source_key_encrypting_key_identifier

Direction: Input/Output	Type: String

A 64-byte area that contains an internal token, or the label of a CKDS entry that contains either an AKEK, a CCA IMPORTER, or a CCA EXPORTER key. If this parameter contains an AKEK, you must specify 1-KD+KK, 2-KD+KK, 1-KD+*KK, or 2-KD+*KK for the source key rule on the *rule_array* parameter. If this parameter contains a CCA IMPORTER or CCA EXPORTER key, you must specify CCA-IMP or CCA-EXP, respectively, for the source key rule on the *rule_array* parameter. ICSF ignores this field if you specify any other source key rule keywords.

transport_key_identifier

Direction: Input/Output	Type: String

A 64-byte area that contains either an internal token or a label that refers to an internal token for an AKEK.

outbound_KEK_count

Direction: Input	Type: String

An 8-byte area that contains an ASCII count that is used in the notarization process. The count is an ASCII character string, left-justified, and padded on the right by ASCII space characters. ICSF interprets a single ASCII space character as a zero counter. The maximum value is 99999999.

target_data_key_1

Direction: Output	Type: String

A 16-byte area where the exported data key 1 is returned. The enciphered key is an ASCII-encoded hexadecimal string.

target_data_key_2

Direction: Output	Type: String

A 16-byte area where the exported data key 2 is returned. The enciphered key is an ASCII-encoded hexadecimal string. This key is returned if 2-KD, 2-KD+KK, or 2-KD+*KK is specified in the *rule_array* parameter.

target_key_encrypting_key

Direction: Output	Type: String

If the *rule_array* parameter specifies 1-KD+KK, 2-KD+KK, 1-KD+*KK, or 2-KD+*KK, this parameter specifies a 32-byte area that contains the exported AKEK. If the *rule_array* parameter specifies CCA-IMP or CCA-EXP, this parameter specifies a 32-byte area that contains the exported key-encrypting key (KEK). The enciphered key is an ASCII-encoded hexadecimal string. If the *rule_array* parameter specifies 1-KD+KK or 2-KD+KK, the 16-byte ASCII-encoded output is left-justified in the field and the rest of the field remains unchanged.

MAC_key_token

Direction: Output	Type: String

A 64-byte area that contains an internal token for a MAC key that is intended for use in the MAC generation or MAC verification process. This field is the EXCLUSIVE OR of the two supplied DATA keys when the source key rule in the *rule_array* parameter specifies 2-KD, 2-KD+KK, or 2-KD+*KK. When the source key rule specifies 1-KD, the DATA key is converted to a MAC key and returned as an internal token in this field.

Usage Note

You must install the ANSI system keys in the CKDS to use this service.

ANSI X9.17 Key Import (CSNAKIM)

Use the ANSI X9.17 key import callable service to import a DATA key or a pair of DATA keys, along with an ANSI key-encrypting key (AKEK), using the ANSI X9.17 protocol. This service converts a single DATA key, or combines two DATA keys, into a single MAC key. The MAC key can be used in either, or both, the MAC generation or the MAC verification service to authenticate the service message. In addition, this service also supports the import of the KEK to a CCA IMPORTER or EXPORTER KEK, as well as an AKEK.

If you are importing only DATA keys, this service assumes that the DATA keys are encrypted under the specified transport AKEK. You have the option of applying the ANSI X9.17 key offset or key notarization process to the transport AKEK.

If you are importing both DATA keys and an AKEK, this service assumes that the AKEK is encrypted under the specified transport AKEK. This service also assumes that the DATA keys are encrypted under the source AKEK that is also being imported. You have the option of applying the ANSI X9.17 key offset or key notarization process to the transport AKEK. ICSF applies the ANSI X9.17 key offset process to the source AKEK with an offset of 1.

Note: You must create the cryptographic service message and maintain the offset counter value that is associated with the AKEK.

Format

```
CALL CSNAKIM(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            origin_identifier,
            destination_identifier,
            source_data_key_1,
            source_data_key_2,
            source_key_encrypting_key,
            inbound_KEK_count,
            transport_key_identifier,
            target_data_key_1,
            target_data_key_2,
            target_key_encrypting_key,
            MAC_key_token)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that are assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you supplied in the *rule_array* parameter. The value can be 0 to 3. If you specify 0, ICSF does not perform either notarization or offset.

rule_array

Direction: Input	Type: String

Zero to three keywords that provide control information to the callable service. See the list of keywords in Table 21. The keywords must be in 8 to 24 bytes of contiguous storage. Each of the keywords must be left-justified in its own 8-byte location and padded on the right with blanks. You must specify this parameter even is you do not specify a keyword.

Table 21. Keywords for ANSI X9.17 Key Import Rule Array

Keyword	Meaning
Notarization and Offset Rule (optional with no defaults)	
NOTARIZE	Perform notarization processing using the values obtained from the *origin_identifier*, *destination_identifier*, and *inbound_KEK_count* parameters.
OFFSET	Perform ANSI X9.17 key offset processing using the origin counter value obtained from the *inbound_KEK_count* parameter.
CPLT-NOT	Complete ANSI X9.17 notarization using the value obtained from the *inbound_KEK_count* parameter. The transport key that the *transport_key_identifier* specifies must be partially notarized.

Table 21. Keywords for ANSI X9.17 Key Import Rule Array (continued)

Keyword	Meaning
Parity Rule (optional)	
ENFORCE	Stop processing if any source keys do not have odd parity. This is the default value.
IGNORE	Ignore the parity of the source key.
Source Key Rule (optional)	
1-KD	Import one DATA key. This is the default parameter.
2-KD	Import two DATA keys.
1-KD+KK	Import one DATA key and a single-length AKEK.
2-KD+KK	Import two DATA keys and a single-length AKEK.
1-KD+*KK	Import one DATA key and a double-length AKEK.
2-KD+*KK	Import two DATA keys and a double-length AKEK.
CCA-IMP	Import a key-encrypting key as a CCA IMPORTER. Requires NOCV keys to be enabled.
CCA-EXP	Import a key-encrypting key as a CCA EXPORTER. Requires NOCV keys to be enabled.

origin_identifier

Direction: Input Type: String

This parameter is valid if you specify the NOTARIZE keyword in the *rule_array* parameter. It specifies an area that contains a 16-byte string that contains the origin identifier that is defined in the ANSI X9.17 standard. The string must be ASCII characters, left-justified, and padded on the right by space characters. The string must be a minimum of four, non-space characters. This parameter is ignored if the OFFSET or CPLT-NOT keyword is specified.

destination_identifier

Direction: Input Type: String

This parameter is valid if you specify the NOTARIZE keyword in the *rule_array* parameter. It specifies an area that contains a 16-byte string that contains the destination identifier that is defined in the ANSI X9.17 standard. The string must be ASCII characters, left-justified, and padded on the right by space characters. It must be a minimum of four non-space characters. This parameter is ignored if the OFFSET or CPLT-NOT keyword is specified.

source_data_key_1

Direction: Input Type: String

A 16-byte area that contains the enciphered DATA key to be imported. You must supply the DATA key as an ASCII-encoded hexadecimal string. The field is ignored if the *rule_array* parameter specifies CCA-IMP or CCA-EXP.

source_data_key_2

Direction: Input Type: String

A 16-byte area that contains the second enciphered DATA key to be imported. This parameter is valid only if the *rule_array* parameter specifies KK, or 2-KD+*KK. You must supply the key as an ASCII-encoded hexadecimal string. This field is ignored if the *rule_array* parameter specifies other source key rules.

source_key_encrypting_key

Direction: Input	Type: String

A 16- or 32-byte area that contains an enciphered AKEK, if the *rule_array* parameter specifies either 1-KD+KK, 2-KD+KK, 1-KD+*KK, or 2-KD+*KK. This parameter specifies a KEK, if the *rule_array* parameter specifies either CCA-IMP or CCA-EXP. The area is 16 bytes if the *rule_array* parameter specifies a single-length AKEK (1-KD+KK or 2-KD+KK). The area is 32 bytes if the *rule_array* parameter specifies a double-length AKEK (1-KD+*KK or 2-KD+*KK). You must supply the key as an ASCII-encoded hexadecimal string. This field is ignored if the *rule_array* parameter specifies 1-KD or 2-KD.

inbound_KEK_count

Direction: Input	Type: String

An 8-byte area that contains an ASCII count for use in the notarization process. The count is an ASCII character string, left-justified, and padded on the right by space characters. ICSF interprets a single space character as a zero counter. The maximum value is 99999999.

transport_key_identifier

Direction: Input/Output	Type: String

A 64-byte area that contains an internal token or a label that refers to an internal token for an AKEK.

target_data_key_1

Direction: Output	Type: String

A 64-byte area where the imported data key 1 is returned as an ICSF internal key token. ICSF does not support the direct import by label.

target_data_key_2

Direction: Output	Type: String

A 64-byte area where the imported data key 2 is returned as an ICSF internal key token. ICSF does not support the direct import by label. This key is returned if 2-KD, 2-KD+KK, or 2-KD+*KK is specified in the *rule_array* parameter.

target_key_encrypting_key

Direction: Output	Type: String

A 64-byte area where the imported key-encrypting key is returned as an ICSF internal key token. If the *rule_array* parameter specifies 1-KD+KK, 1-KD+*KK, 2-KD+KK, or 2-KD+*KK, the internal key token contains an AKEK. If the *rule_array* parameter specifies either CCA-IMP or CCA-EXP, the internal token contains a CCA IMPORTER or a CCA EXPORTER, respectively.

MAC_key_token

Direction: Output	Type: String

A 64-byte area that contains an internal token for a MAC key that is intended for use in the MAC generation or MAC verification function. This field is the EXCLUSIVE OR of the two imported DATA keys if the source key rule in the *rule_array* parameter specifies 2-KD, 2-KD+KK, or 2-KD+*KK. If the source key rule in the *rule_array* parameter specifies 1-KD, ICSF converts the DATA key to a MAC key and returns it as an internal token in this field.

Usage Note

You must install the ANSI system keys in the CKDS to use this service.

ANSI X9.17 Key Translate (CSNAKTR)

Use the ANSI X9.17 key translate callable service to translate a key from encryption under one AKEK to encryption under another AKEK. In a single service call you can translate either one or two encrypted DATA keys, or a single encrypted key-encrypting key. In addition, this service also imports the supplied DATA keys. If the *rule_array* parameter specifies 2-KD, this service exclusive-ORs the two imported DATA keys and converts the result into a MAC key, which it returns in the *MAC_key_token* field. The MAC key is used to perform MAC processing on the service message. If the *rule_array* specifies keywords 1-KD and 2-KD, ICSF translates only DATA keys. The service uses the inbound transport key-encrypting key to decrypt the DATA keys, and uses the outbound transport key-encrypting key to reencrypt the DATA keys. The service uses the ANSI X9.17 key offset process during decryption or importing. The service can use the ANSI X9.17 notarization process during reencryption or exporting of the DATA keys.

If the *rule_array* parameter specifies 1-KD+KK or 1-KD+*KK , the service translates only the AKEK. The service uses the inbound transport key-encrypting key to decrypt or import the input AKEK, applying the ANSI X9.17 offset process. The service uses the outbound transport key-encrypting key to reencipher or export the AKEK, with or without applying the optional ANSI X9.17 notarization process. ICSF uses the inbound key-encrypting key that is being translated to import the supplied DATA key, applying the ANSI X9.17 offset processing only with an offset of 0. The DATA key is imported as above then converted to a MAC key token and returned in the *MAC_key_token* field.

Format

```
CALL CSNAKTR(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             rule_array_count,
             rule_array,
             inbound_KEK_count,
             inbound_transport_key_identifier,
             inbound_data_key_1,
             inbound_data_key_2,
             inbound_key_encrypting_key,
             outbound_origin_identifier,
             outbound_destination_identifier,
             outbound_KEK_count,
             outbound_transport_key_identifier,
             outbound_data_key_1,
             outbound_data_key_2,
             outbound_key_encrypting_key,
             MAC_key_token)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that are assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you supplied in the *rule_array* parameter. The value can be 0 to 3. If you specify 0, the service does not perform notarization or offset.

rule_array

Direction: Input	Type: String

Zero to three keywords that provide control information to the callable service. See the list of keywords in Table 22. The keywords must be in 8 to 24 bytes of contiguous storage. Each of the keywords must be left-justified in its own 8-byte location and padded on the right with blanks. You must specify this parameter even if do not specify any keywords.

Table 22. Keywords for ANSI X9.17 Key Translate Rule Array

Keyword	Meaning
Notarization Rule (optional with no defaults)	
NOTARIZE	Perform notarization processing using the values obtained from the *outbound_origin_identifier*, the *outbound_destination_identifier*,and the *outbound_KEK_count*.
CPLT-NOT	Complete ANSI X9.17 notarization using the value obtained from the *outbound_KEK_count* parameter. The outbound transport key specified must be partially notarized.
Parity Rule (optional)	
ENFORCE	Stop processing if any source keys do not have odd parity. This is the default value.
IGNORE	Ignore the parity of the source key.
Source Key Rule (optional)	
1-KD	Import and translate one DATA key. This is the default parameter.
2-KD	Import and translate two DATA keys.
1-KD+KK	Import and translate one DATA key and a single-length AKEK.
1-KD+*KK	Import and translate one DATA key and a double-length AKEK.

inbound_KEK_count

Direction: Input	Type: String

An 8-byte area that contains an ASCII count for use in the offset process. The count is an ASCII character string, left-justified, and padded on the right by space characters. ICSF interprets a single space character as a zero counter. The maximum value is 99999999.

inbound_transport_key_identifier

Direction: Input/Output	Type: String

A 64-byte area that contains either an internal token, or a label that refers to an internal token for an AKEK.

inbound_data_key_1

Direction: Input Type: String

A 16-byte area that contains the enciphered DATA key that the service is importing and translating. You must specify the DATA key as an ASCII-encoded hexadecimal string.

inbound_data_key_2

Direction: Input Type: String

A 16-byte area that contains the second enciphered DATA key that the service is importing and translating. This field is valid if the *rule_array* parameter specifies 2-KD. You must supply the key as an ASCII-encoded hexadecimal string. This field is ignored if the *rule_array* parameter specifies other source key rules.

inbound_key_encrypting_key

Direction: Input Type: String

A 16- or 32-byte area that contains an enciphered AKEK that the service is to translate. The area is 16 bytes if the *rule_array* parameter specifies a source key rule of single-length AKEK. The area is 32 bytes if the source key rule specifies a double-length AKEK (1-KD+*KK). You must supply the key as an ASCII-encoded hexadecimal string. ICSF ignores this field if the *rule_array* specifies either 1-KD or 2-KD.

outbound_origin_identifier

Direction: Input Type: String

This parameter is valid if the *rule_array* parameter specifies a keyword of NOTARIZE. It specifies an area that contains a 16-byte string that contains the origin identifier that is defined in the ANSI X9.17 standard. The string must be ASCII characters, left-justified, and padded on the right by space characters. The string must be a minimum of four non-space characters. ICSF ignores this field if the *rule_array* parameter specifies a keyword of CPLT-NOT.

outbound_destination_identifier

Direction: Input Type: String

This parameter is valid if the *rule_array* parameter specifies a keyword of NOTARIZE. It specifies an area that contains a 16-byte string that contains the destination identifier that is defined in the ANSI X9.17 standard. The string must be ASCII characters, left-justified, and padded on the right by space characters. The string must be a minimum of four non-space characters. This parameter is ignored if the *rule_array* parameter specifies a keyword of CPLT-NOT.

outbound_KEK_count

Direction: Input Type: String

An 8-byte area that contains an ASCII count for use in the notarization process. The count is an ASCII character string, left-justified, and padded on the right by space characters. ICSF interprets a single space character as a zero counter. The maximum value is 99999999.

outbound_transport_key_identifier

Direction: Input/Output	Type: String

A 64-byte area that contains either an internal token, or a label that refers to an internal token for an AKEK.

outbound_data_key_1

Direction: Output	Type: String

A 16-byte area where the service returns the translated data key 1 an ASCII-encoded hexadecimal string. The service returns the key only if the *rule_array* specifies 1-KD or 2-KD. ICSF ignores this field if the *rule_array* parameter specifies either 1-KD+KK or 1-KD+*KK.

outbound_data_key_2

Direction: Output	Type: String

A 16-byte area where the service returns the translated data key 2 as an ASCII-encoded hexadecimal string. The service returns the key only if the *rule_array* parameter specifies 2-KD. ICSF ignores this field if the *rule_array* parameter specifies 1-KD, 1-KD+KK, or 1-KD+*KK.

outbound_key_encrypting_key

Direction: Output	Type: String

A 16- or 32-byte area that contains the enciphered, translated AKEK. The area is 16 bytes if the *rule_array* parameter specifies a single-length AKEK (1-KD+KK). The area is 32 bytes if the *rule_array* parameter specifies a double-length AKEK (1-KD+*KK). The service returns the key as an ASCII-encoded hexadecimal string. ICSF ignores this field if the *rule_array* parameter specifies either 1-KD or 2-KD.

MAC_key_token

Direction: Output	Type: String

A 64-byte area that contains an internal token for a MAC key that is intended for use in the MAC generation or MAC verification process. This field is the EXCLUSIVE OR of the two imported DATA keys when the *rule_array* parameter specifies 2-KD for the source key rule. If the *rule_array* parameter specifies 1-KD, the service returns the imported key in this field as an ICSF internal key token.

Usage Note

You must install the ANSI system keys in the CKDS to use this service.

ANSI X9.17 Transport Key Partial Notarize (CSNATKN)

Use the ANSI X9.17 transport key partial notarize callable service to preprocess an ANSI X9.17 transport key-encrypting key with origin and destination identifiers. ICSF completes the notarization process when you use the partially notarized key in the ANSI X9.17 key export, ANSI X9.17 key import, or ANSI X9.17 key translate services and specify the CPLT-NOT *rule_array* keyword.

Note: You cannot reverse the partial notarization process. If you want to keep the original value of the AKEK, you must record the value.

Format

```
CALL CSNATKN(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            origin_identifier,
            destination_identifier,
            source_transport_key_identifier,
            target_transport_key_identifier)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that are assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you supplied in the *rule_array* parameter. Currently no *rule_array* keywords are defined; thus, this field must be set to 0.

rule_array

Direction: Input	Type: String

Currently, no *rule_array* keywords are defined for this service. You must still specify this parameter for possible future use.

origin_identifier

Direction: Input	Type: String

A 16-byte string that contains the origin identifier that is defined in the ANSI X9.17 standard. The string must be ASCII characters, left-justified, and padded on the right by space characters. The string must be a minimum of four non-space characters.

destination_identifier

Direction: Input	Type: String

A 16-byte string that contains the destination identifier that is defined in the ANSI X9.17 standard. The string must be ASCII characters, left-justified, and padded on the right by space characters. The string must be a minimum of four non-space characters.

source_transport_key_identifier

Direction: Input/Output	Type: String

A 64-byte area that contains either an internal token, or a label of an internal token for an AKEK that permits notarization.

target_transport_key_identifier

Direction: Output	Type: String

A 64-byte area where the internal token of a partially notarized AKEK will be returned. This AKEK cannot be used directly as a notarizing KEK until the notarization process has been completed. To do this, specify CPLT-NOT as the *rule_array* keyword in any service in which you intend to use this key as a notarizing KEK.

Usage Note

You must install the ANSI system keys in the CKDS to use this service.

Chapter 6. Protecting Data

Use ICSF to protect sensitive data stored on your system, sent between systems, or stored off your system on magnetic tape. To protect data, encipher it under a key. When you want to read the data, decipher it from ciphertext to plaintext form.

ICSF provides *encipher* and *decipher callable services* to perform these functions. If you use a key to encipher data, you must use the same key to decipher the data. To use clear keys directly, ICSF provides *encode* and *decode callable services*. These services encipher and decipher with clear keys. You can use clear keys indirectly by first using the clear key import callable service, and then using the encipher and decipher callable services.

This chapter describes the following services:
- "Encipher (CSNBENC and CSNBENC1)" on page 123
- "Decipher (CSNBDEC and CSNBDEC1)" on page 130
- "Encode (CSNBECO)" on page 135
- "Decode (CSNBDCO)" on page 137

Modes of Operation

To encipher or decipher data or keys, ICSF uses either the U.S. National Institute of Standards and Technology (NIST) Data Encryption Standard (DES) algorithm or the Commercial Data Masking Facility (CDMF). The DES algorithm is documented in *Federal Information Processing Standard #46*. CDMF provides DES cryptography using an effectively shortened DATA key. See "System Encryption Algorithm" on page 13 for more information.

ICSF enciphers and deciphers using the following modes of operation:
- *Cipher block chaining (CBC)*
- *Electronic code book (ECB)*

Cipher Block Chaining (CBC) Mode

The CBC mode uses an initial chaining vector (ICV) in its processing. The CBC mode only processes blocks of data in exact multiples of eight. The ICV is exclusive ORed with the first 8 bytes of plaintext before the encryption step; the 8-byte block of ciphertext just produced is exclusive ORed with the next 8-byte block of plaintext, and so on. You must use the same ICV to decipher the data. This disguises any pattern that may exist in the plaintext. ICSF uses the CBC encipherment mode for encrypting and decrypting data using the encipher and decipher callable services.

Electronic Code Book (ECB) Mode

In the ECB mode, each 64-bit block of plaintext is separately enciphered and each block of the ciphertext is separately deciphered. In other words, the encipherment or decipherment of a block is totally independent of other blocks. ICSF uses the ECB encipherment mode for enciphering and deciphering data with clear keys using the encode and decode callable services.

ICSF does not support ECB encipherment mode on CDMF-only systems.

Triple DES Encryption

Triple-DES encryption uses a triple-length DATA key comprised of three 8-byte DES keys to encipher 8 bytes of data using the following method:

- Encipher the data using the first key
- Decipher the result using the second key
- Encipher the second result using the third key

The procedure is reversed to decipher data that has been triple-DES enciphered:
- Decipher the data using the third key
- Encipher the result using the second key
- Decipher the second result using the first key

ICSF uses the triple-DES encryption in the CBC encipherment mode.

A variation of the triple DES algorithm supports the use of a double-length DATA key comprised of two 8-byte DATA keys. In this method, the first 8-byte key is reused in the last encipherment step.

Triple-DES encryption is available only on the S/390 G4 Enterprise Server (with LIC driver 98), or above. Due to export regulations, triple-DES encryption may not be available on your processor.

Processing Rules

ICSF handles this chaining for each 8-byte block of data, from the first block until the last complete 8-byte block of data in each encipher call. There are different types of *processing rules* you can choose for cipher block chaining. You choose the type of processing rule that the callable service should use for CBC mode:
- **Cipher block chaining (CBC).** In exact multiples of 8 bytes.
- **Cryptographic Unit Support Program (CUSP).** Not necessarily in exact multiples of 8 bytes. The ciphertext is the same length of the plaintext.
- **Information Protection System (IPS).** Not necessarily in exact multiples of 8 bytes. The ciphertext is the same length of the plaintext.
- **ANSI X9.23.** Not necessarily in exact multiples of 8 bytes. This processing rule pads the plaintext so that the ciphertext produced is in exact multiples of 8 bytes.
- **IBM 4700.** Not necessarily in exact multiples of 8 bytes. This processing rule pads the plaintext so that the ciphertext produced is in exact multiples of 8 bytes.

Appendix C. Cipher Processing Rules describes the cipher processing rules in detail.

The resulting chaining value, after an encipher call, is known as an *output chaining vector (OCV)*. When there are multiple cipher requests, the application can pass the output chaining vector from the previous encipher call as the ICV in the next encipher call. This produces chaining between successive calls, which is known as *record chaining*. ICSF provides the ICV selection keyword CONTINUE in the *rule_array* parameter that an application can use to select record chaining with the CBC, IPS, and CUSP processing rules.

A chaining vector allows you to simulate CUSP or IPS record chaining by calculating the correct OCV. To do either the CUSP or IPS method of record chaining in the encipher and decipher callable services, the OCV from one service invocation is passed as the initialization vector to the next invocation. An OCV is produced for all processing rules. The OCV is the leftmost 8 bytes of the *chaining_vector* parameter.

Encipher (CSNBENC and CSNBENC1)

Use the encipher callable service to encipher data in an address space or a data space using the cipher block chaining mode. ICSF supports the following processing rules to encipher data. You choose the type of processing rule that the encipher callable service should use for the block chaining.

Processing Rule	Purpose
CBC	For block chaining in exact multiples of 8 bytes.
CUSP	For block chaining not necessarily in exact multiples of 8 bytes. The ciphertext will be the same length as the plaintext.
IPS	For block chaining not necessarily in exact multiples of 8 bytes. The ciphertext will be the same length as the plaintext.
ANSI X9.23	For block chaining not necessarily in exact multiples of 8 bytes. This process rule pads the plaintext so that ciphertext produced is an exact multiple of 8 bytes.
IBM 4700	For block chaining not necessarily in exact multiples of 8 bytes. This process rule pads the plaintext so that the ciphertext produced is an exact multiple of 8 bytes.

For more information about the processing rules, see Table 23 on page 127 and Appendix C. Cipher Processing Rules.

The cipher block chaining (CBC) mode of operation uses an initial chaining vector (ICV) in its processing. The ICV is exclusive ORed with the first 8 bytes of plaintext before the encryption step, and thereafter, the 8-byte block of ciphertext just produced is exclusive ORed with the next 8-byte block of plaintext, and so on. This disguises any pattern that may exist in the plaintext.

The selection between single-DES encryption mode and triple-DES encryption mode is controlled by the length of the key supplied in the *key_identifier* parameter. If a single-length key is supplied, single-DES encryption is performed. If a double-length or triple-length key is supplied, triple-DES encryption is performed.

To nullify the CBC effect on the first 8-byte block, supply 8 bytes of zero. However, the ICV may require zeros.

Cipher block chaining also produces a resulting chaining value called the output chaining vector (OCV). The application can pass the OCV as the ICV in the next encipher call. This results in *record chaining*.

Note that the OCV that results is the same, whether an encipher or a decipher callable service was invoked, assuming the same text, ICV, and key were used.

Short blocks are text lengths of 1 to 7 bytes. A short block can be the only block. Trailing short blocks are blocks of 1 to 7 bytes that follow an exact multiple of 8 bytes. For example, if the text length is 21, there are two 8-byte blocks, and a trailing short block of 5 bytes. Short blocks and trailing short blocks of 1 to 7 bytes of data are processed according to the Cryptographic Unit Support Program (CUSP) rules, or by the record chaining scheme devised by and used by the

Information Protection System (IPS) in the IPS/CMS program product. These methods of treating short blocks and trailing short blocks do not increase the length of the ciphertext over the plaintext.

An alternative method is to pad the plaintext and produce a ciphertext that is longer than the plaintext. The plaintext can be padded with up to 8 bytes using one of several padding schemes. This padding produces a ciphertext that is an exact multiple of 8 bytes long.

If the ciphertext is to be transmitted over a network, where one or more intermediate nodes will use the ciphertext translate callable service, the ciphertext *must* be produced using one of the following methods of padding:
- ANSI X9.23
- 4700

If the cleartext is already a multiple of 8, the ciphertext can be created using any processing rule.

Because of padding, the returned ciphertext length is longer than the provided plaintext; the *text_length* parameter *will have been modified*. The returned ciphertext field should be 8 bytes longer than the length of the plaintext to accommodate the maximum amount of padding. You should provide this extension in your installation's storage because ICSF cannot detect whether the extension was done.

The minimum length of data that can be enciphered is one byte. The maximum length of data that can be enciphered in one request is determined by installation management through the MAXLEN keyword. See the *OS/390 ICSF System Programmer's Guide* for details on how the length is specified.

Attention: If you lose the data-encrypting key under which the data (plaintext) is enciphered, the data enciphered under that key (ciphertext) **cannot** be recovered.

Choosing between CSNBENC and CSNBENC1

CSNBENC and CSNBENC1 provide identical functions. When choosing which service to use, consider the following:
- **CSNBENC** requires the cleartext and ciphertext to reside in the caller's primary address space. Also, a program using CSNBENC adheres to the IBM Common Cryptographic Architecture: Cryptographic Application Programming Interface.
- **CSNBENC1** allows the cleartext and ciphertext to reside either in the caller's primary address space or in a data space. This can allow you to encipher more data with one call. However, a program using CSNBENC1 does not adhere to the IBM Common Cryptographic Architecture: Cryptographic Application Programming Interface, and may need to be modified before it can run with other cryptographic products that follow this programming interface.

  For CSNBENC1, *clear_text_id* and *cipher_text_id* are access list entry token (ALET) parameters of the data spaces containing the cleartext and ciphertext.

Format

```
CALL CSNBENC(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            key_identifier,
            text_length,
            clear_text,
            initialization_vector,
            rule_array_count,
            rule_array,
            pad_character,
            chaining_vector,
            cipher_text )
```

```
CALL CSNBENC1(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             key_identifier,
             text_length,
             clear_text,
             initialization_vector,
             rule_array_count,
             rule_array,
             pad_character,
             chaining_vector,
             cipher_text,
             clear_text_id,
             cipher_text_id )
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output Type: String

The data that is passed to the installation exit.

key_identifier

Direction: Input/Output Type: String

A 64-byte string that is the internal key token containing the data-encrypting key, or the label of a CKDS record containing the data-encrypting key, to be used for encrypting the data. If the key token or CKDS contains a single-length key, single-DES encryption is performed. If the key token or CKDS contains a double-length or triple-length key, triple-DES encryption is performed.

text_length

Direction: Input/Output Type: Integer

On entry, the length of the plaintext (*clear_text* parameter) you supply. The MAXLEN keyword in the options file, as provided by the installation, determines the upper limit of the length of the text, including any necessary padding. A zero value for the *text_length* parameter is not valid. If the returned enciphered text (*cipher_text* parameter) is a different length because of the addition of padding bytes, the value is updated to the length of the ciphertext.

The application program passes the length of the plaintext to the callable service. The callable service returns the length of the ciphertext to the application program.

clear_text

Direction: Input Type: String

The text that is to be enciphered.

initialization_vector

Direction: Input Type: String

The 8-byte supplied string for the cipher block chaining. The first 8 bytes (or less) block of the data is exclusive ORed with the ICV and then enciphered. The input block is enciphered and the next ICV is created. You must use the same ICV to decipher the data.

rule_array_count

Direction: Input Type: Integer

The number of keywords you supply in the *rule_array* parameter. The value must be 1, 2, or 3.

rule_array

Direction: Input	Type: Character string

An array of 8-byte keywords providing the processing control information. The array is positional. See the keywords in Table 23. The first keyword in the array is the processing rule. You choose the processing rule you want the callable service to use for enciphering the data. The second keyword is the ICV selection keyword. The third keyword (or the second if the ICV selection keyword is allowed to default to INITIAL) is the encryption algorithm to use.

The service will fail if keyword DES is specified in the *rule_array* in a CDMF-only system. The service will likewise fail if the keyword CDMF is specified in the *rule_array* in a DES-only system.

Table 23. Keywords for the Encipher Rule Array Control Information

Keyword	**Meaning**
Processing Rule (required)	
CBC	Performs ANSI X3.102 cipher block chaining. The data must be a multiple of 8 bytes. An OCV is produced and placed in the *chaining_vector* parameter. If the ICV selection keyword CONTINUE is specified, the CBC OCV from the previous call is used as the ICV for this call.
X9.23	Performs cipher block chaining with 1 to 8 bytes of padding. This is compatible with the requirements in ANSI standard X9.23. If the data is not in exact multiples of 8 bytes, X9.23 pads the plaintext so that the ciphertext produced is an exact multiple of 8 bytes. The plaintext is padded to the next multiple 8 bytes, even if this adds 8 bytes. An OCV is produced.
IPS	Performs ciphering that is compatible with IBM's IPS product. The data may be of any length and does not need to be in multiples of 8 bytes. The ciphertext will be the same length as the plaintext. The IPS OCV is placed in the *chaining_vector* parameter. If the ICV selection keyword CONTINUE is specified, the IPS OCV from the previous call is used as the ICV for this call.
CUSP	Performs ciphering that is compatible with IBM's CUSP and PCF products. The data can be of any length and does not need to be in multiples of 8 bytes. The ciphertext will be the same length as the plaintext. The CUSP/PCF OCV is placed in the *chaining_vector* parameter. If the ICV selection keyword CONTINUE is specified, the CUSP/PCF OCV from the previous call is used as the ICV for this call.
4700-PAD	Performs padding by extending the user's plaintext with the caller's specified pad character, followed by a one-byte binary count field that contains the total number of bytes added to the message. 4700-PAD pads the plaintext so that the ciphertext produced is an exact multiple of 8 bytes. An OCV is produced.
ICV Selection (optional)	

Table 23. Keywords for the Encipher Rule Array Control Information (continued)

Keyword	**Meaning**
INITIAL	This specifies taking the initialization vector from the *initialization_vector* parameter. INITIAL is the default value.
CONTINUE	This specifies taking the initialization vector from the output chaining vector (OCV) contained in the work area to which the *chaining_vector* parameter points. CONTINUE is valid only for processing rules CBC, IPS, and CUSP.
Encryption Algorithm (optional)	
TOKEN	This specifies using the data encryption algorithm in the DATA key token. TOKEN is the default.
DES	This specifies using the data encryption standard and ignoring the token marking.
CDMF	This specifies using the Commercial Data Masking Facility and ignoring the token marking. You cannot use double-length or triple-length keys with CDMF.

The following recommendations help the caller determine which encipher processing rule to use:

- If you are exchanging enciphered data with a specific implementation, for example, CUSP or ANSI X9.23, use that processing rule.
- If the ciphertext translate callable service is to be invoked on the enciphered data at an intermediate node, ensure that the ciphertext is a multiple of 8 bytes. Use CBC, X9.23, or 4700-PAD to prevent the creation of ciphertext that is not a multiple of 8 bytes and that cannot be processed by the ciphertext translate callable service.
- If the ciphertext length must be equal to the plaintext length and the plaintext length cannot be a multiple of 8 bytes, use either the IPS or CUSP processing rule.

Appendix C. Cipher Processing Rules describes the cipher processing rules in detail.

pad_character

Direction: Input	Type: Integer

An integer, 0 to 255, that is used as a padding character for the 4700-PAD process rule (*rule_array* parameter).

chaining_vector

Direction: Input/Output	Type: String

An 18-byte field that ICSF uses as a system work area. Your application program must not change the data in this string. The chaining vector holds the output chaining vector (OCV) from the caller. The OCV is the first 8 bytes in the 18-byte string.

The direction is output if the ICV selection keyword of the *rule_array* parameter is INITIAL.

The direction is input/output if the ICV selection keyword of the *rule_array* parameter is CONTINUE.

cipher_text

Direction: Output	Type: String

The enciphered text the callable service returns. The length of the ciphertext is returned in the *text_length* parameter. The *cipher_text* may be 8 bytes longer than the length of the *clear_text* field because of the padding that is required for some processing rules.

clear_text_id

Direction: Input	Type: Integer

For CSNBENC1 only, the ALET of the clear text to be enciphered.

cipher_text_id

Direction: Input	Type: Integer

For CSNBENC1 only, the ALET of the ciphertext that the application supplied.

Restrictions

The service will fail under the following conditions:
- If the keyword DES is specified in the *rule_array* parameter in a CDMF-only system
- If the keyword CDMF is specified in the *rule_array* parameter in a DES-only system
- If the key token contains double- or triple-length keys and triple-DES is not enabled.

Related Information

You **cannot** overlap the plaintext and ciphertext fields. For example:

```
pppppp
     cccccc  is incorrect.

cccccc
     pppppp  is incorrect.
ppppppcccccc is correct.

P represents the plaintext and c represents the ciphertext.
```

The method used to produce the OCV is the same with the CBC, 4700-PAD, and X9.23 processing rules. However, that method is different from the method used by the CUSP and IPS processing rules.

Appendix C. Cipher Processing Rules discusses the cipher processing rules.

The decipher callable services (CSNBDEC and CSNBDEC1) are described under "Decipher (CSNBDEC and CSNBDEC1)" on page 130.

Decipher (CSNBDEC and CSNBDEC1)

Use the decipher callable service to decipher data in an address space or a data space using the cipher block chaining mode. ICSF supports the following processing rules to decipher data. You choose the type of processing rule that the decipher callable service should use for block chaining.

Processing Rule	**Purpose**
CBC	For cipher block chaining. The ciphertext must be an exact multiple of 8 bytes, and the plaintext will have the same length.
CUSP	For cipher block chaining, but the ciphertext can be of any length. The plaintext will be the same length as the ciphertext.
IPS	For cipher block chaining, but the ciphertext can be of any length. The plaintext will be the same length as the ciphertext.
ANSI X9.23	For cipher block chaining. The ciphertext must be an exact multiple of 8 bytes, but the plaintext will be 1 to 8 bytes shorter than the ciphertext. The *text_length* will also be reduced to show the original length of the plaintext.
IBM 4700	For cipher block chaining. The ciphertext must be an exact multiple of 8 bytes, but the plaintext will be 1 to 8 bytes shorter than the ciphertext. The *text_length* will also be reduced to show the original length of the plaintext.

The cipher block chaining (CBC) mode uses an initial chaining value (ICV) in its processing. The first 8 bytes of ciphertext is deciphered and then the ICV is exclusive ORed with the resulting 8 bytes of data to form the first 8-byte block of plaintext. Thereafter, the 8-byte block of ciphertext is deciphered and exclusive ORed with the previous 8-byte block of ciphertext until all the ciphertext is deciphered.

The selection between single-DES decryption mode and triple-DES decryption mode is controlled by the length of the key supplied in the *key_identifier* parameter. If a single-length key is supplied, single-DES decryption is performed. If a double-length or triple-length key is supplied, triple-DES decryption is performed.

A different ICV may be passed on each call to the decipher callable service. However, the same ICV that was used in the corresponding encipher callable service must be passed.

Short blocks are text lengths of 1 to 7 bytes. A short block can be the only block. Trailing short blocks are blocks of 1 to 7 bytes that follow an exact multiple of 8 bytes. For example, if the text length is 21, there are two 8-byte blocks and a trailing short block of 5 bytes. Because the DES and CDMF process only text in exact multiples of 8 bytes, some special processing is required to decipher such short blocks. Short blocks and trailing short blocks of 1 to 7 bytes of data are processed according to the Cryptographic Unit Support Program (CUSP) rules, or by the record chaining scheme devised by and used in the Information Protection System (IPS) in the IPS/CMS product.

These methods of treating short blocks and trailing short blocks do not increase the length of the ciphertext over the plaintext. If the plaintext was *padded* during encipherment, the length of the ciphertext will always be an exact multiple of 8 bytes.

ICSF supports the following padding schemes:

- ANSI X9.23
- 4700-PAD

Choosing Between CSNBDEC and CSNBDEC1

CSNBDEC and CSNBDEC1 provide identical functions. When choosing which service to use, consider the following:

- **CSNBDEC** requires the ciphertext and plaintext to reside in the caller's primary address space. Also, a program using CSNBDEC adheres to the IBM Common Cryptographic Architecture: Cryptographic Application Programming Interface.
- **CSNBDEC1** allows the ciphertext and plaintext to reside either in the caller's primary address space or in a data space. This can allow you to decipher more data with one call. However, a program using CSNBDEC1 does not adhere to the IBM Common Cryptographic Architecture: Cryptographic Application Programming Interface, and may need to be modified before it can run with other cryptographic products that follow this programming interface.

  For CSNBDEC1, *cipher_text_id* and *clear_text_id* are access list entry token (ALET) parameters of the data spaces containing the ciphertext and plaintext.

Format

```
CALL CSNBDEC(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             key_identifier,
             text_length,
             cipher_text,
             initialization_vector,
             rule_array_count,
             rule_array,
             chaining_vector,
             clear_text )
```

```
CALL CSNBDEC1(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             key_identifier,
             text_length,
             cipher_text,
             initialization_vector,
             rule_array_count,
             rule_array,
             chaining_vector,
             clear_text,
             cipher_text_id,
             clear_text_id )
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

key_identifier

Direction: Input/Output	Type: String

A 64-byte string that is the internal key token containing the data-encrypting key, or the label of a CKDS record containing a data-encrypting key, to be used for deciphering the data. If the key token or CKDS contains a single-length key, single-DES decryption is performed. If the key token or CKDS contains a double-length or triple-length key, triple-DES decryption is performed.

text_length

Direction: Input/Output	Type: Integer

On entry, you supply the length of the ciphertext. The MAXLEN keyword in the options file, as provided by the installation, determines the upper limit of the length of the text. A zero value for the *text_length* parameter is not valid. If the returned deciphered text (*clear_text* parameter) is a different length because of the removal of padding bytes, the value is updated to the length of the plaintext.

The application program passes the length of the ciphertext to the callable service. The callable service returns the length of the plaintext to your application program.

cipher_text

Direction: Input	Type: String

The text to be deciphered.

initialization_vector

Direction: Input	Type: String

The 8-byte supplied string for the cipher block chaining. The first block of the ciphertext is deciphered and exclusive ORed with the initial chaining vector (ICV) to get the first block of cleartext. The input block is the next ICV. To decipher the data, you must use the same ICV used when you enciphered the data.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you supply in the *rule_array* parameter. The value must be 1, 2, or 3.

rule_array

Direction: Input	Type: Character string

An array of 8-byte keywords providing the processing control information. The array is positional. See the keywords in Table 24. The first keyword in the array is the processing rule. You choose the processing rule you want the callable service to use for deciphering the data. The second keyword is the ICV selection keyword. The third keyword (or the second if the ICV selection keyword is allowed to default) is the encryption algorithm to use.

The service will fail if keyword DES is specified in the *rule_array* in a CDMF-only system. The service will likewise fail if keyword CDMF is specified in the *rule_array* in a DES-only system.

Table 24. Keywords for the Decipher Rule Array Control Information

Keyword	**Meaning**
Processing Rule (required)	
CBC	Performs ANSI X3.102 cipher block chaining. The data must be a multiple of 8 bytes. An OCV is produced and placed in the *chaining_vector* parameter. If the ICV selection keyword CONTINUE is specified, the CBC OCV from the previous call is used as the ICV for this call.
X9.23	Deciphers with cipher block chaining and text length reduced to the original value. This is compatible with the requirements in ANSI standard X9.23. The ciphertext length must be an exact multiple of 8 bytes. Padding is removed from the plaintext.

Table 24. Keywords for the Decipher Rule Array Control Information (continued)

Keyword	Meaning
IPS	Performs deciphering that is compatible with IBM's IPS product. The data can be of any length and does not need to be in multiples of 8 bytes. The ciphertext will be the same length as the plaintext. The IPS OCV is placed in the *chaining_vector* parameter. If the ICV selection keyword CONTINUE is specified, the IPS OCV from the previous call is used as the ICV for this call.
CUSP	Performs deciphering that is compatible with IBM's CUSP and PCF products. The data can be of any length and does not need to be in multiples of 8 bytes. The ciphertext will be the same length as the plaintext. The CUSP/PCF OCV is placed in the *chaining_vector* parameter. If the ICV selection keyword CONTINUE is specified, the CUSP/PCF OCV from the previous call is used as the ICV for this call.
4700-PAD	Deciphers with cipher block chaining and text length reduced to the original value. The ciphertext length must be an exact multiple of 8 bytes. Padding is removed from the plaintext.
ICV Selection (optional)	
INITIAL	This specifies taking the initialization vector from the *initialization_vector* parameter. INITIAL is the default value.
CONTINUE	This specifies taking the initialization vector from the output chaining vector (OCV) contained in the work area to which the *chaining_vector* parameter points. CONTINUE is valid only for processing rules CBC, IPS, and CUSP.
Encryption Algorithm (optional)	
TOKEN	This specifies using the data encryption algorithm in the DATA key token. This is the default.
DES	This specifies using the data encryption standard and ignoring the token marking.
CDMF	This specifies using the Commercial Data Masking Facility and ignoring the token marking. You cannot use double- or triple-length keys with CDMF.

Appendix C. Cipher Processing Rules describes the cipher processing rules in detail.

chaining_vector

Direction: Input/Output Type: String

An 18-byte field that ICSF uses as a system work area. Your application program must not change the data in this string. The chaining vector holds the output chaining vector (OCV) from the caller. The OCV is the first 8 bytes in the 18-byte string.

The direction is output if the ICV selection keyword of the *rule_array* parameter is INITIAL. The direction is input/output if the ICV selection keyword of the *rule_array* parameter is CONTINUE.

clear_text

Direction: Output	Type: String

The field where the callable service returns the deciphered text.

cipher_text_id

Direction: Input	Type: Integer

For CSNBDEC1 only, the ALET of the ciphertext to be deciphered.

clear_text_id

Direction: Input	Type: Integer

For CSNBDEC1 only, the ALET of the clear text supplied by the application.

Restrictions

The service will fail under the following conditions:

- If the keyword DES is specified in the *rule_array* parameter in a CDMF-only system
- If the keyword CDMF is specified in the *rule_array* parameter in a DES-only system
- If the key token contains double or triple-length keys and triple-DES is not enabled.

Usage Note

Only a DATA key token or DATA key label can be used in this service.

Related Information

You **cannot** overlap the plaintext and ciphertext fields. For example:

```
pppppp
     cccccc  is incorrect.

cccccc
     pppppp  is incorrect.

ppppppcccccc is correct.

P represents the plaintext and c represents the ciphertext.
```

Appendix C. Cipher Processing Rules discusses the cipher processing rules.

The encipher callable services (CSNBENC and CSNBENC1) are described under "Encipher (CSNBENC and CSNBENC1)" on page 123.

Encode (CSNBECO)

Use the encode callable service (CSNBECO) to encipher an 8-byte string using a clear key. The callable service uses the electronic code book (ECB) mode of the DES. (This service is available only on a DES-capable system.)

Considerations

If you have only a clear key, you are *not* limited to using just the encode and decode callable services. You can pass your clear key to the clear key import service, and get back a token that will allow you to use the encipher and decipher callable services.

Format

```
CALL CSNBECO(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            clear_key,
            clear_text,
            cipher_text)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

clear_key

Direction: Input	Type: String

The 8-byte clear key value that is used to encode the data.

clear_text

Direction: Input	Type: String

The plaintext that is to be encoded. Specify 8 bytes of text.

cipher_text

Direction: Output	Type: String

The 8-byte field where the ciphertext is returned by the callable service.

Restriction

You cannot use this service on a CDMF-only system.

Decode (CSNBDCO)

Use the decode callable service (CSNBDCO) to decipher an 8-byte string using a clear key. The callable service uses the electronic code book (ECB) mode of the DES. (This service is available only on a DES-capable system.)

Considerations

If you have only a clear key, you are *not* limited to using only the encode and decode callable services. You can pass your clear key to the clear key import service, and get back a token that will allow you to use the encipher and decipher callable services.

Format

```
CALL CSNBDCO(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             clear_key,
             cipher_text,
             clear_text)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

clear_key

Direction: Input	Type: String

The 8-byte clear key value that is used to decode the data.

cipher_text

Direction: Input	Type: String

The ciphertext that is to be decoded. Specify 8 bytes of text.

clear_text

Direction: Output	Type: String

The 8-byte field where the plaintext is returned by the callable service.

Restriction

You cannot use this service on a CDMF-only system.

Chapter 7. Generating Random Numbers

Use the random number generate callable service (CSNBRNG) to generate an 8-byte random number. The *form* parameter determines the characteristic of the returned number. The returned number can have the following forms:

- Random, for possible use as an initialization vector or other general use, such as non-cryptographic.
- Each byte with odd parity, for possible use as a clear key or first key part.
- Each byte with even parity, for possible use as a subsequent key part.

Random Number Generate (CSNBRNG)

The callable service uses the cryptographic feature to generate a random number. The foundation for the random number generator is a time variant input with a very low probability of recycling.

Format

```
CALL CSNBRNG(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             form,
             random_number )
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output   Type: String

The data that is passed to the installation exit.

form

Direction: Input   Type: Character string

The 8-byte keyword that defines the characteristics of the random number should be left-justify and pad on the right with blanks. The keywords are listed in Table 25.

Table 25. Keywords for the Form Parameter

Keyword	**Meaning**
RANDOM	Generate a 64-bit random number.
ODD	Generate a 64-bit random number with odd parity in each byte.
EVEN	Generate a 64-bit random number with even parity in each byte.

Parity is calculated on the 7 high-order bits in each byte and is presented in the low-order bit in the byte.

random_number

Direction: Output   Type: String

The generated number returned by the callable service in an 8-byte variable.

Chapter 8. Translating Ciphertext

ICSF provides a ciphertext translate callable service on DES-capable systems. The callable service deciphers encrypted data (ciphertext) under one data translation key and reenciphers it under another data translation key without having the data appear in the clear outside the Integrated Cryptographic Feature. ICSF uses the data translation key as either the input or the output data transport key. Such a function is useful in a multiple node network, where sensitive data is passed through multiple nodes before it reaches its final destination.

"Using the Ciphertext Translate Callable Service" on page 44 provides some tips on using the callable service.

Ciphertext Translate (CSNBCTT and CSNBCTT1)

Use the ciphertext translate callable service to decipher text under an "input" key and then to encipher the text under an "output" key. The callable service uses the cipher block chaining (CBC) mode of the DES. This service is available only on a DES-capable system.

Choosing Between CSNBCTT and CSNBCTT1

CSNBCTT and CSNBCTT1 provide identical functions. When choosing the service to use, consider the following:

- **CSNBCTT** requires the input text and output text to reside in the caller's primary address space. Also, a program using CSNBCTT adheres to the IBM Common Cryptographic Architecture: Cryptographic Application Programming Interface.
- **CSNBCTT1** allows the input text and output text to reside either in the caller's primary address space or in a data space. This allows you to translate more data with one call. However, a program using CSNBCTT1 does not adhere to the IBM Common Cryptographic Architecture: Cryptographic Application Programming Interface, and may need to be modified before it can run with other cryptographic products that follow this programming interface.

  For CSNBCTT1, *text_id_in* and *text_id_out* are access list entry token (ALET) parameters of the data spaces containing the input text and output text.

Format

```
CALL CSNBCTT(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            key_identifier_in,
            key_identifier_out,
            text_length,
            text_in,
            initialization_vector_in,
            initialization_vector_out,
            text_out )
```

Ciphertext Translate (CSNBCTT and CSNBCTT1)

```
CALL CSNBCTT1(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             key_identifier_in,
             key_identifier_out,
             text_length,
             text_in,
             initialization_vector_in,
             initialization_vector_out,
             text_out,
             text_id_in,
             text_id_out )
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

key_identifier_in

Direction: Input/Output	Type: String

The 64-byte string of the internal key token containing the data translation (DATAXLAT) key, or the label of the CKDS record containing the DATAXLAT key used to encipher the input string.

key_identifier_out

Direction: Input/Output	Type: String

The 64-byte string of an internal key token containing the DATAXLAT key, or the label of the CKDS record containing the DATAXLAT key, used to reencipher the encrypted text.

text_length

Direction: Input	Type: Integer

The length of the ciphertext that is to be processed. The text length must be a multiple of 8 bytes. The MAXLEN keyword in the options file determines the upper limit of the length of the text.

text_in

Direction: Input	Type: String

The text that is to be translated. The text is enciphered under the data translation key specified in the *key_identifier_in* parameter.

initialization_vector_in

Direction: Input	Type: String

The 8-byte initialization vector that is used to decipher the input data. This parameter is the initialization vector used at the previous cryptographic node.

initialization_vector_out

Direction: Input	Type: String

The 8-byte initialization vector that is used to encipher the input data. This is the new initialization vector used when the callable service enciphers the plaintext.

text_out

Direction: Output	Type: String

The field where the callable service returns the translated text.

text_id_in

Direction: Input	Type: Integer

For CSNBCTT1 only, the ALET of the text to be translated.

text_id_out

Direction: Input	Type: Integer

For CSNBCTT1 only, the ALET of the *text_out* field that the application supplies.

Restrictions

The input ciphertext length must be an exact multiple of 8 bytes. The minimum length of the ciphertext that can be translated is 8 bytes.

You cannot use this service on a CDMF-only system.

Usage Note

The initialization vectors must have already been established between the communicating applications or must be passed with the data.

Chapter 9. Verifying Data Integrity and Authenticating Messages

ICSF provides several methods to verify the integrity of transmitted messages and stored data:

- Message authentication code (MAC)
- Hash functions, including modification detection code (MDC) processing and one-way hash generation

Note: You can also use digital signatures (see "Chapter 15. Using Digital Signatures" on page 247) to authenticate messages.

The choice of callable service depends on the security requirements of the environment in which you are operating. If you need to ensure the authenticity of the sender as well as the integrity of the data, and both the sender and receiver can share a secret key, consider message authentication code processing. If you need to ensure the integrity of transmitted data in an environment where it is not possible for the sender and the receiver to share a secret cryptographic key, consider hashing functions, such as the modification detection code process.

The callable services are described in the following topics:

- "MAC Generation (CSNBMGN and CSNBMGN1)" on page 147
- "MAC Verification (CSNBMVR and CSNBMVR1)" on page 152
- "MDC Generation (CSNBMDG and CSNBMDG1)" on page 156
- "One-Way Hash Generate (CSNBOWH and CSNBOWH1)" on page 160
- "VISA CVV Service Generate (CSNBCSG)" on page 163
- "VISA CVV Service Verify (CSNBCSV)" on page 166

How MACs are Used

When a message is sent, an application program can generate an authentication code for it using the MAC generation callable service. ICSF supports the ANSI X9.9-1 basic procedure and both the ANSI X9.19 basic procedure and optional double key MAC procedure. The service computes the text of the message authentication code using the algorithm and a key. The ANSI X9.9-1 or ANSI X9.19 basic procedures accept either a single-length MAC generation (MAC) key or a data-encrypting (DATA) key, and the message text. The ANSI X9.19 optional double key MAC procedure accepts a double-length MAC key and the message text. The message text may be in clear or encrypted form. The originator of the message sends the MAC with the message text.

When the receiver gets the message, an application program calls the *MAC verification callable service*. The callable service generates a MAC using the same algorithm as the sender and either the single-length (MACVER) or double-length (DATAMV) MAC verification key, the single-length (MAC) or double-length (DATAM) MAC generation key, or DATA key, and the message text. The MACVER callable service compares the MAC it generates with the one sent with the message and issues a return code that indicates whether the MACs match. If the return code indicates that the MACs match, the receiver can accept the message as genuine and unaltered. If the return code indicates that the MACs do not match, the receiver can assume that the message is either bogus or has been altered. The newly computed MAC is not revealed outside the cryptographic feature.

Note: The use of a double-length MACVER key is supported only on S/390 G5 Enterprise Servers, or above.

In a similar manner, MACs can be used to ensure the integrity of data stored on the system or on removable media, such as tape.

Secure use of the MAC generation and MAC verification services requires the use of MAC and MACVER keys in these services, respectively. To accomplish this, the originator of the message generates a MAC/MACVER key pair, uses the MAC key in the MAC generation service, and exports the MACVER key to the receiver. The originator of the message enforces key separation on the link by encrypting the MACVER key under a transport key that is not an NOCV key before exporting the key to the receiver. With this type of key separation enforced, the receiver can only receive a MACVER key and can use only this key in the MAC verification service. This ensures that the receiver cannot alter the message and produce a valid MAC with the altered message. These security features are not present if DATA keys are used in the MAC generation service, or if DATA or MAC keys are used in the MAC verification service.

By using MACs, you get the following benefits:

- **For data transmitted over a network,** you can validate the authenticity of the message as well as ensure that the data has not been altered during transmission. For example, an active eavesdropper can tap into a transmission line, and interject bogus messages or alter sensitive data being transmitted. If the data is accompanied by a MAC, the recipient can use a callable service to detect whether the data has been altered. Since both the sender and receiver share a secret key, the receiver can use a callable service that calculates a MAC on the received message and compares it to the MAC transmitted with the message. If the comparison is equal, the message may be accepted as unaltered. Furthermore, since the shared key is secret, when a MAC is verified it can be assumed that the sender was, in fact, the other person who knew the secret key.
- **For data stored on tape or DASD,** you can ensure that the data read back onto the system was the same as the data written onto the tape or DASD. For example, someone might be able to bypass access controls. Such an access might escape the notice of auditors. However, if a MAC is stored with the data, and verified when the data is read, you can detect alterations to the data.

How Hashing Functions Are Used

Hashing functions include the MDC and one-way hash. You need to hash text before submitting it to digital signature services (see "Chapter 15. Using Digital Signatures" on page 247).

How MDCs Are Used

When a message is sent, an application program can generate a modification detection code for it using the *MDC generation callable service*. The service computes the modification detection code, a 128-bit value, using a one-way cryptographic function and the message text (which itself may be in clear or encrypted form). The originator of the message ensures that the MDC is transmitted with integrity to the intended receiver of the message. For example, the MDC could be published in a reliable source of public information.

When the receiver gets the message, an application program calls the *MDC callable service*. The callable service generates an MDC by using the same one-way cryptographic function and the message text. The application program can compare the new MDC with the one generated by the originator of the message. If the MDCs match, the receiver knows that the message was not altered.

In a similar manner, MDCs can be used to ensure the integrity of data stored on the system or on removable media, such as tape.

By using MDCs, you get the following benefits:

- **For data transmitted over a network between locations that do not share a secret key,** you can ensure that the data has not been altered during transmission. It is easy to compute an MDC for specific data, yet hard to find data that will result in a given MDC. In effect, the problem of ensuring the integrity of a large file is reduced to ensuring the integrity of a 128-bit value.
- **For data stored on tape or DASD,** you can ensure that the data read back onto the system was the same as the data written onto the tape or DASD. Once an MDC has been established for a file, the MDC generation callable service can be run at any later time on the file. The resulting MDC can be compared with the stored MDC to detect deliberate or inadvertent modification.

SHA-1 is a FIPS standard required for DSS. MD5 is a hashing algorithm used to derive Message Digests in Digital Signature applications.

How VISA Card Verification Values Are Used

The Visa International Service Association (VISA) and MasterCard International, Incorporated have specified a cryptographic method to calculate a value that relates to the personal account number (PAN), the card expiration date, and the service code. The VISA card-verification value (CVV) and the MasterCard card-verification code (CVC) can be encoded on either track 1 or track 2 of a magnetic striped card and are used to detect forged cards. Because most online transactions use track-2, the ICSF callable services generate and verify the CVV[4] by the track-2 method.

| The VISA CVV service generate callable service calculates a 1- to 5-byte value
| through the DES-encryption of the PAN, the card expiration date, and the service
| code using two data-encrypting keys or two MAC keys. The VISA CVV service
| verify callable service calculates the CVV by the same method, compares it to the
| CVV supplied by the application (which reads the credit card's magnetic stripe) in
| the *CVV_value*, and issues a return code that indicates whether the card is
| authentic.

MAC Generation (CSNBMGN and CSNBMGN1)

Use the MAC generation callable service to generate a 4-, 6-, or 8-byte message authentication code (MAC) for an application-supplied text string. You can specify that the callable service uses either the ANSI X9.9-1 procedure or the ANSI X9.19 optional double key MAC procedure to compute the MAC. For the ANSI X9.9-1 procedure you identify either a MAC generation key or a DATA key, and the message text. For the ANSI X9.19 optional double key MAC procedure, you identify a double-length MAC key and the message text.

The MAC generation callable service also supports the padding rules specified in the EMV Specification.

4. The VISA CVV and the MasterCard CVC refer to the same value. CVV is used here to mean both CVV and CVC.

Choosing Between CSNBMGN and CSNBMGN1

CSNBMGN and CSNBMGN1 provide identical functions. When choosing which service to use, consider the following:

- **CSNBMGN** requires the application-supplied text to reside in the caller's primary address space. Also, a program using CSNBMGN adheres to the IBM Common Cryptographic Architecture: Cryptographic Application Programming Interface.
- **CSNBMGN1** allows the application-supplied text to reside either in the caller's primary address space or in a data space. This can allow you to process more data with one call. However, a program using CSNBMGN1 does not adhere to the IBM Common Cryptographic Architecture: Cryptographic Application Programming Interface, and may need to be modified before it can run with other cryptographic products that follow this programming interface.

  For CSNBMGN1, *text_id_in* is an access list entry token (ALET) parameter of the data space containing the application-supplied text.

Format

```
CALL CSNBMGN(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            key_identifier,
            text_length,
            text,
            rule_array_count,
            rule_array,
            chaining_vector,
            mac )
```

```
CALL CSNBMGN1(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             key_identifier,
             text_length,
             text,
             rule_array_count,
             rule_array,
             chaining_vector,
             mac,
             text_id_in )
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

key_identifier

Direction: Input/Output	Type: String

The 64-byte key label or internal key token that identifies a single-length or double-length MAC generation key or a single-length DATA key. The type of key depends on the MAC process rule in the *rule_array* parameter.

text_length

Direction: Input	Type: Integer

The length of the text you supply in the *text* parameter. The MAXLEN keyword in the options file determines the maximum length of the text. (See *OS/390 ICSF System Programmer's Guide* for a description of the MAXLEN keyword in the options file.) If the *text_length* is not a multiple of 8 bytes and if the ONLY or LAST keyword of the *rule_array* parameter is called, the text is padded with binary zeros.

text

Direction: Input	Type: String

The application-supplied text for which the MAC is generated.

rule_array_count

Direction: Input	Type: Integer

The number of keywords specified in the *rule_array* parameter. The value can be 0, 1, 2, or 3.

rule_array

Direction: Input	Type: Character string

Zero to three keywords that provide control information to the callable service. The keywords are shown in Table 26. The keywords must be in 24 bytes of contiguous storage with each of the keywords left-justified in its own 8-byte location and padded on the right with blanks. For example,

```
'X9.9-1  MIDDLE  MACLEN4 '
```

The order of the *rule_array* keywords is not fixed.

You can specify one of the MAC processing rules and then choose one of the segmenting control keywords and one of the MAC length keywords.

Table 26. Keywords for MAC Generation Control Information

Keyword	Meaning
MAC Process Rules (optional)	
X9.9-1	ANSI X9.9-1 and X9.19 basic procedure. The *key_identifier* parameter must identify a single-length MAC or a single-length DATA key. X9.9-1 causes the MAC to be computed from all of the data. The text is padded only if the text length is not a multiple of 8 bytes. If padding is required, the pad character X'00' is used. This is the default value.
X9.19OPT	ANSI X9.19 optional double key MAC procedure. The *key_identifier* parameter must identify a double-length MAC key. The padding rules are the same as for X9.9-1.
EMVMAC	EMV padding rule with a single-length MAC key. The *key_identifier* parameter must identify a single-length MAC or a single-length DATA key. The text is always padded with 1 to 8 bytes so that the resulting text length is a multiple of 8 bytes. The first pad character is X'80'. The remaining 0 to 7 pad characters are X'00'.
EMVMACD	EMV padding rule with a double-length MAC key. The *key_identifier* parameter must identify a double-length MAC key. The padding rules are the same as for EMVMAC.
Segmenting Control (optional)	
ONLY	Only call; segmenting is not employed by the application program. This is the default value.
FIRST	First call, this is the first segment of data from the application program.
MIDDLE	Middle call; this is an intermediate data segment.
LAST	Last call; this is the last data segment.
MAC Length and Presentation (optional)	
MACLEN4	Generates a 4-byte MAC value. This is the default value.
MACLEN6	Generates a 6-byte MAC value.
MACLEN8	Generates an 8-byte MAC value.
HEX-8	Generates a 4-byte MAC value and presents it as 8 hexadecimal characters.
HEX-9	Generates a 4-byte MAC value and presents it as 2 groups of 4 hexadecimal characters with a space between the groups.

chaining_vector

Direction: Input/Output   Type: String

An 18-byte string that ICSF uses as a system work area. Your application program must not change the data in this string. The chaining vector permits data to be chained from one invocation call to another.

On the first call, initialize this parameter as binary zeros.

mac

Direction: Output	Type: String

The 8-byte or 9-byte field in which the callable service returns the MAC value if the segmenting rule is ONLY or LAST. Allocate an 8-byte field for MAC values of 4 bytes, 6 bytes, 8 bytes, or HEX-8. Allocate a 9-byte MAC field if you specify HEX-9 in the *rule_array* parameter.

text_id_in

Direction: Input	Type: Integer

For CSNBMGN1 only, the ALET of the text for which the MAC is generated.

Restrictions

To use double-length MAC keys on hardware available prior to the S/390 G5 Enterprise Server, the system must be DES-enabled and the NOCV-enablement keys must be installed in the CKDS.

Usage Notes

To use a DATA key, the NOCV-enablement keys must be present in the CKDS. Using a DATA key instead of a MAC generation key in this service substantially increases the path length for generating the MAC.

To calculate a MAC in one call, specify the ONLY keyword for segmenting control for the *rule_array* parameter. For two or more calls, specify the FIRST keyword for the first input block, the MIDDLE keyword for intermediate blocks (if any), and the LAST keyword for the last block.

For a given text string, the resulting MAC is the same whether the text is segmented or not.

Related Information

For more information about MAC processing rules and segmenting control, refer to *IBM Common Cryptographic Architecture: Cryptographic Application Programming Interface Reference*.

The MAC verification callable service is described in “MAC Verification (CSNBMVR and CSNBMVR1)” on page 152.

MAC Verification (CSNBMVR and CSNBMVR1)

Use the MAC verification callable service to verify a 4-, 6-, or 8-byte message authentication code (MAC) for an application-supplied text string. You can specify that the callable service uses either the ANSI X9.9-1 procedure or the ANSI X9.19 optional double key MAC procedure to compute the MAC. For the ANSI X9.9-1 procedure you identify either a MAC verification key, a MAC generation key, or a DATA key, and the message text. For the ANSI X9.19 optional double key MAC procedure, you identify either a double-length MAC verification key or a double-length MAC generation key and the message text. The cryptographic feature compares the generated MAC with the one sent with the message. A return code indicates whether the MACs are the same. If the MACs are the same, the receiver knows the message was not altered. The generated MAC never appears in storage is not revealed outside the cryptographic feature.

The MAC verification callable service also supports the padding rules specified in the EMV Specification.

Choosing Between CSNBMVR and CSNBMVR1

CSNBMVR and CSNBMVR1 provide identical functions. When choosing which service to use, consider the following:

- **CSNBMVR** requires the application-supplied text to reside in the caller's primary address space. Also, a program using CSNBMVR adheres to the IBM Common Cryptographic Architecture: Cryptographic Application Programming Interface.
- **CSNBMVR1** allows the application-supplied text to reside either in the caller's primary address space or in a data space. This can allow you to verify more data with one call. However, a program using CSNBMVR1 does not adhere to the IBM Common Cryptographic Architecture: Cryptographic Application Programming Interface, and may need to be modified before it can run with other cryptographic products that follow this programming interface.

  For CSNBMVR1, *text_id_in* is an access list entry token (ALET) parameter of the data space containing the application-supplied text.

Format

```
CALL CSNBMVR(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             key_identifier,
             text_length,
             text,
             rule_array_count,
             rule_array,
             chaining_vector,
             mac )
```

```
CALL CSNBMVR1(
              return_code,
              reason_code,
              exit_data_length,
              exit_data,
              key_identifier,
              text_length,
              text,
              rule_array_count,
              rule_array,
              chaining_vector,
              mac,
              text_id_in )
```

Parameters

return_code

Direction: Output   Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output   Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output   Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output   Type: String

The data that is passed to the installation exit.

key_identifier

Direction: Input/Output

The 64-byte key label or internal key token that identifies a single-length or double-length MAC verification key, a single-length or double-length MAC generation key or a single-length DATA key. The type of key depends on the MAC process rule in the *rule_array* parameter.

text_length

Direction: Input Type: Integer

The length of the clear text you supply in the *text* parameter. The MAXLEN keyword in the options file determines the maximum length of the text. (See the *OS/390 ICSF System Programmer's Guide* for a description of the MAXLEN keyword in the options file.) If the *text_length* parameter is not a multiple of 8 bytes and if the ONLY or LAST keyword of the *rule_array* parameter is called, the text is padded with binary zeros.

text

Direction: Input Type: String

The application-supplied text for which the MAC is verified.

rule_array_count

Direction: Input Type: Integer

The number of keywords specified in the *rule_array* parameter. The value can be 0, 1, 2, or 3.

rule_array

Direction: Input Type: Character string

Zero to three keywords that provide control information to the callable service. The keywords are shown in Table 27. The keywords must be in 24 bytes of contiguous storage with each of the keywords left-justified in its own 8-byte location and padded on the right with blanks. For example,

```
'X9.9-1  MIDDLE  MACLEN4 '
```

The order of the *rule_array* keywords is not fixed.

You can specify one of the MAC processing rules and then choose one of the segmenting control keywords and one of the MAC length keywords.

Table 27. Keywords for MAC Verification Control Information

Keyword	Meaning
MAC Process Rules (optional)	
X9.9-1	ANSI X9.9-1 and X9.19 basic procedure. The *key_identifier* parameter must identify a single-length MAC, MACVER, or DATA key. X9.9-1 causes the MAC to be computed from all of the data. The text is padded only if the text length is not a multiple of 8 bytes. If padding is required, the pad character X'00' is used. This is the default value.
X9.19OPT	ANSI X9.19 optional double-length MAC procedure. The *key_identifier* parameter must identify a double-length MAC or MACVER key. The padding rules are the same as for X9.9-1.

Table 27. Keywords for MAC Verification Control Information (continued)

Keyword	Meaning
EMVMAC	EMV padding rule with a single-length MAC key. The *key_identifier* parameter must identify a single-length MAC, MACVER, or DATA key. The text is always padded with 1 to 8 bytes so that the resulting text length is a multiple of 8 bytes. The first pad character is X'80'. The remaining 0 to 7 pad characters are X'00'.
EMVMACD	EMV padding rule with a double-length MAC key. The *key_identifier* parameter must identify a double-length MAC or MACVER key. The padding rules are the same as for EMVMAC.
Segmenting Control (optional)	
ONLY	Only call; the application program does not employ segmenting. This is the default value.
FIRST	First call; this is the first segment of data from the application program.
MIDDLE	Middle call; this is an intermediate data segment.
LAST	Last call; this is the last data segment.
MAC Length and Presentation (optional)	
MACLEN4	Verifies a 4-byte MAC value. This is the default value.
MACLEN6	Verifies a 6-byte MAC value.
MACLEN8	Verifies an 8-byte MAC value.
HEX-8	Verifies a 4-byte MAC value that is represented as 8 hexadecimal characters.
HEX-9	Verifies a 4-byte MAC value that is represented as 2 groups of 4 hexadecimal characters with a space character between the groups.

chaining_vector

Direction: Input/Output Type: String

An 18-byte string that ICSF uses as a system work area. Your application program must not change the data in this string. The chaining vector permits data to be chained from one invocation call to another.

On the first call, initialize this parameter to binary zeros.

mac

Direction: Input Type: String

The 8- or 9-byte field that contains the MAC value you want to verify. The value in the field must be left-justified and padded with zeros. If you specified the HEX-9 keyword in the *rule_array* parameter, the input MAC is 9 bytes.

text_id_in

Direction: Input Type: Integer

For CSNBMVR1 only, the ALET of the text for which the MAC is to be verified.

Restrictions

To use double-length MACVER keys, this service must be run on an S/390 G5 Enterprise Server or above; otherwise, the service returns a return code of 12 with a reason code of 8.

Usage Notes

To verify a MAC in one call, specify the ONLY keyword on the segmenting rule keyword for the *rule_array* parameter. For two or more calls, specify the FIRST keyword for the first input block, MIDDLE for intermediate blocks (if any), and LAST for the last block.

For a given text string, the MAC resulting from the verification process is the same regardless of how the text is segmented, or how it was segmented when the original MAC was generated.

To use a MAC generation key or a DATA key, the NOCV enablement keys must be present in the CKDS. Using either a MAC generation key or a DATA key instead of a MAC verification key in this service substantially increases the path length for verifying the MAC.

Related Information

For more information about MAC processing rules and segmenting control, refer to *IBM Common Cryptographic Architecture: Cryptographic Application Programming Interface Reference*.

The MAC generation callable service is described in “MAC Generation (CSNBMGN and CSNBMGN1)” on page 147.

MDC Generation (CSNBMDG and CSNBMDG1)

A modification detection code (MDC) can be used to provide a form of support for data integrity.

Use the MDC Generation callable service to generate a 128-bit modification detection code (MDC) for an application-supplied text string.

The returned MDC value should be securely stored and/or sent to another user. To validate the integrity of the text string at a later time, the MDC Generation callable service is again used to generate a 128-bit MDC. The new MDC value is compared with the original MDC value. If the values are equal, the text is accepted as unchanged.

Choosing Between CSNBMDG and CSNBMDG1

CSNBMDG and CSNBMDG1 provide identical functions. When choosing which service to use, consider the following:

- **CSNBMDG** requires the application-supplied text to reside in the caller’s primary address space. Also, a program using CSNBMDG adheres to the IBM Common Cryptographic Architecture: Cryptographic Application Programming Interface.
- **CSNBMDG1** allows the application-supplied text to reside either in the caller’s primary address space or in a data space. This can allow you to process more data with one call. However, a program using CSNBMDG1 does not adhere to

the IBM Common Cryptographic Architecture: Cryptographic Application Programming Interface and may need to be modified before it can run with other cryptographic products that follow this programming interface.

For CSNBMDG1, *text_id_in* parameter specifies the access list entry token (ALET) for the data space containing the application-supplied text.

Format

```
CALL CSNBMDG(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             text_length,
             text,
             rule_array_count,
             rule_array,
             chaining_vector,
             mdc )
```

```
CALL CSNBMDG1(
              return_code,
              reason_code,
              exit_data_length,
              exit_data,
              text_length,
              text,
              rule_array_count,
              rule_array,
              chaining_vector,
              mdc,
              text_id_in )
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. "Appendix A. ICSF and TSS Return and Reason Codes" on page 319 lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. "Appendix A. ICSF and TSS Return and Reason Codes" on page 319 lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

text_length

Direction: Input	Type: Integer

The length of the text you supply in the *text* parameter.

The MAXLEN keyword in the options file determines the maximum length of the text for this call. (See *OS/390 ICSF System Programmer's Guide* for a description of the MAXLEN keyword in the options file.)

Additional restrictions on length of the text depend on whether padding of the text is requested, and on the segmenting control used.

- When padding is requested (by specifying a process rule of PADMDC-2 or PADMDC-4 in the *rule_array* parameter), a text length of 0 is valid for any segment control specified in the *rule_array* parameter (FIRST, MIDDLE, LAST, or ONLY). When LAST or ONLY is specified, the supplied text will be padded with X'FF's and a padding count in the last byte to bring the total text length to the next multiple of 8 that is greater than or equal to 16,
- When no padding is requested (by specifying a process rule of MDC-2 or MDC-4), the total length of the text provided (over a single or segmented calls) must be at least 16 bytes, and a multiple of 8.

  For segmented calls with no padding, text length of 0 is valid on any of the calls provided the total length over the segmented calls is at least 16 and a multiple of 8.

  For a single call (that is, segment control is ONLY) with no padding, the length the text provided must be at least 16, and a multiple of 8.

text

Direction: Input	Type: String

The application-supplied text for which the MDC is generated.

rule_array_count

Direction: Input	Type: Integer

The number of keywords specified in the *rule_array* parameter. This value must be 2.

rule_array

Direction: Input	Type: Character string

The two keywords that provide control information to the callable service are shown in Table 28. The two keywords must be in 16 bytes of contiguous storage with each of the two keywords left-justified in its own 8-byte location and padded on the right with blanks. For example,

```
'MDC-2   FIRST   '
```

Choose one of the MDC process rule control keywords and one of the segmenting control keywords from the following table.

Table 28. Keywords for MDC Generation Control Information

Keyword	Meaning
MDC Process Rules (required)	
MDC-2	MDC-2 specifies two encipherments per 8 bytes of input text and no padding of the input text.
MDC-4	MDC-4 specifies four encipherments per 8 bytes of input text and no padding of the input text.
PADMDC-2	PADMDC-2 specifies two encipherments per 8 bytes of input text and padding of the input text. When the segment rule specifies ONLY or LAST, the input text is padded with X'FF's and a padding count in the last byte to bring the total text length to the next even multiple of 8 that is greater than, or equal to, 16.
PADMDC-4	PADMDC-4 specifies four encipherments per 8 bytes of input text and padding of the input text. When the segment rule specifies ONLY or LAST, the input text is padded with X'FF's and a padding count in the last byte to bring the total text length to the next even multiple of 8 that is greater than, or equal to, 16.
Segmenting Control (required)	
ONLY	Only call; segmenting is not employed by the application program.
FIRST	First call; this is the first segment of data from the application program.
MIDDLE	Middle call; this is an intermediate data segment.
LAST	Last call; this is the last data segment.

chaining_vector

Direction: Input/Output	Type: String

An 18-byte string that ICSF uses as a system work area. Your application program must not change the data in this string. The chaining vector permits data to be chained from one invocation call to another.

On the first call, initialize this parameter as binary zeros.

mdc

Direction: Input/Output	Type: String

A 16-byte field in which the callable service returns the MDC value when the segmenting rule is ONLY or LAST. When the segmenting rule is FIRST or

MIDDLE, the value returned in this field is an intermediate MDC value that will be used as input for a subsequent call and must not be changed by the application program.

text_id_in

Direction: Input	Type: Integer

For CSNBMDG1 only, the ALET for the data space containing the text for which the MDC is to be generated.

Usage Notes

To calculate an MDC in one call, specify the ONLY keyword for segmenting control in the *rule_array* parameter. For more than one call, specify the FIRST keyword for the first input block, the MIDDLE keyword for any intermediate blocks, and the LAST keyword for the last block. For a given text string, the resulting MDC is the same whether the text is segmented or not.

The two versions of MDC calculation (with two or four encipherments per 8 bytes of input text) allow the caller to trade a performance improvement for a decrease in security. Since 2 encipherments create results different from the results of 4 encipherments, ensure that you use the same number of encipherments to verify the MDC value.

Related Information

The MAC generation service, using a publicly known key, can be used similarly to the MDC generation service, while providing better performance. The cryptographic work factor to break a MAC generated with a publicly known key, although much less than that for MDC generation, may be enough for some applications.

One-Way Hash Generate (CSNBOWH and CSNBOWH1)

Use the one-way hash generate callable service to generate a one-way hash on specified text. This service supports the following methods:

- MD5
- SHA-1

Note: MDC-2, MDC-4, PADMDC-2 and PADMDC-4 are supported through the MDC generation service (see “MDC Generation (CSNBMDG and CSNBMDG1)” on page 156).

Format

```
CALL CSNBOWH(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            text_length,
            text,
            chaining_vector_length,
            chaining_vector,
            hash_length,
            hash)
```

```
CALL CSNBOWH1(
              return_code,
              reason_code,
              exit_data_length,
              exit_data,
              rule_array_count,
              rule_array,
              text_length,
              text,
              chaining_vector_length,
              chaining_vector,
              hash_length,
              hash,
              text_id_in)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you are supplying in the *rule_array* parameter. The value must be 1 or 2.

rule_array

Direction: Input Type: String

Keywords that provide control information to the callable service are listed in Table 29. The optional chaining flag keyword indicates whether calls to this service are chained together logically to overcome buffer size limitations. Each keyword is left-justified in an 8-byte field and padded on the right with blanks. All keywords must be in contiguous storage.

Table 29. Keywords for One-Way Hash Generate Rule Array Control Information

Keyword	Meaning
Hash Method (required)	
MD5	Hash algorithm is MD5 algorithm. Use this hash method for PKCS-1.0 and PKCS-1.1. Length of hash generated is 16 bytes.
SHA-1	Hash algorithm is SHA-1 algorithm. Use this hash method for DSS. Length of hash generated is 20 bytes.
Chaining Flag (optional)	
FIRST	Specifies this is the first call in a series of chained calls. Intermediate results are stored in the *hash* field.
MIDDLE	Specifies this is a middle call in a series of chained calls. Intermediate results are stored in the *hash* field.
LAST	Specifies this is the last call in a series of chained calls.
ONLY	Specifies this is the only call and the call is not chained. This is the default.

text_length

Direction: Input Type: Integer

The length of the *text* parameter in bytes.

Note: If you specify the FIRST or MIDDLE keyword, then the text length must be a multiple of the blocksize of the hash method. For MD5 and SHA-1, this is a multiple of 64 bytes.

For ONLY and LAST, this service performs the required padding according to the algorithm specified.

text

Direction: Input Type: String

The application-supplied text on which this service performs the hash.

chaining_vector_length

Direction: Input Type: Integer

The byte length of the *chaining_vector* parameter. This must be 128 bytes.

chaining_vector

Direction: Input/Output Type: String

This field is a 128-byte work area. Your application must not change the data in this string. The chaining vector permits chaining data from one call to another.

hash_length

Direction: Input	Type: Integer

The length of the supplied *hash* field in bytes.

Note: For SHA-1 this must be at least 20 bytes; for MD5 this must be at least 16 bytes.

hash

Direction: Input/Output	Type: String

This field contains the hash, left-justified. The processing of the rest of the field depends on the implementation. If you specify the FIRST or MIDDLE keyword, this field contains the intermediate hash value. Your application must not change the data in this field between the sequence of FIRST, MIDDLE, and LAST calls for a specific message.

text_id_in

Direction: Input	Type: Integer

For CSNBOWH1 only, the ALET for the data space containing the text for which to generate the hash.

Usage Note

Although MD5 and SHA-1 allow it, bit length text is not supported for any hashing method.

VISA CVV Service Generate (CSNBCSG)

Use the VISA CVV Service Generate callable service to generate a VISA Card Verification Value (CVV) or MasterCard Card Verification Code (CVC) as defined for track 2. This service generates a CVV that is based upon the information that the *PAN_data*, the *expiration_date*, and the *service_code* parameters provide. The service uses the Key-A and the Key-B keys to cryptographically process this information. If the input values for Key-A and Key-B are not both single-length data keys, they will be routed to the PCI Cryptographic Coprocessor for processing. The PCI Cryptographic Coprocessor will allow Key-A and Key-B to be single-length MAC keys. If the requested CVV is shorter than 5 characters, the CVV is padded on the right by space characters. The CVV is returned in the 5-byte variable that the *CVV_value* parameter identifies. When you verify a CVV, compare the result to the value that the *CVV_value* supplies.

Format

```
CALL CSNBCSG(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            PAN_data,
            expiration_date,
            service_code,
            CVV_key_A_Identifier,
            CVV_key_B_Identifier,
            CVV_value)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Section Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicates specific processing problems. Section Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you are supplying in the *rule_array* parameter. The parameter *rule_array_count* must be 0, 1, or 2.

rule_array

Direction: Input Type: String

Keywords that provide control information to the callable service. Each keyword is left-justified in 8-byte fields, and padded on the right with blanks. All keywords must be in contiguous storage.

Table 30. CVV_Generate rule_array Keywords

Keyword	Meaning
PAN data length (optional)	
PAN-13	Specifies that the length of the PAN data is 13 bytes. **PAN-13 is the default value.**
PAN-16	Specifies that the length of the PAN data is 16 bytes.
CVV length (optional)	
CVV-1	Specifies that the CVV is to be computed as one byte, followed by 4 blanks. **CVV-1 is the default value.**
CVV-2	Specifies that the CVV is to be computed as 2 bytes, followed by 3 blanks.
CVV-3	Specifies that the CVV is to be computed as 3 bytes, followed by 2 blanks.
CVV-4	Specifies that the CVV is to be computed as 4 bytes, followed by 1 blank.
CVV-5	Specifies that the CVV is to be computed as 5 bytes.

PAN_data

Direction: Input Type: String

The *PAN_data* parameter specifies an address that points to the place in application data storage that contains personal account number (PAN) information in character form. The PAN is the account number as defined for the track-2 magnetic-stripe standards. If the **PAN-13** keyword is specified in the rule array, 13 characters are processed; if the **PAN-16** keyword is specified in the rule array, 16 characters are processed.

Even if you specify the **PAN-13** keyword, the server might copy 16 bytes to a work area. Therefore ensure that the verb can address 16 bytes of storage.

expiration_date

Direction: Input Type: String

The *expiration_date* parameter specifies an address that points to the place in application data storage that contains the card expiration date in numeric character form in a 4-byte field. The application programmer must determine whether the CVV will be calculated with the date form of YYMM or MMYY.

service_code

Direction: Input Type: String

The *service_code* parameter specifies an address that points to the place in application data storage that contains the service code in numeric character form in a 3-byte field. The service code is the number that the track-2 magnetic-stripe standards define. The service code of '000' is supported.

CVV_key_A_Identifier

Direction: Input/Output	Type: String

The *CVV_key_A_Identifier* parameter specifies an address that contains a 64-byte internal key token or a key label of an internal key token record in key storage. The internal key token contains the key-A key that encrypts information in the CVV process.

CVV_key_B_Identifier

Direction: Input/Output	Type: String

The *CVV_key_B_Identifier* parameter specifies an address that contains a 64-byte internal key token or a key label of an internal key token record in key storage. The internal key token contains the key-B key that decrypts information in the CVV process.

CVV_value

Direction: Output	Type: String

The *CVV_value* parameter specifies an address that points to the place in application data storage that will be used to store the computed 5-byte character output value.

Restriction

The CVV Generate verb is not supported on CDMF-only configurations.

VISA CVV Service Verify (CSNBCSV)

Use the VISA CVV service verify callable service to verify a VISA Card Verification Value (CVV) or MasterCard Card Verification Code (CVC) as defined for track 2. This service generates a CVV that is based upon the information that the *PAN_data*, the *expiration_date*, and the *service_code* parameters provide. The service uses the Key-A and the Key-B keys to cryptographically process this information. If the input values for Key-A and Key-B are not both single-length data keys, they will be routed to the PCI Cryptographic Coprocessor for processing. The PCI Cryptographic Coprocessor will allow Key-A and Key-B to be single-length MAC or MACVER keys. If the requested CVV is shorter than 5 characters, the CVV is padded on the right by space characters. The generated CVV is then compared to the value that the *CVV_value* supplies for verification.

Format

```
CALL CSNBCSV(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             rule_array_count,
             rule_array,
             PAN_data,
             expiration_date,
             service_code,
             CVV_key_A_Identifier,
             CVV_key_B_Identifier,
             CVV_value)
```

Parameters

return_code

Direction: Output   Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output   Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicates specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output   Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output   Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input   Type: Integer

The number of keywords you are supplying in the *rule_array* parameter. The parameter *rule_array_count* must be 0, 1, or 2.

rule_array

Direction: Input Type: String

Keywords that provide control information to the callable service. Each keyword is left-justified in 8-byte fields, and padded on the right with blanks. All keywords must be in contiguous storage.

Table 31. CVV_Verify rule_array Keywords

Keyword	Meaning
PAN data length (optional)	
PAN-13	Specifies that the length of the PAN data is 13 bytes. **PAN-13 is the default value.**
PAN-16	Specifies that the length of the PAN data is 16 bytes.
CVV length (optional)	
CVV-1	Specifies that the CVV is to be computed as one byte, followed by 4 blanks. **CVV-1 is the default value.**
CVV-2	Specifies that the CVV is to be computed as 2 bytes, followed by 3 blanks.
CVV-3	Specifies that the CVV is to be computed as 3 bytes, followed by 2 blanks.
CVV-4	Specifies that the CVV is to be computed as 4 bytes, followed by 1 blank.
CVV-5	Specifies that the CVV is to be computed as 5 bytes.

PAN_data

Direction: Input Type: String

The *PAN_data* parameter specifies an address that points to the place in application data storage that contains personal account number (PAN) information in character form. The PAN is the account number as defined for the track-2 magnetic-stripe standards. If the **PAN-13** keyword is specified in the rule array, 13 characters are processed; if the **PAN-16** keyword is specified in the rule array, 16 characters are processed.

Even if you specify the **PAN-13** keyword, the server might copy 16 bytes to a work area. Therefore ensure that the verb can address 16 bytes of storage.

expiration_date

Direction: Input Type: String

The *expiration_date* parameter specifies an address that points to the place in application data storage that contains the card expiration date in numeric character form in a 4-byte field. The application programmer must determine whether the CVV will be calculated with the date form of YYMM or MMYY.

service_code

Direction: Input Type: String

The *service_code* parameter specifies an address that points to the place in application data storage that contains the service code in numeric character form in a 3-byte field. The service code is the number that the track-2 magnetic-stripe standards define. The service code of ’000’ is supported.

CVV_key_A_Identifier

Direction: Input/Output	Type: String

The *CVV_key_A_Identifier* parameter specifies an address that contains a 64-byte internal key token or a key label of an internal key token record in key storage. The internal key token contains the key-A key that encrypts information in the CVV process.

CVV_key_B_Identifier

Direction: Input/Output	Type: String

The *CVV_key_B_Identifier* parameter specifies an address that contains a 64-byte internal key token or a key label of an internal key token record in key storage. The internal key token contains the key-B key that decrypts information in the CVV process.

CVV_value

Direction: Input	Type: String

The *CVV_value* parameter specifies an address that contains the CVV value which will be compared to the computed CVV value.

Restrictions

The CVV Verify verb is not supported on CDMF-only configurations.

Chapter 10. Managing Personal Identification Numbers

The process of validating personal identities in a financial transaction system is called *personal authentication*. The personal identification number (PIN) is the basis for verifying the identity of a customer across financial industry networks. ICSF provides callable services to translate, verify, and generate PINs. You can use the callable services to prevent unauthorized disclosures when organizations handle PINs.

The following callable services are described in the following topics:

- “Clear PIN Generate (CSNBPGN)” on page 175
- “Encrypted PIN Generate (CSNBEPG)” on page 179
- “Clear PIN Encrypt (CSNBCPE)” on page 183
- “Clear PIN Generate Alternate (CSNBCPA)” on page 186
- “Encrypted PIN Verification (CSNBPVR)” on page 191
- “Encrypted PIN Translation (CSNBPTR)” on page 197

How Personal Identification Numbers (PINs) are Used

Many people are familiar with PINs, which allow them to use an automated teller machine (ATM). From the system point of view, PINs are used primarily in financial networks to authenticate users — typically, a user is assigned a PIN, and enters the PIN at automated teller machines (ATMs) to gain access to his or her accounts. It is extremely important that the PIN be kept private, so that no one other than the account owner can use it. ICSF allows your applications to generate PINs, to verify supplied PINs, and to translate PINs from one format to another.

Translating Data and PINs in Networks

More and more data is being transmitted across networks where, for various reasons, the keys used on one network cannot be used on another network. Encrypted data and PINs that are transmitted across these boundaries must be “translated” securely from encryption under one key to encryption under another key. For example, a traveler visiting a foreign city might wish to use an ATM to access an account at home. The PIN entered at the ATM might need to be encrypted at the ATM and sent over one or more financial networks to the traveler’s home bank. At the home bank, the PIN must be verified before access is allowed. On intermediate systems (between networks), applications can use the Encrypted PIN translate callable service to re-encrypt a PIN block from one key to another. Running on ICSF, such applications can ensure that PINs never appear in the clear and that the PIN-encrypting keys are isolated on their own networks.

PIN Callable Services

You use the PIN callable services to generate, verify, and translate PINs. This section discusses the PIN callable services, as well as the various PIN algorithms and PIN block formats supported by ICSF. It also explains the use of PIN-encrypting keys.

Generating a PIN

To generate personal identification numbers, call the Clear PIN Generate or Encrypted PIN Generate callable service. Using a PIN generation algorithm, data used in the algorithm, and the PIN generation key, the Clear PIN generate callable service generates a clear PIN and a PIN verification value, or offset. The Clear PIN

Generate callable service can only execute in special secure mode. For a description of this mode, see “Special Secure Mode” on page 9. Using a PIN generation algorithm, data used in the algorithm, the PIN generation key, and an outbound PIN encrypting key, the encrypted PIN generate callable service generates and formats a PIN and encrypts the PIN block.

Encrypting a PIN

To format a PIN into a supported PIN block format and encrypt the PIN block, call the Clear PIN encrypt callable service.

Generating a PIN Validation Value from an Encrypted PIN Block

To generate a clear VISA PIN validation value (PVV) from an encrypted PIN block, call the *clear PIN generate alternate* callable service. The PIN block can be encrypted under an input PIN-encrypting key (IPINENC) or an output PIN encrypting key (OPINENC). Using an IPINENC key requires that NOCV keys are enabled in the CKDS.

Verifying a PIN

To verify a supplied PIN, call the *Encrypted PIN verify* callable service. You supply the enciphered PIN, the PIN-encrypting key that enciphers the PIN, and other data. You must also specify the PIN verification key and PIN verification algorithm. The callable service generates a verification PIN. The service compares the two personal identification numbers and if they are the same, it verifies the supplied PIN.

Translating a PIN

To translate a PIN block format from one PIN-encrypting key to another or from one PIN block format to another, call the *Encrypted PIN translate* callable service. You must identify the input PIN-encrypting key that originally enciphered the PIN. You also need to specify the output PIN-encrypting key that you want the callable service to use to encipher the PIN. If you want to change the PIN block format, specify a different output PIN block format from the input PIN block format.

Algorithms for Generating and Verifying a PIN

ICSF supports the following algorithms for generating and verifying personal identification numbers:
- IBM 3624 institution-assigned PIN
- IBM 3624 customer-selected PIN (through a PIN offset)
- IBM German Bank Pool PIN (verify through an institution key)
- IBM German Bank Pool PIN (verify through a pool key and a PIN offset). This algorithm is supported when the service using the PIN is processed on the Cryptographic Coprocessor Feature.
- VISA PIN through a VISA PIN validation value
- Interbank PIN

The algorithms are discussed in detail in Appendix D. PIN Formats and Algorithms.

Using PINs on Different Systems

ICSF allows you to translate different PIN block formats, which lets you use personal identification numbers on different systems. ICSF supports the following formats:
- IBM 3624

- IBM 3621 (same as IBM 5906)
- IBM 4704 encrypting PINPAD format
- ISO 0 (same as ANSI 9.8, VISA 1, and ECI 1)
- ISO 1 (same as ECI 4)
- ISO 2
- VISA 2
- VISA 3
- VISA 4
- ECI 2
- ECI 3

The formats are discussed in “Appendix D. PIN Formats and Algorithms” on page 359.

PIN-Encrypting Keys

A unique master key variant enciphers each type of key. For further key separation, an installation can choose to have each PIN block format enciphered under a different PIN-encrypting key. The PIN-encrypting keys can have a 16-byte PIN block variant constant exclusive ORed on them before they are used to translate or verify PIN blocks. This is specified in the format control field in the Encrypted PIN translate and Encrypted PIN verify callable services.

You should only use PIN block variant constants when you are communicating with another host processor with the Integrated Cryptographic Service Facility.

For more information about PIN-encrypting keys, see *OS/390 ICSF Administrator’s Guide*.

The PIN Profile

The PIN profile consists of the following:
- PIN block format
- Format control
- Pad digit

Table 32 shows the format of a PIN profile.

Table 32. Format of a PIN Profile

Bytes	Description
0–7	PIN block format
8–15	Format control
16–23	Pad digit

PIN Block Format

This keyword specifies the format of the PIN block. The 8-byte value must be left-justified and padded with blanks. Refer to Table 33 for a list of valid values.

Table 33. Format Values of PIN Blocks

Format Value	Description
ISO-0	ISO format 0, ANSI X9.8, VISA 1, and ECI 1
ISO-1	ISO format 1 and ECI 4
ISO-2	ISO format 2

Table 33. Format Values of PIN Blocks (continued)

Format Value	Description
VISA-2	VISA format 2
VISA-3	VISA format 3
VISA-4	VISA format 4
4704-EPP	IBM 4704 with encrypting PIN pad
3624	IBM 3624
3621	IBM 3621 and 5906
ECI-2	Eurocheque International format 2
ECI-3	Eurocheque International format 3

Format Control

This keyword specifies whether there is any control on the user-supplied PIN format. The 8-byte value must be left-justified and padded with blanks. Specify one of the following values:

NONE No format control.

PBVC A PIN block variant constant (PBVC) enforces format control. Use the PBVC value only if you have coded PBVC in the encrypted PIN translate callable service. For the PBVC, the clear PIN key-encrypting key has been exclusive ORed with one of the PIN block formats. The cryptographic feature removes the pattern from the clear PIN key-encrypting key before it decrypts the PIN block.

Notes:

1. Only control vectors and extraction methods valid for the Cryptographic Coprocessor Feature may be used if the PBVC format control is desired.
2. PBVC is supported for compatibility with prior releases of OS/390 ICSF and existing ICSF applications. It is recommended that a format control of NONE be specified.

If you do not specify a value for the format control parameter, ICSF uses hexadecimal zeros.

Table 48 on page 190 lists the PIN block variant constants.

Pad Digit

Some PIN formats require this parameter. If the PIN format does not need a pad digit, the callable service ignores this parameter. Table 34 shows the format of a pad digit. The PIN profile pad digit must be specified in upper case.

Table 34. Format of a Pad Digit

Bytes	Description
16–22	Seven space characters
23	Character representation of a hexadecimal pad digit or a space if a pad digit is not needed. Characters must be one of the following: 0–9, A–F, or a blank.

Each PIN format supports only a pad digit in a certain range. Refer to “The PIN Profile” on page 173 for a list of the valid pad digits for each PIN block format.

Table 35. Pad Digits for PIN Block Formats

PIN Block Format	Output PIN Profile	Input PIN Profile
ISO-0	F	Pad digit is not used
ISO-1	Pad digit is not used	Pad digit is not used
ISO-2	Pad digit is not used	Pad digit is not used
VISA-2	0 through 9	Pad digit is not used
VISA-3	0 through F	Pad digit is not used
VISA-4	F	Pad digit is not used
3624	0 through F	0 through F
3621	0 through F	0 through F
4704-EPP	F	Pad digit is not used
ECI-2	Pad digit is not used	Pad digit is not used
ECI-3	Pad digit is not used	Pad digit is not used

Recommendations for the Pad Digit

IBM recommends that you use a nondecimal pad digit in the range of A through F when processing IBM 3624 and IBM 3621 PIN blocks. If you use a decimal pad digit, the creator of the PIN block must ensure that the calculated PIN does not contain the pad digit, or unpredictable results may occur.

For example, you can exclude a specific decimal digit from being in any calculated PIN by using the IBM 3624 calculation procedure and by specifying a decimalization table that does not contain the desired decimal pad digit.

Clear PIN Generate (CSNBPGN)

Use the Clear PIN generate callable service to generate a clear PIN, a PIN validation value (PVV), or an offset according to an algorithm. You supply the algorithm or process rule using the *rule_array* parameter.
- IBM 3624 (IBM-PIN or IBM-PINO)
- IBM German Bank Pool (GBP-PIN or GBP-PINO)
- VISA PIN validation value (VISA-PVV)
- Interbank PIN (INBK-PIN)

The callable service can execute only when ICSF is in special secure mode. This mode is described in “Special Secure Mode” on page 9.

For guidance information about VISA, see their appropriate publications. The Interbank PIN algorithm is available only on S/390 G3, or higher, Enterprise Servers and S/390 Multiprise Servers.

ICSF routes the Clear PIN Generate request to a PCI Cryptographic Coprocessor if the control vector of the PIN generating key cannot be processed on the Cryptographic Coprocessor Feature. If no PCI Cryptographic Coprocessor is online in this case, the request fails.

Format

```
CALL CSNBPGN(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            PIN_generating_key_identifier,
            rule_array_count,
            rule_array,
            PIN_length,
            PIN_check_length,
            data_array,
            returned_result )
```

Parameters

return_code

Direction: Output Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFFF' (2 gigabytes). The data is defined in the *exit_data* parameter.

exit_data

Direction: Input/Output Type: String

The data that is passed to the installation exit.

PIN_generating_key_identifier

Direction: Input/Output Type: Character string

| The 64-byte key label or internal key token that identifies the PIN generation
| (PINGEN) key. If the *PIN_generating_key_identifier* identifies a key which does
| not have the default PIN generation key control vector, the request will be
| routed to a PCI Cryptographic Coprocessor.

rule_array_count

Direction: Input Type: Integer

The number of process rules specified in the *rule_array* parameter. The value must be 1.

rule_array

Direction: Input Type: Character string

The process rule provides control information to the callable service. Specify one of the values in Table 36. The keyword is left-justified in an 8-byte field, and padded on the right with blanks.

Table 36. Process Rules for the Clear PIN Generate Callable Service

Process Rule	Description
IBM-PIN	The IBM 3624 PIN, which is an institution-assigned PIN. It does not calculate the PIN offset.
IBM-PINO	The IBM 3624 PIN offset, which is a customer-selected PIN and calculates the PIN offset (the output).
GBP-PIN	The IBM German Bank Pool PIN, which uses the institution PINGEN key to generate an institution PIN (IPIN).
GBP-PINO	The IBM German Bank Pool PIN offset, which uses the pool PINGEN key to generate a pool PIN (PPIN). It uses the institution PIN (IPIN) as input and calculates the PIN offset, which is the output.
VISA-PVV	The VISA PIN validation value. Input is the customer PIN.
INBK-PIN	The Interbank PIN is generated.

PIN_length

Direction: Input Type: Integer

| The length of the PIN used for the IBM algorithms only, IBM-PIN or IBM-PINO.
| Otherwise, this parameter is ignored. Specify an integer from 4 through 16. If
| the length is greater than 12, the request will be routed to the PCI
| Cryptographic Coprocessor.

PIN_check_length

Direction: Input Type: Integer

The length of the PIN offset used for the IBM-PINO process rule only. Otherwise, this parameter is ignored. Specify an integer from 4 through 16.

Note: The PIN check length must be less than or equal to the integer specified in the *PIN_length* parameter.

data_array

Direction: Input Type: String

Three 16-byte data elements required by the corresponding *rule_array* parameter. The data array consists of three 16-byte fields or elements whose specification depends on the process rule. If a process rule only requires one or two 16-byte fields, then the rest of the data array is ignored by the callable service. Table 37 describes the array elements.

Table 37. Array Elements for the Clear PIN Generate Callable Service

Array Element	Description
Decimalization_table	Decimalization table for IBM and GBP only. Sixteen digits of 0 through 9.
Validation_data	Validation data for IBM and IBM German Bank Pool padded to 16 bytes. One to sixteen characters of hexadecimal account data left-justified and padded on the right with blanks.
Clear_PIN	Clear user selected PIN of 4 to 12 digits of 0 through 9. Left-justified and padded with spaces. For IBM-PINO, this is the clear customer PIN (CSPIN). For GBP-PINO, this is the institution PIN. For IBM-PIN and GBP-PIN, this field is ignored.
Trans_sec_parm	For VISA only, the leftmost sixteen digits. Eleven digits of the personal account number (PAN). One digit key index. Four digits of customer selected PIN. For Interbank only, sixteen digits. Eleven right-most digits of the personal account number (PAN). A constant of 6. One digit key selector index. Three digits of PIN validation data.

Table 38 lists the data array elements required by the process rule (*rule_array* parameter). The numbers refer to the process rule's position within the array.

Table 38. Array Elements Required by the Process Rule

Process Rule	IBM-PIN	IBM-PINO	GBP-PIN	GBP-PINO	VISA-PVV	INBK-PIN
Decimalization_table	1	1	1	1		
Validation_data	2	2	2	2		
Clear_PIN		3		3		
Trans_sec_parm					1	1

Note: Generate offset for GBP algorithm is equivalent to IBM offset generation with *PIN_check_length* of 4 and *PIN_length* of 6.

returned_result

Direction: Output   Type: Character string

The 16-byte generated output, left-justified and padded on the right with blanks.

| **Restriction**

| PIN lengths of 13-16 require the optional PCI Cryptographic Coprocessor.

Usage Note

If you are using the IBM 3624 PIN and IBM German Bank Pool PIN algorithms, you can supply an unencrypted customer selected PIN to generate a PIN offset.

Related Information

PIN algorithms are shown in Appendix D. PIN Formats and Algorithms.

Encrypted PIN Generate (CSNBEPG)

The Encrypted PIN Generate callable service formats a PIN and encrypts the PIN block. To generate the PIN, the service uses one of the following PIN calculation methods:
- IBM 3624 PIN
- IBM German Bank Pool Institution PIN
- Interbank PIN

To format the PIN, the service uses one of the following PIN block formats:
- IBM 3621 format
- IBM 3624 format
- ISO-0 format (same as the ANSI X9.8, VISA-1, and ECI-1 formats)
- ISO-1 format (same as the ECI-4 format)
- ISO-2 format
- IBM 4704 encrypting PINPAD (4704-EPP) format
- VISA 2 format
- VISA 3 format
- VISA 4 format
- ECI-2 format
- ECI-3 format

ICSF routes the Encrypted PIN Generate request to a PCI Cryptographic Coprocessor for processing. If no PCI Cryptographic Coprocessor is online, the request fails.

Format

```
CALL CSNBEPG(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            PIN_generating_key_identifier,
            outbound_PIN_encrypting_key_identifier
            rule_array_count,
            rule_array,
            PIN_length,
            data_array,
            PIN_profile,
            PAN_data,
            sequence_number
            encrypted_PIN_block )
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFFF' (2 gigabytes). The data is defined in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

PIN_generating_key_identifier

Direction: Input/Output	Type: String

The 64-byte internal key token or a key label of an internal key token in the CKDS. The internal key token contains the PIN-generating key. The control vector must specify the PINGEN key type and have the EPINGEN usage bit set to 1.

outbound_PIN_encrypting_key_identifier

Direction: Input	Type: String

A 64-byte internal key token or a key label of an internal key token in the CKDS. The internal key token contains the key to be used to encrypt the formatted PIN and must contain a control vector that specifies the OPINENC key type and has the EPINGEN usage bit set to 1.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you are supplying in the *rule_array* parameter. The value must be 1.

rule_array

Direction: Input	Type: Character string

Keywords that provide control information to the callable service. Each keyword is left-justified in an 8-byte field, and padded on the right with blanks. All keywords must be in contiguous storage. The rule array keywords are shown as follows:

Table 39. Process Rules for the Encrypted PIN Generate Callable Service

Process Rule	Description
IBM-PIN	This keyword specifies the IBM 3624 PIN calculation method is to be used to generate a PIN.
GBP-PIN	This keyword specifies the IBM German Bank Pool Institution PIN calculation method is to be used to generate a PIN.
INBK-PIN	This keyword specifies the Interbank PIN calculation method is to be used to generate a PIN.

PIN_length

Direction: Input Type: Integer

A integer defining the PIN length for those PIN calculation methods with variable length PINs; otherwise, the variable should be set to zero.

data_array

Direction: Input Type: String

Three 16-byte character strings, which are equivalent to a single 48-byte string. The values in the data array depend on the keyword for the PIN calculation method. Each element is not always used, but you must always declare a complete data array. The numeric characters in each 16-byte string must be from 1 to 16 bytes in length, uppercase, left-justified, and padded on the right with space characters. Table 40 describes the array elements.

Table 40. Array Elements for the Encrypted PIN Generate Callable Service

Array Element	Description
Decimalization_table	Decimalization table for IBM and GBP only. Sixteen characters that are used to map the hexadecimal digits (X'0' to X'F') of the encrypted validation data to decimal digits (X'0' to X'9').
Validation_data	Validation data for IBM and IBM German Bank Pool padded to 16 bytes. One to sixteen characters of hexadecimal account data left-justified and padded on the right with blanks.
Clear_PIN	Clear user selected PIN of 4 to 12 digits of 0 through 9. Left-justified and padded with spaces. For IBM-PINO, this is the clear customer PIN (CSPIN). For GBP-PINO, this is the institution PIN. For IBM-PIN and GBP-PIN, this field is ignored.
Trans_sec_parm	For Interbank only, sixteen digits. Eleven right-most digits of the personal account number (PAN). A constant of 6. One digit key selector index. Three digits of PIN validation data.

Encrypted PIN Generate (CSNBEPG)

Table 41 lists the data array elements required by the process rule (*rule_array* parameter). The numbers refer to the process rule's position within the array.

Table 41. Array Elements Required by the Process Rule

Process Rule	IBM-PIN	IBM-PINO	GBP-PIN	GBP-PINO	VISA-PVV	INBK-PIN
Decimalization_table	1	1	1	1		
Validation_data	2	2	2	2		
Clear_PIN		3		3		
Trans_sec_parm					1	1

PIN_profile

Direction: Input	Type: String array

A 24-byte string containing the PIN profile including the PIN block format. See "The PIN Profile" on page 173 for additional information.

PAN_data

Direction: Input	Type: String

A 12-byte string that contains 12 digits of Personal Account Number (PAN) data. The service uses this parameter if the PIN profile specifies the ISO-0 or VISA-4 keyword for the PIN block format. Otherwise, ensure that this parameter is a 4-byte variable in application storage. The information in this variable will be ignored, but the variable must be specified.

Note: When using the ISO-0 keyword, use the 12 rightmost digit of the PAN data, excluding the check digit. When using the VISA-4 keyword, use the 12 leftmost digits of the PAN data, excluding the check digit.

sequence_number

Direction: Input	Type: Integer

The 4-byte string that contains the sequence number used by certain PIN block formats. The service uses this parameter if the PIN profile specifies the 3621 or 4704-EPP keyword for the PIN block format. Otherwise, ensure that this parameter is a 4-byte variable in application data storage. The information in the variable will be ignored, but the variable must be declared. To enter a sequence number, do the following:

- Enter 99999 to use a random sequence number that the service generates.
- For the 3621 PIN block format, enter a value in the range from 0 to 65535.
- For the 4704-EPP PIN block format, enter a value in the range from 0 to 255.

encrypted_PIN_block

Direction: Output	Type: String

The field where the service returns the 8-byte encrypted PIN.

Restrictions

The caller must be in task mode, not in SRB mode.

The format control specified in the PIN profile must be NONE. If PBVC is specified as the format control, the service will fail.

Usage Note

SAF will be invoked to check authorization to use the Encrypted PIN Generate service and any key labels specified as input.

Clear PIN Encrypt (CSNBCPE)

The Clear PIN Encrypt callable service formats a PIN into one of the following PIN block formats and encrypts the results. You can use this service to create an encrypted PIN block for transmission. With the RANDOM keyword, you can have the service generate random PIN numbers.

Note: A clear PIN is a sensitive piece of information. Ensure that your application program and system design provide adequate protection for any clear PIN value.

- IBM 3621 format
- IBM 3624 format
- ISO-0 format (same as the ANSI X9.8, VISA-1, and ECI formats)
- ISO-1 format (same as the ECI-4 format)
- ISO-2 format
- IBM 4704 encrypting PINPAD (4704-EPP) format
- VISA 2 format
- VISA 3 format
- VISA 4 format
- ECI2 format
- ECI3 format

ICSF routes the Clear PIN Encrypt request to a PCI Cryptographic Coprocessor for processing. If no PCI Cryptographic Coprocessor is online, the request fails.

Format

```
CALL CSNBCPE(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            PIN_encrypting_key_identifier,
            rule_array_count,
            rule_array,
            clear_PIN,
            PIN_profile,
            PAN_data,
            sequence_number
            encrypted_PIN_block )
```

Parameters

return_code

Direction: Output Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFFFF' (2 gigabytes). The data is defined in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

PIN_encrypting_key_identifier

Direction: Input/Output	Type: String

The 64-byte string containing an internal key token or a key label of an internal key token. The internal key token contains the key that encrypts the PIN block. The control vector in the internal key token must specify an OPINENC key type and have the CPINENC usage bit set to 1.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you are supplying in the *rule_array* parameter.

rule_array

Direction: Input	Type: Character string

Keywords that provide control information to the callable service. The keyword is left-justified in an 8-byte field, and padded on the right with blanks. All keywords must be in contiguous storage. The rule array keywords are shown as follows:

Table 42. Process Rules for the Clear PIN Encryption Callable Service

Process Rule	Description
ENCRYPT	This is the default. Use of this keyword is optional.

Table 42. Process Rules for the Clear PIN Encryption Callable Service (continued)

Process Rule	Description
RANDOM	Causes the service to generate a random PIN value. The length of the PIN is based on the value in the *clear_PIN* variable. Set the value of the clear PIN to zero and use as many digits as the desired random PIN; pad the remainder of the clear PIN variable with space characters.

clear_PIN

Direction: Input Type: String

A 16-character string with the clear PIN. The value in this variable must be left-justified and padded on the right with space characters.

PIN_profile

Direction: Input Type: String

A 24-byte string containing three 8-byte elements with a PIN block format keyword, a format control keyword (NONE), and a pad digit as required by certain formats. See “The PIN Profile” on page 173 for additional information.

PAN_data

Direction: Input Type: String

A 16-byte PAN in character format. The service uses this parameter if the PIN profile specifies the ISO-0 or VISA-4 keyword for the PIN block format. Otherwise, ensure that this parameter is a 12-byte variable in application storage. This information in this variable will be ignored, but the variable must be specified. For ISO-0, use the rightmost 12 digits of the PAN, excluding the check digit. For VISA-4, use the leftmost 12 digits of the PAN, excluding the check digit.

sequence_number

Direction: Input Type: Integer

The 4-byte character integer. The service currently ignores the value in this variable. For future compatibility, the suggested value is 99999.

encrypted_PIN_block

Direction: Output Type: String

The field that receives the 8-byte encrypted PIN block.

Restrictions

The caller must be in task mode, not in SRB mode.

The format control specified in the PIN profile must be NONE. If PBVC is specified as the format control, the service will fail.

| ### Usage Note

| SAF will be invoked to check authorization to use the Clear PIN encrypt service and
| the label of the *PIN_encrypting_key_identifier*.

Clear PIN Generate Alternate (CSNBCPA)

Use the clear PIN generate alternate service to generate a clear VISA PVV (PIN validation value) from an input encrypted PIN block, or to produce a 3624 offset from a customer-selected encrypted PIN. The PIN block can be encrypted under either an input PIN-encrypting key (IPINENC) or an output PIN-encrypting key (OPINENC). Using an input PIN-encrypting key requires that the NOCV-enablement keys be present in the CKDS.

| If the *PIN_encryption_key_identifier* identifies a key which does not have the default
| PIN encrypting control vector (either IPINENC or OPINENC), the request will be
| routed to a PCI Cryptographic Coprocessor for processing. If the IBM-PINO PIN
| calculation method is specified, the request will be routed to a PCI Cryptographic
| Coprocessor for processing. If PBVC is specified for format control, the request will
| be routed to the Cryptographic Coprocessor Feature.

Format

```
CALL CSNBCPA(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            PIN_encryption_key_identifier,
            PIN_generation_key_identifier,
            PIN_profile,
            PAN_data,
            encrypted_PIN_block,
            rule_array_count,
            rule_array,
            PIN_check_length,
            data_array,
            returned_PVV)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that are assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

PIN_encryption_key_identifier

Direction: Input/Output	Type: String

A 64-byte string consisting of an internal token that contains an IPINENC or OPINENC key or the label of an IPINENC or OPINENC key that is used to encrypt the PIN block. If you specify a label, it must resolve uniquely to either an IPINENC or OPINENC key. If the *PIN_encryption_key_identifier* identifies a key which does not have the default PIN encrypting control vector (either IPINENC or OPINENC), the request will be routed to the PCI Cryptographic Coprocessor for processing.

PIN_generation_key_identifier

Direction: Input/Output	Type: String

A 64-byte string that consists of an internal token that contains a PIN generation (PINGEN) key or the label of a PINGEN key. If the *PIN_generation_key_identifier* identifies a key which does not have the default PIN generating control vector, the request will be routed to the PCI Cryptographic Coprocessor for processing.

PIN_profile

Direction: Input	Type: Character string

The three 8-byte character elements that contain information necessary to extract a PIN from a formatted PIN block. The pad digit is needed to extract the PIN from a 3624 or 3621 PIN block in the clear PIN generate alternate service. See "The PIN Profile" on page 173 for additional information.

PAN_data

Direction: Input	Type: String

A 12-byte field that contains 12 characters of PAN data. The personal account number recovers the PIN from the PIN block if the PIN profile specifies ISO-0 or VISA-4 block formats. Otherwise it is ignored, but you must specify this parameter.

For ISO-0, use the rightmost 12 digits of the PAN, excluding the check digit. For VISA-4, use the leftmost 12 digits of the PAN, excluding the check digit.

encrypted_PIN_block

Direction: Input	Type: String

An 8-byte field that contains the encrypted PIN that is input to the VISA PVV generation algorithm. The service uses the IPINENC or OPINENC key that is specified in the *PIN_encryption_key_identifier* parameter to encrypt the block.

rule_array_count

Direction: Input	Type: Integer

The number of process rules specified in the *rule_array* parameter. The value may be 1 or 2. If the default extraction method for a PIN block format is used, the rule array count value is 1.

rule_array

Direction: Input	Type: Character string

The process rule for the PIN generation algorithm. Specify IBM-PINO or “VISA-PVV” (the VISA PIN verification value) in an 8-byte field, left-justified, and padded with blanks. The *rule_array* points to an array of one or two 8-byte elements as follows:

Table 43. Rule Array Elements for the Clear PIN Generate Alternate Service

Rule Array Element	Function of Rule Array keyword
1	PIN calculation method
2	PIN extraction method

The first element in the rule array must specify one of the keywords that indicate the PIN calculation method as shown below:

Table 44. Rule Array Keywords (first element) for the Clear PIN Generate Alternate Service

PIN Calculation Method Keyword	Meaning
IBM-PINO	This keyword specifies use of the IBM 3624 PIN Offset calculation method.
VISA-PVV	This keyword specifies use of the VISA PVV calculation method.

The second element in the rule array must specify one of the PIN extraction method keywords by PIN block format as shown below. The keyword listed first in a list is the default.

Table 45. PIN Extraction Method Keywords

PIN Block Format	PIN Extraction Method Keywords
3621	PADDIGIT, HEXDIGIT, PINLEN04 to PINLEN12, PADEXIST
3624	PADDIGIT, HEXDIGIT, PINLEN04 to PINLEN16, PADEXIST

Table 45. PIN Extraction Method Keywords (continued)

PIN Block Format	PIN Extraction Method Keywords
ISO-0	PINBLOCK
ISO-1	PINBLOCK
ISO-2	PINBLOCK
4704-EPP	PINBLOCK
ECI-2	PINLEN04
ECI-3	PINBLOCK
VISA-2	PINBLOCK
VISA-3	PINBLOCK
VISA-4	PINBLOCK

The PIN extraction methods operate as follows:

PINBLOCK
Specifies that the service use one of the following:
- the PIN length, if the PIN block contains a PIN length field
- the PIN delimiter character, if the PIN block contains a PIN delimiter character.

PADDIGIT
Specifies that the service use the pad value in the PIN profile to identify the end of the PIN.

HEXDIGIT
Specifies that the service use the first occurrence of a digit in the range from X'A' to X'F' as the pad value to determine the PIN length.

PINLENxx
Specifies that the service use the length specified in the keyword, where xx can range from 4 to 16 digits, to identify the PIN.

PADEXIST
Specifies that the service use the character in the 16th position of the PIN block as the value of the pad value.

PIN_check_length

Direction: Input   Type: Integer

The length of the PIN offset used for the IBM-PINO process rule only. Otherwise, this parameter is ignored. Specify an integer from 4 through 16.

Note: The PIN check length must be less than or equal to the integer specified in the *PIN_length* parameter.

data_array

Direction: Input   Type: String

Three 16-byte elements. Table 46 on page 190 describes the format when IBM-PINO is specified. Table 47 on page 190 describes the format when VISA-PVV is specified.

Table 46. Data Array Elements for the Clear PIN Generate Alternate Service (IBM-PINO)

Array Element	Description
decimalization_table	This element contains the decimalization table of 16 characters (0 to 9) that are used to convert hexadecimal digits (X'0' to X'F') of the enciphered validation data to the decimal digits X'0' to X'9').
validation_data	This element contains one to 16 characters of account data. The data must be left justified and padded on the right with space characters.
Reserved-3	This field is ignored, but you must specify it.

Table 47. Data Array Elements for the Clear PIN Generate Alternate Service (VISA-PVV)

Array Element	Description
Trans_sec_parm	For VISA-PVV only, the leftmost twelve digits. Eleven digits of the personal account number (PAN). One digit key index. The rest of the field is ignored.
Reserved-2	This field is ignored, but you must specify it.
Reserved-3	This field is ignored, but you must specify it.

returned_PVV

Direction: Output   Type: Character

A 16-byte area that contains the 4-byte PVV left-justified and padded with blanks.

Restriction

The IBM-PINO PIN calculation method requires the optional PCI Cryptographic Coprocessor.

Usage Notes

To use an IPINENC key, you must install the NOCV-enablement keys in the CKDS.

The following table lists the PIN block variant constants (PBVC) to use.

Note: PBVC is supported for compatibility with prior releases of OS/390 ICSF and existing ICSF applications. If PBVC is specified in the format control parameter of the PIN profile, the Clear PIN Generate Alternate service will not be routed to a PCI Cryptographic Coprocessor for processing. This means that only control vectors and extraction methods valid for the Cryptographic Coprocessor Feature may be used if PBVC formatting is desired. It is recommended that a format control of NONE be used for maximum flexibility.

Table 48. PIN Block Variant Constants (PBVCs)

PIN Format Name	PIN Block Variant Constant (PBVC)
3624	X'00000000000082000000000000008200'
3621	X'00000000000084000000000000008400'
4704-EPP	X'00000000000087000000000000008700'
ISO-0	X'00000000000088000000000000008800'

Table 48. PIN Block Variant Constants (PBVCs) (continued)

PIN Format Name	PIN Block Variant Constant (PBVC)
ISO-1	X'0000000000008B000000000000008B00'
VISA-2	X'0000000000008D000000000000008D00'
VISA-3	X'0000000000008E000000000000008E00'
VISA-4	X'00000000000090000000000000009000'
ECI-2	X'00000000000093000000000000009300'
ECI-3	X'00000000000095000000000000009500'

Encrypted PIN Verification (CSNBPVR)

Use the Encrypted PIN verification callable service to verify that one of the following customer selected trial PINs is valid:
- IBM 3624 (IBM-PIN)
- IBM 3624 PIN offset (IBM-PINO)
- IBM German Bank Pool (GBP-PIN)
- IBM German Bank Pool PIN offset (GBP-PINO)
- VISA PIN validation value (VISA-PVV)
- Interbank PIN (INBK-PIN)

ICSF routes the Encrypted PIN Verification request to a PCI Cryptographic Coprocessor if the control vector in a supplied PIN key cannot cannot be processed on the Cryptographic Coprocessor Feature. The request is also routed to a PCI Cryptographic Coprocessor if the PIN profile specifies the ISO-2 PIN block format. If no PCI Cryptographic Coprocessor is online in this case, the request fails. If PBVC is specified for format control, the request will be routed to the Cryptographic Coprocessor Feature.

Format

```
CALL CSNBPVR(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            input_PIN_encrypting_key_identifier,
            PIN_verifying_key_identifier,
            input_PIN_profile,
            PAN_data,
            encrypted_PIN_block,
            rule_array_count,
            rule_array,
            PIN_check_length,
            data_array )
```

Parameters

return_code

Direction: Output Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output Type: String

The data that is passed to the installation exit.

input_PIN_encrypting_key_identifier

Direction: Input/Output Type: String

| The 64-byte key label or internal key token containing the PIN-encrypting key
| (IPINENC) that enciphers the PIN block. If the
| *input_PIN_encrypting_key_identifier* identifies a key which does not have the
| default PIN encrypting control vector (IPIENC), the request will be routed to a
| PCI Cryptographic Coprocessor.

PIN_verifying_key_identifier

Direction: Input/Output Type: String

| The 64-byte key label or internal key token that identifies the PIN verification
| (PINVER) key. If the *PIN_verifying_key_identifier* identifies a key which does not
| have the default PIN verification key control vector, the request will be routed to
| a PCI Cryptographic Coprocessor.

input_PIN_profile

Direction: Input Type: Character string

The three 8-byte character elements that contain information necessary to either create a formatted PIN block or extract a PIN from a formatted PIN block. A particular PIN profile can be either an input PIN profile or an output PIN profile depending on whether the PIN block is being enciphered or deciphered by the callable service. See "The PIN Profile" on page 173 for additional information.

The pad digit is needed to extract the PIN from a 3624 or 3621 PIN block in the encrypted PIN verify callable service.

PAN_data

Direction: Input Type: Character string

The personal account number (PAN) is required for ISO-0 and VISA-4 only. Otherwise, this parameter is ignored. Specify 12 digits of account data in character format.

For ISO-0, use the rightmost 12 digits of the PAN, excluding the check digit.

For VISA-4, use the leftmost 12 digits of the PAN, excluding the check digit.

encrypted_PIN_block

Direction: Input Type: String

The 8-byte enciphered PIN block that contains the PIN to be verified.

rule_array_count

Direction: Input Type: Integer

The number of process rules specified in the *rule_array* parameter. The value may be 1 or 2. If the default extraction method for the PIN block format is used, the rule array count value is 1.

rule_array

Direction: Input Type: Character string

The process rule for the PIN verification algorithm. The *rule_array* points to an array of one or two 8-byte elements as follows:

Table 49. Rule Array Elements for the Encrypted PIN Verification Service

Rule Array Element	Function of Rule Array keyword
1	PIN calculation method
2	PIN extraction method

The first element in the rule array must specify the PIN verification algorithm. The second element in the rule array must specify one of the keywords that indicate a PIN extraction method as shown below.

Note: The PIN block format key is the keyword that you specify in the *input_PIN_profile* or the *output_PIN_profile* parameter.

Table 50. Calculation methods for the PIN Verification Process

Algorithm Value	Description
IBM-PIN	The IBM 3624 PIN, which is an institution-assigned PIN. It does not calculate the PIN offset.
IBM-PINO	The IBM 3624 PIN offset, which is a customer-selected PIN and calculates the PIN offset.

Table 50. Calculation methods for the PIN Verification Process (continued)

Algorithm Value	Description
GBP-PIN	The IBM German Bank Pool PIN. It verifies the PIN entered by the customer and compares that PIN with the institution generated PIN by using an institution key.
GBP-PINO	The IBM German Bank Pool PIN offset. It verifies the PIN entered by the customer by comparing with the calculated institution PIN (IPIN) and adding the specified offset to the pool PIN (PPIN) generated by using a pool key.
VISA-PVV	The VISA PIN verification value.
INBK-PIN	The Interbank PIN verification algorithm.

Appendix D. PIN Formats and Algorithms discusses the IBM PIN algorithms.

Note: If the PIN block format allows you to choose the PIN extraction method, and if you specify a rule array of 1, the keyword that is listed first in the following table is the default keyword.

Table 51. PIN Verification Rule Array Keywords (Second Element)

PIN Block Format keyword	PIN extraction method keyword	Meaning
3621	PADDIGIT, HEXDIGIT, PINLEN04 to PINLEN12, PADEXIST	The PIN extraction method keywords specify a PIN extraction method for an IBM 3621 PIN block format. The first keyword, PADDIGIT, is the default PIN extraction method for the PIN block format.
3624	PADDIGIT, HEXDIGIT, PINLEN04 to PINLEN16, PADEXIST	The PIN extraction method keywords specify a PIN extraction method for an IBM 3624 PIN block format. The first keyword, PADDIGIT, is the default PIN extraction method for the PIN block format.
ISO-0	PINBLOCK	The PIN extraction method keywords specify a PIN extraction method for a PINBLOCK format.
ISO-1	PINBLOCK	The PIN extraction method keywords specify a PIN extraction method for a PINBLOCK format.
ISO-2	PINBLOCK	The PIN extraction method keywords specify a PIN extraction method for a PINBLOCK format.
4704-EPP	PINBLOCK	The PIN extraction method keywords specify a PIN extraction method for a PINBLOCK format.

Table 51. PIN Verification Rule Array Keywords (Second Element) (continued)

PIN Block Format keyword	PIN extraction method keyword	Meaning
ECI-2	PINLEN04	The PIN extraction method keywords specify a PIN extraction method for a PINLEN04 format.
ECI-3	PINBLOCK	The PIN extraction method keywords specify a PIN extraction method for a PINBLOCK format.
VISA-2	PINBLOCK	The PIN extraction method keywords specify a PIN extraction method for a PINBLOCK format.
VISA-3	PINBLOCK	The PIN extraction method keywords specify a PIN extraction method for a PINBLOCK format.
VISA-4	PINBLOCK	The PIN extraction method keywords specify a PIN extraction method for a PINBLOCK format.

PIN_check_length

Direction: Input Type: Integer

The PIN check length for the IBM-PIN or IBM-PINO process rules only. Otherwise, it is ignored. Specify the rightmost digits, 4 through 16, for the PIN to be verified.

data_array

Direction: Input Type: String

Three 16-byte elements required by the corresponding *rule_array* parameter. The data array consists of three 16-byte fields whose specification depend on the process rule. If a process rule only requires one or two 16-byte fields, then the rest of the data array is ignored by the callable service. Table 52 describes the array elements.

Table 52. Array Elements for the Encrypted PIN Verification Callable Service

Array Element	Description
Decimalization_table	Decimalization table for IBM and GBP only. Sixteen decimal digits of 0 through 9.
Validation_data	Validation data for IBM and GBP padded to 16 bytes. One to sixteen characters of hexadecimal account data left-justified and padded on the right with blanks.

Table 52. Array Elements for the Encrypted PIN Verification Callable Service (continued)

Array Element	Description
PIN_offset	Offset data for IBM-PINO and GBP-PINO. One to twelve numeric characters, 0 through 9, left-justified and padded on the right with blanks. For IBM-PINO, the PIN offset length is specified in the *PIN_check_length* parameter. For GBP-PINO, the PIN offset is always 4 digits. For IBM-PIN and GBP-PIN, the field is ignored.
trans_sec_parm	For VISA, only the leftmost twelve digits of the 16-byte field are used. These consist of the rightmost eleven digits of the personal account number (PAN) and a one-digit key index. The remaining four characters are ignored. For Interbank only, all 16 bytes are used. These consist of the rightmost eleven digits of the PAN, a constant of X'6', a one-digit key index, and three numeric digits of PIN validation data.
RPVV	For VISA-PVV only, referenced PVV (4 bytes) that is left-justified. The rest of the field is ignored.

Table 53 lists the data array elements required by the process rule (*rule_array* parameter). The numbers refer to the process rule's position within the array.

Table 53. Array Elements Required by the Process Rule

Process Rule	IBM-PIN	IBM-PINO	GBP-PIN	GBP-PINO	VISA-PVV	INBK-PIN
Decimalization_table	1	1	1	1		
Validation_data	2	2	2	2		
PIN_offset	3	3	3	3		
Trans_sec_parm					1	1
RPVV					2	

Restrictions

GBP-PINO is only supported if the CSNBPVR service is processed on the Cryptographic Coprocessor Feature. If the service is routed to a PCI Cryptographic Coprocessor, the service request will fail if the GBP-PINO calculation method is specified.

Use of the ISO-2 PIN block format requires the optional PCI Cryptographic Coprocessor.

Usage Notes

The following table lists the PIN block variant constants (PBVC) to be used.

Note: PBVC is supported for compatibility with prior releases of OS/390 ICSF and existing ICSF applications. If PBVC is specified in the format control parameter of the PIN profile, the Encrypted PIN Verification service will not be routed to a PCI Cryptographic Coprocessor for processing. This means that only control vectors and extraction methods valid for the Cryptographic Coprocessor Feature may be used if PBVC formatting is desired. It is recommended that a format control of NONE be used for maximum flexibility.

Table 54. PIN Block Variant Constants (PBVCs)

PIN Format Name	PIN Block Variant Constant (PBVC)
3624	X'00000000000082000000000000008200'
3621	X'00000000000084000000000000008400'
4704-EPP	X'00000000000087000000000000008700'
ISO-0	X'00000000000088000000000000008800'
ISO-1	X'0000000000008B0000000000008B00'
VISA-2	X'0000000000008D0000000000008D00'
VISA-3	X'0000000000008E0000000000008E00'
VISA-4	X'00000000000090000000000000009000'
ECI-2	X'00000000000093000000000000009300'
ECI-3	X'00000000000095000000000000009500'

Related Information

Appendix D. PIN Formats and Algorithms discusses the PIN algorithms in detail.

Encrypted PIN Translation (CSNBPTR)

Use the encrypted PIN translation callable service to reencipher a PIN block from one PIN-encrypting key to another and, optionally, to change the PIN block format, such as the pad digit or sequence number.

ICSF routes the Encrypted PIN Translation request to a PCI Cryptographic Coprocessor if the control vector in a supplied PIN encrypting key cannot cannot be processed on the Cryptographic Coprocessor Feature. The request is also routed to a PCI Cryptographic Coprocessor if the PIN profile specifies the ISO-2 PIN block format. If no PCI Cryptographic Coprocessor is online in this case, the request fails. If PBVC is specified for format control, the request will be routed to the Cryptographic Coprocessor Feature.

Format

```
CALL CSNBPTR(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            input_PIN_encrypting_key_identifier,
            output_PIN_encrypting_key_identifier,
            input_PIN_profile,
            PAN_data_in,
            PIN_block_in,
            rule_array_count,
            rule_array,
            output_PIN_profile,
            PAN_data_out,
            sequence_number,
            PIN_block_out )
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

input_PIN_encrypting_key_identifier

Direction: Input/Output	Type: String

| The input PIN-encrypting key (IPINENC) for the *PIN_block_in* parameter
| specified as a 64-byte internal key token or a key label. If the
| *input_PIN_encrypting_key_identifier* identifies a key which does not have the
| default input PIN encrypting key control vector (IPINENC), the request will be
| routed to a PCI Cryptographic Coprocessor.

output_PIN_encrypting_key_identifier

Direction: Input/Output	Type: String

| The output PIN-encrypting key (OPINENC) for the *PIN_block_out* parameter
| specified as a 64-byte internal key token or a key label. If the
| *output_PIN_encrypting_key_identifier* identifies a key which does not have the
| default output PIN encrypting key control vector (OPINENC), the request will be
| routed to a PCI Cryptographic Coprocessor.

input_PIN_profile

Direction: Input	Type: Character string

The three 8-byte character elements that contain information necessary to either create a formatted PIN block or extract a PIN from a formatted PIN block. A particular PIN profile can be either an input PIN profile or an output PIN profile depending on whether the PIN block is being enciphered or deciphered by the callable service. See “The PIN Profile” on page 173 for additional information.

If you choose the TRANSLAT processing rule in the *rule_array* parameter, the *input_PIN_profile* and the *output_PIN_profile* must specify the same PIN block format. If you choose the REFORMAT processing rule in the *rule_array* parameter, the input PIN profile and output PIN profile can have different PIN block formats.

The pad digit is needed to extract the PIN from a 3624 or 3621 PIN block in the Encrypted PIN translation callable service with a process rule (*rule_array* parameter) of REFORMAT. If the process rule is TRANSLAT, the pad digit is ignored.

PAN_data_in

Direction: Input	Type: Character string

The personal account number (PAN) if the process rule (*rule_array* parameter) is REFORMAT and the input PIN format is ISO-0 or VISA-4 only. Otherwise, this parameter is ignored. Specify 12 digits of account data in character format.

For ISO-0, use the rightmost 12 digits of the PAN, excluding the check digit.

For VISA-4, use the leftmost 12 digits of the PAN, excluding the check digit.

PIN_block_in

Direction: Input	Type: String

The 8-byte enciphered PIN block that contains the PIN to be translated.

rule_array_count

Direction: Input	Type: Integer

| The number of process rules specified in the *rule_array* parameter. The value
| may be 1 or 2.

rule_array

Direction: Input	Type: Character string

| The process rule for the callable service. The *rule_array* points to an array of
| one or two 8-byte elements, as follows:

| *Table 55. Rule Array Elements for the Encrypted PIN Translation Service*

Rule Array Element	Function of Rule Array keyword
1	Mode
2	PIN extraction method

The first element in the rule array must specify the mode. If you use the REFORMAT mode, the second element in the rule array must specify one of the keywords that indicate a PIN extraction method.

Table 56. Modes for the Encrypted PIN Translation Callable Service

Process Rule	Description
TRANSLAT	Changes the PIN-encrypting key only. It does not change the PIN format and the contents of the PIN block.
REFORMAT	Changes the PIN format, the contents of the PIN block, and the PIN-encrypting key.

Table 57. Encrypted PIN Translate Rule Array Keywords (Second Element)

PIN Block Format keyword	PIN extraction method keyword	Meaning
3621	PADDIGIT, HEXDIGIT, PINLEN04 to PINLEN12, PADEXIST	The PIN extraction method keywords specify a PIN extraction method for an IBM 3621 PIN block format. The first keyword, PADDIGIT, is the default PIN extraction method for the PIN block format.
3624	PADDIGIT, HEXDIGIT, PINLEN04 to PINLEN16, PADEXIST	The PIN extraction method keywords specify a PIN extraction method for an IBM 3624 PIN block format. The first keyword, PADDIGIT, is the default PIN extraction method for the PIN block format.
ISO-0	PINBLOCK	The PIN extraction method keywords specify a PIN extraction method for a PINBLOCK format.
ISO-1	PINBLOCK	The PIN extraction method keywords specify a PIN extraction method for a PINBLOCK format.
ISO-2	PINBLOCK	The PIN extraction method keywords specify a PIN extraction method for a PINBLOCK format.
4704-EPP	PINBLOCK	The PIN extraction method keywords specify a PIN extraction method for a PINBLOCK format.
ECI-2	PINLEN04	The PIN extraction method keywords specify a PIN extraction method for a PINLEN04 format.
ECI-3	PINBLOCK	The PIN extraction method keywords specify a PIN extraction method for a PINBLOCK format.

Table 57. Encrypted PIN Translate Rule Array Keywords (Second Element) (continued)

PIN Block Format keyword	PIN extraction method keyword	Meaning
VISA-2	PINBLOCK	The PIN extraction method keywords specify a PIN extraction method for a PINBLOCK format.
VISA-3	PINBLOCK	The PIN extraction method keywords specify a PIN extraction method for a PINBLOCK format.
VISA-4	PINBLOCK	The PIN extraction method keywords specify a PIN extraction method for a PINBLOCK format.

Note: If the PIN block format allows you to choose the PIN extraction method, and if you specify a rule array of 1, the keyword that is listed first in the following table is the default keyword.

output_PIN_profile

Direction: Input Type: Character string

The three 8-byte character elements that contain information necessary to either create a formatted PIN block or extract a PIN from a formatted PIN block. A particular PIN profile can be either an input PIN profile or an output PIN profile, depending on whether the PIN block is being enciphered or deciphered by the callable service.

If you choose the TRANSLAT processing rule in the *rule_array* parameter, the *input_PIN_profile* and the *output_PIN_profile* must specify the same PIN block format. If you choose the REFORMAT processing rule in the *rule_array* parameter, the input PIN profile and output PIN profile can have different PIN block formats.

The PIN profile consists of the following:
- PIN block format
- Format control
- Pad digit

Information about the PIN profile is under the *input_PIN_profile* parameter.

PAN_data_out

Direction: Input Type: Character string

The personal account number (PAN) if the process rule (*rule_array* parameter) is REFORMAT and the output PIN format is ISO-0 or VISA-4 only. Otherwise, this parameter is ignored. Specify 12 digits of account data in character format.

For ISO-0, use the rightmost 12 digits of the PAN, excluding the check digit.

For VISA-4, use the leftmost 12 digits of the PAN, excluding the check digit.

sequence_number

Direction: Input   Type: Integer

The sequence number if the process rule (*rule_array* parameter) is REFORMAT and the output PIN block format is 3621 or 4704-EPP only. Specify the integer value 99999. Otherwise, this parameter is ignored.

PIN_block_out

Direction: Output   Type: String

The 8-byte output PIN block that is reenciphered.

Restriction

Use of the ISO-2 PIN block format requires the optional PCI Cryptographic Coprocessor.

Usage Notes

Some PIN block formats are known by several names. The following table shows the additional names.

Table 58. Additional Names for PIN Formats

PIN Format	Additional Name
ISO-0	ANSI X9.8, VISA format 1, ECI format 1
ISO-1	ECI format 4

The following table lists the PIN block variant constants (PBVC) to be used.

Note: PBVC is supported for compatibility with prior releases of OS/390 ICSF and existing ICSF applications. If PBVC is specified in the format control parameter of the PIN profile, the Encrypted PIN Translation service will not be routed to a PCI Cryptographic Coprocessor for processing. This means that only control vectors and extraction methods valid for the Cryptographic Coprocessor Feature may be used if PBVC formatting is desired. It is recommended that a format control of NONE be used for maximum flexibility.

Table 59. PIN Block Variant Constants (PBVCs)

PIN Format Name	PIN Block Variant Constant (PBVC)
3624	X'00000000000082000000000000008200'
3621	X'00000000000084000000000000008400'
4704-EPP	X'00000000000087000000000000008700'
ISO-0	X'00000000000088000000000000008800'
ISO-1	X'0000000000008B000000000000008B00'
VISA-2	X'0000000000008D000000000000008D00'
VISA-3	X'0000000000008E000000000000008E00'
VISA-4	X'00000000000090000000000000009000'
ECI-2	X'00000000000093000000000000009300'
ECI-3	X'00000000000095000000000000009500'

Chapter 11. DES Utilities

This chapter presents utilities to perform the following tasks:
- Build DES key tokens
- Encipher plaintext using the Cipher Block Chaining (CBC) method
- Build a control vector from specified keywords
- Change the control vector used to encipher an external key
- Convert EBCDIC data to ASCII data or ASCII data to EBCDIC data
- Convert a binary string to a character string or a character string to a binary string
- Edit an ASCII string according to the editing rules of ANSI X9.9-4

Key Token Build (CSNBKTB)

Use the key token build callable service to build an external or internal key token from information which you supply. The token can be used as input for the key generate and key part import callable services. You can specify a control vector or the service can build a control vector based upon the key type you specify and the control vector-related keywords in the rule array. ICSF supports the building of an internal key token with the key encrypted under a master key other than the current master key.

You can also use this service to update the DES, CDMF, or SYS-ENC markings in a supplied DATA, IMPORTER, or EXPORTER token and to build CCA key tokens for all key types ICSF supports.

Format

```
CALL CSNBKTB(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             key_token,
             key_type,
             rule_array_count,
             rule_array,
             key_value,
             master_key_version_number,
             key_register_number,
             secure_token,
             control_vector,
             initialization_vector,
             pad_character,
             cryptographic_period_start,
             masterkey_verify_parm
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output   Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output   Type: Integer

Reserved field.

exit_data

Direction: Input/Output   Type: String

Reserved field.

key_token

Direction: Input/Output   Type: String

If the following parameter *key_type* is TOKEN then this is a 64-byte internal token that is updated as specified in the *rule_array*. The internal token must be a DATA, IMPORTER or EXPORTER key type. Otherwise this field is an output-only field.

key_type

Direction: Input   Type: String

An 8-byte field that specifies the type of key you want to build or the keyword TOKEN for updating a supplied token. If *key_type* is TOKEN, then the *key_token* field cannot contain a double- or triple-length DATA key token. For a list of keywords, see Table 60. No other keywords are valid. The TOKEN keyword indicates changing an internal token in the *key_token* parameter. A valid *key_type* indicates building a key token from the parameters specified.

Table 60. Key Type Values for the Key Token Build Callable Service

Key Type	Meaning
DATA	Data-encrypting key. Use this single-, double-, or triple-length key to encipher and decipher data.
DATAXLAT	Data translation key. Use this single-length key to reencipher text from one DATA key to another.
MAC	MAC generation key. Use this single-length key to generate a message authentication code.
MACVER	MAC verification key. Use this single-length key to verify a message authentication code.
| DATAM	MAC generation key. Use this double-length key to generate a message authentication code.

Table 60. Key Type Values for the Key Token Build Callable Service (continued)

Key Type	Meaning
DATAMV	MAC verification key. Use this double-length key to generate a message authentication code.
PINGEN	PIN generation key. Use this double-length key to generate PINs.
PINVER	PIN verification key. Use this double-length key to verify PINs.
IPINENC	Input PIN-encrypting key. Use this double-length input key to translate PINs. PIN blocks received from other nodes or automatic teller machine (ATM) terminals are encrypted under this type of key. These encrypted PIN blocks are the input to the Encrypted PIN translate and Encrypted PIN verify callable services.
OPINENC	Output PIN-encrypting key. Use this double-length output key to translate PINs. The output PIN block from the Encrypted PIN translate callable service is encrypted under this type of key.
EXPORTER	Exporter key-encrypting key. Use this double-length key to convert any key (including a DATA key) from operational form into exportable form.
IMPORTER	Importer key-encrypting key. Use this double-length key to convert a key from importable form into operational form.
AKEK	ANSI X9.17 key-encrypting key. A single- or double-length key that must be ANSI-notarized and offset before use as a key-encrypting key. Default is double-length.
DECIPHER	Used only to decrypt data.
ENCIPHER	Used only to encrypt data.
IKEYXLAT	Used to decrypt an input key in the Key Translate callable service.
OKEYXLAT	Used to encrypt an output key in the Key Translate callable service.
CIPHER	Used only to encrypt or decrypt data.
DATAC	Used to specify a DATA-class key that will perform in the Encipher and Decipher callable services, but not in the MAC Generate or MAC Verify callable services.
USE-CV	Specifies that the key type should be obtained from the control vector specified in the *control_vector* parameter. The CV rule array keyword should be specified if USE-CV is specified.
CVARPINE	Used to encrypt a PIN value for decryption in a PIN-printing application.
CVARDEC	The TSS Cryptographic Variable Decipher service uses a CVARDEC key to decrypt plaintext by using the Cipher Block Chaining (CBC) method.
CVARENC	Cryptographic variable encipher service uses a CVARENC key to encrypt plaintext by using the Cipher Block Chaining (CBC) method.
CVARXCVL	Used to encrypt special control values in DES key management.
CVARXCVR	Used to encrypt special control values in DES key management.

rule_array_count

Direction: Input Type: Integer

| The number of keywords you supplied in the *rule_array* parameter.

rule_array

Direction: Input Type: String

One to four keywords that provide control information to the callable service. See Table 61 for a list. The keywords must be in 8 to 32 bytes of contiguous storage with each of the keywords left-justified in its own 8-byte location and padded on the right with blanks. For any key type, there are no more than four valid *rule_array* values.

If you specify TOKEN for the *key_type*, then the only valid *rule_array* values are INTERNAL and DES, CDMF, or SYS-ENC. The Data Encryption Algorithm (see the table that follows) keyword has no default. If you specify a *key_type* of DATA, IMPORTER or EXPORTER, the Data Encryption Algorithm selection keyword defaults to SYS-ENC. The other *rule_array* keywords do not apply.

Table 61. Keywords for Key Token Build Control Information

Keyword	Meaning
Token Type (required)	
INTERNAL	Specifies an internal key token.
EXTERNAL	Specifies an external key token.
Key Status (optional)	
KEY	This keyword indicates that the key token to build will contain an encrypted key. The *key_value* parameter identifies the field that contains the key.
NO-KEY	This keyword indicates that the key token to build will not contain a key. This is the default key status.
Data Encryption Algorithm (optional) — valid only for single-length DATA keys and KEKs.	
CDMF	For a DATA key, this keyword indicates marking the key token as usable only with the CDMF. For a KEK, it indicates marking the key token to specify that the KEK can encrypt only a CDMF DATA key.
DES	For a DATA key, this keyword indicates marking the key token as usable only with the DES. For a KEK, it indicates marking the key token to specify that the KEK can encrypt only a DES DATA key.
SYS-ENC	For a KEK, this keyword indicates marking the key token as B'00'. This means that the KEK can protect CDMF- or DES-marked DATA key tokens. For a DATA key, this indicates marking the key token according to the encryption algorithm of the system. For a CDMF system, the DATA key token is marked CDMF; for a DES-CDMF or DES system, it is marked DES. When *key_type* of DATA, IMPORTER or EXPORTER is specified, SYS-ENC is the default.
CV on the Link Specification (optional) — valid only for IMPORTER and EXPORTER.	
CV-KEK	This keyword indicates marking the KEK as a CV KEK. The control vector is applied to the KEK before use in encrypting other keys. This is the default.

Table 61. Keywords for Key Token Build Control Information (continued)

Keyword	Meaning
NOCV-KEK	This keyword indicates marking the KEK as a NOCV KEK. The control vector is not applied to the KEK before use in encrypting other keys. Services using NO-CV keys must be processed on the Cryptographic Coprocessor Feature.
CV Status optional)	
CV	This keyword indicates to obtain the control vector from the variable identified by the *control_vector* parameter.
NO-CV	Default. This keyword indicates that the control vector is to be supplied based on the key type and the control vector related keywords.
Key Length Keywords (optional)	
SINGLE	Single-length 8-byte key valid only for AKEK.
DOUBLE-O	Double-length 16-byte key valid only for AKEK. Both halves may have the same clear values. DOUBLE-O is mutually exclusive with SINGLE keyword. For AKEKs, DOUBLE-O is the default. DOUBLE-O AKEKs generated by CSNBKGN will have different left and right clear values.
KEYLN8	Single-length, 8-byte key valid only for a DATA key type. This is the default.
KEYLN16	Double-length, 16-byte key valid only for a DATA key type.
KEYLN24	Triple-length, 24-byte key valid only for a DATA key type.
Key Part Indicator (optional)	
KEY-PART	This token is to be used as input to the key part import service.
Control Vector Keywords. Specify one or more of the following (optional)	
See Table 62 on page 210 for the key-usage keywords that can be specified for a given key type.	
Master Key Verification Pattern (optional)	
MKVP	This keyword indicates that the *key_value* is enciphered under the master key which corresponds to the master key verification pattern specified in the *masterkey_verify_parm* parameter. If this keyword is not specified, the key contained in the *key_value* field must be enciphered under the current master key.

key_value

Direction: Input Type: String

If you use the KEY keyword, this parameter is a 16-byte string that contains the encrypted key value. Single-length keys must be left-justified in the field and padded on the right with X'00'. If you are building a triple-length DATA key, this parameter is a 24-byte string containing the ecrypted key value. If you supply an encrypted key value and also specify INTERNAL, the service will check for the presence of the MKVP keyword. If MKVP is present, the service will assume the *key_value* is enciphered under the master key which corresponds to the master key verification pattern specified in the *masterky_verify_parm* parameter, and will place the key into the internal token along with the verification pattern from the *masterky_verify_parm* parameter. If MKVP is not specified, ICSF assumes the key is enciphered under the current host master key and places the key into an internal token along with the verification pattern for the current master key. In this case, the application must ensure that the master key has not changed since the key was generated or imported to this system. Otherwise, use of this parameter is not recommended.

master_key_version_number

Direction: Input	Type: Integer

This field is examined only if the KEY keyword is specified, in which case, this field must be zero. If the KEY and INTERNAL keywords are specified in *rule_array*, the service will check for the existence of the MKVP rule array keyword. If MKVP is specified, the service will make use of the last parameter specified (*masterky_verify_parm*). The service assumes the key provided by the *key_value* parameter is enciphered under the corresponding master key and will place the key into the internal token along with the verification pattern from the *masterkey_verify_parm* parameter.

key_register_number

Direction: Input	Type: Integer

This field is ignored.

secure_token

Direction: Input	Type: String

This field is ignored.

control_vector

Direction: Input	Type: String

A pointer to 16 byte sting variable. If this parameter is specified, and you use the CV rule array keyword, the variable is copied to the control vector field of the key token. See “Appendix K. Control Vector Table” on page 413 for additional information.

initialization_vector

Direction: Input	Type: String

This field is ignored.

pad_character

Direction: Input	Type: Integer

The only allowed value for key types MAC and MACVER is 0. This field is ignored for all other key types.

cryptographic_period_start

Direction: Input	Type: String

This field is ignored.

masterkey_verify_parm

Direction: Input   Type: String

A pointer to an 8-byte string variable. The value is inserted into the key token when you specify both the KEY and INTERNAL keywords in rule array.

Usage Notes

You can use this service to create skeleton key tokens with the desired data encryption algorithm bits for use in some key management services to override the default system specifications.

- To generate an operational CDMF DATA key, build an internal DATA key token with the CDMF keyword and pass that token to the key generate service in the *generated_key_identifier_1* parameter. This generates the desired DATA key independently of the system encryption algorithm default. Similarly, for token copying to override the system default data encryption algorithm bits, you can use this service to build a skeleton token for input to the key generate, key import, or secure key import callable services.
- To generate operational AKEKs, use *key_type* of TOKEN and provide a skeleton AKEK key token as the *generated_key_identifier_1* into the key generate service.
- The KEY-PART AKEK key token can also be used as input to key part import service.
- To create an internal token with a specified KEY value, ICSF needs to supply a valid master key verification pattern (MKVP).

The TOKEN *key_type* changes the data encryption algorithm bits **only** on an existing DATA, IMPORTER or EXPORTER key token. Thus, if you specify TOKEN as the key_type, the only valid *rule_array* values are INTERNAL and DES, CDMF, or SYS-ENC. There is no default for the encryption algorithm selection.

Note: No pre- or post-processing or security exits are enabled for this service. No RACF checking is done, and no calls to RACF are issued when this service is used.

Use of NOCV keys is supported by ICSF. Services using NOCV keys must be processed on a CCF. This means that the key token build service will fail a request to build a key type which is not supported on the CCF if NOCV-KEK is also specified in the rule array.

The following illustrates the key type and key usage keywords that can be combined in the Control Vector Generate and Key Token Build callable services to create a control vector.

Table 62. Control Vector Generate and Key Token Build Control Vector Keyword Combinations

Key Type	Key Usage **Default keys are indicated in bold.** *** All keywords in the list below the note are defaults unless one or more keywords in the list are specified.** **** The NOOFFSET keyword is only valid if NO-SPEC, IBM-PIN, GBP-PIN, or the default (NO-SPEC) is specified.**						
DATA CIPHER ENCIPHER DECIPHER MAC MACVER CVARPINE CVARENC CVARDEC CVARXCVL CVARXCVR					**SINGLE** KEYLN8 DOUBLE KEYLN16 MIXED	**XPORT-OK** NO-XPORT	KEY-PART
DATAC DATAM DATAMV					**DOUBLE** KEYLN16 MIXED	**XPORT-OK** NO-XPORT	KEY-PART
IKEYXLAT OKEYXLAT				**ANY** NOT-KEK DATA PIN LMTD-KEK	**DOUBLE** KEYLN16 MIXED	**XPORT-OK** NO-XPORT	KEY-PART
IMPORTER	OPIM* IMEX* IMIM* IMPORT*	XLATE		**ANY** NOT-KEK DATA PIN LMTD-KEK	**DOUBLE** KEYLN16 MIXED	**XPORT-OK** NO-XPORT	KEY-PART
EXPORTER	OPEX* IMEX* EXEX* EXPORT*	XLATE		**ANY** NOT-KEK DATA PIN LMTD-KEK	**DOUBLE** KEYLN16 MIXED	**XPORT-OK** NO-XPORT	KEY-PART
PINVER			**NO-SPEC**** IBM-PIN** GBP-PIN** IBM-PINO GBP-PINO VISA-PVV INBK-PIN	NOOFFSET	**DOUBLE** KEYLN16 MIXED	**XPORT-OK** NO-XPORT	KEY-PART
PINGEN	CPINGEN* CPINGENA* EPINGENA* EPINGEN* EPINVER*		**NO-SPEC**** IBM-PIN** GBP-PIN** IBM-PINO GBP-PINO VISA-PVV INBK-PIN	NOOFFSET	**DOUBLE** KEYLN16 MIXED	**XPORT-OK** NO-XPORT	KEY-PART
IPINENC	CPINGENA* EPINVER* REFORMAT* TRANSLAT*				**DOUBLE** KEYLN16 MIXED	**XPORT-OK** NO-XPORT	KEY-PART

Table 62. Control Vector Generate and Key Token Build Control Vector Keyword Combinations (continued)

Key Type	Key Usage Default keys are indicated in bold. * All keywords in the list below the note are defaults unless one or more keywords in the list are specified. ** The NOOFFSET keyword is only valid if NO-SPEC, IBM-PIN, GBP-PIN, or the default (NO-SPEC) is specified.			
OPINENC	CPINENC* EPINGEN* REFORMAT* TRANSLAT*	**DOUBLE** KEYLN16 MIXED	**XPORT-OK** NO-XPORT	KEY-PART

Related Information

The ICSF key token build callable service provides a subset of the parameters and keywords available with the Transaction Security System key token build verb.

The following key types are not supported: ADATA, AMAC, CIPHERXI, CIPHERXL, CIPHERXO, UKPTBASE.

The following rule array keywords are not supported: KEY-REF, ADAPTER, READER, CARD, ACTIVE, INACTIVE, CLEAR-IV, NO-IV, CBC, X9.23, IPS, CUSP, X9.9-1, MACLEN4, MACLEN6, MACLEN8.

The *master_key_verification_number* parameter has been replaced by the *master_key_version_number* parameter. The *master_key_version_number* parameter is examined only if the KEY keyword is specified, and in this case must be zero. If KEY and INTERNAL are both specified in the rule array, the service will check for the existence of a new optional rule array keyword, MKVP. If MKVP is specified, the service will make use of the last parameter specified. Currently, this is called *cryptographic_period_end* and is always ignored. It will now be used to contain a master key verification parameter if MKVP is specified. The service assumes the key provided by the *key_value* parameter is enciphered under the corresponding master key and will place the key into the internal token along with the verification pattern from the *MKV_PATTERN* parameter.

The *key_register_number*, *secure_token*, and *initialization_vector* parameters are ignored.

The *pad_character* parameter must have a value of zero.

Cryptographic Variable Encipher (CSNBCVE)

The Cryptographic Variable Encipher callable service uses a CVARENC key to encrypt plaintext by using the Cipher Block Chaining (CBC) method. You can use this service to prepare a mask array for the Control Vector Translate service. The plaintext must be a multiple of eight bytes in length.

ICSF routes the cryptographic variable encipher request to a PCI Cryptographic Coprocessor for processing. If no PCI Cryptographic Coprocessor is online, the request fails.

Format

```
CALL CSNBCVE(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            c-variable_encrypting_key_identifier,
            text_length,
            plaintext,
            initialization_vector,
            ciphertext )
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFFFF' (2 gigabytes). The data is defined in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

c-variable_encrypting_key_identifier

Direction: Input/Output	Type: String

The 64-byte string variable containing an internal key or a key label of an internal key token record in the CKDS. The internal key must contain a control vector that specifies a CVARENC key type.

text_length

Direction: Input	Type: Integer

An integer variable containing the length of the plaintext and the returned ciphertext.

plaintext

Direction: Input	Type: String

A string of length 8 to 256 bytes which contains the plaintext.

initialization_vector

Direction: Input	Type: String

A string variable containing the 8-byte initialization vector that the service uses in encrypting the plaintext.

ciphertext

Direction: Output	Type: String

The field which receives the ciphertext. The length of this field is the same as the length of the plaintext.

Restrictions

- The text length must be a multiple of 8 bytes.
- The maximum length of text that the security server can process is 256 bytes.
- The caller must be in task mode, not in SRB mode.

Usage Note

SAF will be invoked to check authorization to use the Cryptographic Variable Encipher service and the key label if specified in the *c-variable_encrypting_key_identifier* parameter.

Control Vector Generate (CSNBCVG)

The Control Vector Generate callable service builds a control vector from keywords specified by the *key_type* and *rule_array* parameters.

Format

```
CALL CSNBCVG(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            key_type,
            rule_array_count,
            rule_array,
            reserved,
            control_vector )
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit.

key_type

Direction: Input	Type: String

A string variable containing a keyword for the key type. The keyword is 8 bytes in length, left justified, and padded on the right with space characters. It is taken from the following list:

```
CIPHER      DATA        EXPORTER    OKEYXLAT
CVARDEC     DATAC       IKEYXLAT    OPINENC
CVARENC     DATAM       IMPORTER    PINGEN
CVARPINE    DATAMV      IPINENC     PINVER
CVARXCVL    DECIPHER    MAC
CVARXCVR    ENCIPHER    MACVER
```

rule_array_count

Direction: Input	Type: Integer

The number of keywords you are supplying in the *rule_array* parameter.

rule_array

Direction: Input	Type: Character String

Keywords that provide control information to the callable service. Each keyword is left justified in 8-byte fields, and padded on the right with blanks. All keywords must be in contiguous storage. “Key Token Build (CSNBKTB)” on page 203 illustrates the key type and key usage keywords that can be combined in the Control Vector Generate and Key Token Build callable services to create a control vector. The rule array keywords are shown below.

ANY	EXPORT	KEYLN8	PIN
CPINENC	GBP-PIN	KEYLN16	REFORMAT
CPINGEN	GBP-PINO	LMTD-KEK	SINGLE
CPINGENA	IBM-PIN	MIXED	TRANSLAT
DATA	IBM-PINO	NOOFFSET	VISA-PVV
DOUBLE	IMEX	NO-SPEC	XLATE
EPINGEN	IMIM	NO-XPORT	XPORT-OK
EPINGEN	IMPORT	NOT-KEK	
EPINVER	INBK-PIN	OPEX	
EXEX	KEY-PART	OPIM	

reserved

Direction: Input	Type: String

The *reserved* parameter must be a variable of 8 bytes of X'00'.

control_vector

Direction: Output	Type: String

A 16-byte string variable in application storage where the service returns the generated control vector.

Usage Notes

SAF will be invoked to check authorization to use the Control Vector Generate service.

See Table 62 on page 210 for an illustration of key type and key usage keywords that can be combined in the Control Vector Generate and Key Token Build callable services to create a control vector.

Control Vector Translate (CSNBCVT)

The Control Vector Translate callable service changes the control vector used to encipher an external key.

ICSF routes the Control Vector Translate request to a PCI Cryptographic Coprocessor for processing. If no PCI Cryptographic Coprocessor is online, the request fails. See “Appendix M. Changing Control Vectors with the Control Vector Translate Callable Service” on page 423 for additional information about this service.

Format

```
CALL CSNBCVT(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             KEK_key_identifier,
             source_key_token,
             array_key_left,
             mask_array_left,
             array_key_right,
             mask_array_right,
             rule_array_count,
             rule_array,
             target_key_token )
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFFFF' (2 gigabytes). The data is defined in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

KEK_key_identifier

Direction: Input/Output	Type: String

The 64-byte string variable containing an internal key token or the key label of an internal key token record containing the key-encrypting key. The control vector in the internal key token must specify the key type of IMPORTER, EXPORTER, IKEYXLAT, or OKEYXLAT.

source_key_token

Direction: Input	Type: String

A 64-byte string variable containing the external key token with the key and control vector to be processed.

array_key_left

Direction: Input/Output	Type: String

A 64-byte string variable containing an internal key token or a key label of an internal key token record that deciphers the left mask array. The internal key token must contain a control vector specifying a CVARXCVL key type.

mask_array_left

Direction: Input	Type: String

A string of seven 8-byte elements containing the mask array enciphered under the left array key.

array_key_right

Direction: Input/Ouput	Type: String

A 64-byte string variable containing an internal key token or a key label of an internal key token record that deciphers the right mask array. The internal key token must contain a control vector specifying a CVARXCVR key type.

mask_array_right

Direction: Input	Type: String

A string of seven 8-byte elements containing the mask array enciphered under the right array key.

rule_array_count

Direction: Input	Type: Integer

An integer containing the number of elements in the rule array. The value of the *rule_array_count* must be zero, one, or two for this service. If the rule array count is zero, the default keywords ADJUST and LEFT are used.

rule_array

Direction: Input	Type: Character String

The *rule_array* parameter is an array of keywords. The keywords are 8 bytes in length, and must be left-justified and padded on the right with space characters. The rule_array keywords are shown below:

Table 63. Keywords for Control Vector Translate

Keyword	Meaning
Parity Adjustment Rule (optional)	
ADJUST	Ensures that all target key bytes have odd parity. This is the default.
NOADJUST	Prevents the parity of the target being altered.
Key-portion Rule (optional)	
LEFT	Causes an 8-byte source key, or the left half of a 16-byte source key, to be processed with the result placed into both halves of the target key. This is the default.
RIGHT	Causes the right half of a 16-byte source key to be processed with the result placed into the right half of the target key. The left half of the target key is unchanged.
BOTH	Causes both halves of a 16-byte source key to be processed with the result placed into corresponding halves of the target key. When you use the BOTH keyword, the mask array must be able to validate the translation of both halves.
SINGLE	Causes the left half of the source key to be processed with the result placed into the left half of the target key token. The right half of the target key is unchanged.

target_key_token

Direction: Input/Output Type: String

A 64-byte string variable containing an external key token with the new control vector. This key token contains the key halves with the new control vector.

Restriction

The caller must be in task mode, not in SRB mode.

Usage Notes

SAF will be invoked to check authorization to use the Control Vector Translate service and any key labels specified as input.

If *KEK_key_identifier* is a label of an IMPORTER or EXPORTER key, the label must be unique in the CKDS.

Code Conversion (CSNBXEA and CSNBXAE)

Use these utilities to convert ASCII data to EBCDIC data (CSNBXAE) or EBCDIC data to ASCII data (CSNBXEA).

Format

```
CALL CSNBXAE(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            text_length,
            source_text,
            target_text,
            code_table)
```

```
CALL CSNBXEA(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            text_length,
            source_text,
            target_text,
            code_table)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Ignored	Type: Integer

Reserved field.

exit_data

Direction: Ignored	Type: String

Reserved field.

text_length

Direction: Input	Type: Integer

The *text_length* contains an integer that is the length of the *source_text*. The length must be a positive nonzero value.

source_text

Direction: Input Type: String

This parameter contains the string to convert.

target_text

Direction: Output Type: String

The converted text that the callable service returns.

code_table

Direction: Input Type: String

A 256-byte conversion table. When value is zero, this service uses the default code table. See “Appendix I. EBCDIC and ASCII Default Conversion Tables” on page 403 for contents of the default table.

Note: The Transaction Security System code table has 2 additional 8-byte fields that are not used in the conversion process. ICSF accepts either a 256-byte or a 272-byte code table, but uses only the first 256 bytes in the conversion.

Usage Notes

These services are structured differently than the other services. They run in the caller's address space in the caller's key and mode. ICSF need not be active for you to run either of these services. No pre- or post-processing exits are enabled for these services, and no calls to RACF are issued when you run these services.

Character/Nibble Conversion (CSNBXBC and CSNBXCB)

Use these utilities to convert a binary string to a character string (CSNBXBC) or convert a character string to a binary string (CSNBXCB).

Format

```
CALL CSNBXBC(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            text_length,
            source_text,
            target_text,
            code_table)
```

```
CALL CSNBXCB(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             text_length,
             source_text,
             target_text,
             code_table)
```

Parameters

return_code

Direction: Output　　Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output　　Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Ignored　　Type: Integer

Reserved field.

exit_data

Direction: Ignored　　Type: String

Reserved field.

text_length

Direction: Input/Output　　Type: Integer

On input, the *text_length* contains an integer that is the length of the *source_text*. The length must be a positive nonzero value. On output, *text_length* is updated with an integer that is the length of the *target_text*.

source_text

Direction: Input　　Type: String

This parameter contains the string to convert.

target_text

Direction: Output Type: String

The converted text that the callable service returns.

code_table

Direction: Input Type: String

A 16-byte conversion table. The code table for binary to EBCDIC conversion is X'F0F1F2F3F4F5F6F7F8F9C1C2C3C4C5C6'.

Usage Notes

These services are structured differently from the other services. They run in the caller's address space in the caller's key and mode.

ICSF need not be active for you to run either of these services. No pre- or post-processing exits are enabled for these services, and no calls to RACF are issued when you run these services.

X9.9 Data Editing (CSNB9ED)

Use this utility to edit an ASCII text string according to the editing rules of ANSI X9.9-4. It edits the text that the *source_text* parameter supplies according to the following rules. The rules are listed here in the order in which they are applied. It returns the result in the *target_text* parameter.

1. This service replaces each carriage-return (CR) character and each line-feed (LF) character with a single-space character.
2. It replaces each lowercase alphabetic character (a through z) with its equivalent uppercase character (A through Z).
3. It deletes all characters other than the following:
   - Alphabetics A...Z
   - Numerics 0...9
   - Space
   - Comma ,
   - Period .
   - Dash -
   - Solidus /
   - Asterisk *
   - Open parenthesis (
   - Close parenthesis)
4. It deletes all leading space characters.
5. It replaces all sequences of two or more space characters with a single-space character.

Format

```
CALL CSNB9ED(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             text_length,
             source_text,
             target_text)
```

Parameters

return_code

Direction: Output   Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output   Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that are assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Ignored   Type: Integer

Reserved field.

exit_data

Direction: Ignored   Type: String

Reserved field.

text_length

Direction: Input/Output   Type: Integer

On input, the *text_length* contains an integer that is the length of the *source_text*. The length must be a positive, nonzero value. On output, *text_length* is updated with an integer that is the length of the edited text.

source_text

Direction: Input   Type: String

This parameter contains the string to edit.

target_text

Direction: Output	Type: String

The edited text that the callable service returns.

Usage Notes

This service is structured differently from the other services. It runs in the caller's address space in the caller's key and mode.

ICSF need not be active for the service to run. There are no pre-processing or post-processing exits that are enabled for this service. While running, this service does not issue any calls to RACF.

Chapter 12. Trusted Key Entry Workstation Interfaces

For S/390 G3, or higher, Enterprise Servers and S/390 Multiprise Servers, you can order an optional feature, the Trusted Key Entry (TKE) workstation. You can use this to load DES and PKA master keys, SYM-MK and ASYM-MK master keys on the PCI Cryptographic Coprocessor, and securely add operational key-encrypting keys and PIN keys to the CKDS. TKE uses the PKSC interface callable service (CSFPKSC) for support of the Cryptographic Coprocessor Feature and the PCI interface callable service (CSFPCI) for the support of the PCI Cryptographic Coprocessor.

PCI Interface Callable Service (CSFPCI)

TKE uses this callable service to send a request to a specific PCI card queue and remove the corresponding response when complete. This service is synchronous. The return and reason codes reflect the success or failure of the NQAP and DQAP functions rather than the success or failure of the actual PCI request.

Format

```
CALL CSFPCI(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            target_pci_coprocessor,
            target_pci_coprocessor_serial_number,
            request_block_length,
            request_block,
            request_data_block_length,
            request_data_block,
            reply_block_length,
            reply_block,
            reply_data_block_length,
            reply_data_block,
            masks_length,
            masks_data)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. See Appendix A. ICSF and TSS Return and Reason Codes, for a list of return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. See Appendix A. ICSF and TSS Return and Reason Codes for a list of reason codes.

exit_data_length

Direction: Input/Output Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input Type: Integer

The number of keywords you are supplying in *rule_array*. The value must be 1.

rule_array

Direction: Input Type: String

Keyword that provides control information to callable services. The keyword is left-justified in an 8-byte field and padded on the right with blanks. The keyword must be in contiguous storage. The keywords listed below are mutually exclusive.

Table 64. Keywords for PCI Interface Callable Service

Keyword	Meaning
ACPOINTS	Queries the list of access control points which may be enabled or disabled by a TKE user.
APNUM	Specifies the *target_pci_coprocessor* field to be used.
SERIALNO	Specifies the *target_pci_coprocessor_number* field to be used
PCIMASKS	This keyword is a request to return both the 64-bit mask indicating which of the PCI cards are online and 64-bit mask indicating which of the PCI cards are active. See the *masks_data* parameter description for more information.
ACTIVECP	This keyword is a request to call the PCI card initialization code to revalidate the PCI cards. After the PCI card initialization is completed, both the 64-bit mask indicating which of the PCI cards are online and 64-bit mask indicating which of the PCI cards are active will be returned. This keyword is used by the TKE workstation code after the ACTIVATE portion of the domain zeroize command. This is to ensure that the status of the PCI card is accurately reflected to the users. See the *masks_data* parameter description for more information.

| **Note:** When the PCIMASKS and ACTIVEP keywords are specified, the *request_data_block_length*, *request_data_block*, *reply_data_block_length*, and the *reply_data_block* parameters are ignored.

| **target_pci_coprocessor**

Direction: Input	Type: Integer

| The PCI Cryptographic Coprocessor card to which this request is directed. Value is 1 - 64.

target_pci_coprocessor_serial_number

Direction: Input	Type: String

The PCI Cryptographic Coprocessor card serial number to which the request is directed. This parameter may be used instead of the *target_pci_coprocessor*. The length is 8 bytes.

request_block_length

Direction: Input/Output	Type: Integer

Length of CPRB and the request block in the *request_block* field. The maximum length allowed is 5,500 bytes.

request_block

Direction: Input	Type: String

PCI Cryptographic Coprocessor command or query request for the target PCI Cryptographic Coprocessor. This is the complete CPRB and request block to be processed by the PCI Cryptographic Coprocessor.

request_data_block_length

Direction: Input	Type: Integer

Length of request data block in the *request_data_block* field. The maximum length allowed is 6,400 bytes. The length field must be a multiple of 4.

request_data_block

Direction: Input	Type: String

The data that accompanies the *request_block* field.

reply_block_length

Direction: Input/Output	Type: Integer

Length of CPRB and the reply block in the *reply_block* field. The maximum length allowed is 5,500 bytes. This field is updated on output with the actual length of the *reply_block* field.

reply_block

Direction: Output	Type: String

PCI Cryptographic Coprocessor reply from the target PCI Cryptographic Coprocessor. This is the CPRB and reply block that has been processed by the PCI Cryptographic Coprocessor.

reply_data_block_length

Direction: Input/Output	Type: Integer

| Length of reply block in the *reply_data_block* field. The maximum length
| allowed is 6,400 bytes. This field is updated on output with the actual length of
| the *reply_data_block* field. This length field must be a multiple of 4. For the
| ACPOINTS keyword, the minimum length is 2572 bytes.

reply_data_block

Direction: Output	Type: String

The data that accompanies the *reply_block* field.

masks_length

Direction: Input	Type: Integer

Length of the reply data being returned in the *masks_data* field. The length must be 32 bytes. This field is only valid when the input *rule_array* keyword is PCIMASKS or ACTIVECP. For all other *rule_array* keywords, this field is ignored.

masks_data

Direction: Output	Type: String

The data being returned for all requests. The first 8 bytes indicate the count of the PCI cards online. The second 8 bytes indicate a bit mask of the actual PCI cards brought online. The third 8 bytes indicate the count of the PCI cards active. The fourth 8 bytes indicate a bit mask of the actual PCI cards that are active. For the ACTIVECP keyword, if the PCI card initialization failed, the appropriate return code and reason code is issued and the *masks_data* field will contain zeros.

Restriction

The caller must be in task mode, not in SRB mode.

Usage Note

The *target_pci_coprocessor*, the *target_pci_coprocessor_serial_number*, the *request_block*, the *reply_block*, the *request_block_data_block*, and the *reply_block_data_block*, are recorded in SMF Record Type 82, subtype 16.

PKSC Interface Callable Service (CSFPKSC)

TKE uses this callable service to send a request to a specific cryptographic module and receive a corresponding response when processing is complete. The service is synchronous. Note that the return and reason codes reflect the success or failure of CSFPKSC's interaction with the cryptographic module rather than the success or failure of the cryptographic module request. The response block contains the results of the cryptographic module request.

Format

```
CALL CSFPKSC(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            target_crypto_module,
            request_length,
            request,
            response)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

target_crypto_module

Direction: Input	Type: Integer

Cryptographic module to which this request is directed. Value is 0 or 1.

request_length

Direction: Input	Type: Integer

Length of request message in the *request* field. The maximum length allowed is 1024 bytes.

request

Direction: Input	Type: String

PKSC command or query request for the target cryptographic module. This is the complete architected command or query for the cryptographic module to process.

response

Direction: Output	Type: String

Area where the PKSC response from the target cryptographic module is returned to the caller. The area returned can be up to 512 bytes.

Restrictions

The caller must be in task mode, not in SRB mode.

The format and content of the PKSC request and response areas are proprietary IBM hardware information that may be licensed. Customers interested in this information may contact the IBM Director of Licensing. For the address, refer to "Appendix N. Notices" on page 429.

Part 2. Public Key Cryptography

This part of the book introduces Public Key Algorithms (PKA) support and discusses PKA key tokens and key management. It presents PKA callable services for using digital signatures to authenticate messages and users, generating and managing PKA keys, distributing DES and CDMF keys securely, and supporting the Secure Electronic Transaction (SET) protocol.

© Copyright IBM Corp. 1997, 2000

Chapter 13. Introducing PKA Support

The preceding sections of this book focus on DES cryptography or secret-key cryptography. This is symmetric—senders and receivers use the same key (which must be exchanged securely in advance) to encipher and decipher data. DES functions are synchronous and performed at high speed.

Public key cryptography does not require exchanging a secret key. It is asymmetric—the sender and receiver each have a pair of keys, a public key and a different but corresponding private key. PKA functions are performed in an asynchronous processor; this is much slower than for DES functions.

You can use PKA support to exchange CDMF or DES secret keys securely and to compute digital signatures for authenticating messages to users. You can also use public key cryptography in support of secure electronic transactions over open networks, using SET protocols.

PKA Key Algorithms

Public key cryptography uses a key pair consisting of a public key and a private key. The PKA public key uses one of two algorithms:

- Rivest-Shamir-Adleman (RSA)
- Digital Signature Standard (DSS)

The RSA Algorithm

The RSA algorithm is the most widely used and accepted of the public key algorithms. It uses three quantities to encrypt and decrypt text: a public exponent (PU), a private exponent (PR), and a modulus (M). Given these three and some cleartext data, the algorithm generates ciphertext as follows:

$\text{ciphertext} = \text{cleartext}^{PU} \pmod{M}$

Similarly, the following operation recovers cleartext from ciphertext:

$\text{cleartext} = \text{ciphertext}^{PR} \pmod{M}$

An RSA key consists of an exponent and a modulus. The private exponent must be secret, but the public exponent and modulus need not be secret.

Digital Signature Standard (DSS)

The U.S. National Institute of Standards and Technology (NIST) defines DSS in Federal Information Processing Standard (FIPS) Publication 186.

PKA Master Keys

PKA master keys protect private keys. On the S/390 Cryptographic Coprocessor Feature, there are two PKA master keys; the Signature Master Key (SMK) and the RSA Key Management Master Key (KMMK). The SMK protects PKA private keys used only in digital signature services. The KMMK protects PKA private keys used in digital signature services and in the CDMF and DES DATA key distribution functions. On the PCI Cryptographic Coprocessor, PKA keys are protected by the Asymmetric Key Master Key (ASYM-MK).

© Copyright IBM Corp. 1997, 2000

The Asymmetric Key Master Key (ASYM-MK) on the PCI Cryptographic Coprocessor is a triple-length key used to encipher and decipher PKA keys. In order for the PCI Cryptographic Coprocessor to function, the hash pattern of the ASYM-MK must match the hash pattern of the SMK on the Cryptographic Coprocessor Feature. The ICSF administrator installs the PKA master keys on the Cryptographic Coprocessor Feature and the ASYM-MK on the PCI Cryptographic Coprocessor by using either the pass phrase initialization routine, the Clear Master Key Entry panels, or the optional Trusted Key Entry (TKE) workstation.

Before services are enabled on the PCI Cryptographic Coprocessor, the following conditions must be met:

- The Symmetric Key Master Key (SYM-MK) must be installed on the PCI Cryptographic Coprocessor. It must match the Cryptographic Coprocessor Feature DES master key and match the master key that the CKDS was enciphered with.
- The PKDS is required for OS/390 V2 R9 ICSF and above.
- The PKA master keys (SMK and KMMK) on the S/390 Cryptographic Coprocessor Feature must be installed and valid.
- The ASYM-MK PKA master key on the PCI Cryptographic Coprocessor must be installed and valid.
- The hash pattern of the ASYM-MK on the PCI Cryptographic Coprocessor must match the hash pattern of the SMK on the S/390 Cryptographic Coprocessor Feature.

On the S/390 Cryptographic Coprocessor Feature, operational private keys are protected under two layers of DES encryption. They are encrypted under an Object Protection Key (OPK) that in turn is encrypted under the SMK or KMMK. You dynamically generate the OPK for each private key at import time. ICSF provides a public key data set (PKDS) for the storage of application PKA keys. You cannot change PKA master keys dynamically, and there is no reencryption capability for keys enciphered under PKA master keys.

PKA Callable Services

The Cryptographic Coprocessor Feature available on S/390 G3, or higher, Enterprise Servers and S/390 Multiprise Servers provides RSA and DSS digital signature functions, key management functions, and DES and CDMF key distribution functions. The S/390 G5 Enterprise Server field upgrade and S/390 G6 Enterprise Server provide the ability to generate RSA keys on the PCI Cryptographic Coprocessor. ICSF provides application programming interfaces to these functions through callable services. PKA callable services perform cryptographic functions, that include:

- Generating and verifying digital signatures
- Generating and managing PKA keys
  - Generating PKA internal tokens for use with DSS
  - Generating RSA keys on the PCI Cryptographic Coprocessor
  - Importing PKA key tokens
  - Extracting PKA public key tokens from private key tokens
- Distributing CDMF and DES DATA keys, using RSA
  - Generating a symmetric DATA key encrypted under both an RSA key and under DES
  - Importing a symmetric DES DATA key encrypted under an RSA public key

  – Exporting a symmetric DES DATA key to encryption under an RSA public key
- Exchanging DES-encrypted and RSA-encrypted data to establish secure transactions over open networks according to the SET protocols

Callable Services Supporting Digital Signatures

ICSF provides the following services that support digital signatures.

Digital Signature Generate Callable Service

This service generates a digital signature. This service may use either type. It supports the following methods:
- ANSI X9.30 (DSS)
- ISO 9796 (RSA)
- RSA DSI PKCS 1.0 and 1.1 (RSA)
- Padding on the left with zeros (RSA)

The input text must have been previously hashed using the one-way hash generate callable service or the MDC generation service.

Digital Signature Verify Callable Service

This service verifies a digital signature using a PKA public key. (There are two types of PKA public key tokens: RSA and DSS. This service can use either type.) It supports the following methods:
- ANSI X9.30 (DSS)
- ISO 9796 (RSA)
- RSA DSI PKCS 1.0 and 1.1 (RSA)
- Padding on the left with zeros (RSA)

The text that is input to this service must be previously hashed using the one-way hash generate callable service or the MDC generation service.

Callable Services for PKA Key Management

ICSF provides the following services for PKA key management.

PKA Key Generate Callable Service

This service generates a PKA internal token for use with the DSS algorithm in digital signature services. You can then use the PKA public key extract callable service to extract a DSS public key token from the internal key token. With OS/390 V2 R9 ICSF, this service has been enhanced to support the generation of RSA keys on the PCI Cryptographic Coprocessor for use on the PCI Cryptographic Coprocessor.

Input to the PKA key generate callable service is either a skeleton key token created by the PKA key token build callable service or a valid key token. Upon examination of the input skeleton key token, the PKA key generate service routes the key generation request as follows:
- If the skeleton is for a DSS key token, ICSF routes the request to a S/390 Cryptographic Coprocessor Feature.
- If the skeleton is for an RSA key, ICSF routes the request to any available PCI Cryptographic Coprocessor.
- If the skeleton is for a retained RSA key, ICSF routes the request to a PCI Cryptographic Coprocessor where the key is generated and retained for additional security.

PKA Key Import Callable Service

This service imports a PKA private key, which may be RSA or DSS.

| The key token to import can be in the clear or encrypted. The PKA key token build
| utility creates a clear PKA key token. The PKA key generate callable service
| generates either a clear or an encrypted PKA key token.

PKA Public Key Extract Callable Service

This service extracts a PKA public key token from a PKA internal (operational) or external (importable) private key token. It performs no cryptographic verification of the PKA private key token.

Callable Services to Update The Public Key Data Set (PKDS)

The Public Key Data Set (PKDS) is a repository for RSA and DSS public and private keys. An application can store keys in the PKDS and refer to them by label when using any of the callable services which accept public key tokens as input. The PKDS update callable services provide support for creating and writing records to the PKDS and reading and deleting records from the PKDS.

PKDS Record Create Callable Service

This service accepts an RSA or DSS private key token in either external or internal format, or an RSA or DSS public key token and writes a new record to the PKDS. An application can create a null token in the PKDS by specifying a token length of zero. The key label must be unique and the caller must be in task mode and cannot be in SRB mode.

PKDS Record Write Callable Service

This service accepts an RSA or DSS private key token in either external or internal format, or an RSA or DSS public key token and writes over an existing record in the PKDS. An application can check the PKDS for a null record with the label provided and overwrite this record if it does exist. Alternatively, an application can specify to overwrite a record regardless of the contents of the record. The caller must be in task mode and cannot be in SRB mode.

Note: Retained keys cannot be written to the PKDS with the PKDS Record Write service, nor can a retained key record in the PKDS be overwritten with this service.

PKDS Record Read Callable Service

This service reads a record from the PKDS and returns the contents of that record to the caller. The key label must be unique and the caller must be in task mode and cannot be in SRB mode.

PKDS Record Delete Callable Service

This service deletes a record from the PKDS. An application can specify that the entire record be deleted, or that only the contents of the record be deleted. If only the contents of the record are deleted, the record will still exist in the PKDS but will contain only binary zeros. The key label must be unique and the caller must be in task mode and cannot be in SRB mode.

Note: Retained keys cannot be deleted from the PKDS with this service. See “Retained Key Delete (CSNDRKD)” on page 314 for information on deleting retained keys.

Callable Services for Working with Retained Private Keys

Private keys can be generated, retained, and used within the secure boundary of a PCI Cryptographic Coprocessor. Retained keys are generated by the PKA Key Generate (CSNDPKG) callable service. The private key values of retained keys never appear in any form outside the secure boundary. All retained keys have an entry in the PKDS that identifies the PCI Cryptographic Coprocessor where the retained private key is stored. ICSF provides the following callable services to list and delete retained private keys.

Retained Key List Callable Service

The retained key list callable service lists the key labels of private keys that are retained within the boundaries of PCI Cryptographic Coprocessors installed on your server.

Retained Key Delete Callable Service

The retained key delete callable service deletes a key that has been retained within a PCI Cryptographic Coprocessor and also deletes the record containing the key token from the PKDS.

Callable Services for Distributing CDMF and DES DATA Keys

ICSF provides the following services for using RSA to distribute CDMF and DES DATA keys.

Symmetric Key Generate Callable Service

This service generates a symmetric key (that is, a DATA key) and returns it encrypted using DES and encrypted under an RSA public key token. (There are two types of PKA public key tokens: RSA and DSS. This callable service can use only the RSA type.)

The DES-encrypted key can be an internal token encrypted under a host DES master key, or an external form encrypted under a KEK. (You can use the symmetric key import callable service to import the PKA-encrypted form.)

Symmetric Key Import Callable Service

This service imports a symmetric (DES) DATA key enciphered under an RSA public key. (There are two types of PKA private key tokens: RSA and DSS. This callable service can use only the RSA type.) This service returns the key in operational form, enciphered under the DES master key.

Symmetric Key Export Callable Service

This service transfers an application-supplied symmetric key (a DATA key) from encryption under the DES host master key to encryption under an application-supplied RSA public key. (There are two types of PKA public key tokens: RSA and DSS. This callable service can use only the RSA type.) The application-supplied DATA key must be an ICSF DES internal key token or the label of such a token in the CKDS. The symmetric key import callable service can import the PKA-encrypted form at the receiving node.

Callable Services for SET Secure Electronic Transaction

SET is an industry-wide open standard for securing bankcard transactions over open networks. The SET protocol addresses the payment phase of a transaction from the individual, to the merchant, to the acquirer (the merchant's current bankcard processor). It can be used to help ensure the privacy and integrity of real time bankcard payments over the Internet. In addition, with SET in place, everyone in the payment process knows who everyone else is. The card holder, the merchant, and the acquirer can be fully authenticated because the core protocol of SET is based on digital certificates. Each participant in the payment transaction holds a certificate that validates his or her identity. The public key infrastructure allows these digital certificates to be exchanged, checked, and validated for every transaction made over the Internet. The mechanics of this operation are transparent to the application.

Under the SET protocol, every online purchase must be accompanied by a digital certificate which identifies the card-holder to the merchant. The buyer's digital certificate serves as an electronic representation of the buyer's credit card but does not actually show the credit card number to the merchant. Once the merchant's SET application authenticates the buyer's identity, it then decrypts the order information, processes the order, and forwards the still-encrypted payment information to the acquirer for processing. The acquirer's SET application authenticates the buyer's credit card information, identifies the merchant, and arranges settlement. With SET, the Internet becomes a safer, more secure environment for the use of payment cards.

ICSF provides the following callable services that can be used in developing SET applications that make use of the S/390 cryptographic hardware at the merchant and acquirer payment gateway.

SET Block Compose Callable Service

The SET Block Compose callable service performs DES encryption of data, OAEP-formatting through a series of SHA-1 hashing operations, and the RSA-encryption of the Optimal Asymmetric Encryption Padding (OAEP) block.

SET Block Decompose Callable Service

The SET Block Decompose callable service decrypts both the RSA-encrypted and the DES-encrypted data.

Callable Services that Support Secure Sockets Layer (SSL)

The Secure Sockets Layer (SSL) protocol, developed by Netscape Development Corporation, provides communications privacy over the Internet. Client/server applications can use the SSL protocol to provide secure communications and prevent eavesdropping, tampering, or message forgery.

ICSF provides callable services that support the RSA-encryption and RSA-decryption of PKCS 1.2-formatted symmetric key data to produce symmetric session keys. These session keys can then be used to establish an SSL session between the sender and receiver.

PKA Encrypt Callable Service

The PKA encrypt callable service encrypts a supplied clear key value under an RSA public key. Currently, the supplied key can be formatted using the PKCS 1.2 method prior to encryption.

PKA Decrypt Callable Service

The PKA decrypt callable service uses the corresponding private RSA key to unwrap the RSA-encrypted key and deformat the key value. This service then returns the clear key value to the application.

PKA Utility

ICSF provides the following PKA utility.

PKA Key Token Build Callable Service

The PKA key token build callable service is a utility you can use to create an external PKA key token containing an unenciphered private RSA or DSS key. You can supply this token as input to the PKA key import callable service to obtain an operational internal token containing an enciphered private key. You can also use this service to input a clear unenciphered public RSA or DSS key and return the public key in a token format that other PKA services can use directly.

Use this service to build skeleton key tokens for input to the PKA key generate callable service for creation of RSA keys on the PCI Cryptographic Coprocessor.

Chapter 14. Programming Considerations for PKA

This chapter focuses on the PKA key token and PKA key management. It also summarizes PKA callable services.

PKA Key Tokens

PKA key tokens contain RSA or DSS private or public keys. Although DES tokens are 64 bytes, PKA tokens are variable length because they contain either RSA or DSS key values, which are variable in length. Consequently, length parameters precede all PKA token parameters. The maximum allowed size is 2500 bytes. PKA key tokens consist of a token header, any required sections, and any optional sections. Optional sections depend on the token type. PKA key tokens can be public or private, and private key tokens can be internal or external. Therefore, there are three basic types of tokens, each of which can contain either RSA or DSS information:

- A public key token
- A private external key token
- A private internal key token

Public key tokens contain only the public key. Private key tokens contain the public and private key pair. Table 65 summarizes the sections in each type of token.

Table 65. Summary of PKA Key Token Sections

Section	Public External Key Token	Private External Key Token	Private Internal Key Token
Header	X	X	X
RSA or DSS private key information		X	X
RSA or DSS public key information	X	X	X
Key name (optional)		X	X
Internal information			X

As with DES key tokens, the first byte of a PKA key token contains the token identifier which indicates the type of token.

A first byte of X'1E' indicates an external token with a cleartext public key and optionally a private key that is either in cleartext or enciphered by a transport key-encrypting key. An external key token is in importable key form. It can be sent on the link.

A first byte of X'1F' indicates an internal token with a cleartext public key and a private key that is enciphered by the PKA master key and ready for internal use. An internal key token is in operational key form. A PKA private key token must be in operational form for ICSF to use it. (PKA public key tokens are used directly in the external form.)

Formats for public and private external and internal RSA and DSS key tokens begin in “Format of the RSA Public Key Token” on page 388.

© Copyright IBM Corp. 1997, 2000

PKA Key Management

You can also generate PKA keys in several ways.

- Using the ICSF PKA key generate callable service.
- Using the Transaction Security System PKA key generate verb, or a comparable product from another vendor.

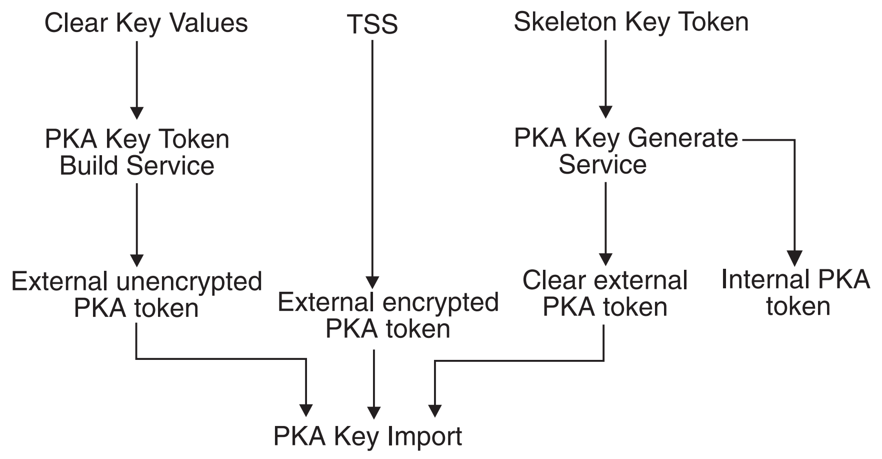


Figure 2. PKA Key Management

If you have a S/390 G5 Enterprise Server, or higher, with a PCI Cryptographic Coprocessor, you can use the ICSF PKA key generate callable service to generate internal and external PKA tokens. You can also generate RSA keys on another system. To input a clear RSA key to ICSF, create the token with the PKA key token build callable service and import it using the PKA key import callable service. To input an encrypted RSA key, generate the key on the Transaction Security System and import it using the PKA key import callable service.

In either case, use the PKA key token build callable service to create a skeleton key token as input (see “PKA Key Token Build (CSNDPKB)” on page 287).

You can generate DSS keys on another system or on ICSF. You need to supply DSS network quantities to the PKA key generate callable service. If you generate DSS keys on another system, you can input them the same way as RSA keys. If you generate a DSS key on ICSF, you can never export it. You can use it on another ICSF host only if the same PKA master keys are installed on both systems.

The PKA key import callable service uses the clear token from the PKA key token build service or a clear or encrypted token from the Transaction Security System to securely import the key token into operational form for ICSF to use. ICSF does not permit the export of the imported PKA key.

The PKA public key extract callable service builds a public key token from a private key token.

Application RSA and DSS public and private keys can be stored in the public key data set (PKDS), a VSAM data set.

Invocation Requirements

The following services have the restriction: The caller must be in task mode, not SRB mode. For all of these, the caller can be in cross-memory mode.

- PKA key import
- Digital signature generate
- Digital signature verify
- Symmetric key export
- Symmetric key import
- Symmetric key generate
- Retained key list
- Retained key delete
- PKA key generate
- SET block compose
- SET block decompose
- PKA encrypt
- PKA decrypt

Exits

Although all services require the *exit_data_length* and *exit_data* parameters, several services ignore them. Installation exits are not enabled for the PKA key token build callable service.

Security and Integrity of the Token

PKA private key tokens may optionally have a 64-byte *private_key_name* field. If *private_key_name* exists, ICSF uses RACHECK to verify it before using the token in a callable service. For additional security, the processor also validates the entire private key token.

Key Identifier for PKA Key Token

A *key identifier* for a PKA key token is a variable length (maximum allowed size is 2500 bytes) area that contains one of the following:

- **Key label** identifies keys that are in the PKDS. Ask your ICSF administrator for the key labels that you can use.
- **Key token** can be either an internal key token, an external key token, or a null key token. Key tokens are generated by an application (for example, using the PKA key generate callable service), or received from another system that can produce external key tokens.

  An **internal key token** can be used only on ICSF, because a PKA master key encrypts the key value. Internal key tokens contain keys in operational form only.

  An **external key token** can be exchanged with other systems because a transport key that is shared with the other system encrypts the key value. External key tokens contain keys in either exportable or importable form.

  A **null key token** consists of 8 bytes of binary zeros. The PKDS Record Create service can be used to write a null token to the PKDS. This PKDS record can subsequently be identified as the target token for the PKA key import or PKA key generate service.

The term *key identifier* is used when a parameter could be one of the above items and to indicate that different inputs are possible. For example, you may want to specify a specific parameter as either an internal key token or a key label. The key label is, in effect, an indirect reference to a stored internal key token.

Key Label

If the first byte of the key identifier is greater than X'40', the field is considered to be holding a **key label**. The contents of a key label are interpreted as a pointer to a public key data set (PKDS) key entry. The key label is an indirect reference to an internal key token.

A key label is specified on callable services with the *key_identifier* parameter as a 64-byte character string, left-justified, and padded on the right with blanks. In most cases, the callable service does not check the syntax of the key label beyond the first byte. One exception is the key record create callable service which enforces the KGUP rules for key labels unless syntax checking is bypassed by a preprocessing exit.

A key label has the following form:

Offset	Length	Data
00-63	64	Key label name

Key Token

A key token is a variable length (maximum allowed size is 2500 bytes) field composed of key value and control information. PKA keys can be either public or private RSA or DSS keys. Each key token can be either an internal key token (the first byte of the key identifier is X'1F'), an external key token (the first byte of the key identifier is X'1E'), or a null PKA private key token (the first byte of the key identifier is X'00'). The following is a list of private key section identifiers for internal and external private RSA key tokens:

Table 66. Internal and External Private RSA Key Token Section Identifiers

Key token	Section identifier
RSA Private Key Token 1024 Modulus-Exponent External Form	X'02'
RSA Private Key Token 2048 Chinese Remainder Theorem External Form	X'08'
RSA Private Key Token 1024 Modulus-Exponent Internal Form (Cryptographic Coprocessor Feature)	X'02'
RSA Private Key Token 1024 Modulus-Exponent Internal Form (PCI Cryptographic Coprocessor)	X'06'
RSA Private Key Token 2048 Chinese Remainder Theorem Internal Form	X'08'

See “Appendix H. Key Token Formats” on page 385 for descriptions of the PKA key tokens.

An internal key token is a token that can be used only on the ICSF system that created it (or another ICSF system with the same PKA master key). It contains a key that is encrypted under the PKA master key.

An application obtains an internal key token by using one of the callable services such as those listed below. The callable services are described in detail in Chapter 20. PKA Key Management.
- PKA key generate

PKA master keys may not be changed dynamically. There is no reencryption capability for keys enciphered under PKA master keys. If a PKA master key is changed, any internal tokens in the PKDS containing keys enciphered by that PKA master key must be recreated.

For debugging information, see Appendix H. Key Token Formats for the format of an internal key token.

If the first byte of the key identifier is X'1E', the key identifier is interpreted as an **external key token**. An external PKA key token contains key (possibly encrypted) and control information. By using the external key token, you can exchange keys between systems.

An application obtains the external key token by using one of the callable services such as those listed below. They are described in detail in Chapter 20. PKA Key Management.

- PKA public key extract
- PKA key import
- PKA key token build
- PKA key generate

For debugging information, see Appendix H. Key Token Formats for the format of an external key token.

If the first byte of the key identifier is X'00', the key identifier is interpreted as a **null key token**. Use the null key token to produce external key tokens.

For debugging information, see Appendix H. Key Token Formats for the format of a null key token.

The Transaction Security System and ICSF Portability

The Transaction Security System PKA verbs from releases prior to 1996 can run only on the Transaction Security System. The PKA96 release of the Transaction Security System PKA verbs generally runs on ICSF without change. As with DES cryptography, you cannot interchange internal PKA tokens but can interchange external tokens.

Summary of the PKA Callable Services

Table 67 lists the PKA callable services, described in this book, and their corresponding verbs. (The PKA services start with CSNDxxx and have corresponding CSFxxx names.) This table also references the chapter that describes the callable service.

Table 67. Summary of PKA Callable Services

Verb	Service Name	Function
Chapter 15. Using Digital Signatures		
CSNDDSG	Digital signature generate	Generates a digital signature using a PKA private key supporting RSA and DSS algorithms.
CSNDDSV	Digital signature verify	Verifies a digital signature using a PKA public key supporting RSA and DSS algorithms.
Chapter 20. PKA Key Management		

Table 67. Summary of PKA Callable Services (continued)

Verb	Service Name	Function
CSNDPKG	PKA key generate	Generates a DSS internal token for use in digital signature services and RSA keys for use on the PCI Cryptographic Coprocessor.
CSNDPKI	PKA key import	Imports a PKA key token containing either a clear PKA key or a PKA key enciphered under a limited authority IMP-PKA KEK.
CSNDPKX	PKA public key extract	Extracts a PKA public key token from a supplied PKA internal or external private key token. Performs no cryptographic verification of the PKA private token.
CSNDKRC	PKDS record create	Writes a new record to the PKDS.
CSNDKRD	PKDS record delete	Delete a record from the PKDS.
CSNDKRR	PKDS record read	Read a record from the PKDS and return the contents of that record.
CSNDKRW	PKDS record write	Write over an existing record in the PKDS.
CSNDRKL	Retained Key List	Lists key labels of keys that have been retained within all currently active PCI Cryptographic Coprocessors.
CSNDRKD	Retained Key Delete	Deletes a key that has been retained within the PCI Cryptographic Coprocessor.
Chapter 16. Key Distribution		
CSNDSYG	Symmetric key generate	Generates a symmetric DATA key and returns the key in two forms: enciphered under the DES master key or KEK and under a PKA public key.
CSNDSYI	Symmetric key import	Imports a symmetric DATA key enciphered under an RSA public key into operational form enciphered under a DES master key.
CSNDSYX	Symmetric key export	Transfers an application-supplied symmetric key (a DATA key) from encryption under the DES host master key to encryption under an application-supplied RSA public key. The application-supplied DATA key must be an ICSF DES internal key token or the label of such a token in the CKDS.
Chapter 17. SET Secure Electronic Transaction		
CSNDSBC	SET block compose	Composes the RSA-OAEP block and the DES-encrypted block in support of the SET protocol.
CSNDSBD	SET block decompose	Decomposes the RSA-OAEP block and the DES-encrypted block to provide unencrypted data back to the caller.
Chapter 18. Secure Sockets Layer (SSL)		
CSNDPKE	PKA encrypt	Encrypts a supplied clear key value under an RSA public key.
CSNDPKD	PKA decrypt	Uses an RSA private key to decrypt the RSA-encrypted key value and return the clear key value to the application.
Chapter 19. PKA Utility		
CSNDPKB	PKA key token build	Creates an external PKA key token containing a clear private RSA or DSS key. Using this token as input to the PKA key import callable service returns an operational internal token containing an enciphered private key. Using CSNDPKB on a clear public RSA or DSS key, returns the public key in a token format that other PKA services can directly use. CSNDPKB can also be used to create a skeleton token for input to the PKA Key Generate service for the generation of an internal DSS or RSA key token.

Chapter 15. Using Digital Signatures

This chapter describes the PKA callable services that support using digital signatures to authenticate messages.
- "Digital Signature Generate (CSNDDSG)"
- "Digital Signature Verify (CSNDDSV)" on page 251

Digital Signature Generate (CSNDDSG)

Use the digital signature generate callable service to generate a digital signature using a PKA private key. The digital signature generate callable service may use either the RSA or DSS private key, depending on the algorithm you are using. This service supports the following methods:
- ANSI X9.30 (DSS)
- ISO 9796 (RSA)
- RSA DSI PKCS 1.0 and 1.1 (RSA)
- Padding on the left with zeros (RSA)

Note: The maximum signature length is 256 bytes (2048 bits).

Input text should have been previously hashed. You can use either the one-way hash generate callable service or the MDC generation callable service.

If the *PKA_private_key_identifier* specifies an RSA private key, you select the method of formatting the text through the *rule_array* parameter. If the *PKA_private_key_identifier* specifies a DSS private key, the DSS signature generated is according to ANSI X9.30. For DSS, the signature is generated on a 20-byte hash created from SHA-1 algorithm.

The digital signature generate callable service examines the RSA key specified in the *PKA_private_key_identifier* to determine how to route the request. If the modulus bit length is less than 512 bits, or if the key is a modulus-exponent form private key with a private section ID of X'02', ICSF routes the request to the S/390 Cryptographic Coprocessor Feature. If the key is a X'08' form CRT private key, or a retained private key, the service routes the request to a PCI Cryptographic Coprocessor. In the case of a retained key, the service routes the request to the specific PCI Cryptographic Coprocessor in which the key is retained. If the key is a modulus-exponent form private key with a private section ID of X'06', the service routes the request as follows:
- If the key use bits indicate signature use only, the digital signature generate service routes the request to either a S/390 Cryptographic Coprocessor Feature or a PCI Cryptographic Coprocessor depending upon availability. If there is no PCI Cryptographic Coprocessor online, the request is routed to a S/390 Cryptographic Coprocessor Feature.
- If the key use bits indicate key-management use is allowed and the KMMK is equal to the SMK on the S/390 Cryptographic Coprocessor Feature, the digital signature generate service routes the request to either a S/390 Cryptographic Coprocessor Feature or a PCI Cryptographic Coprocessor depending upon availability. If there is no PCI Cryptographic Coprocessor online, the request is routed to a S/390 Cryptographic Coprocessor Feature.
- If the key use bits indicate key-management use is allowed and the KMMK is not equal to the SMK on the S/390 Cryptographic Coprocessor Feature, the request

must be processed on a PCI Cryptographic Coprocessor. If there is no PCI Cryptographic Coprocessor online, the request will fail and issue a return and reason code.

Note: For PKCS the message digest and the message-digest algorithm identifier are combined into an ASN.1 value of type DigestInfo, which is BER-encoded to give an octet string D (see Table 68). D is the text string supplied in the *hash* variable.

Format

```
CALL CSNDDSG(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            PKA_private_key_identifier_length,
            PKA_private_key_identifier,
            hash_length,
            hash,
            signature_field_length,
            signature_bit_length,
            signature_field)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input Type: Integer

The number of keywords you are supplying in the *rule_array* parameter. The value must be 0 or 1.

rule_array

Direction: Input Type: String

Keywords that provide control information to the callable service. A keyword specifies the method for calculating the RSA digital signature. Table 68 lists the keywords. Each keyword is left-justified in an 8-byte field and padded on the right with blanks. All keywords must be in contiguous storage.

Table 68. Keywords for Digital Signature Generate Control Information.. Valid only for RSA key types.

Keyword	**Meaning**
ISO-9796	Calculate the digital signature on the *hash* according to ISO-9796. Any hash method is allowed. This is the default.
PKCS-1.0	Calculate the digital signature on the BER-encoded ASN.1 value of the type DigestInfo containing the hash according to the RSA Data Security, Inc. Public Key Cryptography Standards #1 block type 00. The text must have been hashed and BER-encoded before input to this service.
PKCS-1.1	Calculate the digital signature on the BER-encoded ASN.1 value of the type DigestInfo containing the hash according to the RSA Data Security, Inc. Public Key Cryptography Standards #1 block type 01. The text must have been hashed and BER-encoded before input to this service.
ZERO-PAD	Format the hash by padding it on the left with binary zeros to the length of the RSA key modulus. Any supported hash function is allowed.

PKA_private_key_identifier_length

Direction: Input Type: Integer

The length of the *PKA_private_key_identifier* field. The maximum size is 2500 bytes.

PKA_private_key_identifier

Direction: Input Type: String

An internal token or label of the PKA private key or Retained key.

hash_length

Direction: Input Type: Integer

The length of the *hash* parameter in bytes. It must be the exact length of the text to sign. The maximum size is 256 bytes. If you specify ZERO-PAD in the *rule_array* parameter, the input hash length is limited to 32 bytes (256 bits).

hash

Direction: Input	Type: String

The application-supplied text on which to generate the signature. The text must have been previously hashed and, for PKCS formatting, BER-encoded as previously described; see the *rule_array* parameter for more information.

signature_field_length

Direction: Input/Output	Type: Integer

The length in bytes of the *signature_field* to contain the generated digital signature.

Note: For RSA this must be at least the RSA modulus size (rounded up to a byte). For DSS this must be at least 40 bytes. For RSA and DSS, this field is updated with the minimum byte length of the digital signature. The maximum size is 256 bytes.

signature_bit_length

Direction: Output	Type: Integer

The bit length of the digital signature generated. For ISO-9796 this is 1 less than the modulus length. For other RSA processing methods, this is the modulus length. For DSS, this is 320.

signature_field

Direction: Output	Type: String

The digital signature generated is returned in this field. The digital signature is in the low-order bits (right-justified) of a string whose length is the minimum number of bytes that can contain the digital signature. This string is left-justified within the *signature_field*. Any unused bytes to the right are undefined.

Restrictions

Although ISO-9796 does not require the input hash to be an integral number of bytes in length, this service requires you to specify the *hash_length* in bytes.

The caller must be in task mode and not in SRB mode.

Usage Notes

ANSI X9.31 can be implemented by using MD2, MD5, SHA-1, or PADMDC-2 as a hashing algorithm on the text and then using the ISO-9796 RSA method for generating digital signatures.

Digital Signature Verify (CSNDDSV)

Use the digital signature verify callable service to verify a digital signature using a PKA public key. The digital signature verify callable service can use the RSA or DSS public key, depending on the digital signature algorithm used to generate the signature. This service supports the following methods:

- ANSI X9.30 (DSS)
- ISO 9796 (RSA)
- RSA DSI PKCS 1.0 and 1.1 (RSA)
- Padding on the left with zeros (RSA)

Input text should have been previously hashed. You can use either the one-way hash generate callable service or the MDC generation callable service.

This service routes requests to the S/390 Cryptographic Coprocessor Feature.

Note: The maximum signature length is 256 bytes (2048 bits).

Format

```
CALL CSNDDSV(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            PKA_public_key_identifier_length,
            PKA_public_key_identifier,
            hash_length,
            hash,
            signature_field_length,
            signature_field)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you are supplying in the *rule_array* parameter. The value must be 0 or 1.

rule_array

Direction: Input	Type: String

Keywords that provide control information to the callable service. A keyword specifies the method to use to verify the RSA digital signature. Table 69 lists the keywords. Each keyword is left-justified in an 8-byte field and padded on the right with blanks. All keywords must be in contiguous storage.

Table 69. Keywords for Digital Signature Verify Control Information. Valid Only for RSA Key Types.

Keyword	Meaning
ISO-9796	Verify the digital signature on the hash according to ISO-9796. Any hash method is allowed. This is the default.
PKCS-1.0	Verify the digital signature on the BER-encoded ASN.1 value of the type DigestInfo as specified in the RSA Data Security, Inc. Public Key Cryptography Standards #1 block type 00. The text must have been hashed and BER-encoded before input to this service.
PKCS-1.1	Verify the digital signature on the BER-encoded ASN.1 value of the type DigestInfo as specified in the RSA Data Security, Inc. Public Key Cryptography Standards #1 block type 01. The text must have been hashed and BER-encoded before input to this service.
ZERO-PAD	Format the hash by padding it on the left with binary zeros to the length of the PKA key modulus. Any supported hash function is allowed.

PKA_public_key_identifier_length

Direction: Input	Type: Integer

The length of the *PKA_public_key_identifier* field containing the public key token or label. The maximum size is 2500 bytes.

PKA_public_key_identifier

Direction: Input	Type: String

A token or label of the PKA public key.

hash_length

Direction: Input	Type: Integer

The length of the *hash* parameter in bytes. It must be the exact length of the text that was signed. The maximum size is 256 bytes.

hash

Direction: Input	Type: String

The application-supplied text on which the supplied signature was generated. The text must have been previously hashed and, for PKCS formatting, BER-encoded as previously described.

signature_field_length

Direction: Input	Type: Integer

The length in bytes of the *signature_field* parameter. The maximum size is 256 bytes.

signature_field

Direction: Input	Type: String

This field contains the digital signature to verify. The digital signature is in the low-order bits (right-justified) of a string whose length is the minimum number of bytes that can contain the digital signature. This string is left-justified within the *signature_field*.

Restrictions

The ability to recover a message from a signature (which ISO-9796 allows but does not require) is **not** supported.

The exponent of the RSA public key must be odd.

Although ISO-9796 does not require the input hash to be an integral number of bytes in length, this service requires you to specify the *hash_length* in bytes.

The caller must be in task mode and not in SRB mode.

Usage Note

For DSS if r=0 or s=0 then verification always fails. The DSS digital signature is of the form r || s, each 20 bytes.

Chapter 16. Key Distribution

This chapter describes the callable services for distributing CDMF and DES DATA keys using RSA.

- "Symmetric Key Generate (CSNDSYG)"
- "Symmetric Key Import (CSNDSYI)" on page 259
- "Symmetric Key Export (CSNDSYX)" on page 262

Symmetric Key Generate (CSNDSYG)

Use the symmetric key generate callable service to generate a symmetric key (a DATA key) and return the key in two forms: DES-encrypted and encrypted under an RSA public key. (There are two types of PKA public key tokens: RSA and DSS. This callable service uses only the RSA type.) The DES encryption may be in the form of an internal token encrypted under the host DES master Key or in the external form encrypted under a key-encrypting key. You can import the PKA-encrypted form by using the symmetric key import service at the receiving node. Also use the symmetric key generate callable service to generate any importer or exporter key-encrypting key encrypted under a PKA96 RSA public key according to the PKA92 formatting structure. See "Appendix L. PKA92 Key Format and Encryption Process" on page 421 for more details about PKA92 formatting.

The generated internal DATA key token is marked according to the system default algorithm.

Note: Token marking is only performed if the service is processed on the Cryptographic Coprocessor Feature.

ICSF routes this service to a PCI Cryptographic Coprocessor if one is available on your server. This service will not be routed to a PCI Cryptographic Coprocessor if the modulus bit length of the RSA public key is less than 512 bits.

Format

```
CALL CSNDSYG(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             rule_array_count,
             rule_array,
             key_encrypting_key_identifier,
             RSA_public_key_identifier_length,
             RSA_public_key_identifier,
             DES_enciphered_key_token_length,
             DES_enciphered_key_token,
             RSA_enciphered_key_length,
             RSA_enciphered_key)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input Type: Integer

The number of keywords you supplied in the *rule_array* parameter. The value must be 1 or 2.

rule_array

Direction: Input Type: String

Keywords that provide control information to the callable service. Table 70 lists the keywords. The recovery method is the method to use to recover the symmetric key. Each keyword is left-justified in an 8-byte field and padded on the right with blanks. All keywords must be in contiguous storage.

Table 70. Keywords for Symmetric Key Generate Control Information

Keyword	Meaning
Recovery Method (required)	
PKCS-1.2	Specifies the method found in RSA DSI PKCS #1 block type 02.
ZERO-PAD	The clear key is right-justified in the field provided, and the field is padded to the left with zeroes up to the size of the RSA encryption block (which is the modulus length).
| PKA92	Specifies the key-encrypting key is to be encrypted under a PKA96 RSA public key according to the PKA92 formatting structure.
Form of the DES_Enciphered_Key_Token (optional)	

Table 70. Keywords for Symmetric Key Generate Control Information (continued)

Keyword	Meaning
OP	The DES enciphered key is enciphered by the master key. The *key_encrypting_key_identifier* parameter is ignored. This is the default.
IM	The DES enciphered key is enciphered by an IMPORTER key that is provided through the *key_encrypting_key_identifier* parameter. This form requires the enabling of Special Secure Mode. Special Secure Mode is not required if a PCI Cryptographic Coprocessor is available and the modulus bit length is greater than or equal to 512 bits.
EX	The DES enciphered key is enciphered by an EXPORTER key that is provided through the *key_encrypting_key_identifier* parameter.
DES Key Length (optional)	
KEYLN8	Generates a single-length DES key. This is the default.
KEYLN16	Generates a double-length DES DATA key.
KEYLN24	Generates a triple-length DES DATA key.
SINGLE	Generates a single-length DES key.
DOUBLE	Generates a double-length DES key.
SINGLE-R	Generates a key-encrypting key that has equal left and right halves allowing it to perform as a single-length key. Valid only for the recovery method of PKA92.

key_encrypting_key_identifier

Direction: Input/Output Type: String

The label or internal token of a key-encrypting key. If the *rule_array* specifies IM, this DES key must be an IMPORTER. If the *rule_array* specifies EX, this DES key must be an EXPORTER.

RSA_public_key_identifier_length

Direction: Input Type: Integer

The length of the *RSA_public_key_identifier* parameter. If the *RSA_public_key_identifier* parameter is a label, this parameter specifies the length of the label. The maximum size is 2500 bytes.

RSA_public_key_identifier

Direction: Input Type: String

The token, or label, of the RSA public key to be used for protecting the generated symmetric key.

DES_enciphered_key_token_length

Direction: Input/Output Type: Integer

The length of the *DES_enciphered_key_token*. This field is updated with the actual length of the *DES_enciphered_key_token* that is generated. The minimum size is 64 bytes. The maximum size is 128 bytes.

DES_enciphered_key_token

Direction: Input/Output	Type: String

This parameter contains the generated DES-enciphered DATA key in the form of an internal or external token, depending on *rule_array* specification.

RSA_enciphered_key_length

Direction: Input/Output	Type: Integer

The length of the *RSA_enciphered_key* parameter. This service updates this with the actual length of the *RSA_enciphered_key* it generates. The maximum size is 256 bytes.

RSA_enciphered_key

Direction: Input/Output	Type: String

| This field contains the RSA enciphered key, which the public key specified in
| the *RSA_public_key_identifier* field protects. If you specify PKA92, on input
| specify an internal (operational) DES key token.

Restrictions

- If you specify IM in the *rule_array*, you must enable Special Secure Mode.
- | Special Secure Mode is not required if a PCI Cryptographic Coprocessor is
  | available and the modulus bit length of the RSA public key is greater than or
  | equal to 512 bits.
- The caller must be in task mode and not in SRB mode.
- | Use of PKA92 requires the optional PCI Cryptographic Coprocessor.

Usage Notes

The hardware configuration sets the limit on the modulus size of keys for key management; thus, this service will fail if the RSA key modulus bit length exceeds this limit. The service will fail with return code 12 and reason code 11020.

| Specification of PKA92 with an input NOCV key-encrypting key token is not
| supported.

| Use the PKA92 key-formatting method to generate a key-encrypting key. The
| service enciphers one key copy using the key encipherment technique employed in
| the IBM Transaction Security System (TSS) 4753, 4755, and AS/400 cryptographic
| product PKA92 implementations (see “Appendix L. PKA92 Key Format and
| Encryption Process” on page 421). The control vector for the RSA-enciphered copy
| of the key is taken from an internal (operational) DES key token that must be
| present on input in the *RSA_enciphered_key* variable. Only key-encrypting keys
| that conform to the rules for an OPEX case under the key generate service are
| permitted. The control vector for the local key is taken from a DES key token that
| must be present on input in the *DES_enciphered_key_token* variable. The control

vector for one key copy must be from the EXPORTER class while the control vector for the other key copy must be from the IMPORTER class.

Symmetric Key Import (CSNDSYI)

Use the symmetric key import callable service to import a symmetric (DES) DATA key enciphered under an RSA public key. (There are two types of PKA private key tokens: RSA and DSS. This callable service uses only the RSA type.) It returns the key in operational form, enciphered under the master key. It marks the key according to the system's default encryption algorithm, unless token copying overrides this. Marking of data encryption algorithm bits and token copying are only performed if the service is executed on the Cryptographic Coprocessor Feature. The symmetric key import service also supports import of a PKA92-formatted DES key-encrypting key under a PKA96 RSA private key.

The symmetric key import callable service examines the RSA key specified in the *RSA_private_key_identifier* parameter to determine how to route the request. If the key is a modulus-exponent form private key with a private section ID of X'02', ICSF routes the request to the S/390 Cryptographic Coprocessor Feature. If the token modulus bit length is less than 512, the request will also be routed to the Cryptographic Coprocessor Feature. In either of these cases, if the PKA92 recovery method is specified, the request will fail. If the key is a modulus-exponent form private key with a private section ID of X'06', a CRT form private key with a section ID of X'08', or a retained private key, ICSF routes the request to a PCI Cryptographic Coprocessor. In the case of a retained key, the service routes the request to the specific PCI Cryptographic Coprocessor in which the key is retained. If there is no PCI Cryptographic Coprocessor online:

- and the *RSA_private_key_identifier* is a retained private key or a CRT form private key, the request will fail and a return and reason code will be issued
- and the KMMK is equal to the SMK on the S/390 Cryptographic Coprocessor Feature, ICSF routes the request to a Cryptographic Coprocessor Feature
- and the KMMK is not equal to the SMK on the S/390 Cryptographic Coprocessor Feature, the request must be processed on a PCI Cryptographic Coprocessor. Since there is no PCI Cryptographic Coprocessor online, the request will fail and a return code and reason code will be issued.
- and the PKA92 recovery method is specified, the request will fail.

Format

```
CALL CSNDSYI(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            RSA_enciphered_key_length,
            RSA_enciphered_key,
            RSA_private_key_identifier_length,
            RSA_private_key_identifier,
            target_key_identifier_length,
            target_key_identifier)
```

Parameters

return_code

Direction: Output   Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output   Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output   Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output   Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input   Type: Integer

The number of keywords you supplied in the *rule_array* parameter. The value must be 1.

rule_array

Direction: Input   Type: String

The keyword that provides control information to the callable service. Table 71 provides a list. The recovery method is the method to use to recover the symmetric key. The keyword is left-justified in an 8-byte field and padded on the right with blanks.

Table 71. Keywords for Symmetric Key Import Control Information

Keyword	Meaning
Recovery Method (required)	
PKCS-1.2	Specifies the method found in RSA DSI PKCS #1 block type 02.

Table 71. Keywords for Symmetric Key Import Control Information (continued)

Keyword	Meaning
ZERO-PAD	The clear key is right-justified in the field provided, and the field is padded to the left with zeroes up to the size of the RSA encryption block (which is the modulus length).
PKA92	Specifies the key-encrypting key is encrypted under a PKA96 RSA public key according to the PKA92 formatting structure.

RSA_enciphered_key_length

Direction: Input Type: integer

The length of the *RSA_enciphered_key* parameter. The maximum size is 256 bytes.

RSA_enciphered_key

Direction: Input Type: String

The key to import, protected under an RSA public key. The encrypted key is in the low-order bits (right-justified) of a string whose length is the minimum number of bytes that can contain the encrypted key. This string is left-justified within the *RSA_enciphered_key* parameter.

RSA_private_key_identifier_length

Direction: Input Type: Integer

The length of the *RSA_private_key_identifier* parameter. When the *RSA_private_key_identifier* parameter is a key label, this field specifies the length of the label. The maximum size is 2500 bytes.

RSA_private_key_identifier

Direction: Input Type: String

An internal RSA private key token or label whose corresponding public key protects the symmetric key.

target_key_identifier_length

Direction: Input/Output Type: Integer

The length of the *target_key_identifier* parameter. This field is updated with the actual length of the *target_key_identifier* that is generated. The size must be 64 bytes.

target_key_identifier

Direction: Input/Output Type: String

This field contains the internal token of the imported symmetric key. It is marked according to the system default algorithm, CDMF or DES. If you supply as input a valid internal token of an 8-byte DATA key, this service propagates the algorithm markings from the supplied token to the imported DATA key. If the key length is 16 or 24, however, the key token is marked as DES. Propagation of token markings is only relevant when this service is processed on the Cryptographic Coprocessor Feature.

Except for PKA-92 processing, this service produces a DATA key token with a key of the same length as that contained in the imported token.

Restrictions

- The exponent of the RSA public key must be odd.
- The caller must be in task mode and not in SRB mode.
- Use of PKA92 requires the optional PCI Cryptographic Coprocessor.

Usage Notes

The hardware configuration sets the limit on the modulus size of keys for key management; thus, this service will fail if the RSA key modulus bit length exceeds this limit. The service will fail with return code 12 and reason code 11020.

Specification of PKA92 with an input NOCV key-encrypting key token is not supported.

During initialization of a PCI Cryptographic Coprocessor, an Environment Identification, or EID, of zero will be set in the coprocessor. This will be interpreted by the PKA Symmetric Key Import service to mean that environment identification checking is to be bypassed. Thus it is possible on a S/390 system for a key-encrypting key RSA-enciphered at a node (EID) to be imported at the same node.

Symmetric Key Export (CSNDSYX)

Use the symmetric key export callable service to transfer an application-supplied symmetric key (a DATA key) from encryption under the DES host master key to encryption under an application-supplied RSA public key. The application-supplied DATA key must be an ICSF DES internal key token or the label of such a token in the CKDS. The symmetric key import callable service can import the PKA-encrypted form at the receiving node.

This service requires the enhanced system keys to be present in the CKDS.

ICSF routes this service to a PCI Cryptographic Coprocessor if one is available on your server. This service will not be routed to a PCI Cryptographic Coprocessor if the modulus bit length of the RSA public key is less than 512 bits.

Format

```
CALL CSNDSYX(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             rule_array_count,
             rule_array,
             DATA_key_identifier_length,
             DATA_key_identifier,
             RSA_public_key_identifier_length,
             RSA_public_key_identifier,
             RSA_enciphered_key_length,
             RSA_enciphered_key)
```

Parameters

return_code

Direction: Output Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input Type: Integer

The number of keywords you are supplying in the *rule_array* parameter. Value must be 1.

rule_array

Direction: Input Type: String

Keywords that provide control information to the callable service. Table 72 lists the keywords. Each keyword is left-justified in 8-byte fields and padded on the right with blanks. All keywords must be in contiguous storage.

Table 72. Keywords for Symmetric Key Export Control Information

Keyword	Meaning
Recovery Method (required)	
PKCS–1.2	Specifies using the method found in RSA DSI PKCS #1 block type 02 to recover the symmetric key.
ZERO-PAD	The clear key is right-justified in the field provided, and the field is padded to the left with zeroes up to the size of the RSA encryption block (which is the modulus length).

DATA_key_identifier_length

Direction: Input Type: Integer

The length of the *DATA_key_identifier* parameter. The minimum size is 64 bytes. The maximum size is 128 bytes.

DATA_key_identifier

Direction: Input/Output Type: Integer

The label or internal token of a DATA key to export for encryption under the supplied RSA public key. This service exports a DATA key of the same length as the key specified in this parameter.

RSA_public_key_identifier_length

Direction: Input Type: Integer

The length of the *RSA_public_key_identifier* parameter. The maximum size is 2500 bytes.

RSA_public_key_identifier

Direction: Input Type: String

A PKA public key token or label of the key to protect the exported symmetric key.

RSA_enciphered_key_length

Direction: Input/Output Type: Integer

The length of the *RSA_enciphered_key* parameter. This is updated with the actual length of the *RSA_enciphered_key* generated. The maximum size is 256 bytes.

RSA_enciphered_key

Direction: Output	Type: String

This field contains the RSA_enciphered key, protected by the public key specified in the *RSA_public_key_identifier* field.

Restrictions

- The enhanced system keys must be present in the CKDS.
- Caller must be task mode and not in SRB mode.

Usage Notes

- This service requires that the enhanced system keys be installed in the CKDS.
- The hardware configuration sets the limit on the modulus size of keys for key management; thus, this service will fail if the RSA key modulus bit length exceeds this limit. The service will fail with return code 12 and reason code 11020.

Chapter 17. SET Secure Electronic Transaction

The SET Secure Electronic Transaction protocol is an industry-wide open standard for securing bankcard transactions over open networks. SET, which was cooperatively developed by MasterCard and Visa, with the assistance of a number of technology industry partners including IBM, is designed to help ensure the privacy and integrity of real time bankcard payments over the Internet. With SET, the Internet becomes a safer, more secure environment for the use of payment cards.

The SET protocol addresses the payment phase of a transaction from the individual, to the merchant, to the acquirer (the merchant's current payment card processor). With SET in place, everyone in the payment process knows who everyone else is. The card holder, the merchant, and the acquirer can be fully authenticated because the core protocol of SET is based on digital certificates. Each participant in the payment transaction holds a certificate that validates his or her identity. The public key infrastructure allows these digital certificates to be exchanged, checked, and validated for every transaction made over the Internet. The mechanics of this operation are transparent to the application.

The SET Block Compose and SET Block Decompose callable services make use of the S/390 cryptographic hardware at the merchant and acquirer payment gateway.

SET Block Compose (CSNDSBC)

The SET Block Compose callable service performs DES-encryption of data, OAEP-formatting through a series of SHA-1 hashing operations, and the RSA-encryption of the Optimal Asymmetric Encryption Padding (OAEP) block.

This service routes the request to a PCI Cryptographic Coprocessor to perform the RSA-OAEP processing. If there are no PCI Cryptographic Coprocessors online, the request is routed to the S/390 Cryptographic Coprocessor Feature.

Format

```
CALL CSNDSBC(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            block_contents_identifier,
            XData_string_length,
            XData_string,
            data_to_encrypt_length,
            data_to_encrypt,
            data_to_hash_length,
            data_to_hash,
            initialization_vector,
            RSA_public_key_identifier_length,
            RSA_public_key_identifier,
            DES_key_block_length,
            DES_key_block,
            RSA-OAEP_block_length,
            RSA-OAEP_block,
            chaining_vector,
            DES_encrypted_data_block )
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicates specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input Type: Integer

The number of keywords you are supplying in the *rule_array* parameter. The value must be at least 1.

rule_array

Direction: Input Type: Character String

Keywords that provides control information to the callable service. The keyword must be in 8 bytes of contiguous storage, left-justified and padded on the right with blanks.

Table 73. Keywords for SET Block Compose Control Information

Keyword	**Meaning**
Block Type (required)	
SET1.00	The structure of the RSA-OAEP encrypted block is defined by SET protocol.
Formatting Information (optional)	
DES-ONLY	DES encryption only is to be performed; no RSA-OAEP formatting will be performed. (See Usage Notes.)

block_contents_identifier

Direction: Input Type: String

A one-byte string, containing a binary value that will be copied into the Block Contents (BC) field of the SET DB data block (indicates what data is carried in the Actual Data Block, ADB, and the format of any extra data (*XData_string*)). This parameter is ignored if DES-ONLY is specified in the rule-array.

XData_string_length

Direction: Input Type: Integer

The length in bytes of the data contained within *XData_string*. The maximum length is 94 bytes. This parameter is ignored if DES-ONLY is specified in the rule-array.

XData_string

Direction: Input Type: String

Extra-encrypted data contained within the OAEP-processed and RSA-encrypted block. The format is indicated by *block_contents_identifier*. For a *XData_string_length* value of zero, *XData_string* must still be specified, but will be ignored by ICSF. The string is treated as a string of hexadecimal digits. This parameter is ignored if DES-ONLY is specified in the rule-array.

data_to_encrypt_length

Direction: Input/Output	Type: Integer

The length in bytes of data that is to be DES-encrypted. The length has a maximum value of 32 MB minus 8 bytes to allow for up to 8 bytes of padding. The data is identified in the *data_to_encrypt* parameter. On output, this value is updated with the length of the encrypted data in the *DES_encrypted_data_block*. The length is not checked against the MAXLEN parameter for an installation-specified maximum length.

data_to_encrypt

Direction: Input	Type: String

The data that is to be DES-encrypted (with a 64-bit DES key generated by this service). The data will be padded by this service according to the PKSC #5 padding rules.

data_to_hash_length

Direction: Input	Type: Integer

The length in bytes of the data to be hashed. The hash is an optional part of the OAEP block. If the *data_to_hash_length* is 0, no hash will be included in the OAEP block. The length is not checked against the MAXLEN parameter for an installation-specified maximum length. This parameter is ignored if DES-ONLY is specified in the *rule_array* parameter.

data_to_hash

Direction: Input	Type: String

The data that is to be hashed and included in the OAEP block. No hash is computed or inserted in the OAEP block if the *data_to_hash_length* is 0. This parameter is ignored if DES-ONLY is specified in the *rule_array* parameter.

initialization_vector

Direction: Input	Type: String

An 8-byte string containing the initialization vector to be used for the cipher block chaining for the DES encryption of the data in the *data_to_encrypt* parameter. The same initialization vector must be used to perform the DES decryption of the data.

RSA_public_key_identifier_length

Direction: Input	Type: Integer

The length of the *RSA_public_key_identifier* field. The maximum size is 2500 bytes. This parameter is ignored if DES-ONLY is specified in the rule-array.

RSA_public_key_identifier

Direction: Input Type: String

| A string containing either the key label of the RSA public key or the RSA public
| key token to be used to perform the RSA encryption of the OAEP block. The
| modulus bit length of the key must be 1024 bytes. This parameter is ignored if
| DES-ONLY is specified in the rule-array.

DES_key_block_length

Direction: Input/Output Type: Integer

The length of the *DES_key_block*. The current length of this field is defined to be exactly 64 bytes.

DES_key_block

Direction: Input/Output Type: String

The DES key information returned from a previous SET Block Compose service. The contents of the *DES_key_block* is the 64-byte DES internal key token (containing the DES key enciphered under the host master key). Your application program must not change the data in this string.

RSA-OAEP_block_length

Direction: Input/Output Type: Integer

The length of a block of storage to hold the *RSA-OAEP_block*. The length must be at least 128 bytes on input. The length value will be updated on exit with the actual length of the *RSA-OAEP_block*, which is exactly 128 bytes. This parameter is ignored if DES-ONLY is specified in the rule-array.

RSA-OAEP_block

Direction: Output Type: String

The OAEP-formatted data block, encrypted under the RSA public key passed as *RSA_public_key_identifier*. When the OAEP-formatted data block is returned, it is left justified within the *RSA-OAEP_block* field if the input field length (*RSA-OAEP_block_length*) was greater than 128 bytes. This parameter is ignored if DES-ONLY is specified in the rule-array.

chaining_vector

Direction: Input/Output Type: String

An 18-byte field that ICSF uses as a system work area. Your application program must not change the data in this string. This field is ignored by this service, but must be specified.

DES_encrypted_data_block

Direction: Output Type: String

The DES-encrypted data block (data passed in as *data_to_encrypt*). The length of the encrypted data is returned in *data_to_encrypt_length*. The *DES_encrypted_data_block* may be 8 bytes longer than the length of the *data_to_encrypt* because of padding added by this service.

Restrictions

- Caller must be task mode and must not be SRB mode.
- Not all CCA implementations support a key label as input in the *RSA_public_key_identifier* parameter. Some implementations may only support a key token.
- The *data_to_encrypt* and the *DES_encrypted_data_block* cannot overlap.
- NOCV keys must be installed in the CKDS to use SET block compose service on a CDMF-only system.

Usage Notes

- RACF will be invoked to check authorization to use the SET Block Compose service.
- The first time the SET Block Compose service is invoked to form an RSA-OAEP block and DES-encrypt data for communication between a specific source and destination (for example, between the merchant and payment gateway), do not specify the DES-ONLY keyword. A DES key will be generated by the service and returned in the key token contained in the *DES_key_block*. On subsequent calls to the Compose SET Block service for communication between the same source and destination, the DES key can be re-used. The caller of the service must supply the *DES_key_block*, the *DES_key_block_length*, the *data_to_encrypt*, the *data_to_encrypt_length*, and the rule-array keywords SET1.00 and DES-ONLY. You do not need to supply the block contents identifier, XDATA string and length, RSA-OAEP block and length, and RSA public key information, although you must still specify the parameters. For this invocation, the RSA-OAEP formatting is bypassed and only DES encryption is performed, using the supplied DES key.

SET Block Decompose (CSNDSBD)

Decomposes the RSA-OAEP block and the DES-encrypted data block of the SET protocol to provide unencrypted data back to the caller.

| The SET block decompose callable service will route the request to a PCI
| Cryptographic Coprocessor for RSA-OAEP processing if there is a PCI
| Cryptographic Coprocessor available. The service has a preference for being
| processed on a PCI Cryptographic Coprocessor so that the symmetric key does not
| appear in the clear. If there is no PCI Cryptographic Coprocessor available, the
| request will be processed on the Cryptographic Coprocessor Feature, unless the
| *RSA_private_key_identifier* specifies a retained private key or a CRT form private
| key with private key section identifier of X'08', or unless the PINBLOCK rule array
| keyword was specified. These cases require a PCI Cryptographic Coprocessor, and
| the service will fail if no PCI Cryptographic Coprocessor is available.

Format

```
CALL CSNDSBD(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             rule_array_count,
             rule_array,
             RSA-OAEP_block_length,
             RSA-OAEP_block,
             DES_encrypted_data_block_length,
             DES_encrypted_data_block,
             initialization_vector,
             RSA_private_key_identifier_length,
             RSA_private_key_identifier,
             DES_key_block_length,
             DES_key_block,
             block_contents_identifier,
             XData_string_length,
             XData_string,
             chaining_vector,
             data_block,
             hash_block_length,
             hash_block)
```

Parameters

return_code

Direction: Output   Type: Integer

The return code specifies the general result of the callable service. "Appendix A. ICSF and TSS Return and Reason Codes" on page 319 lists the return codes.

reason_code

Direction: Output   Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicates specific processing problems. "Appendix A. ICSF and TSS Return and Reason Codes" on page 319 lists the reason codes.

exit_data_length

Direction: Input/Output   Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output   Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input Type: Integer

The number of keywords you are supplying in the *rule_array* parameter. The value must be at least 1.

rule_array

Direction: Input Type: String

One keyword that provides control information to the callable service. The keyword indicates the block type. The keyword must be in 8 bytes of contiguous storage, left-justified and padded on the right with blanks.

Table 74. Keywords for SET Block Compose Control Information

Keyword	Meaning
Block Type (required)	
SET1.00	The structure of the RSA-OAEP encrypted block is defined by SET protocol.
Formatting Information (optional)	
DES-ONLY	DES decryption only is to be performed; no RSA-OAEP block decryption will be performed. (See Usage Notes.)
PINBLOCK	Specifies that the OAEP block will contain PIN information in the XDATA field, including an ISO-0 format PIN block. The *DES_key_block* must be 128 bytes in length and contain a IPINENC or OPINENC key. The PIN block will be encrypted under the PIN encrypting key. The PIN information and the encrypted PIN block are returned in the *XDATA_string* parameter.

RSA-OAEP_block_length

Direction: Input Type: Integer

The length of *RSA-OAEP_block* must be 128 bytes. This parameter is ignored if DES-ONLY is specified in the rule-array.

RSA-OAEP_block

Direction: Input Type: String

The RSA-encrypted OAEP-formatted data block. This parameter is ignored if DES-ONLY is specified in the rule-array.

DES_encrypted_data_block_length

Direction: Input/Output Type: Integer

The length in bytes of the DES-encrypted data block. The input length must be a multiple of 8 bytes. Updated on return to the length of the decrypted data returned in *data_block*. The maximum value of

DES_encrypted_data_block_length is 32MB bytes. The length is not checked against the MAXLEN parameter for an installation-specified maximum length.

DES_encrypted_data_block

Direction: Input	Type: String

The DES-encrypted data block. The data will be decrypted and passed back as *data_block*.

initialization_vector

Direction: Input	Type: String

An 8-byte string containing the initialization vector to be used for the cipher block chaining for the DES decryption of the data in the *DES_encrypted_data_block* parameter. You must use the same initialization vector that was used to perform the DES encryption of the data.

RSA_private_key_identifier_length

Direction: Input	Type: Integer

The length of the *RSA_private_key_identifier* field. The maximum size is 2500 bytes. This parameter is ignored if DES-ONLY is specified in the rule-array.

RSA_private_key_identifier

Direction: Input	Type: String

A key label of the RSA private key or an internal token of the RSA private key to be used to decipher the RSA-OAEP block passed in *RSA-OAEP_block*. The modulus bit length of the key must be 1024. This parameter is ignored if DES-ONLY is specified in the rule-array.

DES_key_block_length

Direction: Input/Output	Type: Integer

The length of the *DES_key_block*. The current length of this field may be 64 or 128 bytes. If rule array keyword PINBLOCK is specified, the length must be 128 bytes.

DES_key_block

Direction: Input/Output	Type: String

The *DES_key_block* contains either one or two DES internal key tokens. If only one token is specified on input, it contains either a null DES token (or binary zeroes) or (if DES-ONLY is specified) the DES key information returned from a previous SET Block Decompose service invocation. This is the 64-byte DES internal key token formed with the DES key which was retrieved from the RSA-OAEP block and enciphered under the host master key. Your application must not change this DES key information. If two tokens are specified in the *DES_key_block*, the first 64 bytes contain the DES token described above. The

| second 64 bytes, used when PINBLOCK is specified in the rule array, contain a
| DES internal token of the IPINENC or OPINENC key which is used to encrypt
| the PIN block returned to the caller in the XData_string parameter.

block_contents_identifier

Direction: Output Type: String

A one-byte string, containing the binary value from the block contents (BC) field of the SET data block (DB). It indicates what data is carried in the actual data block (ADB) and the format of any extra data (*XData_string*). This parameter is ignored if DES-ONLY is specified in the rule-array.

XData_string_length

Direction: Input/Output Type: Integer

The length of a string where the data contained within *XData_string* will be returned. The string must be at least 94 bytes in length. The value will be updated upon exit with the actual length of the returned *XData_string*. This parameter is ignored if DES-ONLY is specified in the rule-array.

XData_string

Direction: Output Type: String

Extra-encrypted data contained within the OAEP-processed and RSA-encrypted block. The format is indicated by *block_contents_identifier*. The string is treated by ICSF as a string of hexadecimal digits. The service will always return the data from the beginning of the XDataString to the end of the SET DB block, a maximum of 94 bytes of data. The caller must examine the value returned in *block_contents_identifier* to determine the actual length of the XDataString. This parameter is ignored if DES-ONLY is specified in the rule-array.

chaining_vector

Direction: Input/Output Type: String

An 18-byte field that ICSF uses as a system work area. Your application program must not change the data in this string. This field is ignored by this service, but must be specified.

data_block

Direction: Output Type: String

The data that was decrypted (passed in as *DES_encrypted_data_block*). Any padding characters are removed.

hash_block_length

Direction: Input/Output Type: Integer

The length in bytes of the SHA-1 hash returned in *hash_block*. On input, this parameter must be set to the length of the *hash_block* field. The length must be at least 20 bytes. On output, this field is updated to reflect the length of the SHA-1 hash returned in the *hash_block* field (exactly 20 bytes). This parameter is ignored if DES-ONLY is specified in the *rule_array* parameter.

hash_block

Direction: Output	Type: String

The SHA-1 hash extracted from the RSA-OAEP block. This parameter is ignored if DES-ONLY is specified in the *rule_array* parameter.

Restrictions

- Caller must be task mode and must not be SRB mode.
- Not all CCA implementations support a key label as input in the *RSA_private_key_identifier* parameter. Some implementations may only support a key token.
- The RSA private key used by this service must have been generated as a signature-only key.
- The *data_block* and the *DES_encrypted_data_block* cannot overlap.
- The ANSI system keys must be installed in the CKDS to use the SET block decompose service on a CDMF-only system.

Usage Notes

- RACF is invoked to check authorization to use the SET Block Decompose service.
- When the SET Block Decompose service is invoked without the DES-ONLY keyword, the DES key is retrieved from the RSA-OAEP block and returned in the key token contained in the *DES_key_block*. On subsequent calls to the SET Block Decompose service, a caller can re-use the DES key. The caller of the service must supply the *DES_key_block*, the *DES_key_block_length*, the *DES_encrypted_data_block*, the *DES_encrypted_data_block_length*, the initialization and chaining vectors, and the *rule_array* keywords SET1.00 and DES-ONLY. The RSA private key information, RSA-OAEP block and length, XData string and length, and hash block and length need not be supplied (although the parameters must still be specified). For this invocation, the decryption of the RSA-OAEP block is bypassed; only DES decryption is performed, using the supplied DES key.
- When the SET Block Decompose service is invoked with the PINBLOCK keyword, DES-ONLY may not also be specified. If both of these rule array keywords are specified, the service will fail with a Return code 8, Reason code 2016 (invalid rule array content). If PINBLOCK is specified and the *DES_key_block_length* field is not 128, the service will fail with Return code 8, Reason code 2790 (rule array keyword parameter mismatch).

Chapter 18. Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) is an industry-standard protocol that provides a data security layer between application protocols and TCP/IP. The SSL protocol was designed by the Netscape Development Corporation, and is widely deployed in both Internet applications and intranet applications. SSL defines methods for data encryption, server authentication, message integrity, and client authentication for a TCP/IP connection. SSL uses public key and symmetric techniques to provide the following security services:

- Message privacy

  SSL uses a combination of public-key and symmetric key encryption to ensure message privacy. Before exchanging messages, an SSL server and SSL client perform an electronic handshake during which they agree to use a session key and an encryption algorithm. All messages between the client and the server are then encrypted. Encryption ensures that the message remains private even if eavesdroppers intercept it.
- Message integrity

  SSL uses the combination of a shared secret key and message hash functions. This ensures that nothing changes the content of a message as it travels between client and server.
- Mutual authentication

  During the initial SSL handshake, the server uses a public-key certificate to convince the client of the server’s identity. Optionally, the client may also exchange a public-key certificate with the server to ensure the authenticity of the client.

SSL requires the decryption of a 48-byte SSL seed and the manipulation of this seed in the clear to produce symmetric session keys. The Common Cryptographic Architecture (CCA), however, does not permit even privacy session keys to appear in the clear in host storage. The SSL support services permit the RSA encryption and decryption of any PKCS 1.2-formatted symmetric key data. Using the PKA decrypt callable service makes it possible to unwrap the RSA-encrypted SSL seed and return it to the application in the clear.

PKA Encrypt (CSNDPKE)

This callable service encrypts a supplied clear key value under an RSA public key. The rule array keyword specifies the format of the key prior to encryption. Currently the key format is limited to PKCS 1.2.

This service routes requests to the Cryptographic Coprocessor Feature unless the modulus bit length of the key specified in the *PKA_key_identifier* is greater than 1024 bits.

© Copyright IBM Corp. 1997, 2000

Format

```
CALL CSNDPKE(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            keyvalue_length,
            keyvalue,
            data_structure_length,
            data_structure,
            PKA_key_identifier_length,
            PKA_key_identifier,
            PKA_enciphered_keyvalue_length,
            PKA_enciphered_keyvalue)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that are assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you supplied in the *rule_array* parameter. This value must be 1.

rule_array

Direction: Input Type: String

A keyword that provides control information to the callable service. The keyword is left-justified in an 8-byte field and padded on the right with blanks.

Table 75. Keywords for PKA Encrypt

Keyword	Meaning
Formatting Method (required) specifies the method to use to format the key value prior to encryption.	
PKCS-1.2	RSA DSI PKCS #1 block type 02 format will be used to format the supplied key value.

keyvalue_length

Direction: Input Type: Integer

The length of the *keyvalue* parameter. The maximum field size is 256 bytes. The actual maximum size depends on the modulus length of *PKA_key_identifier* and the formatting method you specify in the *rule_array* parameter. See Usage Notes.

keyvalue

Direction: Input Type: String

This field contains the supplied clear key value to be encrypted under the *PKA_key_identifier*.

data_structure_length

Direction: Input Type: Integer

This value must be 0.

data_structure

Direction: Input Type: String

This field is currently ignored.

PKA_key_identifier_length

Direction: Input Type: Integer

The length of the *PKA_key_identifier* parameter. When the *PKA_key_identifier* is a key label, this field specifies the length of the label. The maximum size that you can specify is 2500 bytes.

PKA_key_identifier

Direction: Input Type: String

The RSA public or private key token or the label of the RSA public or private key to be used to encrypt the supplied key value.

PKA_enciphered_keyvalue_length

Direction: Input/Output	Type: integer

The length of the *PKA_enciphered_keyvalue* parameter in bytes. The maximum size that you can specify is 256 bytes. On return, this field is updated with the actual length of *PKA_enciphered_keyvalue*.

PKA_enciphered_keyvalue

Direction: Output	Type: String

This field contains the key value protected under an RSA public key. This byte-length string is left-justified within the *PKA_enciphered_keyvalue* parameter.

Restrictions

- The exponent of the RSA public key must be odd.
- The caller must be in task mode and must not be in SRB mode.

Usage Notes

- For RSA DSI PKCS #1 formatting, the key value length must be at least 11 bytes less than the modulus length of the RSA key.
- The hardware configuration sets the limit on the modulus size of keys for key management; thus, this service will fail if the RSA key modulus bit length exceeds this limit. The service will fail with return code 12 and reason code 11020.

PKA_Decrypt (CSNDPKD)

This callable service accepts a PKCS 1.2-formatted, wrapped key value, along with an RSA private key in an internal key token. The service assumes that the sender used the corresponding RSA public key to wrap the input key value. The service unwraps the key, deformats it, and returns the deformatted value to the application in the clear.

The PKA decrypt callable service examines the RSA key specified in the *PKA_key_identifier* parameter to determine how to route the request. If the modulus bit length is less than 512 bits, or if the key is a X'02' form modulus-exponent private key, ICSF routes the request to the S/390 Cryptographic Coprocessor Feature. If the key is a X'08' form CRT private key or a retained private key, the service routes the request to a PCI Cryptographic Coprocessor. In the case of a retained key, the service routes the request to the specific PCI Cryptographic Coprocessor in which the key is retained. If the key is a modulus-exponent form private key with a private section ID of X'06', then the service routes the request as follows:

- Since the key must be a key-management key, if the KMMK is equal to the SMK on the S/390 Cryptographic Coprocessor Feature, the PKA decrypt service uses load balancing to route the request to either a S/390 Cryptographic Coprocessor Feature or to an available PCI Cryptographic Coprocessor.

- If the KMMK is not equal to the SMK on the S/390 Cryptographic Coprocessor Feature, the request must be processed on a PCI Cryptographic Coprocessor. If there is no PCI Cryptographic Coprocessor online, the request will fail and issue a return and reason code.

Format

```
CALL CSNDPKD(
              return_code,
              reason_code,
              exit_data_length,
              exit_data,
              rule_array_count,
              rule_array,
              PKA_enciphered_keyvalue_length,
              PKA_enciphered_keyvalue,
              data_structure_length,
              data_structure,
              PKA_key_identifier_length,
              PKA_key_identifier,
              target_keyvalue_length,
              target_keyvalue)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that are assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input   Type: Integer

The number of keywords you supplied in the *rule_array* parameter. This value must be 1.

rule_array

Direction: Input   Type: String

The keyword that provides control information to the callable service. The keyword is left-justified in an 8-byte field and padded on the right with blanks.

Table 76. Keywords for PKA Decrypt

Keyword	Meaning
Recovery Method (required) specifies the method to use to recover the key value.	
PKCS-1.2	RSA DSI PKCS #1 block type 02 will be used to recover the key value.

PKA_enciphered_keyvalue_length

Direction: Input   Type: integer

The length of the *PKA_enciphered_keyvalue* parameter in bytes. The maximum size that you can specify is 256 bytes.

PKA_enciphered_keyvalue

Direction: Input   Type: String

This field contains the key value protected under an RSA public key. This byte-length string is left-justified within the *PKA_enciphered_keyvalue* parameter.

data_structure_length

Direction: Input   Type: Integer

The value must be 0.

data_structure

Direction: Input   Type: String

This field is currently ignored.

PKA_key_identifier_length

Direction: Input   Type: Integer

The length of the *PKA_key_identifier* parameter. When the *PKA_key_identifier* is a key label, this field specifies the length of the label. The maximum size that you can specify is 2500 bytes.

PKA_key_identifier

Direction: Input	Type: String

| An external token with clear key values in ME format may also be used.

target_keyvalue_length

Direction: Input/Output	Type: Integer

The length of the *target_keyvalue* parameter. The maximum size that you can specify is 256 bytes. On return, this field is updated with the actual length of *target_keyvalue*.

target_keyvalue

Direction: Output	Type: String

This field will contain the decrypted, deformatted key value.

Restrictions

- The exponent of the RSA public key must be odd.
- Caller must be in task mode and must not be in SRB mode.

Usage Notes

- The RSA private key must be enabled for key management functions.
- The hardware configuration sets the limit on the modulus size of keys for key management; thus, this service will fail if the RSA key modulus bit length exceeds this limit. The service will fail with return code 12 and reason code 11020.

Chapter 19. PKA Utility

This chapter presents the PKA key token build utility.

PKA Key Token Build (CSNDPKB)

Use this utility to build external PKA key tokens containing unenciphered private RSA or DSS keys. You can use this token as input to the PKA key import service to obtain an operational internal token containing an enciphered private key. This service builds a skeleton token you can use as input to the PKA key generate callable service (see Table 80 on page 299). You can also input to this service a clear unenciphered public RSA or DSS key and return the public key in a token format that other ICSF PKA services can use directly.

With OS/390 V2 R9 ICSF, you can use this service to build a key token for an RSA private key in optimized Chinese Remainder Theorem (CRT) form.

DSS key generation requires the following information in the input skeleton token:
- Size of modulus p in bits
- Prime modulus p
- Prime divisor q
- Public generator g
- Optionally, the private key name

Note: DSS standards define restrictions on the prime modulus p, prime divisor q, and public generator g. (Refer to the Federal Information Processing Standard (FIPS) Publication 186 for DSS standards.) This callable service does not verify all of these restrictions. If you do not follow the restrictions, the keys you generate may not be valid DSS keys.

Format

```
CALL CSNDPKB(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            key_value_structure_length,
            key_value_structure,
            private_key_name_length,
            private_key_name,
            reserved_1_length,
            reserved_1,
            reserved_2_length,
            reserved_2,
            reserved_3_length,
            reserved_3,
            reserved_4_length,
            reserved_4,
            reserved_5_length,
            reserved_5,
            key_token_length,
            key_token)
```

© Copyright IBM Corp. 1997, 2000

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Ignored	Type: Integer

Reserved field.

exit_data

Direction: Input/Output	Type: String

Reserved field.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you supplied in the *rule_array* parameter. Value must be 1 or 2.

rule_array

Direction: Input	Type: String

One or two keywords that provide control information to the callable service. Table 77 lists the keywords. The keywords must be in 8 to 16 bytes of contiguous storage with each of the keywords left-justified in its own 8-byte location and padded on the right with blanks.

Table 77. Keywords for PKA Key Token Build Control Information

Keyword	Meaning
Key Type (required)	
RSA-CRT	This keyword indicates building a token containing an RSA private key in the optimized Chinese Remainder Theorem (CRT) form. The parameter *key_value_structure* identifies the input key values, if supplied.

Table 77. Keywords for PKA Key Token Build Control Information (continued)

Keyword	Meaning
RSA-PRIV	This keyword indicates building a token containing both public and private RSA key information. The parameter *key_value_structure* identifies the input key values, if supplied.
RSA-PUBL	This keyword indicates building a token containing public RSA key information. The parameter *key_value_structure* identifies the input values, if supplied.
DSS-PRIV	This keyword indicates building a key token containing both public and private DSS key information. The parameter *key_value_structure* identifies the input key values, if supplied.
DSS-PUBL	This keyword indicates building a key token containing public DSS key information. The parameter *key_value_structure* identifies the input key values, if supplied.
Key Usage Control (optional)	
SIG-ONLY	Indicates that an RSA private key cannot be used in symmetric key distribution. This is the default. Note that for DSS-PRIV the keyword is allowed but extraneous; DSS keys are defined only for digital signature.
KEY-MGMT	Indicates that an RSA private key can be used in both the symmetric key import and the digital signature generate callable services.
KM-ONLY	Indicates that an RSA private key can be used only in symmetric key distribution.

key_value_structure_length

Direction: Input   Type: Integer

This is a segment of contiguous storage containing a variable number of input clear key values. The length depends on the key type parameter in the rule array and on the actual values input. The length is in bytes.

Table 78. Key Value Structure Length Maximum Values for Key Types

Key Type	Key Value Structure Maximum Value
RSA-CRT	2500
RSA-PRIV	648
RSA-PUBL	520
DSS-PRIV	436
DSS-PUBL	416

key_value_structure

Direction: Input   Type: String

This is a segment of contiguous storage containing a variable number of input clear key values and the lengths of these values in bits or bytes, as specified.

The structure elements are ordered, of variable length, and the input key values must be right-justified within their respective structure elements and padded on the left with binary zeros. Table 79 defines the structure and contents as a function of key type.

Table 79. Key Value Structure Elements for PKA Key Token Build

Offset	Length (bytes)	Description
Key Value Structure (Optimized RSA, Chinese Remainder Theorem form, RSA-CRT)		
000	002	Modulus length in bits (512 to 2048). This is required.
002	002	Modulus field length in bytes, “nnn.” This value can be zero if the key token is used as a *skeleton_key_token* in the PKA key generate callable service. This value must not exceed 256.
004	002	Public exponent field length in bytes, “eee.” This value can be zero if the key token is used as a *skeleton_key_token* in the PKA key generate callable service.
006	002	Reserved, binary zero.
008	002	Length of the prime number, p, in bytes, “ppp.” This value can be zero if the key token is used as a *skeleton_key_token* in the PKA key generate callable service. Maximum size of p + q is 256 bytes.
010	002	Length of the prime number, q, in bytes, “qqq.” This value can be zero if the key token is used as a *skeleton_key_token* in the PKA key generate callable service. Maximum size of p + q is 256 bytes.
012	002	Length of d_p, in bytes, “rrr.” This value can be zero if the key token is used as a *skeleton_key_token* in the PKA key generate callable service. Maximum size of $d_p + d_q$ is 256 bytes.
014	002	Length of d_q, in bytes, “sss.” This value can be zero if the key token is used as a *skeleton_key_token* in the PKA key generate callable service. Maximum size of $d_p + d_q$ is 256 bytes.
016	002	Length of U, in bytes, “uuu.” This value can be zero if the key token is used as a *skeleton_key_token* in the PKA key generate callable service. Maximum size of U is 256 bytes.
018	nnn	Modulus, n.

Table 79. Key Value Structure Elements for PKA Key Token Build (continued)

Offset	Length (bytes)	Description
018 + nnn	eee	Public exponent, e. This is an integer such that 1<e<n. e must be odd. When you are building a *skeleton_key_token* to control the generation of an RSA key pair, the public key exponent can be one of the following values: 3, 65537 (2^{16} + 1), or 0 to indicate that a full random exponent should be generated. The exponent field can be a null-length field if the exponent value is 0.
018 + nnn + eee	ppp	Prime number, p.
018 + nnn + eee + ppp	qqq	Prime number, q.
018 + nnn + eee + ppp + qqq	rrr	d_p = d mod(p-1).
018 + nnn + eee + ppp + qqq + rrr	sss	d_q = d mod(q-1).
018 + nnn + eee + ppp + qqq + rrr + sss	uuu	U = q^{-1}mod(p).
Key Value Structure (RSA Private or RSA Public)		
000	002	Modulus length in bits. This is required. When building a skeleton token, the modulus length in bits must be greater than or equal to 512 bits.
002	002	Modulus field length in bytes, “XXX”. This value can be zero if you are using the key token as a skeleton in the PKA key generate verb. This value must not exceed 256 when the RSA-PUBL keyword is used, and must not exceed 128 when the RSA-PRIV keyword is used. This service can build a key token for a public RSA key with a 2048-bit modulus length, or it can build a key token for a 1024-bit modulus length private key.
004	002	Public exponent field length in bytes, “YYY”. This value must not exceed 256 when the RSA-PUBL keyword is used, and must not exceed 128 when the RSA-PRIV keyword is used. This value can be zero if you are using the key token as a skeleton token in the PKA key generate verb. In this case, a random exponent is generated. To obtain a fixed, predetermined public key exponent, you can supply this field and the public exponent as input to the PKA key generate verb.

Table 79. Key Value Structure Elements for PKA Key Token Build (continued)

Offset	Length (bytes)	Description
006	002	Private exponent field length in bytes, “ZZZ”. This field can be zero, indicating that private key information is not provided. This value must not exceed 128 bytes. This value can be zero if you are using the key token as a skeleton token in the PKA key generate verb.
008	XXX	Modulus, n. This is an integer such that $1<n<2^{2048}$. The n is the product of p and q for primes p and q.
008 + XXX	YYY	RSA public exponent e, which is an odd integer where 1<e<n. You can supply this value in a skeleton to generate an RSA private key with a predetermined public exponent value.
008 + XXX + YYY	ZZZ	RSA secret exponent d. This is an integer such that 1<d<n. The value of d is e^{-1} mod(p-1)(q-1); the You need not specify this value if you specify RSA-PUBL in the rule array.
Key Value Structure (DSS Private or DSS Public)		
000	002	Modulus length in bits. This is required.
002	002	Prime modulus field length in bytes, “XXX”. You can supply this as a network quantity to the ICSF PKA key generate callable service, which uses the quantity to generate DSS keys. The maximum allowed value is 128.
004	002	Prime divisor field length in bytes, “YYY”. You can supply this as a network quantity to the ICSF PKA key generate callable service, which uses the quantity to generate DSS keys. The allowed values are 0 or 20 bytes.
006	002	Public generator field length in bytes, “ZZZ”. You can supply this in a skeleton token as a network quantity to the ICSF PKA key generate callable service, which uses the quantity to generate DSS keys. The maximum allowed value is 128 bytes and is exactly the same length as the prime modulus.

Table 79. Key Value Structure Elements for PKA Key Token Build (continued)

Offset	Length (bytes)	Description
008	002	Public key field length in bytes, “AAA”. This field can be zero, indicating that the ICSF PKA key generate callable service generates a value at random from supplied or generated network quantities. The maximum allowed value is 128 bytes and is exactly the same length as the prime modulus.
010	002	Secret key field length in bytes, “BBB”. This field can be zero, indicating that the ICSF PKA key generate callable service generates a value at random from supplied or generated network quantities. The allowed values are 0 or 20 bytes.
012	XXX	DSS prime modulus p. This is an integer such that $2^{L-1}<p<2^{L}$. The p must be prime. You can supply this value in a skeleton token as a network quantity; it is used in the algorithm that generates DSS keys.
012 + XXX	YYY	DSS prime divisor q. This is an integer that is a prime divisor of p-1 and $2^{159}<q<2^{160}$. You can supply this value in a skeleton token as a network quantity; it is used in the algorithm that generates DSS keys.
012 + XXX+ YYY	ZZZ	DSS public generator g. This is an integer such that $1<g<p$. You can supply this value in a skeleton token as a network quantity; it is used in the algorithm that generates DSS keys.
012 + XXX+ YYY+ ZZZ	AAA	DSS public key y. This is an integer such that $y = g^{x} \bmod p$.
012 + XXX+ YYY+ ZZZ+ AAA	BBB	DSS secret private key x. This is an integer such that $0<x<q$. The x is random. You need not supply this value if you specify DSS-PUBL in the rule array.

Notes:

1. All length fields are in binary.
2. All binary fields (exponent, lengths, modulus, and so on) are stored with the high-order byte field first. This integer number is right-justified within the key structure element field.
3. You must supply all values in the structure to create a token containing an RSA or DSS private key for input to the PKA key import service.

private_key_name_length

Direction: Input	Type: Integer

The length can be 0 or 64.

private_key_name

Direction: Input	Type: EBCDIC character

This field contains the name of a private key. The name must conform to ICSF label syntax rules. That is, allowed characters are alphanumeric, national (@,#,$) or period (.). The first character must be alphabetic or national. The name is folded to upper case and converted to ASCII characters. ASCII is the permanent form of the name because the name should be independent of the platform. The name is then cryptographically coupled with clear private key data before encryption of the private key. Because of this coupling, the name can never change after the key token is imported. The parameter is valid only with key types RSA-PRIV and DSS-PRIV.

reserved_1_length

Direction: Input	Type: Integer.

Length in bytes of a reserved parameter. You must set this variable to 0.

reserved_1

Direction: Input	Type: String

The *reserved_1* parameter identifies a string that is reserved. The service ignores it.

reserved_2_length

Direction: Input	Type: Integer.

Length in bytes of a reserved parameter. You must set this variable to 0.

reserved_2

Direction: Input	Type: String

The *reserved_2* parameter identifies a string that is reserved. The service ignores it.

reserved_3_length

Direction: Input	Type: Integer.

Length in bytes of a reserved parameter. You must set this variable to 0.

reserved_3

Direction: Input	Type: String

The *reserved_3* parameter identifies a string that is reserved. The service ignores it.

reserved_4_length

Direction: Input	Type: Integer.

Length in bytes of a reserved parameter. You must set this variable to 0.

reserved_4

Direction: Input	Type: String

The *reserved_4* parameter identifies a string that is reserved. The service ignores it.

reserved_5_length

Direction: Input	Type: Integer.

Length in bytes of a reserved parameter. You must set this variable to 0.

reserved_5

Direction: Input	Type: String

The *reserved_5* parameter identifies a string that is reserved. The service ignores it.

key_token_length

Direction: Input/Output	Type: Integer

Length of the returned key token. The service checks the field to ensure it is at least equal to the size of the token to return. On return from this service, this field is updated with the exact length of the *key_token* created. On input, a size of 1024 bytes is sufficient to contain the largest *key_token* created.

key_token

Direction: Output	Type: String

The returned key token containing an unenciphered private or public key. The private key is in an external form that can be exchanged with different Common Cryptographic Architecture (CCA) PKA systems. You can use the public key token directly in appropriate ICSF signature verification or key management services.

Usage Note

If you are building a skeleton for use in a PKA Key Generate request to generate a retained PKA private key, you must build a private key name section in the skeleton token.

Chapter 20. PKA Key Management

This chapter describes the callable services that generate and manage PKA keys.

- "PKA Key Generate (CSNDPKG)"
- "PKA Key Import (CSNDPKI)" on page 300
- "PKA Public Key Extract (CSNDPKX)" on page 303
- "PKDS Record Create (CSNDKRC)" on page 305
- "PKDS Record Write (CSNDKRW)" on page 306
- "PKDS Record Read (CSNDKRR)" on page 308
- "PKDS Record Delete (CSNDKRD)" on page 310
- "Retained Key List (CSNDRKL)" on page 312
- "Retained Key Delete (CSNDRKD)" on page 314

PKA Key Generate (CSNDPKG)

Use the PKA key generate callable service to generate the following PKA keys:

- PKA internal tokens for use with the DSS algorithm in the digital signature services
- RSA keys for use on the Cryptographic Coprocessor Feature or PCI Cryptographic Coprocessor

Input to the PKA key generate callable service is either a skeleton key token that has been built by the PKA key token build service or a valid internal token. In the case of a valid internal token, PKG will generate a key with the same modulus length and the same exponent. The service examines the skeleton token and routes the generation request to the appropriate cryptographic processor. If the skeleton is a DSS key token, processing takes place on the S/390 Cryptographic Coprocessor Feature. If the skeleton is an RSA key token, processing takes place on the PCI Cryptographic Coprocessor.

DSS key generation requires the following information in the input skeleton token:

- Size of modulus p in bits
- Prime modulus p
- Prime divisor q
- Public generator g
- Optionally, the private key name

DSS standards define restrictions on p, q, and g. (Refer to the Federal Information Processing Standard (FIPS) Publication 186 for DSS standards.) This callable service does not verify all of these restrictions. If you do not follow these restrictions, the keys you generate may not be valid DSS keys. The PKA Key Token Build service or an existing internal or external PKA DSS token can generate the input skeleton token, but all of the preceding must be provided. You can extract the DSS public key token from the internal private key token by calling the PKA public key extract callable service.

RSA key generation requires the following information in the input skeleton token:

- Size of the modulus in bits. The modulus for modulus-exponent form keys is between 512 and 1024. The CRT modulus is between 512 and 2048.

RSA key generation has the following restrictions: For modulus-exponent, there are restrictions on modulus, public exponent, and private exponent. For CRT, there are restrictions on dp, dq, U, and public exponent. See the Key value structure in "PKA Key Token Build (CSNDPKB)" on page 287 for a summary of restrictions.

PKA Key Generate (CSNDPKG)

Note: The Transaction Security System PKA96 PKA key generate verb supports RSA key generation only; it does not support DSS key generation.

Format

```
CALL CSNDPKG(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            regeneration_data_length,
            regeneration_data,
            skeleton_key_identifier_length,
            skeleton_key_identifier,
            transport_key_identifier,
            generated_key_token_length,
            generated_key_token)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you supplied in the *rule_array* parameter. Value may be 1 or 2.

rule_array

Direction: Input	Type: String

A keyword that provides control information to the callable service. See Table 80 for a list. A keyword is left-justified in an 8-byte field and padded on the right with blanks.

Table 80. Keyword for PKA Key Generate Rule Array

Keyword	Meaning
Private Key Encryption (required)	
CLEAR	Return the private key in clear text. The private key in clear text is an external token. Only valid for RSA keys.
MASTER	Encipher the private key under the master key.
RETAIN	Retain the private key within the PCI Cryptographic Coprocessor for additional security. Only valid for RSA keys.
Options (optional)	
CLONE	Mark a generated and retained private key as usable in cryptographic engine cloning process. This keyword is supported only if RETAIN is also specified. Only valid for RSA keys.

regeneration_data_length

Direction: Input	Type: Integer

The value must be 0 for DSS tokens. For RSA tokens, the regeneration_data_length can be non-zero. If it is non-zero, it must be between 8 and 256 bytes inclusive.

regeneration_data

Direction: Input	Type: String

This field points to a string variable containing a string used as the basis for creating a particular public-private key pair in a repeatable manner.

skeleton_key_identifier_length

Direction: Input	Type: Integer

The length of the *skeleton_key_identifier* parameter in bytes. The maximum allowed value is 2500 bytes.

skeleton_key_identifier

Direction: Input	Type: String

The application-supplied skeleton key token generated by PKA key token build or label of the token that contains the required network quantities for DSS key generation, or the required modulus length and public exponent for RSA key generation.

transport_key_identifier

Direction: Input	Type: String

A 64-byte field to contain a DES key identifier. This field must be binary zeros.

generated_key_token_length

Direction: Input/Output	Type: Integer

The length of the generated key token. The field is checked to ensure it is at least equal to the token being returned. The maximum size is 2500 bytes. On output, this field is updated with the actual token length.

generated_key_token

Direction: Input/Output	Type: String

The internal token or label of the generated DSS or RSA key. The label can be that of a retained key. Checks are made to ensure that a retained key is not overlayed in PKDS. If the label is that of a retained key, the private name in the token must match the label name. If a label is specified in the *generated_key_token_field*, the *generated_key_token_length* returned to the application will be the same as the input length. If RETAIN was specified, but the *generated_key_token* was not specified as a label, the generated key length returned to the application will be zero (the key was retained in the PCI Cryptographic Coprocessor). If the record already exists in the PKDS with the same label as the one specified as the *generated_key_token*, the record will be overwritten with the newly generated key token (unless the PKDS record is an existing retained private key, in which case it cannot be overwritten). If there is no existing PKDS record with this label in the case of generating a retained key, a record will be created. For generation of a non-retained key, if a label is specified in the generated-key-token field, a record must already exist in the PKDS with this same label or the service will fail.

Restriction

The caller must be in task mode and not in SRB mode.

Usage Note

When a Retained key is created, ICSF records this event in a type 82 SMF record with a subtype of 15.

PKA Key Import (CSNDPKI)

| This service imports an external PKA private key token. (This consists of a PKA
| private key and public key.) The secret values of the key may be clear or encrypted
| under a limited-authority DES importer key.

This service can also import a clear PKA key. The PKA key token build service creates a clear PKA key token.

Output of this service is an ICSF internal token of the RSA or DSS private key.

ICSF examines the key token supplied in the *source_key_identifier* to determine where to route the request. If the *source_key_identifier* contains an RSA private key with a modulus length of at least 512 bits, ICSF routes the PKA key import request to a PCI Cryptographic Coprocessor. If no PCI Cryptographic Coprocessor is online, or if the *source_key_identifier* contains either an RSA private key with a modulus length less than 512 bits or a DSS private key, ICSF routes the PKA key import request to the S/390 Cryptographic Coprocessor Feature. An RSA modulus-exponent form token imported on the PCI Cryptographic Coprocessor results in an X'06' format, while a token imported on a Cryptographic Coprocessor Feature will result in a X'02' format. If no PCI Cryptographic Coprocessor is online and the *source_key_identifier* is an RSA-CRT token, the request fails.

Format

```
CALL CSNDPKI(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            source_key_identifier_length,
            source_key_identifier,
            importer_key_identifier,
            target_key_identifier_length,
            target_key_identifier)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you supplied in the *rule_array* parameter. This must be 0.

rule_array

Direction: Input	Type: String

Reserved field. This field is not used, but you must specify it.

source_key_identifier_length

Direction: Input	Type: Integer

The length of the *source_key_identifier* parameter. The maximum size is 2500 bytes.

source_key_identifier

Direction: Input	Type: String

The external token or label of a PKA private key. This cannot be the label of a retained private key. This is the output of the PKA key generate (CSNDPKG) callable service or the PKA key token build (CSNDPKB) callable service. If encrypted, it was created on another platform.

importer_key_identifier

Direction: Input/Output	Type: String

A DES internal token or the label of an IMP-PKA key. This is a limited authority key-encrypting key. It is ignored for clear tokens.

target_key_identifier_length

Direction: Input/Output	Type: Integer

The length of the *target_key_identifier* parameter. The maximum size is 2500 bytes.

target_key_identifier

Direction: Output	Type: String

This field contains the internal token or label of the imported PKA private key. If a label is specified, a PKDS record with this label must exist. The PKDS record with this label will be overwritten with imported key unless the existing record is a retained key. If the record is a retained key, the import will fail. A retained key record cannot be overwritten.

Restrictions

This service imports RSA keys of up to 2048 bits. However, the hardware configuration sets the limits on the modulus size of keys for digital signatures and key management; thus, the key may be successfully imported but fail when used if the limits are exceeded.

The *importer_key_identifier* is a limited-authority key-encrypting key.

The caller must be in task mode and not in SRB mode.

CRT form tokens with a private section ID of X'05' cannot be imported into ICSF.

Usage Notes

This service imports keys of any modulus size up to 2048 bits. However, the hardware configuration sets the limits on the modulus size of keys for digital signatures and key management; thus, the key may be successfully imported but fail when used if the limits are exceeded.

PKA Public Key Extract (CSNDPKX)

Use the PKA public key extract callable service to extract a PKA public key token from a supplied PKA internal or external private key token. This service performs no cryptographic verification of the PKA private token. You can verify the private token by using it in a service such as digital signature generate.

Format

```
CALL CSNDPKX(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            source_key_indentifier_length,
            source_key_identifier,
            target_public_key_token_length,
            target_public_key_token)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Ignored	Type: Integer

Reserved field.

exit_data

Direction: Ignored	Type: String

Reserved field.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you are supplying in the *rule_array* parameter. The value must be 0.

rule_array

Direction: Input	Type: String

Reserved field. This field is not used, but you must specify it.

source_key_identifier_length

Direction: Input	Type: integer

The length of the *source_key_identifier* parameter. The maximum size is 2500 bytes.

source_key_identifier

Direction: Input/output	Type: string

The internal or external token of a PKA private key or the label of a PKA private key. This can be the input or output from PKA key import or from PKA key generate.

This service supports the RSA private key token formats supported on the PCI Cryptographic Coprocessor. If the *source_key_identifier* specifies a label for a private key that has been retained within a PCI Cryptographic Coprocessor, this service extracts only the public key section of the token.

target_public_key_token_length

Direction: Input/Output	Type: Integer

The length of the *target_public_key_token* parameter. The maximum size is 2500 bytes. On output, this field will be updated with the actual byte length of the *target_public_key_token*.

target_public_key_token

Direction: Output	Type: String

This field contains the token of the extracted PKA public key.

Usage Note

This service extracts the public key from the internal or external form of a private key. However, it does not check the cryptographic validity of the private token.

PKDS Record Create (CSNDKRC)

This callable service writes a new record to the PKDS.

Format

```
CALL CSNDKRC(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            label,
            token_length,
            token)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicates specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you are supplying in the *rule_array* parameter. This parameter is ignored by ICSF.

rule_array

Direction: Input	Type: String

This parameter is ignored by ICSF.

label

Direction: Input	Type: String

The label of the record to be created. A 64 byte character string.

token_length

Direction: Input	Type: Integer

The length of the field containing the token to be written to the PKDS. If zero is specified, a null token will be added to the PKDS. The maximum value of *token_length* is the maximum length of a private RSA or DSS token.

token

Direction: Input	Type: String

Data to be written to the PKDS if *token_length* is non-zero. A RSA or DSS private token in either external or internal format, or a DSS or RSA public token.

Restriction

Caller must be task mode and must not be SRB mode.

Usage Note

PKA callable services must be enabled for you to use this service.

PKDS Record Write (CSNDKRW)

Writes over an existing record in the PKDS.

Format

```
CALL CSNDKRW(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            label,
            token_length,
            token)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicates specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you are supplying in the *rule_array* parameter. Its value must be 0 or 1.

rule_array

Direction: Input	Type: String

Keywords that provide control information to the callable service. Each keyword is left-justified in 8-byte fields and padded on the right with blanks. All keywords must be in contiguous storage.

Table 81. Keywords for PKDS Record Write

Keyword	Meaning
Write Mode (optional) specifies the circumstances under which the record is to be written.	
CHECK	Specifies that the record will be written only if a record of type NULL with the same label exists in the PKDS. If such a record exists, ICSF overwrites it. This is the default condition.
OVERLAY	Specifies that the record will be overwritten regardless of the current content of the record. If a record with the same label exists in the PKDS, ICSF overwrites it.

label

Direction: Input	Type: String

The label of the record to be overwritten. A 64 byte character string.

token_length

Direction: Input	Type: Integer

The length of the field containing the token to be written to the PKDS.

token

Direction: Input	Type: String

The data to be written to the PKDS, which is a DSS or RSA private token in either external or internal format, or a DSS or RSA public token.

Restrictions

- Caller must be task mode and must not be SRB mode.
- This service cannot update a PKDS record for a retained key.

Usage Note

PKA callable services must be enabled for you to use this service.

PKDS Record Read (CSNDKRR)

Reads a record from the PKDS and returns the content of the record. This is true even when the record contains a null PKA token.

Format

```
CALL CSNDKRR(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            label,
            token_length,
            token)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicates specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you are supplying in the *rule_array* parameter. This parameter is ignored by ICSF.

rule_array

Direction: Input	Type: String

This parameter is ignored by ICSF.

label

Direction: Input	Type: String

The label of the record to be read. A 64 byte character string.

token_length

Direction: Input/Output	Type: Integer

The length of the area to which the record is to be returned. On successful completion of this service, token_length will contain the actual length of the record returned.

token

Direction: Output	Type: String

Area into which the returned record will be written. The area should be at least as long as the record.

Restriction

Caller must be task mode and must not be SRB mode.

Usage Note

PKA callable services must be enabled for you to use this service.

PKDS Record Delete (CSNDKRD)

Use PKDS record delete to delete a record from the PKDS.

Format

```
CALL CSNDKRD(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            label)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicates specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input	Type: Integer

The number of keywords you are supplying in the *rule_array* parameter. This parameter is ignored by ICSF, except that its value must be 0, or 1.

rule_array

Direction: Input	Type: String

Keywords that provide control information to the callable service. Each keyword is left-justified in 8-byte fields and padded on the right with blanks. All keywords must be in contiguous storage.

Table 82. Keywords for PKDS Record Delete

Keyword	Meaning
Deletion Mode (optional) specifies whether the record is to be deleted entirely or whether only its contents are to be erased.	
LABEL-DL	Specifies that the record will be deleted from the PKDS entirely. This is the default deletion mode.
TOKEN-DL	Specifies that the only the contents of the record are to be deleted. The record will still exist in the PKDS, but will contain only binary zeroes.

label

Direction: Input	Type: String

The label of the record to be deleted. A 64 byte character string.

Restrictions

- Caller must be task mode and must not be SRB mode.
- This service cannot delete the PKDS record for a retained key.

Usage Note

PKA callable services must be enabled for you to use this service.

Retained Key List (CSNDRKL)

Use the retained key list callable service to list the key labels of those keys that have been retained within all currently active PCI Cryptographic Coprocessors.

Format

```
CALL CSNDRKL(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            key_label_mask
            retained_keys_count
            key_labels_count
            key_labels)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input	Type: Integer

The number of keywords supplied in the *rule_array* parameter. The value must be 0.

rule_array

Direction: Input	Type: Character String

This parameter is ignored by ICSF.

key_label_mask

Direction: Input	Type: String

A 64-byte key label mask that is used to filter the list of key names returned by the verb. You can use a wild card (*) to identify multiple keys retained within the PCI Cryptographic Coprocessor.

Note: If an asterisk (*) is used, it must be the last character in key_label_mask. There can only be one *.

retained_keys_count

Direction: Output	Type: Integer

An integer variable to receive the number of retained keys stored within all active PCI Cryptographic Coprocessors.

key_labels_count

Direction: Input/Output	Type: Integer

On input this variable defines the maximum number of key labels to be returned. On output this variable defines the total number of key labels returned. The value returned in the *retained_keys_count* variable can be larger if you have not provided for the return of a sufficiently large number of key labels in the *key_labels_count* field.

key_labels

Direction: Output	Type: String

A string variable where the key label information will be returned. This field must be at least 64 times the key label count value. The key label information is a string of zero or more 64-byte entries. The first 64-byte entry contains a PCI Cryptographic Coprocessor card serial number, and is followed by one or more 64-byte entries that each contain a key label of a key retained within that PCI Cryptographic Coprocessor. The format of the first 64-byte entry is as follows:

```
 /nnnnnnnnbbbbb...bbb
where
 "/" is the character "/" (EBCDIC: X'61')
 "nnnnnnnn" is the 8-byte PCI Cryptographic Coprocessor card
   serial number
 "bbbbb...bbb" is 55 bytes of blank pad characters
   (EBCDIC: X'40')
```

This information (64-byte card serial number entry followed by one or more 64-byte label entries) is repeated for each active PCI Cryptographic Coprocessor that contains retained keys that match the *key_label_mask*. All data returned is EBCDIC characters. The number of bytes of information returned is governed by the value specified in the *key_labels_count* field. The *key_labels* field must be large enough to hold the number of 64-byte labels specified in the *key_labels_count* field plus one 64-byte entry for each active PCI Cryptographic Coprocessor (a maximum of 64 PCI Cryptographic Coprocessors).

Restriction

Caller must be task mode and must not be SRB mode.

Usage Notes

- Not all CCA platforms may support multiple PCI Cryptographic Coprocessor cards. In the case where only one card is supported, the *key_labels* field will contain one or more 64-byte entries that each contain a key label of a key retained within the PCI Cryptographic Coprocessor. There will be no 64-byte entry or entries containing a PCI Cryptographic Coprocessor card serial number.
- ICSF calls RACF to check authorization to use the Retained Key List service.
- ICSF caller must be authorized to the *key_label_mask* name including the *.
- Retained private keys are domain-specific. ICSF lists only those keys that were created by the LPAR domain that issues the Retained Key List request.

Retained Key Delete (CSNDRKD)

Use the retained key delete callable service to delete a key that has been retained within the PCI Cryptographic Coprocessor. This service also deletes the record that contains the associated key token from the PKDS. It also allows the deletion of a
| retained key in the PCI Cryptographic Coprocessor even if there isn't a PKDS
| record, or deletion of a PKDS record for a retained key even if the PCI
| Cryptographic Coprocessor holding the retained key is not online. Use the *rule_array* parameter specifying the FORCE keyword and serial number of the PCI Cryptographic Coprocessor that contains the retained key to be deleted. If a PKDS record exists for the same label, but the serial number doesn't match the serial number in rule_array, the service will fail. If any applications still need the public key, use public key extract to create a public key token before deletion of the retained key.

Format

```
CALL CSNDRKD(
            return_code,
            reason_code,
            exit_data_length,
            exit_data,
            rule_array_count,
            rule_array,
            key_label)
```

Parameters

return_code

Direction: Output	Type: Integer

The return code specifies the general result of the callable service. Appendix A. ICSF and TSS Return and Reason Codes lists the return codes.

reason_code

Direction: Output	Type: Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems. Appendix A. ICSF and TSS Return and Reason Codes lists the reason codes.

exit_data_length

Direction: Input/Output	Type: Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction: Input/Output	Type: String

The data that is passed to the installation exit.

rule_array_count

Direction: Input	Type: Integer

The number of keywords supplied in the *rule_array* parameter. The value may be 0 or 2.

rule_array

Direction: Input	Type: Character String

This parameter may be FORCE and the PCI Cryptographic Coprocessor serial number.

key_label

Direction: Input	Type: String

A 64-byte label of a key that has been retained in a PCI Cryptographic Coprocessor.

Restriction

Caller must be task mode and must not be SRB mode.

Usage Notes

- ICSF calls RACF to check authorization to use the Retained Key Delete service and the label of the key specified in key_label.
- Retained private keys are domain-specific. Only the LPAR domain that created a Retained private key can delete the key via the Retained Key Delete service.
- When a Retained key is deleted using the Retained Key Delete service, ICSF records this event in a type 82 SMF record with a subtype of 15.
- If the Retained key does not exist in the PCI Cryptographic Coprocessor and the PKDS record exists and the domain that created the retained key matches the domain of the requestor, ICSF deletes the PKDS record. This situation may occur if the PCI Cryptographic Coprocessor has been zeroed through TKE or the service processor.
- If a PKDS record containing the retained key exists but the PCI Cryptographic Coprocessor holding the retained key is not online, ICSF deletes the PKDS record if the FORCE keyword is specified.
- If the retained key exists on the specified PCI Cryptographic Coprocessor but there is no corresponding PKDS record, ICSF deletes the retained key from the PCI Cryptographic Coprocessor: if the FORCE keyword is specified.

Part 3. Appendixes

© Copyright IBM Corp. 1997, 2000

Appendix A. ICSF and TSS Return and Reason Codes

This appendix includes the following information:

- Return codes and reason codes issued on the completion of a call to an ICSF callable service
- Return codes and reason codes issued on the completion of a process on a PCI Cryptographic Coprocessor
- Conversion tables showing the relationship between ICSF and Transaction Security System return and reason codes. ICSF or TSS return and reason codes can be specified in the installation options dataset on the REASONCODES parameter. If the REASONCODES option is not specified, the default of REASONCODES(ICSF) is used.

ICSF Return Codes and Reason Codes

This section describes the ICSF return codes and reason codes and also lists ICSF to TSS return codes and reason codes. Each ICSF return code returns unique reason codes to your application program. The reason codes associated with each return code are described in the following sections. The reason code tables present the ICSF hexadecimal code followed by the decimal code in parenthesis. If there is a 1-to-1 mapping, the codes will be converted. If there is not a map to TSS, the column will be blank. If there are multiple mappings, they will be listed as reference only and will not be converted.

Return Codes

Table 83 lists return codes from the ICSF callable services.

Table 83. ICSF Return Codes

Return Code Hex (Decimal)	Description
Return Code 0 (0)	The call to the service or PCI Cryptographic Coprocessor was successfully processed. See the reason code for more information.
Return Code 4 (4)	The call to the service or PCI Cryptographic Coprocessor was successfully processed, but some minor event occurred during processing. See the reason code for more information. **User action**: Review the reason code.
Return Code 8 (8)	The call to the service or PCI Cryptographic Coprocessor was unsuccessful. The parameters passed into the call are unchanged, except for the return code and reason code. There are rare examples where output areas are filled, but their contents are not guaranteed to be accurate. These are described under the appropriate reason code descriptions. The reason code identifies which error was found. **User action**: Review the reason code, correct the problem, and retry the call.
Return Code C (12)	The call to the service or PCI Cryptographic Coprocessor could not be processed because ICSF was not active, ICSF found something wrong in its environment, a TSS security product is not available, or a processing error occurred in a TSS product. The parameters passed into the call are unchanged, except for the return code and reason code. **User action**: Review the reason code and take the appropriate action.
Return Code 10 (16)	The call to the service or PCI Cryptographic Coprocessor could not be processed because ICSF found something seriously wrong in its environment or a processing error occurred in the PCI Cryptographic Coprocessor. The parameters passed into the call are unchanged, except for the return code and reason code. **User action**: Review the reason code and contact your system programmer.

© Copyright IBM Corp. 1997, 2000

ICSF Reason Codes for Return Code 0 (0)

Table 84 lists reason codes returned from callable services that give return code 0.

Table 84. ICSF Reason Codes for Return Code 0 (0)

ICSF Reason Code Hex (Decimal)	TSS Reason Code Hex (Decimal)	Description
0 (0)	0 (0)	The call to the ICSF callable service or TSS verb was successfully processed. No error was encountered. **User action**: None.
4 (4)	2 (2)	The call to the ICSF callable service or TSS verb was successfully processed. A minor error was detected. A key used in the service did not have odd parity. This key could be one provided by you as a parameter or be one (perhaps of many) that was retrieved from the in-storage CKDS. **User action**: Refer to the reason code obtained when the key passed to this service was transformed into operational form using clear key import, multiple clear key import, key import, secure key import, or multiple secure key import callable services. Check if any of the services prepared an even parity key. If one of these service reported an even parity key, you need to know which key is affected. If none of these services identified an even parity key, then the even parity key detected was found on the CKDS. Report this to your administrator.
8 (8)	8 (8)	The key record read callable service attempted to read a NULL key record. The returned key token contains only binary zeros. **User action**: None required.
2710 (10000)	2710 (10000)	The call to the TSS verb was successfully processed. The keys in one or more key identifiers have been reenciphered from encipherment under the old master key to encipherment under the current master key. **User action**: If you obtained your operational token from a file, replace the token in the file with the token just returned from ICSF. Management of internal tokens is a user responsibility. Consider the possible case where the token for this call was fetched from a file, and where this reason code is ignored. For the next invocation of the service, the token will be fetched from the file again, and the service will give this reason code again. If this continues until the master key is changed again, then the next use of the internal token will fail.

ICSF Reason Codes for Return Code 4 (4)

Table 85 lists reason codes returned from callable services that give return code 4.

Table 85. ICSF Reason Codes for Return Code 4 (4)

ICSF Reason Code Hex (Decimal)	TSS Reason Code Hex (Decimal)	Description
0 (0)	0 (0)	Master key verification warning. There is a possible mismatch between the master key verification pattern in the CKDS and the system master key verification pattern. **User action**: Ensure that you specified the correct CKDS. If you specified the correct CKDS, check to see if the data set has been corrupted.
7D0 (2000)	014 (020)	The input text length was odd rather than even. The right nibble of the last byte is padded with X'00'. **User action**: None
BBA (3002)		The call to the CVV Verify callable service was successfully processed. However, the trial CVV that was supplied does not match the generated CVV. In addition, a key in the key identifier has been reenciphered. **User action**: See reason code 4000 for more details about the incorrect CVV. See reason code 10000 for more details about the key reencipherment.

Table 85. ICSF Reason Codes for Return Code 4 (4) (continued)

ICSF Reason Code Hex (Decimal)	TSS Reason Code Hex (Decimal)	Description
BD4 (3028)	013 (019)	The call to the Encrypted PIN verify (PINVER) callable service was successfully processed. However, the trial PIN that was supplied does not match the PIN in the PIN block. **User action**: The PIN is incorrect. If you expected the reason code to be zero, check that you are using the correct key.
BD8 (3032)	013 (019)	This is a combination reason code value. The call to the Encrypted PIN verify (PINVER) callable service was successfully processed. However, the trial PIN that was supplied does not match the PIN in the PIN block. In addition, a key in a key identifier token has been reenciphered. **User action**: See reason code 3028 for more detail about the incorrect PIN. See reason code 10000 for more detail about the key reencipherment.
FA0 (4000)	01 (01)	The CVV did not verify. **User action**: Regenerate the CVV.
1F40 (8000)	01 (01)	The call to the MAC verification (MACVER) callable service was successfully processed. However, the trial MAC that you supplied does not match that of the message text. **User action**: The message text may have been modified, such that its contents cannot be trusted. If you expected the reason code to be zero, check that you are using the correct key. Check that all segments of the message were presented and in the correct sequence. Also check that the trial MAC corresponds to the message being authenticated.
1F44 (8004)	01 (01)	This is a combination reason code value. The call to the MAC verification (MACVER) callable service was successfully processed. However, the trial MAC that was supplied does not match the message text provided. In addition, a key in a key identifier token has been reenciphered. **User action**: See reason code 8000 for more detail about the incorrect MAC. See reason code 10000 for more detail about the key reencipherment.
2328 (9000)	01 (01)	The call to the key test service processed successfully, but the key test pattern was not verified. **User action**: Investigate why the key failed. After determining this, you can reinstall or regenerate the key.
232C (9004)	01 (01)	This is a combination reason code value. The call to the key test service processed successfully, but the key test pattern was not verified. Also, the key token has been reenciphered. **User action**: Investigate why the key failed. After determining this, you can reinstall or regenerate the key.
2AF8 (11000)	1AD (429)	The digital signature verify ICSF callable service or TSS verb completed successfully but the supplied digital signature failed verification. **User action**: None
36B8 (14008)	01 (01)	The PKDS record failed the authentication test. **User action**: The record has changed since ICSF wrote it to the PKDS. The user action is application dependent.

ICSF Reason Codes for Return Code 8 (8)

Table 86 on page 322 lists reason codes returned from callable services that give return code 8.

Most of these reason codes indicate that the call to the service was unsuccessful. No cryptographic processing took place. Therefore, no output parameters were filled. Exceptions to this are noted in the descriptions.

Table 86. ICSF Reason Codes for Return Code 8 (8)

ICSF Reason Code Hex (Decimal)	TSS Reason Code Hex (Decimal)	Description
7D1 (2001)		TKE: DH generator is greater than the modulus.
7D2 (2002)		TKE: DH registers are not in a valid state for the requested operation.
7D3 (2003)		TKE: TSN does not match TSN in pending change buffer.
7D4 (2004)	019 (025)	A length parameter has an incorrect value. The value in the length parameter could have been zero (when a positive value was required) or a negative value. If the supplied value was positive, it could have been larger than your installation's defined maximum, or for MDC generation with no padding, it could have been less than 16 or not an even multiple of 8. **User action**: Check the length you specified. If necessary, check your installation's maximum length with your ICSF administrator. Correct the error.
7D5 (2005)		TKE: PCB data exceeds maximum data length.
7D8 (2008)	A4 (164)	Two parameters (perhaps the plaintext and ciphertext areas, or *text_in* and *text_out* areas) overlap each other. That is, some part of these two areas occupy the same address in memory. This condition cannot be processed. **User action**: Determine which two areas are responsible, and redefine their positions in memory.
7D9 (2009)		TKE: ACI can not load both loads and profiles in one call.
7DA (2010)		TKE: ACI can only load one role or one profile at a time.
7DB (2011)		TKE: DH transport key algorithm match.
7DC (2012)	023 (035)	The *rule_array_count* parameter contains a number that is not valid. **User action**: Refer to the *rule_array_count* parameter described in this book under the appropriate callable service for the correct value.
7DD (2013)		TKE: Length of hash pattern for keypart is not valid for DH transport key algorithm specified.
7DE (2014)		TKE: PCB buffer is empty.
7E0 (2016)	021 (033), 09D (157)	The *rule_array* parameter contents are incorrect. **User action**: Refer to the *rule_array* parameter described in this book under the appropriate callable service for the correct value.
7E2 (2018)	021 (033)	The *form* parameter specified in the random number generate callable service should be ODD, EVEN, or RANDOM. One of these values was not supplied. **User action**: Change your parameter to use one of the required values for the *form* parameter.
7E3 (2019)		TKE: Signature in request CPRB did not verify.
7E4 (2020)		TKE: TSN in request CPRB is not valid.
7E8 (2024)	302 (770), 041 (065)	A reserved field in a parameter, probably a key identifier, has a value other than zero. **User action**: Key identifiers should not be changed by application programs for other uses. Review any processing you are performing on key identifiers and leave the reserved fields in them at zero.
7EB (2027)		TKE: DH transport key hash pattern doesn not match.

Table 86. ICSF Reason Codes for Return Code 8 (8) (continued)

ICSF Reason Code Hex (Decimal)	TSS Reason Code Hex (Decimal)	Description
7EC (2028)	2C2 (706)	While deciphering ciphertext that had been created using a padding technique, it was found that the last byte of the plaintext did not contain a valid count of pad characters. Note that all cryptographic processing has taken place, and the *clear_text* parameter contains the deciphered text. **User action**: The *text_length* parameter was not reduced. Therefore, it contains the length of the base message, plus the length of the padding bytes and the count byte. Review how the message was padded before it was enciphered. The count byte that is not valid was created before the message's encipherment. You may need to check whether the ciphertext was not created using a padding scheme. Otherwise, check with the creator of the ciphertext on the method used to create it. You could also look at the plaintext to review the padding scheme used, if any.
7ED (2029)		TKE: Request data block hash does not match hash in CPRB.
7EE (2030)		TKE: DH supplied hash length is not correct.
| 7EF (2031)		Reply data block too large.
7F0 (2032)		The *key_form, key_type_1*, and *key_type_2* parameters for the key generate callable service form a combination, a three-element string. This combination is checked against all valid combinations. Your combination was not found among this list. **User action**: Check the allowable combinations described for each parameter in Key Generate callable service and correct the appropriate parameter(s).
7F1 (2033)		TKE: Change type does not match PCB change type.
7F4 (2036)	0A5 (165)	The contents of a chaining vector passed to a callable service are not valid. If you called the MAC generation callable service, or the MDC generation callable service with a MIDDLE or LAST segmenting rule, the count field has a number that is not valid. If you called the MAC verification callable service, then this will have been a MIDDLE or LAST segmenting rule. The master key verification pattern (MKVP) field does not match the MKVP in the key identifier provided. **User action**: Check to ensure that the chaining vector is not modified by your program. The chaining vector returned by ICSF should only be used to process one message set, and not intermixed between alternating message sets. This means that if you receive and process two or more independent message streams, each should have its own chaining vector. Similarly, each message stream should have its own key identifier. If you use the same chaining vector and key identifier for alternating message streams, you will **not** get the correct processing performed.
7F6 (2038)		The caller must be in task mode, not SRB mode.
7F8 (2040)	0B5 (181), 03F (063), 09A (154)	This check is based on the first byte in the key identifier parameter. The key identifier provided is either an internal token, where an external or null token was required; or an external or null token, where an internal token was required. The token provided may be none of these, and, therefore, the parameter is not a key identifier at all. Another cause is specifying a *key_type* of IMP-PKA for a key in importable form. **User action**: Check the type of key identifier required and review what you have provided. Also check that your parameters are in the required sequence.
800 (2048)		The *key_form* is not valid for the *key_type* **User action**: Review the *key_form* and *key_type* parameters. For a *key_type* of IMP-PKA, the secure key import callable service supports only a *key_form* of OP.

Table 86. ICSF Reason Codes for Return Code 8 (8) (continued)

ICSF Reason Code Hex (Decimal)	TSS Reason Code Hex (Decimal)	Description
804 (2052)		A single-length key, passed to the secure key import callable service in the *clear_key* parameter, must be padded on the right with binary zeros. The fact that it is a single-length key is identified by the *key_form* parameter, which identifies the key as being DATA, MACGEN, MACVER, and so on. **User action**: If you are providing a single-length key, pad the parameter on the right with zeros. Alternatively, if you meant to pass a double-length key, correct the *key_form* parameter to a valid double-length key type.
808 (2056)	029 (041)	The *key_form* parameter is neither IM nor OP. Most constants, these included, can be supplied in lower or uppercase. Note that this parameter is 4 bytes long, so the value IM or OP is not valid. They must be padded on the right with blanks. **User action**: Review the value provided and change it to IM or OP, as required.
80C (2060)	02B (043)	The *key_length* parameter passed to the key generate callable service holds a value that is not valid. This value must be SINGLE or DOUBLE. The parameter is 8 bytes. Most constants, these included, can be supplied in lower or uppercase. **User action**: Review the value provided and change it to SINGLE or DOUBLE, as appropriate.
| 810 (2064)	0A0 (160)	The key_type and the key_length are not consistent. **User action**: Review the *key_type* parameter provided and match it with the *key_length* parameter.
814 (2068)		You supplied a key identifier or token to the key generate, key import, multiple secure key import, key export, or key record write callable service. This key identifier holds an importer or exporter key, and the NOCV bit is on in the token. Only programs running in supervisor state or in a system key (key 0–7) may provide a key identifier with this bit set on. Your program was not running in supervisor state or a system key. **User action**: Either use a different key identifier, or else run in supervisor state or a system key.
818 (2072)		A request was made to the key generate callable service to generate double-length keys of SINGLE effective length, in the IMEX form. This request is valid only if the *kek_key_identifier_1* parameter identifies a NOCV importer, and the caller (wrongly) supplies a CV importer. The combination of IMEX for the *key_form* parameter and a CV importer key-encrypting key can only be used for single-length keys. **User action**: Either use a key identifier that holds (or identifies) a NOCV importer, or specify a single-length key in the *key_type* parameter.
81C (2076)		A request was made to the key import callable service to import a single-length key. However, the right half of the key in the *import_key_identifier* parameter is not zeros. Therefore, it appears to identify the right half of a double-length key. This combination is not valid. This error does not occur if you are using the word TOKEN in the *key_type* parameter. **User action**: Check that you specified the value in the *key_type* parameter correctly, and that you are using the correct or corresponding *import_key_identifier* parameter.
824 (2084)		The key token is not valid for the CSNBTCK service. If the *source_key_identifier* is an external token, then the *kek_key_identifier* cannot be marked as CDMF. **User action**: Correct the appropriate key identifiers.
828 (2088)		The *origin_identifier* or *destination_identifier* you supplied is not a valid ASCII hexadecimal string. **User action**: Check that you specified a valid ASCII string for the *origin_identifier* or *destination_identifier* parameter.

Table 86. ICSF Reason Codes for Return Code 8 (8) (continued)

ICSF Reason Code Hex (Decimal)	TSS Reason Code Hex (Decimal)	Description
82C (2092)	079 (121)	The *source_key_identifier* or *inbound_key_identifier* you supplied in an ANSI X9.17 service is not a valid ASCII hexadecimal string. **User action**: Check that you specified a valid ASCII string for the *source_key_identifier* or *inbound_key_identifier* parameter.
830 (2096)	07A (122)	The *outbound_KEK_count* or *inbound_KEK_count* you supplied is not a valid ASCII hexadecimal string. **User action**: Check that you specified a valid ASCII hexadecimal string for the *outbound_KEK_count* or *inbound_KEK_count* parameter.
834 (2100)	2CB (715)	You supplied a *pad_character* that is not valid for a Transaction Security System compatibility parameter for which ICSF supports only one value; or, you supplied a KEY keyword and a non-zero *master_key_version_number* in the Key Token Build service; or, you supplied a non-zero regeneration data length for a DSS key in the PKA Generate service. **User action**: Check that you specified the valid value for the TSS compatibility parameter.
838 (2104)	02D (045)	An input character is not in the code table. **User action**: Correct the code table or the source text.
83C (2108)	02F (047)	An unused field must be binary zeros, and an unused key identifier field generally must be zeros. **User action**: Correct the parameter list.
840 (2112)		The length is incorrect for the key type. **User action**: Check the key length parameter. DATA keys may have a length of 8, 16, or 24. DATAXLAT and MAC keys must have a length of 8. All other keys should have a length of 16. Also check that the parameters are in the required sequence.
844 (2116)	021 (033)	Parameter contents or a parameter value is not correct. **User action**: Specify a valid value for the parameter.
BB9 (3001)		HCR7703 and higher systems - SET block decompose service was called with an encrypted OAEP block with a block contents identifier that indicates a PIN block is present. No PIN encrypting key was supplied to process the PIN block. The block contents identifier is returned in the *block_contents_identifier* parameter. OR HCRP220 or lower systems - A PKDS access has been attempted for a PKA token which exceeds the maximum PKA token size of 1024 bytes. This can occur if systems are sharing a PKDS and not all of the sharing systems support PKA tokens larger than 1024 bytes. **User action**: HCR7703 and higher systems - Supply a PIN encrypting key and resubmit the job. HCRP220 and lower systems - Check the key label supplied. The label must represent a PKDS record representing a PKA token of length less than or equal to 1024 bytes.
BBC (3004)	064 (100)	A request was made to the Clear PIN generate or Encrypted PIN verify callable service, and the *PIN_length* parameter has a value outside the valid range. The valid range is from 4 to 16, inclusive. **User action**: Correct the value in the *PIN_length* parameter to be within the valid range from 4 to 16.
BBE (3006)		The UDX verb in the PCI Cryptographic Coprocessor is not authorized to be executed.

Table 86. ICSF Reason Codes for Return Code 8 (8) (continued)

ICSF Reason Code Hex (Decimal)	TSS Reason Code Hex (Decimal)	Description
BC0 (3008)	065 (101)	A request was made to the Clear PIN generate callable service, and the *PIN_check_length* parameter has a value outside the valid range. The valid range is from 4 to 16, inclusive. **User action**: Correct the value in the *PIN_check_length* parameter to be within the valid range from 4 to 16.
BC4 (3012)	069 (105)	A request was made to the Clear PIN generate callable service to generate a VISA-PVV PIN, and the *trans_sec_parm* field has a value outside the valid range. The field being checked in the *trans_sec_parm* is the key index, in the 12th byte. This *trans_sec_parm* field is part of the *data_array* parameter. **User action**: Correct the value in the key index, held within the *trans_sec_parm* field in the *data_array* parameter, to hold a number from the valid range.
BC8 (3016)	06A (106)	A request was made to the Encrypted PIN translate or the Encrypted PIN verify callable service, and the PIN block format value in the *input_PIN_profile* or *output_PIN_profile* parameter has a value that is not valid. **User action**: Correct the PIN block format value.
BD0 (3024)	06B (107)	A request was made to the Encrypted PIN translate callable service and the format control value in the *input_PIN_profile* or *output_PIN_profile* parameter has a value that is not valid. The valid values are NONE or PBVC. **User action**: Correct the format control value to either NONE or PBVC.
BD4 (3028)	074 (116)	A request was made to the Clear PIN generate callable service. The clear_PIN supplied as part of the *data_array* parameter for an GBP-PINO request begins with a zero (0). This value is not valid. **User action**: Correct the clear_PIN value.
BDC (3036)	06F (111)	A request was made to the Encrypted PIN translate callable service. The *sequence_number* parameter was required, but was not the integer value 99999. **User action**: Specify the integer value 99999.
| BE0 (3040)	06E (110)-PAN, 028 (040)-ser. code, 02A (042)-exp. date, 066 (102)-dec table, 067 (103)-val. table, 06C (198)-pad data	The PAN, expiration date, service code, decimalization table data, validation data, or pad data is not numeric (X'F0' through X'F9'). The parameter must be character representations of numerics or hexadecimal data. **User action**: Review the numeric parameters or fields required in the service that you called and change to the format and values required.
FA0 (4000)	033 (051)	The encipher and decipher callable services sometime require text (plaintext or ciphertext) to have a length that is an exact multiple of 8 bytes. Padding schemes always create ciphertext with a length that is an exact multiple of 8. If you want to decipher ciphertext that was produced by a padding scheme, and the text length is not an exact multiple of 8, then an error has occurred. The CBC mode of enciphering requires a text length that is an exact multiple of 8. The ciphertext translate callable service cannot process ciphertext whose length is not an exact multiple of 8. **User action**: Review the requirements of the service you are using. Either adjust the text you are processing or use another process rule.
1388 (5000)		Target cryptographic module is not available in the configuration. **User action**: Correct the target cryptographic module parameter and resubmit.
138C (5004)		Format of the cryptographic request message is not valid. **User action**: Correct the request and resubmit it.
1390 (5008)		Length of the cryptographic request message is not valid. **User action**: Message length of request must be nonzero, a multiple of eight, and less than the system maximum. Correct the request and resubmit it.

Table 86. ICSF Reason Codes for Return Code 8 (8) (continued)

ICSF Reason Code Hex (Decimal)	TSS Reason Code Hex (Decimal)	Description
2710 (10000)	01D (029), 00C (012), 02B (043)	A key identifier was passed to a service or token. It is checked in detail to ensure that it is a valid token, and that the fields within it are valid values. There is a token validation value (TVV) in the token, which is a non-cryptographic value. This value was again computed from the rest of the token, and compared to the stored TVV. If these two values are not the same, this reason code is returned. **User action**: The contents of the token have been altered because it was created by ICSF or TSS. Review your program to see how this could have been caused.
2714 (10004)	018 (024)	A key identifier was passed to a service. The master key verification pattern in the token shows that the key was created with a master key that is neither the current master key nor the old master key. Therefore, it cannot be reenciphered to the current master key. **User action**: Re-import the key from its importable form (if you have it in this form), or repeat the process you used to create the operational key form. If you cannot do one of these, you cannot repeat any previous cryptographic process that you performed with this token.
271C (10012)	01E (030)	A key label was supplied for a key identifier parameter. This label is the label of a key in the in-storage CKDS or the PKDS. Either the key could not be found, or a key record with that label and the specific type required by the ICSF callable service or TSS verb could not be found. For a retained key label, this error code is also returned if the key is not found in the PCI Cryptographic Coprocessor specified in the PKDS record. **User action**: Check with your administrator if you believe that this key should be in the in-storage CKDS or the PKDS. The administrator may be able to bring it into storage. If this key cannot be in storage, use a different label.
2720 (10016)	03D (061)	You specified a value for a *key_type* parameter that is not an ICSF-defined name. **User action**: Review the ICSF key types and use the appropriate one.
2724 (10020)	027 (039)	You specified the word TOKEN for a *key_type* parameter, but the corresponding key identifier, which implies the key type to use, has a value that is not valid in the control vector field. Therefore, a valid key type cannot be determined. **User action**: Review the value that you stored in the corresponding key identifier. Check that the value for *key_type* is obtained from the appropriate *key_identifier* parameter.
272C (10028)	027 (039)	Either the *left* half of the control vector in a key identifier (internal or external) equates to a key type that is not valid for the service you are using, or the value is not that of any ICSF control vector. For example, an exporter key-encrypting key is not valid in the key import callable service. **User action**: Determine which key identifier is in error and use the key identifier that is required by the service.
2730 (10032)	027 (039)	Either the *right* half of the control vector in a key identifier (internal or external) equates to a key type that is not valid for the service you are using, or the value is not that of any ICSF control vector. For example, an exporter key-encrypting key is not valid in the key import callable service. **User action**: Determine which key identifier is in error and use the key identifier that is required by the service.
2734 (10036)	027 (039)	Either the complete control vector (CV) in a key identifier (internal or external) equates to a key type that is not valid for the service you are using, or the value is not that of any ICSF control vector. The difference between this and reason codes 10028 and 10032 is that each half of the control vector is valid, but *as a combination*, the whole is not valid. For example, the left half of the control vector may be the importer key-encrypting key and the right half may be the input PIN-encrypting (IPINENC) key. **User action**: Determine which key identifier is in error and use the key identifier that is required by the service.

Table 86. ICSF Reason Codes for Return Code 8 (8) (continued)

ICSF Reason Code Hex (Decimal)	TSS Reason Code Hex (Decimal)	Description
2738 (10040)	031 (049)	Key identifiers contain a version number. The version number in a supplied key identifier (internal or external) is inconsistent with one or more fields in the key identifier, making the key identifier unusable. **User action**: Use a token containing the required version number.
273C (10044)	0B7 (183)	A cross-check of the control vector the key type implies has shown that it does not correspond with the control vector present in the supplied internal key identifier. **User action**: Change either the key type or key identifier.
2740 (10048)	03D (061)	The *key_type* parameter does not contain one of the valid types for the service or the keyword TOKEN. **User action**: Check the supplied parameter with the ICSF key types. If you supplied the keyword TOKEN, check that you have padded it on the right with blanks.
2744 (10052)	027 (039)	A null key identifier was supplied and the *key_type* parameter contained the word TOKEN. This combination of parameters is not valid. **User action**: Use either a null key identifier or the word TOKEN, not both.
2748 (10056)		You called the key import callable service. The importer key-encrypting key is a NOCV importer and you specified TOKEN for the *key_type* parameter. This combination is not valid. **User action**: Specify a value in the *key_type* parameter for the operational key form.
274C (10060)	03D (061)	You called the key export callable service. A label was supplied in the *key_identifier* parameter for the key to be exported and the *key_type* was TOKEN. This combination is not valid because the service needs a key type in order to retrieve a key from the CKDS. **User action**: Specify the type of key to be exported in the *key_type* parameter.
2754 (10068)	02F (047)	A flag in a key identifier indicates the master key verification pattern (MKVP) is not present in an internal key token. This setting is not valid. **User action**: Use a token containing the required flag values.
2758 (10072)	02F (047)	A flag in a key identifier indicates the encrypted key is not present in an external token. This setting is not valid. **User action**: Use a token containing the required flag values.
275C (10076)	02F (047)	A flag in a key identifier indicates the control vector is not present. This setting is not valid. **User action**: Use a token containing the required flag values.
2760 (10080)		An ICSF private flag in a key identifier has been set to a value that is not valid. **User action**: Use a token containing the required flag values. Do not modify ICSF or the reserved flags for your own use.
2768 (10088)	027 (039)	If you supplied a label in the *key_identifier* parameter, a record with the supplied label was found in the CKDS, but the key type (CV) is not valid for the service. If you supplied an internal key token for the *key_identifier* parameter, it contained a key type that is not valid. **User action**: Check with your ICSF administrator if you believe that this key should be in the in-storage CKDS. The administrator may be able to bring it into storage. If this key cannot be in storage, use a different label.
276C (10092)		You supplied a source key that does not have odd parity and specified ENFORCE as the parity rule on the *rule_array* parameter for either the ANSI X9.17 key export, ANSI X9.17 key import, or ANSI X9.17 key translate callable service. **User action**: Either supply an ODD parity key or change the *rule_array* parameter to specify a parity rule of IGNORE.

Table 86. ICSF Reason Codes for Return Code 8 (8) (continued)

ICSF Reason Code Hex (Decimal)	TSS Reason Code Hex (Decimal)	Description
2770 (10096)		The transport key you specified is a single-length key, which cannot be used to encrypt a double-length AKEK or (*KK). **User action**: Use a double-length AKEK for the transport key.
2774 (10100)		You specified a transport key that cannot be notarized and specified the keyword NOTARIZE in the *rule_array* parameter. The transport key may have already been partially notarized. **User action**: Use a transport key that allows notarization or change the *rule_array* parameter keyword to CPLT-NOT.
2778 (10104)		The AKEK you specified is either partially notarized or is a partial AKEK, which is not valid for this service. **User action**: Use a correct AKEK that is not partially notarized. A partially notarized key can be used as a transport key if you specify CPLT-NOT in the *rule_array* parameter.
277C (10108)		You did not supply a partial AKEK for the *key_identifier* parameter of the key part import service. **User action**: Correct the key_id parameter.
2780 (10112)		The transport key you specified has not been partially notarized and you have specified CPTL-NOT for the *rule_array* parameter. **User action**: Use a transport key that has been partially notarized or change the *rule_array* parameter.
2784 (10116)		You attempted to export an AKEK with a CCA key export service, which is not supported. **User action**: Use the ANSI X9.17 key export callable service (CSNAKEX).
2788 (10120)		The internal key token you supplied, or the key token that was retrieved by the label you supplied, contains a flag setting or data encryption algorithm bit that is not valid for this service. **User action**: Ensure that you supply a key token, or label, for a non-ANSI key type.
278C (10124)	027 (039)	The key identifier you supplied cannot be exported because there is a prohibit-export restriction on the key. **User action**: Use the correct key for the service.
2790 (10128)		The keyword you supplied in the *rule_array* parameter is not consistent or not valid with another parameter you specified. For example, the keyword SINGLE is not valid with the key type of EXPORTER in the key token build callable service. **User action**: Correct either the *rule_array* parameter or the other parameter.
2AF8 (11000)	048 (072)	The value specified for length parameter for a key token, key, or text field is not valid. **User action**: Correct the appropriate length field parameter.
2AFC (11004)	02F (047)	The hash value (of the secret quantities) in the private key section of the internal token failed validation. The values in the token are corrupted. You cannot use this key. **User action**: Recreate the token using the appropriate combination of the PKA key token build, PKA key generate, and PKA key import callable services.
2B00 (11008)	302 (770)	The public or private key values are not valid. (For example, the modulus or an exponent is zero.) You cannot use the key. **User action**: You may need to recreate the token using the PKA key token build or PKA key import callable service or regenerate the key values on another platform.

Table 86. ICSF Reason Codes for Return Code 8 (8) (continued)

ICSF Reason Code Hex (Decimal)	TSS Reason Code Hex (Decimal)	Description
2B04 (11012)	02F (047)	The internal or external private key token contains flags that are not valid. **User action**: You may need to recreate the token using the PKA key token build or PKA key import callable service.
2B08 (11016)	02F (047)	The calculated hash of the public information in the PKA token does not match the hash in the private section of the token. The values in the token are corrupted. **User action**: Verify the public key section and the key name section of the token. If the token is still rejected, then you need to recreate the token using the appropriate combination of the PKA key token build, PKA key generate, and PKA key import callable services.
2B0C (11020)	030 (048)	The hash pattern of the PKA master key (SMK or KMMK) in the supplied internal PKA private key token does not match the current system's PKA master key. This indicates the system PKA master key has changed since the token was created. You cannot use the token. **User action**: Recreate the token using the appropriate combination of the PKA key token build, PKA key generate, and PKA key import callable services.
2B10 (11024)	02F (047)	The PKA tokens have incomplete values, for example, a PKA public key token without modulus. **User action**: Recreate the key.
2B14 (11028)	048 (072)	The modulus of the PKA key is too short for processing the hash or PKCS block. **User action**: Either use a PKA key with a larger modulus size, use a hash algorithm that generates a smaller hash (digital signature services), or specify a shorter DATA key size (symmetric key export, symmetric key generate).
2B18 (11032)	040 (064)	The supplied private key can be used only for digital signature. Key management services are disallowed. **User action**: Supply a key with key management enabled.
2B20 (11040)	042 (066)	The recovered encryption block was not a valid PKCS-1.2 or zero-pad format. (The format is verified according to the recovery method specified in the rule-array.) If the recovery method specified was PKCS-1.2, refer to PKCS-1.2 for the possible error in parsing the encryption block. **User action**: Ensure that the parameters passed to CSNDSYI are correct. Possible causes for this error are incorrect values for the RSA private key or incorrect values in the *RSA_enciphered_key* parameter, which must be formatted according to PKCS-1.2 or zero-pad rules when created.
2B24 (11044)	0B5 (181)	The first section of a supplied PKA token was not a private or public key section. **User action**: Recreate the key.
2B28 (11048)		The eyecatcher on the PKA internal private token is not valid. **User action**: Reimport the private token using the PKA key import callable service.
| 2B2C (11052)		An incorrect PKA token was supplied. The service requires a private key token. | **User action**: Supply a PKA private key token as input.
2B30 (11056)		The input PKA token contains length fields that are not valid. **User action**: Recreate the key token.
2B38 (11064)	2CF (719)	The RSA-OAEP block did not verify after the decompose. The block type is incorrect (must be X'03'). **User action**: Recreate the RSA-OEAP block.
2B3C (11068)	2D1 (721)	The RSA-OAEP block did not verify after the decompose. The verification code is not correct (must be all zeros). **User action**: Recreate the RSA-OEAP block.

Table 86. ICSF Reason Codes for Return Code 8 (8) (continued)

ICSF Reason Code Hex (Decimal)	TSS Reason Code Hex (Decimal)	Description
2B40 (11072)	2D0 (720)	The RSA-OAEP block did not verify after the decompose. The random number I is not correct (must be non-zero with the high-order bit equal to zero). **User action**: Recreate the RSA-OAEP block.
2B48 (11080)	041 (65), 2F8 (760)	The RSA public or private key specified a modulus length that is incorrect for this service. **User action**: Re-invoke the service with an RSA key with the proper modulus length.
2B4C (11084)		This service requires an RSA public key and the key identifier specified is not a public key. **User action**: Re-invoke the service with an RSA public key.
2B50 (11088)		This service requires an RSA private key that is for signature use only. **User action**: Re-invoke the service with a supported private key.
2B54 (11092)		There was an invalid subsection in the PKA token. **User action**: Correct the PKA token.
2B58 (11096)	040 (064)	This service requires an RSA private key that is for signature use. The specified key may be used for key management purposes only. **User action**: Re-invoke the service with a supported private key.
3E80 (16000)	Reason code 0, return code 308(776)	RACF failed your request to use this service. **User action**: Contact your ICSF or RACF administrator if you need this service.
3E84 (16004)	Reason code 1, return code 308(776)	RACF failed your request to use the key label. **User action**: Contact your ICSF or RACF administrator if you need this key.
3E8C (16012)		You requested the conversion service, but you are not running in MVS-authorized state. **User action**: You must be running in supervisor state to use the conversion service. Contact your ICSF administrator.
| 3E90 (16016)	027 (039)	The input/output field contained a valid internal token with the NOCV bit on or encryption algorithm mark, but the key type was incorrect or did not match the type of the generated or imported key. Processing failed. **User action**: Correct the calling application.
3E94 (16020)		You requested dynamic CKDS update services for a system key, which is not allowed. **User action**: Correct the calling application.
3E98 (16024)	0B5 (181)	You called the key record write callable service, but the key token you supplied is not valid. **User action**: Check with your ICSF administrator if you believe that this key should be in the in-storage CKDS. The administrator may be able to bring it into storage. If this key cannot be in storage, use a different label.
3EA0 (16032)	020 (032)	You called the key record create callable service, but the *key_label* parameter syntax was incorrect. **User action**: Correct *key_label* syntax.
3EA4 (16036)	02C (044)	The key record create callable service requires that the key created not already exist in the CKDS. A key of the same label was found. **User action**: Make sure the application specifies the correct label. If the label is correct, contact your ICSF security administrator or system programmer.

Table 86. ICSF Reason Codes for Return Code 8 (8) (continued)

ICSF Reason Code Hex (Decimal)	TSS Reason Code Hex (Decimal)	Description
3EA8 (16040)		Data in the PKDS record did not match the expected data. This occurs if the record does not contain a null PKA token and CHECK was specified. **User action**: If the record is to be overwritten regardless of its content, specify OVERLAY.
3EAC (16044)		One or more key labels specified as input to the PKA key generate or PKA key import service incorrectly refer to a retained private key. If generating a retained private key, this error may result from one of the following conditions: • The private key name of the retained private key being generated is the same as an existing PKDS record, but the PKDS record label was not specified as the input skeleton (source) key identifier. • The label specified in the *generated_key_token* parameter as the target for the retained private key was not the same as the private key name If generating or importing a non-retained key, this error occurs when the label specified as the target key specifies a retained private key. The retained private key cannot be over-written. **User action:** Make sure the application specifies the correct label. If the label is correct, contact your ICSF security administrator or system programmer.
3EB0 (16048)		Retained keys on the PKDS cannot be deleted or updated using the PKDS key record delete or PKDS key record write callable services, respectively. **User action:** Use the retained key delete callable service to delete retained keys.

ICSF Reason Codes for Return Code C (12)

Table 87 lists reason codes returned from callable services that give return code 12. These reason codes indicate that the call to the callable service was not successful. Either cryptographic processing did not take place, or the last cryptographic unit was switched offline. Therefore, no output parameters were filled. |

| **Note:** The higher-order halfword of the reason code field for return code C (12) may contain additional coding. See reason codes 273C and 2740 in the following table. For example, in the reason code 42738, the 4 is an SVC 99 error code and the 2738 is listed in the table below.

| Table 87. ICSF Reason Codes for Return Code C (12)

ICSF Reason Code Hex (Decimal)	TSS Reason Code Hex (Decimal)	Description
0 (0)		ICSF: ICSF is not available. Either ICSF was not started, or ICSF has started, but does not have access to any cryptographic units. Your request cannot be processed. **User action**: Check the availability of ICSF with your ICSF administrator.
4 (4)		The CKDS management service you called is not available because it has been disallowed by the administrator panel. **User action**: Contact the security administrator or system programmer to determine why the CKDS management services have been disallowed.
8 (8)		The service or algorithm is not available on current hardware. Your request cannot be processed. **User action**: Correct the calling program or run on applicable hardware.
C (12)		The service that you called is unavailable because the installation exit for that service had previously failed. **User action**: Contact your ICSF administrator or system programmer.

Table 87. ICSF Reason Codes for Return Code C (12) (continued)

ICSF Reason Code Hex (Decimal)	TSS Reason Code Hex (Decimal)	Description
10 (16)		A requested installation service routine could not be found. Your request was not processed. **User action**: Contact your ICSF administrator or system programmer.
1C (28)		Cryptographic asynchronous processor failed. **User action**: Contact your IBM support center.
20 (32)		Cryptographic asynchronous instruction was not executed. **User action**: Ensure cryptographic services are enabled.
32 (50)		An ICSF PKA service could not be performed because ICSF is being terminated. Any of the PKA services can issue this. **User action**: Review the reason code.
178C (6028)		ESTAE could not be established in common I/O routines. **User action**: Contact your system programmer or the IBM Support Center.
7D6 (2006)		TKE: PCB service error.
7D7 (2007)		TKE: Change type in PCB is not recognized.
7DF (2015)		Domain in CPRB not enabled by EMB mask.
7E1 (2017)		MKVP mismatch on Set MK.
7E5 (2021)		PCI Cryptographic Coprocessor adapter disabled.
7E9 (2025)		Enforcement mask error.
7F3 (2035)		Intrusion latch has been tripped. Services disabled.
7F5 (2037)		The domain specified is not valid.
7FB (2043)		OA certificate not found.
1790 (6032)		The dynamic allocation of the DASD copy of the CKDS or PKDS in use by ICSF failed. **User action**: Contact your ICSF security administrator or system programmer. The SVC 99 error code will be placed in the high-order halfword of the reason code field.
1794 (6036)		A dynamic deallocation error occurred when closing and deallocating a CKDS or PKDS. **User action**: Contact your security administrator or system programmer. The SVC 99 error code will be placed in the high-order halfword of the reason code field.
2724 (10020)		A key retrieved from the in-storage CKDS failed the MAC verification (MACVER) check and is unusable. **User action**: Contact your ICSF administrator.
2728 (10024)		A key retrieved from the in-storage CKDS or a key to be written to the PKDS was rejected for use by the installation exit. **User action**: Contact your ICSF administrator or system programmer.
272C (10028)		You cannot use the secure key import or multiple secure key import callable services because the cryptographic unit is not enabled for processing. The cryptographic unit is not in special secure mode or is disabled in the environment control mask (ECM). **User action**: Contact your ICSF administrator (your administrator can enable the processing mode or the ECM).

Table 87. ICSF Reason Codes for Return Code C (12) (continued)

ICSF Reason Code Hex (Decimal)	TSS Reason Code Hex (Decimal)	Description
2734 (10036)		More than one key with the same label was found in the CKDS or PKDS. This function requires a unique key per label. The probable cause may be the use of an incorrect label pointing to a key type that allows multiple keys per label. **User action**: Make sure the application specifies the correct label. If the label is correct, contact your ICSF security administrator or system programmer to verify the contents of the CKDS or PKDS.
273C (10044)		OPEN of the PKDS in use by ICSF failed. **User action**: Contact your ICSF security administrator or system programmer.
2740 (10048)	0C5 (197)	I/O error reading or writing to the DASD copy of the CKDS or PKDS in use by ICSF. **User action**: Contact your ICSF security administrator or system programmer. The RPL feedback code will be placed in the high-order halfword of the reason code field.
2744 (10052)		Automatic REFRESH to free storage in the linear section of the CKT failed. **User action**: Contact your ICSF security administrator or system programmer and request that a REFRESH be done.
274C (10060)		The I/O subtask terminated for an unexpected reason before completing the request. No dynamic CKDS or PKDS update services are possible at this point. **User action**: Contact your system programmer who can investigate the problem and restart the I/O subtask by stopping and restarting ICSF.
2B04 (11012)		This function is disabled in the environment control mask (ECM). **User action**: Contact your ICSF administrator.
2B08 (11016)	2FC (764)	The PKA master key is not in a valid state. **User action**: Contact your ICSF administrator.
2B0C (11020)	Return code 8, reason code 30F (783)	The modulus of the public or private key is larger than allowed and configured in the CCC. You cannot use this key on this system. **User action**: Regenerate the key with a smaller modulus size.
2B10 (11024)		The system administrator has used the ICSF User Control Functions Panel to disable the PKA functions. **User action**: Wait until administrator functions are complete and the PKA functions are again enabled.
2B18 (11032)		A CAMQ is valid for PKSC but not for PKA. **User action**: Contact your ICSF administrator.
2B1C (11036)		A PKDS is not available for processing. **User action**: Contact your ICSF administrator.
2B20 (11040)		The PKDS Control Record hash pattern is not valid. **User action**: Contact your ICSF administrator.
2B24 (11044)		The PKDS could not be accessed. **User action**: Contact your ICSF administrator.
2B28 (11048)		The PCI Cryptographic Coprocessor failed. **User action**: Contact your IBM support center.

Table 87. ICSF Reason Codes for Return Code C (12) (continued)

ICSF Reason Code Hex (Decimal)	TSS Reason Code Hex (Decimal)	Description
2B2C (11052)		The specific PCI Cryptographic Coprocessor requested for service is temporarily unavailable. PKDS could not be accessed. The specific PCI Cryptographic Coprocessor may be attempting some recovery action. If recovery action is successful, the PCI Cryptographic Coprocessor will be made available. If the recovery action fails, the PCI Cryptographic Coprocessor will be made permanently unavailable. **User action**: Retry the function.
2B30 (11056)		The PCI Cryptographic Coprocessor failed. The response from the processor was incomplete. **User action**: Contact your IBM support center.
2B34 (11060)		The service could not be performed because the required PCI Cryptographic Coprocessor was not active. **User action**: If the service required a specific PCI Cryptographic Coprocessor, verify that the value specified is correct. Reissue the request when the required PCI Cryptographic Coprocessor is available.
2B38 (11064)		Service could not be performed because of a hardware error on the PCI Cryptographic Coprocessor.
2EDC (11996)		The Integrated Cryptographic Feature is not available for CKDS initialization because the cryptographic unit is not in special secure mode. **User action**: Contact your ICSF administrator.
2EE0 (12000)		You cannot use the Clear PIN generate callable service because the cryptographic unit is not enabled for processing. The cryptographic unit is not in special secure mode. **User action**: Contact your ICSF administrator who can enable the processing mode.
2EE4 (12004)		An error occurred in a latch manager call. **User action**: Contact your ICSF security administrator or system programmer.
8CB4 (36020)		A refresh of the CKDS failed because the DASD copy of the CKDS is enciphered under the wrong master key. This may have resulted from an automatic refresh during processing of the key record create callable service. **User action**: Contact your ICSF administrator.

ICSF Reason Codes for Return Code 10 (16)

Table 88 lists reason codes returned from callable services that give return code 16.

Table 88. ICSF Reason Codes for Return Code 10 (16)

ICSF Reason Code Hex (Decimal)	TSS Reason Code Hex (Decimal)	Description
4 (4)		ICSF: Your call to an ICSF callable service resulted in an abnormal ending. The request parameter block failed consistency checking. **User action**: Contact your system programmer or the IBM Support Center.

Transaction Security System Return Codes and Reason Codes

The following section describes the return codes and reason codes that are returned after a call to a Transaction Security System verb has been completed. It also lists TSS to ICSF return codes and reason codes. Each TSS return code returns unique reason codes to your application program. The reason codes associated with each return code are described in the following sections. The reason code tables present the TSS hexadecimal code followed by the decimal code in parenthesis. If there is a 1-to-1 mapping, the codes will be converted. If there is not a map to ICSF, the column will be blank. If there are multiple mappings, they will be listed as reference only and will not be converted.

TSS Reason Codes for Return Code 0 (0)

Table 89 lists reason codes returned from TSS verbs that give return code 0 and any corresponding ICSF reason codes.

Table 89. TSS Reason Codes for Return Code 0 (0)

TSS Reason Code Hex (Decimal)	ICSF Reason Code Hex (Decimal)	Description
0 (0)	0 (0)	The call to the ICSF callable service or TSS verb was successfully processed. No error was encountered. **User action**: None.
2 (2)	4 (4)	The call to the ICSF callable service or TSS verb was successfully processed. A minor error was detected. A key used in the service was shown to have even parity. This key could be one provided by you as a parameter or be one (perhaps of many) that was retrieved from the in-storage CKDS. **User action**: Refer to the reason code obtained when the key passed to this service was transformed into operational form using clear key import, multiple clear key import, key import, secure key import, or multiple secure key import callable services. Check if any of the services prepared an even parity key. If one of these service reported an even parity key, you need to know which key is affected. If none of these services identified an even parity key, then the even parity key detected was found on the CKDS. Report this to your administrator.
8 (8)	8 (8)	The key record read callable service attempted to read a NULL key record. The returned key token contains only binary zeros. **User action**: None required.
2710 (10000)	2710 (10000)	The call to the TSS verb was successfully processed. The keys in one or more key identifiers have been reenciphered from encipherment under the old master key to encipherment under the current master key. **User action**: If you obtained your operational token from a file, replace the token in the file with the token just returned from ICSF. Management of internal tokens is a user responsibility. Consider the possible case where the token for this call was fetched from a file, and where this reason code is ignored. For the next invocation of the service, the token will be fetched from the file again, and the service will give this reason code again. If this continues until the master key is changed again, then the next use of the internal token will fail.
2711 (10001)		The call to the TSS verb was successfully processed. The keys in one or more key identifiers were encrypted under the old master key. The verb was unable to reencipher the key.

TSS Reason Codes for Return Code 4 (4)

Table 90 lists reason codes returned from TSS verbs that give return code 4 and any corresponding ICSF reason codes.

Table 90. TSS Reason Codes for Return Code 4 (4)

TSS Reason Code Hex (Decimal)	ICSF Reason Code Hex (Decimal)	Description
01 (01)	FA0 (4000), 1F40 (8000), 1F44 (8004), 2328 (9000), 232C (9004), 36B8 (14008)	The verification test failed.

Table 90. TSS Reason Codes for Return Code 4 (4) (continued)

TSS Reason Code Hex (Decimal)	ICSF Reason Code Hex (Decimal)	Description
013 (019)	BD4 (3028)	The call to the Encrypted PIN verify (PINVER) callable service was successfully processed. However, the trial PIN that was supplied does not match the PIN in the PIN block. **User action**: The PIN is incorrect. If you expected the reason code to be zero, check that you are using the correct key.
014 (020)	7D0 (2000)	The input text length was odd rather than even. The right nibble of the last byte is padded with X'00'. **User action**: None
0A6 (166)		The control vector is not valid because of parity bits, anti-variant bits, inconsistent KEK bits, or because bits 59 to 62 are not zero.
0B3 (179)		The control vector keywords that are in the rule array are ignored.
1AD (429)	2AF8 (11000)	The digital signature verify ICSF callable service or TSS verb completed successfully but the supplied digital signature failed verification. **User action**: None

Reason Codes for Return Code 8 (8)

Table 91 lists reason codes returned from TSS verbs that give return code 8 and any corresponding ICSF reason codes.

Table 91. TSS Reason Codes for Return Code 8 (8)

TSS Reason Code Hex (Decimal)	ICSF Reason Code Hex (Decimal)	Description
00C (012)	2710 (10000)	A key identifier was passed to a service or token. It is checked in detail to ensure that it is a valid token, and that the fields within it are valid values. There is a token validation value (TVV) in the token, which is a non-cryptographic value. This value was again computed from the rest of the token, and compared to the stored TVV. If these two values are not the same, this reason code is returned. **User action**: The contents of the token have been altered because it was created by ICSF or TSS. Review your program to see how this could have been caused.
016 (022)		The ID number in the request field is not valid. Missing section in PKA token.
017 (023)		An access to the data area was outside the data area boundary.
01D (029)	2710 (10000)	A key identifier was passed to a service or token. It is checked in detail to ensure that it is a valid token, and that the fields within it are valid values. There is a token validation value (TVV) in the token, which is a non-cryptographic value. This value was again computed from the rest of the token, and compared to the stored TVV. If these two values are not the same, this reason code is returned. **User action**: The contents of the token have been altered because it was created by ICSF or TSS. Review your program to see how this could have been caused.
01E (030)	271C (10012)	A key label was supplied for a key identifier parameter. This label is the label of a key in the in-storage CKDS or the PKDS. Either the key could not be found, or a key record with that label and the specific type required by the ICSF callable service or TSS verb could not be found. For a retained key label, this error code is also returned if the key is not found in the PCI Cryptographic Coprocessor specified in the PKDS record. **User action**: Check with your administrator if you believe that this key should be in the in-storage CKDS or the PKDS. The administrator may be able to bring it into storage. If this key cannot be in storage, use a different label.
01F (031)	272C (10028)	The control vector did not specify a DATA key.

Table 91. TSS Reason Codes for Return Code 8 (8) (continued)

TSS Reason Code Hex (Decimal)	ICSF Reason Code Hex (Decimal)	Description
020 (032)	3EA0 (16032)	You called the key record create callable service, but the *key_label* parameter syntax was incorrect. **User action**: Correct *key_label* syntax.
021 (033)	7E0 (2016)	The *rule_array* parameter contents or a parameter value is not correct. **User action**: Refer to the *rule_array* parameter described in this book under the appropriate callable service for the correct value.
022 (034)	7E0 (2016)	A rule array keyword combination is not valid.
023 (035)	7DC (2012)	The *rule_array_count* parameter contains a number that is not valid. **User action**: Refer to the *rule_array_count* parameter described in this book under the appropriate callable service for the correct value.
027 (039)	272C (10028), 2730 (10032), 2734 (10036), 2744 (10052), 2768 (10088), 278C (10124), 3E90 (16016), 2724 (10020)	A control vector violation occurred.
028 (040)	BE0 (3040)	The service code does not contain numerical character data.
029 (041)	808 (2056)	The *key_form* parameter is neither IM nor OP. Most constants, these included, can be supplied in lower or uppercase. Note that this parameter is 4 bytes long, so the value IM or OP is not valid. They must be padded on the right with blanks. **User action**: Review the value provided and change it to IM or OP, as required.
02A (042)- expiration date	BE0 (3040)	The expiration date is not numeric (X'F0' through X'F9'). The parameter must be character representations of numerics or hexadecimal data. **User action**: Review the numeric parameters or fields required in the service that you called and change to the format and values required.
02B (043)	2710 (10000), 80C (2060)	A key identifier was passed to a service or token. It is checked in detail to ensure that it is a valid token, and that the fields within it are valid values. There is a token validation value (TVV) in the token, which is a non-cryptographic value. This value was again computed from the rest of the token, and compared to the stored TVV. If these two values are not the same, this reason code is returned. **User action**: The contents of the token have been altered because it was created by ICSF or TSS. Review your program to see how this could have been caused.
02C (044)		The key record create callable service requires that the key created not already exist in the CKDS. A key of the same label was found. **User action**: Make sure the application specifies the correct label. If the label is correct, contact your ICSF security administrator or system programmer.
02D (045)		An input character is not in the code table. **User action**: Correct the code table or the source text.
02F (047)	83C (2108), 2754 (10068), 2758 (10072), 275C (10076), 2AFC (11004), 2B04 (11012), 2B08 (11016), 2B10 (11024)	A source key token is unusable because it contains data that is not valid or undefined.
030 (048)		One or more keys has a master key verification pattern that is not valid.

Table 91. TSS Reason Codes for Return Code 8 (8) (continued)

TSS Reason Code Hex (Decimal)	ICSF Reason Code Hex (Decimal)	Description
031 (049)	2738 (10040)	Key identifiers contain a version number. The version number in a supplied key identifier (internal or external) is inconsistent with one or more fields in the key identifier, making the key identifier unusable. **User action**: Use a token containing the required version number.
03D (061)	2720 (10016), 2740 (10048), 274C (10060)	The keyword supplied with the *key_type* parameter is not valid.
03E (062)	271C (10012)	The source key was not found.
03F (063)	7F8 (2040)	This check is based on the first byte in the key identifier parameter. The key identifier provided is either an internal token, where an external or null token was required; or an external or null token, where an internal token was required. The token provided may be none of these, and, therefore, the parameter is not a key identifier at all. Another cause is specifying a *key_type* of IMP-PKA for a key in importable form. **User action**: Check the type of key identifier required and review what you have provided. Also check that your parameters are in the required sequence.
040 (064)	2B18 (11032), 2B58 (11096)	The supplied private key can be used only for digital signature. Key management services are disallowed. **User action**: Supply a key with key management enabled.
041 (065)	7E8 (2024)	The RSA public or private key specified a modulus length that is incorrect for this service. **User action**: Re-invoke the service with an RSA key with the proper modulus length.
042 (066)	2B20 (11040)	The recovered encryption block was not a valid PKCS-1.2 or zero-pad format. (The format is verified according to the recovery method specified in the rule-array.) If the recovery method specified was PKCS-1.2, refer to PKCS-1.2 for the possible error in parsing the encryption block. **User action**: Ensure that the parameters passed to CSNDSYI are correct. Possible causes for this error are incorrect values for the RSA private key or incorrect values in the *RSA_enciphered_key* parameter, which must be formatted according to PKCS-1.2 or zero-pad rules when created.
043 (067)		RSA encryption failed.
044 (068)		RSA decryption failed.
048 (072)	2AF8 (11000), 2B14 (11028)	The value specified for length parameter for a key token, key, or text field is not valid. **User action**: Correct the appropriate length field parameter.
05A (090)		Access is denied for this verb. The authorization level is either too low or is not identical.
064 (100)	BBC (3004)	The PIN length is not valid.
065 (101)	BC0 (3008)	The PIN check length is not valid. It must be in the range from 4 to the PIN length inclusive.
066 (102)	BE0 (3040)	The value of the decimalization table is not valid.
067 (103)	BE0 (3040)	The value of the validation data is not valid.
068 (104)	BE0 (3040)	The value of the customer-selected PIN is not valid, or the PIN length does not match the value specified.
069 (105)	BE0 (3040)	The value of the *transaction_security_parameter* is not valid.
06A (106)	BC8 (3016)	The PIN block format keyword is not valid.
06B (107)	BD0 (3024)	The format control keyword is not valid.
06C (108)	BC8 (3016)	The value of the PAD data is not valid.
06D (109)		The extraction method keyword is not valid.
06E (110)	BE0 (3040)	The value of the PAN data is not numeric character data.

Table 91. TSS Reason Codes for Return Code 8 (8) (continued)

TSS Reason Code Hex (Decimal)	ICSF Reason Code Hex (Decimal)	Description
074 (116)	BBC (3004)	The clear PIN value is not valid.
079 (121)		The *source_key_identifier* or *inbound_key_identifier* you supplied in an ANSI X9.17 service is not a valid ASCII hexadecimal string. **User action**: Check that you specified a valid ASCII string for the *source_key_identifier* or *inbound_key_identifier* parameter.
09A (154)	7F8 (2040)	This check is based on the first byte in the key identifier parameter. The key identifier provided is either an internal token, where an external or null token was required; or an external or null token, where an internal token was required. The token provided may be none of these, and, therefore, the parameter is not a key identifier at all. Another cause is specifying a *key_type* of IMP-PKA for a key in importable form. **User action**: Check the type of key identifier required and review what you have provided. Also check that your parameters are in the required sequence.
09B (155)		The value that the *generated_key_identifier* parameter specifies is not valid,or it is not consistent with the value that the *key_form* parameter specifies.
09C (156)	2790 (10128)	A keyword is not valid with the specified parameters.
09D (157)	7E0 (2016)	The key-token type is not specified in the rule array.
0A0 (160)		The key type and the key length are not consistent.
0B5 (181)		This check is based on the first byte in the key identifier parameter. The key identifier provided is either an internal token, where an external or null token was required; or an external or null token, where an internal token was required. The token provided may be none of these, and, therefore, the parameter is not a key identifier at all. Another cause is specifying a *key_type* of IMP-PKA for a key in importable form. **User action**: Check the type of key identifier required and review what you have provided. Also check that your parameters are in the required sequence.
0B7 (183)	273C (10044)	A cross-check of the control vector the key type implies has shown that it does not correspond with the control vector present in the supplied internal key identifier. **User action**: Change either the key type or key identifier.
0B8 (184)		An input pointer is null.
0CC (204)		A memory allocation failed.
154 (340)		One of the input control vectors has odd parity.
157 (343)		Either the data block or the buffer for the block is too small.
159 (345)		Insufficient storage space exists for the data in the data block buffer.
15A (346)		The requested command is not valid in the current state of the cryptographic hardware component.
176 (374)	7D4 (2004), 7E0 (2016)	Less data was supplied than expected or less data exists than was requested.
181 (385)		The cryptographic hardware component reported that the data passed as part of the command is not valid for that command.
197 (407)	BC8 (3016)	A PIN block consistency check error occurred.
25D (605)		The number of output bytes is greater than the number that is permitted.
2BF (703)		A new master key value was found to be one of the weak DES keys.
2C0 (704)		The new master key would have the same master key verification pattern as the current master key.
2C1 (705)		The same key-encrypting key was specified for both exporter keys.

Table 91. TSS Reason Codes for Return Code 8 (8) (continued)

TSS Reason Code Hex (Decimal)	ICSF Reason Code Hex (Decimal)	Description
2C2 (706)	7EC (2028)	While deciphering ciphertext that had been created using a padding technique, it was found that the last byte of the plaintext did not contain a valid count of pad characters. Note that all cryptographic processing has taken place, and the *clear_text* parameter contains the deciphered text. **User action**: The *text_length* parameter was not reduced. Therefore, it contains the length of the base message, plus the length of the padding bytes and the count byte. Review how the message was padded before it was enciphered. The count byte that is not valid was created before the message's encipherment. You may need to check whether the ciphertext was not created using a padding scheme. Otherwise, check with the creator of the ciphertext on the method used to create it. You could also look at the plaintext to review the padding scheme used, if any.
2C3 (707)		The master key registers are not in the state required for the requested function.
2CA (714)	844 (2116)	A reserved parameter was not a null pointer or an expected value.
2CB (715)	834 (2100)	A non-zero value was specified for a field that must be zero.
2CF (719)	2B38 (11064)	The RSA-OAEP block did not verify after the decompose. The block type is incorrect (must be X'03'). **User action**: Recreate the RSA-OEAP block.
2D0 (720)	2B40 (11072)	The RSA-OAEP block did not verify after the decompose. The random number I is not correct (must be non-zero with the high-order bit equal to zero). **User action**: Recreate the RSA-OEAP block.
2D1 (721)	2B3C (11068)	The RSA-OAEP block did not verify after the decompose. The verification code is not correct (must be all zeros). **User action**: Recreate the RSA-OEAP block.
2F8 (760)	2B48 (11080)	The RSA public or private key specified a modulus length that is incorrect for this service. **User action**: Re-invoke the service with an RSA key with the proper modulus length.
302 (770)	2B00 (11008)	A reserved field in a parameter, probably a key identifier, has a value other than zero. **User action**: Key identifiers should not be changed by application programs for other uses. Review any processing you are performing on key identifiers and leave the reserved fields in them at zero.
30F (783)	Return code 12, reason code 2B0C (11020)	The command is not permitted by Function-Control-Vector value.
405 (1029)		There is an error in the Environment Identification data.
41A (1050)		A KEK RSA-enciphered at this node (EID) cannot be imported at this same node.
7DF (2015)		An error occurred in the Domain Manager.

TSS Reason Codes for Return Code C (12)

Table 92 on page 342 lists reason codes returned from TSS verbs that give return code C and any corresponding ICSF reason codes.

Table 92. TSS Reason Codes for Return Code C (12)

TSS Reason Code Hex (Decimal)	ICSF Reason Code Hex (Decimal)	Description
2FC (764)		The PKA master key is not in a valid state. **User action**: Contact your ICSF administrator.

TSS Reason Codes for Return Code 10 (16)

Table 93 lists reason codes returned from TSS verbs that give return code 10 and any corresponding ICSF reason codes. These error codes will result in an ICSF 18F abend with reason code X'50'. The caller will get return code 16, reason code 4.

Table 93. TSS Reason Codes for Return Code 10 (16)

TSS Reason Code Hex (Decimal)	ICSF Reason Code Hex (Decimal)	Description
150 (336)	4 (4)	An error occurred in the cryptographic hardware component.
22C (556)	4 (4)	The request parameter block failed consistency checking.
2C4 (708)	4 (4)	Inconsistent data was returned from the cryptographic engine.
2C5 (709)	4 (4)	Cryptographic engine internal error; could not access the master key data.
2C8 (712)	4 (4)	An unexpected error occurred in the Master Key manager.

Appendix B. Coding Examples

This appendix provides sample routines using the ICSF callable services for the following languages:
- C
- COBOL
- Assembler
- PL/1

The COBOL and Assembler H examples that follow use the key generate, encipher, and decipher callable services to determine whether the deciphered text matches the starting text.

C

```
/*-------------------------------------------------------------------*
 * Example using C:                                                  *
 *   Invokes CSNBKGN (key generate), CSNBENC (DES encipher) and      *
 *   CSNBDEC (DES decipher)                                          *
 *-------------------------------------------------------------------*/
#include <stdio.h>
#include "csfhdrs.h"

/*-------------------------------------------------------------------*
 * Prototypes for functions in this example                          *
 *-------------------------------------------------------------------*/

/*-------------------------------------------------------------------*
 * Utility for printing hex strings                                  *
 *-------------------------------------------------------------------*/
void printHex(unsigned char *, unsigned int);

/*********************************************************************/
/* Main Function                                                     */
/*********************************************************************/
int main(void) {

  /*-----------------------------------------------------------------*
   * Constant inputs to ICSF services                                *
   *-----------------------------------------------------------------*/
  static int textLen = 24;
  static unsigned char clearText[24]="ABCDEFGHIJKLMN0987654321";
  static unsigned char cipherProcessRule[8]="CUSP    ";
  static unsigned char keyForm[4]="OP  ";
  static unsigned char keyLength[8]="SINGLE  ";
  static unsigned char dataKeyType[8]="DATA    ";
  static unsigned char nullKeyType[8]="        ";
  static unsigned char ICV[8]={0};
  static unsigned char pad[1]={0};
  static int exitDataLength = 0;
  static unsigned char exitData[4]={0};
  static int ruleArrayCount = 1;

  /*-----------------------------------------------------------------*
   * Variable inputs/outputs for ICSF services           *
   *-----------------------------------------------------------------*/
  unsigned char cipherText[24]={0};
  unsigned char compareText[24]={0};
  unsigned char dataKeyId[64]={0};
  unsigned char nullKeyId[64]={0};
  unsigned char dummyKEKKeyId1[64]={0};
  unsigned char dummyKEKKeyId2[64]={0};
  int returnCode = 0;
```

© Copyright IBM Corp. 1997, 2000

```
int reasonCode = 0;
unsigned char OCV[18]={0};

/*-----------------------------------------------------------------*
 * Begin executable code                                           *
 *-----------------------------------------------------------------*/
do {
  /*---------------------------------------------------------------*
   * Call key generate                                             *
   *---------------------------------------------------------------*/
  if ((returnCode = CSNBKGN(&returnCode,
                            &reasonCode,
                            &exitDataLength,
                            exitData,
                            keyForm,
                            &keyLength,
                            dataKeyType,
                            nullKeyType,
                            dummyKEKKeyId1,
                            dummyKEKKeyId2,
                            dataKeyId,
                            nullKeyId)) != 0) {
    printf("\nKey Generate failed:\;n");
    printf("   Return Code = %04d\n",returnCode);
    printf("   Reason Code = %04d\n",reasonCode);
    break;
    }
 /*----------------------------------------------------------------*
  * Call encipher                                                  *
  *----------------------------------------------------------------*/
 printf("\nClear Text\n");
 printHex(clearText,sizeof(clearText));

 if ((returnCode = CSNBENC(&returnCode,
                           &reasonCode,
                           &exitDataLength,
                           exitData,
                           dataKeyId,
                           &textLen,
                           clearText,
                           ICV,
                           &ruleArrayCount,
                           cipherProcessRule,
                           pad,
                           OCV,
                           cipherText)) != 0) {
   printf("\nReturn from Encipher:\n");
   printf("   Return Code = %04d\n",returnCode);
   printf("   Reason Code = %04d\n",reasonCode);
   if (returnCode > 4)
     break;
   }

 /*----------------------------------------------------------------*
  * Call decipher                                                  *
  *----------------------------------------------------------------*/
 printf("\nCipher Text\n");
 printHex(cipherText,sizeof(cipherText));

 if ((returnCode = CSNBDEC(&returnCode,
                           &reasonCode,
                           &exitDataLength,
                           exitData,
                           dataKeyId,
                           &textLen,
                           cipherText,
                           ICV,
                             &ruleArrayCount,
                             cipherProcessRule,
                             OCV,
                             compareText)) != 0) {
     printf("\nReturn from Decipher:\n");
     printf("   Return Code = %04d\n",returnCode);
     printf("   Reason Code = %04d\n",reasonCode);
     if (returnCode > 4)
       break;
     }

   /*-----------------------------------------------------------------*
    * End                                                             *
    *-----------------------------------------------------------------*/
   printf("\nClear Text after decipher\n");
   printHex(compareText,sizeof(compareText));

   } while(0);

   return returnCode;

} /* end main */

void printHex (unsigned char * text, unsigned int len)
/*--------------------------------------------------------------------*
 * Prints a string as hex characters                                  *
 *--------------------------------------------------------------------*/

{
  unsigned int i;

  for (i = 0; i < len; ++i)
    if ( ((i & 7) == 7) || (i == (len - 1)) )
      printf ("  %02x\n", text&[i]);
    else
      printf ("  %02x", text[i]);
  printf ("\n");
} /* end printHex */
```

COBOL

```
      **************************
       IDENTIFICATION DIVISION.
      ***************************
       PROGRAM-ID. COBOLXMP.
      *****************************
       ENVIRONMENT DIVISION.
      *****************************************************************
       CONFIGURATION SECTION.
       SOURCE-COMPUTER.  IBM-370.
       OBJECT-COMPUTER.  IBM-370.
      *****************************
       DATA DIVISION.
      *****************************************************************
       FILE SECTION.
       WORKING-STORAGE SECTION.
       77  INPUT-TEXT                   PIC       X(24)
           VALUE 'ABCDEFGHIJKLMN0987654321'.
       77  OUTPUT-TEXT                  PIC       X(24)
           VALUE LOW-VALUES.
       77  COMPARE-TEXT                 PIC       X(24)
           VALUE LOW-VALUES.
       77  CIPHER-PROCESSING-RULE       PIC       X(08)
           VALUE 'CUSP    '.
       77  KEY-FORM                     PIC       X(08)
           VALUE 'OP      '.
```

```
 77  KEY-LENGTH                    PIC       X(08)
     VALUE 'SINGLE  '.
 77  KEY-TYPE-1                    PIC       X(08)
     VALUE 'DATA    '.
 77  KEY-TYPE-2                    PIC       X(08)
     VALUE '        '.
 77  ICV                           PIC       X(08)
     VALUE LOW-VALUES.
 77  PAD                           PIC       X(01)
     VALUE LOW-VALUES.
************* DEFINE SAPI INPUT/OUTPUT PARAMETERS ************
 01  SAPI-REC.
     05  RETURN-CODE-S             PIC       9(08) COMP.
     05  REASON-CODE-S             PIC       9(08) COMP.
     05  EXIT-DATA-LENGTH-S        PIC       9(08) COMP.
     05  EXIT-DATA-S               PIC       X(04).
     05  KEK-KEY-ID-1-S            PIC       X(64)
         VALUE LOW-VALUES.
     05  KEK-KEY-ID-2-S            PIC       X(64)
         VALUE LOW-VALUES.
     05  DATA-KEY-ID-S             PIC       X(64)
         VALUE LOW-VALUES.
     05  NULL-KEY-ID-S             PIC       X(64)
         VALUE LOW-VALUES.
     05  KEY-FORM-S                PIC       X(08).
     05  KEY-LENGTH-S              PIC       X(08).
     05  DATA-KEY-TYPE-S           PIC       X(08).
     05  NULL-KEY-TYPE-S           PIC       X(08).
     05  TEXT-LENGTH-S             PIC       9(08) COMP.
     05  TEXT-S                    PIC       X(24).
     05  ICV-S                     PIC       X(08).
     05  PAD-S                     PIC       X(01).
     05  CPHR-TEXT-S               PIC       X(24).
     05  COMP-TEXT-S               PIC       X(24).
     05  RULE-ARRAY-COUNT-S        PIC       9(08) COMP.
     05  RULE-ARRAY-S.
         10  RULE-ARRAY            PIC       X(08).
     05  CHAINING-VECTOR-S         PIC       X(18).
*****************************************************************
 PROCEDURE DIVISION.
*****************************************************************
 MAIN-RTN.
*************  CALL KEY GENERATE  ***************************
     MOVE 0              TO   EXIT-DATA-LENGTH-S.
     MOVE KEY-FORM       TO   KEY-FORM-S.
     MOVE KEY-LENGTH     TO   KEY-LENGTH-S.
     MOVE KEY-TYPE-1     TO   DATA-KEY-TYPE-S.
     MOVE KEY-TYPE-2     TO   NULL-KEY-TYPE-S.
     CALL 'CSFKGN'   USING RETURN-CODE-S
                             REASON-CODE-S
                             EXIT-DATA-LENGTH-S
                             EXIT-DATA-S
                             KEY-FORM-S
                             KEY-LENGTH-S
                             DATA-KEY-TYPE-S
                             NULL-KEY-TYPE-S
                             KEK-KEY-ID-1-S
                             KEK-KEY-ID-2-S
                             DATA-KEY-ID-S
                             NULL-KEY-ID-S.
     IF RETURN-CODE-S NOT = 0 OR
        REASON-CODE-S NOT = 0 THEN
        DISPLAY '*** KEY-GENERATE ***'
        DISPLAY '*** RETURN-CODE = ' RETURN-CODE-S
        DISPLAY '*** REASON-CODE = ' REASON-CODE-S
     ELSE
        MOVE 24                 TO  TEXT-LENGTH-S
```

```
            MOVE INPUT-TEXT          TO  TEXT-S
            MOVE 1                   TO  RULE-ARRAY-COUNT-S
            MOVE CIPHER-PROCESSING-RULE TO RULE-ARRAY-S
            MOVE LOW-VALUES          TO  CHAINING-VECTOR-S
            MOVE ICV             TO   ICV-S.
            MOVE PAD             TO   PAD-S.
    *************  CALL ENCIPHER ***********************************
            CALL 'CSFENC' USING    RETURN-CODE-S
                                     REASON-CODE-S
                                     EXIT-DATA-LENGTH-S
                                     EXIT-DATA-S
                                     DATA-KEY-ID-S
                                     TEXT-LENGTH-S
                                     TEXT-S
                                     ICV-S
                                     RULE-ARRAY-COUNT-S
                                     RULE-ARRAY-S
                                     PAD-S
                                     CHAINING-VECTOR-S
                                     CPHR-TEXT-S
            IF RETURN-CODE-S NOT = 0 OR
               REASON-CODE-S NOT = 0 THEN
               DISPLAY '*** ENCIPHER ***'
               DISPLAY '*** RETURN-CODE = ' RETURN-CODE-S
               DISPLAY '*** REASON-CODE = ' REASON-CODE-S
            ELSE
    *************  CALL DECIPHER ***********************************
               CALL 'CSFDEC' USING RETURN-CODE-S
                                     REASON-CODE-S
                                     EXIT-DATA-LENGTH-S
                                     EXIT-DATA-S
                                     DATA-KEY-ID-S
                                     TEXT-LENGTH-S
                                     CPHR-TEXT-S
                                     ICV-S
                                     RULE-ARRAY-COUNT-S
                                     RULE-ARRAY-S
                                     CHAINING-VECTOR-S
                                     COMP-TEXT-S
               IF RETURN-CODE-S  NOT = 0 OR
                  REASON-CODE-S  NOT = 0 THEN
                  DISPLAY '*** DECIPHER ***'
                  DISPLAY '*** RETURN-CODE = ' RETURN-CODE-S
                  DISPLAY '*** REASON-CODE = ' REASON-CODE-S
                ELSE
                  IF COMP-TEXT-S = TEXT-S THEN
                    DISPLAY '*** DECIPHERED TEXT = PLAIN TEXT ***'
                  ELSE
                    DISPLAY '*** DECIPHERED TEXT ê= PLAIN TEXT ***'.
         DISPLAY '*** TEST PROGRAM ENDED ***'
         STOP RUN.
```

Assembler H

```
         TITLE 'SAMPLE ENCIPHER/DECIPHER S/370 PROGRAM.'
*======================================================================*
*       SYSTEM/370 ASSEMBLER H EXAMPLE                                 *
*                                                                      *
*======================================================================*
         SPACE
SAMPLE   START 0
         DS    0H
         STM   14,12,12(13)      SAVE REGISTERS
         BALR  12,0              USE R12 AS BASE REGISTER
         USING *,12              PROVIDE SAVE AREA FOR SUBROUTINE
         LA    14,SAVE           PERFORM SAVE AREA CHAINING
         ST    13,4(14)            "
         ST    14,8(13)            "
         LR    13,14               "
*
         CALL  CSFKGN,(RETCD,                                          *
               RESCD,                                                  *
               EXDATAL,                                                *
               EXDATA,                                                 *
               KEY_FORM,                                               *
               KEY_LEN,                                                *
               KEYTYP1,                                                *
               KEYTYP2,                                                *
               KEK_ID1,                                                *
               KEK_ID2,                                                *
               DATA_ID,                                                *
               NULL_ID)
         CLC   RETCD,=F'0'      CHECK RETURN CODE
         BNE   BACK             OUTPUT RETURN/REASON CODE AND STOP
         CLC   RESCD,=F'0'      CHECK REASON CODE
         BNE   BACK             OUTPUT RETURN/REASON CODE AND STOP
*
* CALL ENCIPHER WITH THE KEY JUST GENERATED
*  OPERATIONAL FORM
*
         MVC   RULEAC,=F'1'           SET RULE ARRAY COUNT
         MVC   RULEA,=CL8'CUSP    '   BUILD RULE ARRAY
         CALL CSFENC,(RETCD,                                           *
               RESCD,                                                  *
               EXDATAL,                                                *
               EXDATA,                                                 *
               DATA_ID,                                                *
               TEXTL,                                                  *
               TEXT,                                                   *
               ICV,                                                    *
               RULEAC,                                                 *
               RULEA,                                                  *
               PAD_CHAR,                                               *
               OCV,                                                    *
               CIPHER_TEXT)
         CLC   RETCD,=F'0'      CHECK RETURN CODE
         BNE   BACK             OUTPUT RETURN/REASON CODE AND STOP
         CLC   RESCD,=F'0'      CHECK REASON CODE
         BNE   BACK             OUTPUT RETURN/REASON CODE AND STOP
         CALL CSFDEC,(RETCD,                                           *
               RESCD,                                                  *
               EXDATAL,                                                *
               EXDATA,                                                 *
               DATA_ID,                                                *
               TEXTL,                                                  *
               CIPHER_TEXT,                                            *
               ICV,                                                    *
               RULEAC,                                                 *
               RULEA,                                                  *
               OCV,                                                    *
               NEW_TEXT)
         CLC   RETCD,=F'0'      CHECK RETURN CODE
         BNE   BACK             OUTPUT RETURN/REASON CODE AND STOP
         CLC   RESCD,=F'0'      CHECK REASON CODE
         BNE   BACK             OUTPUT RETURN/REASON CODE AND STOP
*
COMPARE  EQU   *                      COMPARE START AND END TEXT
         CLC   TEXT,NEW_TEXT
         BE    GOODENC
         WTO   'DECIPHERED TEXT DOES NOT MATCH STARTING TEXT'
         B      BACK
GOODENC  WTO   'DECIPHERED TEXT MATCHES STARTING TEXT'
*
*
```

```
         WTO   'TEST PROGRAM TERMINATING'
         B     RETURN
*
*--------------------------------------------------
* CONVERT RETURN/REASON CODES FROM BINARY TO EBCDIC
*--------------------------------------------------
BACK     DS    0F                 OUTPUT RETURN & REASON CODE
         L     5,RETCD            LOAD RETURN CODE
         L     6,RESCD            LOAD REASON CODE
         CVD   5,BCD1             CONVERT TO PACK-DECIMAL
         CVD   6,BCD2
         UNPK  ORETCD,BCD1        CONVERT TO EBCDIC
         UNPK  ORESCD,BCD2
         OI    ORETCD+7,X'F0'     CORRECT LAST DIGIT
         OI    ORESCD+7,X'F0'
*
         MVC   ERROUT+21(4),ORETCD
         MVC   ERROUT+41(4),ORESCD
ERROUT   WTO   'ERROR CODE =     , REASON CODE =     '
RETURN   EQU   *
         L     13,4(13)           SAVE AREA RESTORATION
         MVC   16(4,13),RETCD     SAVE RETURN CODE
         LM    14,12,12(13)
         BR    14                 RETURN TO CALLER
*
BCD1     DS    D                  CONVERT TO BCD TEMP AREA
BCD2     DS    D                  CONVERT TO BCD TEMP AREA
ORETCD   DS    CL8'0'             OUTPUT RETURN CODE
ORESCD   DS    CL8'0'             OUTPUT REASON CODE
*
KEY_FORM DC    CL8'OP      '      KEY FORM
KEY_LEN  DC    CL8'SINGLE  '      KEY LENGTH
KEYTYP1  DC    CL8'DATA    '      KEY TYPE 1
KEYTYP2  DC    CL8'        '      KEY TYPE 2
TEXT     DC    C'ABCDEFGHIJKLMNOPQRSTUV0987654321'
TEXTL    DC    F'32'              TEXT LENGTH
CIPHER_TEXT DC CL32' '
NEW_TEXT DC    CL32' '
DATA_ID  DC    XL64'00'           DATA KEY TOKEN
NULL_ID  DC    XL64'00'           NULL KEY TOKEN - UNFILLED
KEK_ID1  DC    XL64'00'           KEK1 KEY TOKEN
KEK_ID2  DC    XL64'00'           KEK2 KEY TOKEN
RETCD    DS    F'0'               RETURN CODE
RESCD    DS    F'0'               REASON CODE
EXDATAL  DC    F'0'               EXIT DATA LENGTH
EXDATA   DS    0C                 EXIT DATA
RULEA    DS    1CL8               RULE ARRAY
RULEAC   DS    F'0'               RULE ARRAY COUNT
ICV      DC    XL8'00'            INITIAL CHAINING VECTOR
OCV      DC    XL18'00'           OUTPUT CHAINING VECTOR
PAD_CHAR DC    F'0'               PAD CHARACTER
SAVE     DS    18F                SAVE REGISTER AREA
         END   SAMPLE
```

PL/1

```
/*********************************************************************/
/*                                                                   */
/* Sample program to call the one-way hash service to generate      */
/* the SHA-1 hash of the input text and call digital signature      */
/* generate with an RSA key using the ISO 9796 text formatting. The */
/* RSA key token is built from supplied data and imported for the   */
/* signature generate service to use.                                */
/*                                                                   */
/*      INPUT:  TEXT          Message digest to be signed           */
/*                                                                   */
/*      OUTPUT: SIGNATURE_LENGTH  Length of the signature in bytes  */
/*                                Written to a dataset.             */
/*                                                                  */
/*              SIGNATURE     Signature for hash.  Written to a     */
/*                            dataset.                              */
/*                                                                  */
/********************************************************************/
DSIGEXP:PROCEDURE( TEXT ) OPTIONS( MAIN );

/* Declarations - Parameters                                        */

DCL TEXT             CHAR( 64 ) VARYING;

/* Declarations - API parameters                                    */

DCL CHAINING_VECTOR_LENGTH  FIXED BINARY( 31, 0 ) INIT( 128 );
DCL CHAINING_VECTOR         CHAR( 128 );
DCL DUMMY_KEK               CHAR( 64 );
DCL EXIT_DATA               CHAR( 4 );
DCL EXIT_LEN                FIXED BINARY( 31, 0 ) INIT( 0 );

DCL HASH                    CHAR( 20 );
DCL HASH_LENGTH             FIXED BINARY( 31, 0 ) INIT( 20 );

DCL INTERNAL_PKA_TOKEN      CHAR( 1024 );
DCL INTERNAL_PKA_TOKEN_LENGTH FIXED BINARY( 31, 0 );

DCL KEY_VALUE_STRUCTURE     CHAR(139)
                         INIT(( '02000040000300408000000000000000'X ||
                                '01AE28DA4606D885EB7E0340D6BAAC51'X ||
                                '991C0CD0EAE835AFD9CFF3CD7E7EA741'X ||
                                '41DADD24A6331BEDF41A6626522CCF15'X ||
                                '767D167D01A16F970100010252BDAD42'X ||
                                '52BDAD425A8C6045D41AFAF746BEBD5F'X ||
                                '085D574FCD9C07F0B38C2C45017C2A1A'X ||
                                'B919ED2551350A76606BFA6AF2F1609A'X ||
                                '00A0A48DD719A55E9CA801'X ));
DCL KEY_VALUE_LENGTH        FIXED BINARY( 31, 0 ) INIT( 139 );

DCL OWH_TEXT                CHAR( 64 );

DCL PKA_KEY_TOKEN           CHAR( 1024 );
DCL PKA_TOKEN_LENGTH        FIXED BINARY( 31, 0 );

DCL PRIVATE_NAME            CHAR( 64 ) INIT( 'PL1.EXAMPLE.FOR.APG' );
DCL PRIVATE_NAME_LENGTH     FIXED BINARY( 31, 0 ) INIT( 0 );

DCL RETURN_CODE             FIXED BINARY( 31, 0 ) INIT( 0 );
DCL REASON_CODE             FIXED BINARY( 31, 0 ) INIT( 0 );

DCL RESERVED_FIELD_LENGTH   FIXED BINARY( 31, 0 ) INIT( 0 );
DCL RESERVED_FIELD          CHAR( 1 );

DCL RULE_ARY_CNT_DSG        FIXED BINARY( 31, 0 ) INIT( 1 );
DCL RULE_ARY_CNT_PKB        FIXED BINARY( 31, 0 ) INIT( 1 );
DCL RULE_ARY_CNT_PKI        FIXED BINARY( 31, 0 ) INIT( 0 );
DCL RULE_ARY_CNT_OWH        FIXED BINARY( 31, 0 ) INIT( 2 );
DCL RULE_ARY_DSG            CHAR( 8 ) INIT( 'ISO-9796' );
DCL RULE_ARY_PKB            CHAR( 8 ) INIT( 'RSA-PRIV' );
DCL RULE_ARY_PKI            CHAR( 8 );
DCL RULE_ARY_OWH            CHAR( 16 ) INIT( 'SHA-1   ONLY    ' );

DCL SIGNATURE_LENGTH        FIXED BINARY( 31, 0 );
DCL SIGNATURE               CHAR( 128 );
DCL SIG_BIT_LENGTH          FIXED BINARY( 31, 0 );

DCL TEXT_LENGTH             FIXED BINARY( 31, 0 );
```

```
/* Declarations - Files and entry points                             */

DCL SYSPRINT  FILE OUTPUT;
DCL SIGOUT    FILE RECORD OUTPUT;

DCL CSNDPKB   ENTRY EXTERNAL OPTIONS( ASM, INTER );
DCL CSNDPKI   ENTRY EXTERNAL OPTIONS( ASM, INTER );
DCL CSNBOWH   ENTRY EXTERNAL OPTIONS( ASM, INTER );
DCL CSNDDSG   ENTRY EXTERNAL OPTIONS( ASM, INTER );

/* Declarations - Internal variables                                 */

DCL DSG_HEADER       CHAR( 32 )
                           INIT( '* DIGITAL SIGNATURE GENERATION *' );
DCL FILE_OUT_LINE    CHAR( 128 );
DCL OWH_HEADER       CHAR( 16 )
                           INIT( '* ONE WAY HASH *' );
DCL PKB_HEADER       CHAR( 16 )
                           INIT( '* PKA TOKEN BUILD *' );
DCL PKI_HEADER       CHAR( 16 )
                           INIT( '* PKA TOKEN IMPORT *' );
DCL RC_STRING        CHAR( 14 ) INIT( 'RETURN CODE = ' );
DCL RS_STRING        CHAR( 14 ) INIT( 'REASON CODE = ' );
DCL SIG_STRING       CHAR( 12 ) INIT( 'SIGNATURE = ' );
DCL SIG_LEN_STRING   CHAR( 26 ) INIT( 'SIGNATURE LENGTH(BYTES) = ' );

/* Declarations - Built-in functions                                 */

DCL (SUBSTR, LENGTH) BUILTIN;

/*******************************************************************/
/* Call one-way hash to get the SHA-1 hash of the text.            */
/*******************************************************************/
TEXT_LENGTH = LENGTH( TEXT );
OWH_TEXT = SUBSTR( TEXT, 1, TEXT_LENGTH );

CALL CSNBOWH( RETURN_CODE,
              REASON_CODE,
              EXIT_LEN,
              EXIT_DATA,
              RULE_ARY_CNT_OWH,
              RULE_ARY_OWH,
              TEXT_LENGTH,
              OWH_TEXT,
              CHAINING_VECTOR_LENGTH,
              CHAINING_VECTOR,
              HASH_LENGTH,
              HASH );

PUT SKIP LIST( OWH_HEADER );
PUT SKIP LIST( RC_STRING || RETURN_CODE );
PUT SKIP LIST( RS_STRING || REASON_CODE );

/*******************************************************************/
/* Create the PKA RSA private external token.                      */
/*******************************************************************/
IF RETURN_CODE = 0 THEN
  DO;

  PKA_TOKEN_LENGTH = 1024;

  CALL CSNDPKB( RETURN_CODE,
                REASON_CODE,
                EXIT_LEN,
                EXIT_DATA,
                RULE_ARY_CNT_PKB,
                RULE_ARY_PKB,
                  KEY_VALUE_LENGTH,
                  KEY_VALUE_STRUCTURE,
                  PRIVATE_NAME_LENGTH,
                  PRIVATE_NAME,
                  RESERVED_FIELD_LENGTH,
                  RESERVED_FIELD,
                  RESERVED_FIELD_LENGTH,
                  RESERVED_FIELD,
                  RESERVED_FIELD_LENGTH,
                  RESERVED_FIELD,
                  RESERVED_FIELD_LENGTH,
                  RESERVED_FIELD,
                  RESERVED_FIELD_LENGTH,
                  RESERVED_FIELD,
                  PKA_TOKEN_LENGTH,
                  PKA_KEY_TOKEN );

    PUT SKIP LIST( PKB_HEADER );
    PUT SKIP LIST( RC_STRING || RETURN_CODE );
    PUT SKIP LIST( RS_STRING || REASON_CODE );

    END;

  /*********************************************************************/
  /* Import the clear RSA private external token.                      */
  /*********************************************************************/
  IF RETURN_CODE = 0 THEN
    DO;

    INTERNAL_PKA_TOKEN_LENGTH = 1024;

    CALL CSNDPKI( RETURN_CODE,
                  REASON_CODE,
                  EXIT_LEN,
                  EXIT_DATA,
                  RULE_ARY_CNT_PKI,
                  RULE_ARY_PKI,
                  PKA_TOKEN_LENGTH,
                  PKA_KEY_TOKEN,
                  DUMMY_KEK,
                  INTERNAL_PKA_TOKEN_LENGTH,
                  INTERNAL_PKA_TOKEN );

    PUT SKIP LIST( PKI_HEADER );
    PUT SKIP LIST( RC_STRING || RETURN_CODE );
    PUT SKIP LIST( RS_STRING || REASON_CODE );

    END;
  /*********************************************************************/
  /* Call digital signature generate.                                  */
  /*********************************************************************/
  IF RETURN_CODE = 0 THEN
    DO;

    SIGNATURE_LENGTH = 128;

    CALL CSNDDSG( RETURN_CODE,
                  REASON_CODE,
                  EXIT_LEN,
                  EXIT_DATA,
                  RULE_ARY_CNT_DSG,
                  RULE_ARY_DSG,
                  INTERNAL_PKA_TOKEN_LENGTH,
                  INTERNAL_PKA_TOKEN,
                  HASH_LENGTH,
                  HASH,
                  SIGNATURE_LENGTH,
                SIG_BIT_LENGTH,
                SIGNATURE );

  PUT SKIP LIST( DSG_HEADER );
  PUT SKIP LIST( RC_STRING || RETURN_CODE );
  PUT SKIP LIST( RS_STRING || REASON_CODE );

  IF RETURN_CODE = 0 THEN
    DO;

    /*****************************************************************/
    /* Write the signature and its length to the output file.       */
    /*****************************************************************/
    FILE_OUT_LINE = SIG_LEN_STRING || SIGNATURE_LENGTH;
    WRITE FILE(SIGOUT) FROM( FILE_OUT_LINE );
    FILE_OUT_LINE = SIG_STRING || SIGNATURE;
    WRITE FILE(SIGOUT) FROM( FILE_OUT_LINE );
    END;

  END;

END DSIGEXP;
```

Appendix C. Cipher Processing Rules

The DES defines operations on 8-byte data strings. Although the fundamental concepts of ciphering (enciphering and deciphering) and data verification are simple, there are different approaches to processing data strings that are not a multiple of 8 bytes in length. These approaches are defined in various standards and IBM products.

CBC and ANSI X3.106

ANSI standard X3.106 defines four methods of operation for ciphering. One of these modes, cipher block chaining (CBC), defines the basic method for performing ciphering on multiple 8-byte data strings. A plaintext data string, which must be a multiple of 8 bytes, is processed as a series of 8-byte groups. The ciphered result from processing an 8-byte group is exclusive ORed with the next group of 8 input bytes. The last 8-byte ciphered result is defined as an output chaining vector (OCV). ICSF stores the output chaining vector value in the *chaining_vector* parameter.

An initial chaining vector is exclusive ORed with the first group of 8 input bytes.

In summary:

- An input chaining vector (ICV) is required.
- If the *text_length* is not an exact multiple of 8 bytes, the request fails.
- The plaintext is not padded, for example, the output text length is not increased.

ANSI X9.23 and IBM 4700

An enhancement to the basic cipher block chaining mode of ANSI X3.106 is defined so the data lengths that are not an exact multiple of 8 bytes can be processed. The ANSI X9.23 method *always* adds from 1 byte to 8 bytes to the plaintext before encipherment. The last added byte is the count of the added bytes and is in the range of X'01' to X'08'. The standard defines that the other added bytes, the pad characters, are random.

When ICSF enciphers the plaintext, the resulting ciphertext is always 1 to 8 bytes longer than the plaintext.

When ICSF deciphers the ciphertext, ICSF uses the last byte of the deciphered data as the number of bytes to be removed (the pad bytes and the count byte). The resulting plaintext is the same as the original plaintext.

The output chaining vector can be used as feedback with this method in the same way as with the X3.106 method.

In summary, for the ANSI X9.23 method:

- X9.23 processing requires the caller to supply an ICV.
- X9.23 encipher does not allow specification of a pad character.

The 4700 padding rule is similar to the X9.23 rule. The only difference is that in the X9.23 method, the padding character is not user-selected, but the padding string is selected by the encipher process.

© Copyright IBM Corp. 1997, 2000

Segmenting

The callable services can operate on large data objects. *Segmenting* is the process of dividing the function into more than one processing step. Your application can divide the process into multiple steps without changing the final outcome.

To provide segmenting capability, the MAC generation, MAC verification, and MDC generation callable services require an 18-byte system work area in the application address space that is provided as the chaining vector parameter to the callable service. The application program must not change the system work area.

Cipher Last-Block Rules

The DES defines cipher-block chaining as operating on multiples of 8 bytes. Various algorithms are used to process strings that are multiples of 8 bytes. The algorithms are generically named “last-block rules”. You select the supported last-block rules by using these keywords:
- X9.23
- IPS
- CUSP (also used with PCF)
- 4700-PAD

You specify which cipher last-block rule you want to use in the *rule_array* parameter of the callable service.

CUSP Considerations

If the length of the data to be enciphered is an exact multiple of 8 bytes, the ICV is exclusive ORed with the first 8-byte block of plaintext, and the resulting 8 bytes are passed to the DES with the specified key. The resulting 8-byte block of ciphertext is then exclusive ORed with the second 8-byte block of plaintext, and the value is enciphered. This process continues until the last 8-byte block of plaintext is to be enciphered. Because the length of this last block is exactly 8 bytes, the last block is processed in an identical manner to all the preceding blocks.

To produce the OCV, the last block of *ciphertext* is enciphered again (thus producing a double-enciphered block). The user can pass this value of the OCV as the ICV in his next encipher call to produce chaining between successive calls. The caller can alternatively pass the same ICV on every call to the callable service.

If the length of data to be enciphered is greater than 7 bytes, and is *not* an exact multiple of 8 bytes, the process is the same as that above, until the last partial block of 1 to 7 bytes is reached. To encipher the last short block, the previous 8-byte block of ciphertext is passed to the DES with the specified key. The first 1 to 7 bytes of this double-enciphered block has two uses. The first use is to exclusive OR this block with the last short block of plaintext to form the last short block of the ciphertext. The second use is to pass it back as the OCV. Thus, the OCV is the last complete 8-byte block of plaintext, doubly enciphered.

If the length of the data to be enciphered is less than 8 bytes, the ICV is enciphered under the specified key. The first 1 to 7 bytes of the enciphered ICV is exclusive ORed with the plaintext to form the ciphertext. The OCV is the enciphered ICV.

The Information Protection System (IPS)

The Information Protection System (IPS) offers two forms of chaining: block and record. Under record chaining, the OCV for each enciphered data string becomes the ICV for the next. Under block chaining, the same ICV is used for each encipherment.

Files that are enciphered directly with the ICSF encipher callable service cannot be properly deciphered using the IPS/CMS CIPHER command or the IPS/CMS subroutines. Both IPS/CMS CIPHER and AMS REPRO ENCIPHER write headers to their files that contain information (principally the ICV and chaining method) needed for decipherment. The encipher callable service does not generate these headers. Specialized techniques are described in IPS/CMS documentation to overcome some, if not all, of these limitations, depending on the chaining mode. As a rough test, you can attempt a decipherment with the CIPHER command HDWARN option, which causes CIPHER to continue processing even though the header is absent.

The encipher callable service returns an OCV used by IPS for record chaining. This allows cryptographic applications using ICSF to be compatible with IPS record chaining.

Record chaining provides a superior method of handling successive short blocks, and has better error recovery features when the caller passes successive short blocks.

The principle used by record chaining is that *the OCV is the last 8 bytes of ciphertext*. This is handled as follows:

- If the length of the data to be enciphered is an exact multiple of 8 bytes, the ICV is exclusive ORed with the first 8 byte block of plaintext, and the resulting 8 bytes are passed to the DES with the specified key. The resulting 8-byte block of ciphertext is then exclusive ORed with the second 8-byte block of plaintext, and the resulting value is enciphered. This process continues until the last 8-byte block of plaintext is to be enciphered. Because the length of this last block is exactly 8 bytes, the last block is processed in an identical manner to all the preceding blocks.

  The OCV is the last 8 bytes of ciphertext.

  The user can pass this value as the ICV in the next encipher call to produce chaining between successive calls.
- If the length of data to be enciphered is greater than 7 bytes, and is *not* an exact multiple of 8 bytes, the process is the same as that above, until the last partial block of 1 to 7 bytes is reached. To encipher the last short block, the previous 8-byte block of ciphertext is passed to the DES with the specified key. The first 1 to 7 bytes of this doubly enciphered block is then exclusive ORed with the last short block of plaintext to form the last short block of the ciphertext. The OCV is the last 8 bytes of ciphertext.
- If the length of the data to be enciphered is less than 8 bytes, then the ICV is enciphered under the specified key. The first 1 to 7 bytes of the enciphered ICV is exclusive ORed with the plaintext to form the ciphertext. The OCV is the rightmost 8 bytes of the plaintext ICV concatenated with the short block of ciphertext. For example:

```
ICV         = ABCDEFGH
ciphertext  = XYZ
OCV         = DEFGHXYZ
```

Appendix D. PIN Formats and Algorithms

This appendix describes the personal identification number (PIN) formats and algorithms.

For PIN calculation procedures, see *IBM Common Cryptographic Architecture: Cryptographic Application Programming Interface Reference*.

PIN Notation

This section describes various PIN block formats. The following notations describe the contents of PIN blocks:

P =	A 4-bit decimal digit that is one digit of the PIN value.
C =	A 4-bit hexadecimal control value. The valid values are X'0' and X'1'.
L =	A 4-bit hexadecimal value that specifies the number of PIN digits. The value ranges from 4 to 12, inclusive.
F =	A 4-bit field delimiter of value X'F'.
f =	A 4-bit delimiter filler that is either P or F, depending on the length of the PIN.
D =	A 4-bit decimal padding value. All pad digits in the PIN block have the same value.
X =	A 4-bit hexadecimal padding value. All pad digits in the PIN block have the same value.
x =	A 4-bit hexadecimal filler that is either P or X, depending on the length of the PIN.
R =	A 4-bit hexadecimal random digit. The sequence of R digits can each take a different value.
r =	A 4-bit random filler that is either P or R, depending on the length of the PIN.
Z =	A 4-bit hexadecimal zero (X'0').
z =	A 4-bit zero filler that is either P or Z, depending on the length of the PIN.
S =	A 4-bit hexadecimal digit that constitutes one digit of a sequence number.
A =	A 4-bit decimal digit that constitutes one digit of a user-specified constant.

PIN Block Formats

This section describes the PIN block formats and assigns a code to each format.

ANSI X9.8

This format is also named ISO format 0, VISA format 1, VISA format 4, and ECI format 1.

```
P1 = CLPPPPffffffffFF

     P2 = ZZZZAAAAAAAAAAAA

PIN Block = P1 XOR P2
```

```
where C = X'0'
      L = X'4' to X'C'
```

Programming Note: The rightmost 12 digits in P2 are the rightmost 12 digits of the account number for all formats except VISA format 4. For VISA format 4, the rightmost 12 digits in P2 are the leftmost 12 digits of the account number.

ISO Format 1

This format is also named ECI format 4.

```
   PIN Block = CLPPPPrrrrrrrrRR

where C = X'1'
      L = X'4' to X'C'
```

ISO Format 2

```
   PIN Block = CLPPPPrrrrrrrrRR

where C = X'2'
      L = X'4' to X'C'
```

VISA Format 2

```
   PIN Block = LPPPPzzDDDDDDDDD

where L = X'4' to X'6'
```

VISA Format 3

This format specifies that the PIN length can be 4-12 digits, inclusive. The PIN starts from the leftmost digit and ends by the delimiter (‘F’), and the remaining digits are padding digits.

An example of a 6-digit PIN:

```
   PIN Block = PPPPPPFXXXXXXXXX
```

IBM 4700 Encrypting PINPAD Format

This format uses the value X'F' as the delimiter for the PIN.

```
   PIN Block = LPPPPffffffffFSS

where L = X'4' to X'C'
```

IBM 3624 Format

This format requires the program to specify the delimiter, X, for determining the PIN length.

```
   PIN Block = PPPPxxxxxxxxXXXX
```

IBM 3621 Format

This format requires the program to specify the delimiter, X, for determining the PIN length.

```
   PIN Block = SSSSPPPPxxxxxxxx
```

ECI Format 2

This format defines the PIN to be 4 digits.

```
   PIN Block = PPPPRRRRRRRRRRRR
```

ECI Format 3

```
   PIN Block = LPPPPzzRRRRRRRRR
```

```
where L = X'4' to X'6'
```

PIN Extraction Rules

This section describes the PIN extraction rules for the Encrypted PIN verify and Encrypted PIN translate callable services.

Encrypted PIN Verify Callable Service

The service extracts the customer-entered PIN from the input PIN block according to the following rules:

- If the input PIN block format is ANSI X9.8, ISO format 0, VISA format 1, VISA format 4, ECI format 1, ISO format 1, ISO format 2, VISA format 2, IBM Encrypting PINPAD format, or ECI format 3, the service extracts the PIN according to the length specified in the PIN block.
- If the input PIN block format is VISA format 3, the specified delimiter (padding) determines the PIN length. The search starts at the leftmost digit in the PIN block. If the input PIN block format is 3624, the specification of a PIN extraction method for the 3624 is supported through rule array keywords. If no PIN extraction method is specified in the rule array, the specified delimiter (padding) determines the PIN length.
- If the input PIN block format is 3621, the specification of a PIN extraction method for the 3621 is supported through rule array keywords. If no PIN extraction method is specified in the rule array, the specified delimiter (padding) determines the PIN length.
- If the input PIN block format is ECI format 2, the PIN is the leftmost 4 digits.

For the VISA algorithm, if the extracted PIN length is less than 4, the services sets a reason code that indicates that verification failed. If the length is greater than or equal to 4, the service uses the leftmost 4 digits as the referenced PIN.

For the IBM German Banking Pool algorithm, if the extracted PIN length is not 4, the service sets a reason code that indicates that verification failed.

For the IBM 3624 algorithm, if the extracted PIN length is less than the PIN check length, the service sets a reason code that indicates that verification failed.

Clear PIN Generate Alternate Callable Service

The service extracts the customer-entered PIN from the input PIN block according to the following rules:

- This service supports the specification of a PIN extraction method for the 3624 and 3621 PIN block formats through the use of the rule_array keyword. *Rule_array* points to an array of one or two 8-byte elements. The first element in the rule array specifies the PIN calculation method. The second element in the rule array (if specified) indicates the PIN extraction method. Refer to the "Clear PIN Generate Alternate (CSNBCPA)" on page 186 for an explanation of PIN extraction method keywords.

Encrypted PIN Translate Callable Service

The service extracts the customer-entered PIN from the input PIN block according to the following rules:

- If the input PIN block format is ANSI X9.8, ISO format 0, VISA format 1, VISA format 4, ECI format 1, ISO format 1, ISO format 2, VISA format 2, IBM Encrypting PINPAD format, or ECI format 3, and if the specified PIN length is less than 4, the service sets a reason code to reject the operation. If the specified PIN length is greater than 12, the operation proceeds to normal completion with unpredictable contents in the output PIN block. Otherwise, the service extracts the PIN according to the specified length.
- If the input PIN block format is VISA format 3, the specified delimiter (padding) determines the PIN length. The search starts at the leftmost digit in the PIN block. If the input PIN block format is 3624, the specification of a PIN extraction method for the 3624 is supported through rule array keywords. If no PIN extraction method is specified in the rule array, the specified delimiter (padding) determines the PIN length.
- If the input PIN block format is 3621, the specification of a PIN extraction method for the 3621 is supported through rule array keywords. If no PIN extraction method is specified in the rule array, the specified delimiter (padding) determines the PIN length.
- If the input block format is ECI format 2, the PIN is always the leftmost 4 digits.

If the maximum PIN length allowed by the output PIN block is shorter than the extracted PIN, only the leftmost digits of the extracted PIN that form the allowable maximum length are placed in the output PIN block. The PIN length field in the output PIN block, it if exists, specifies the allowable maximum length.

IBM PIN Algorithms

This section describes the IBM PIN generation algorithms, IBM PIN offset generation algorithm, and IBM PIN verification algorithms.

3624 PIN Generation Algorithm

This algorithm generates a n-digit PIN based on an account-related data or person-related data, namely the validation data. The assigned PIN length parameter specifies the length of the generated PIN.

The algorithm requires the following input parameters:

- A 64-bit validation data
- A 64-bit decimalization table
- A 4-bit assigned PIN length
- A 128-bit PIN-generation key

The service uses the PIN generation key to encipher the validation data. Each digit of the enciphered validation data is replaced by the digit in the decimalization table whose displacement from the leftmost digit of the table is the same as the value of the digit of the enciphered validation data. The result is an intermediate PIN. The leftmost n digits of the intermediate PIN are the generated PIN, where n is specified by the assigned PIN length.

Figure 3 illustrates the 3624 PIN generation algorithm.

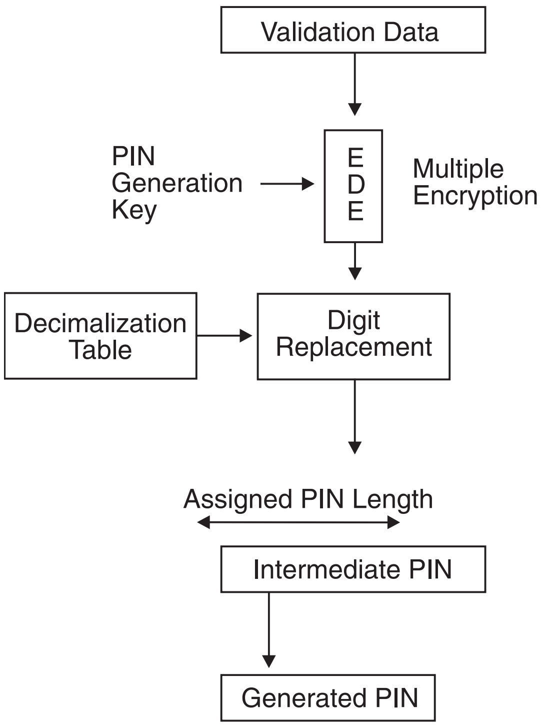


Figure 3. 3624 PIN Generation Algorithm

German Banking Pool PIN Generation Algorithm

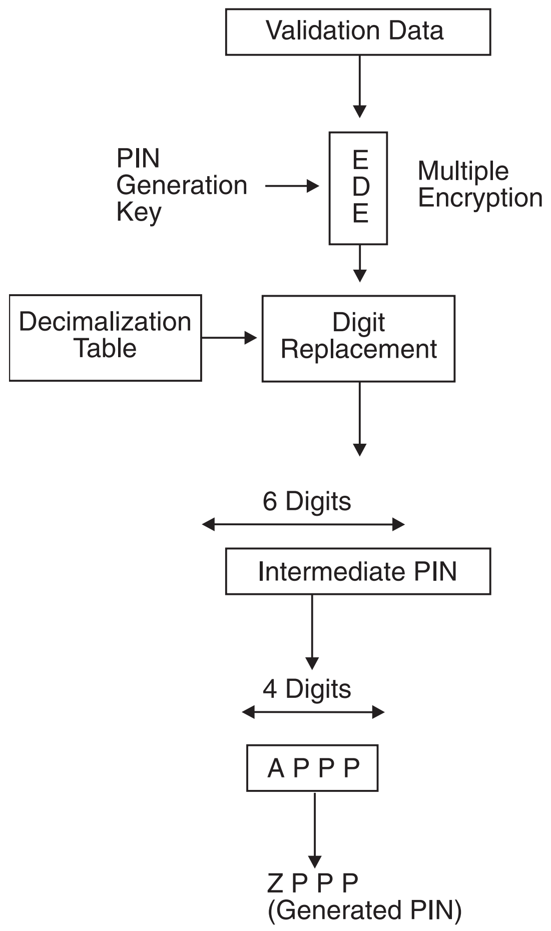
This algorithm generates a 4-digit PIN based on an account-related data or person-related data, namely the validation data.

The algorithm requires the following input parameters:

- A 64-bit validation data
- A 64-bit decimalization table
- A 128-bit PIN-generation key

The validation data is enciphered using the PIN generation key. Each digit of the enciphered validation data is replaced by the digit in the decimalization table whose displacement from the leftmost digit of the table is the same as the value of the digit of enciphered validation data. The result is an intermediate PIN. The rightmost 4 digits of the leftmost 6 digits of the intermediate PIN are extracted. The leftmost digit of the extracted 4 digits is checked for zero. If the digit is zero, the digit is changed to one; otherwise, the digit remains unchanged. The resulting four digits is the generated PIN.

Figure 4 illustrates the German Banking Pool (GBP) PIN generation algorithm.



If A = 0, then Z = 1; otherwise, Z = A.

Figure 4. GBP PIN Generation Algorithm

PIN Offset Generation Algorithm

To allow the customer to select his own PIN, a PIN offset is used by the IBM 3624 and GBP PIN generation algorithms to relate the customer-selected PIN to the generated PIN.

The PIN offset generation algorithm requires two parameters in addition to those used in the 3624 PIN generation algorithm. They are a customer-selected PIN and a 4-bit PIN check length. The length of the customer-selected PIN is equal to the assigned-PIN length, n.

The 3624 PIN generation algorithm described in the previous section is performed. The offset data value is the result of subtracting (modulo 10) the leftmost n digits of the intermediate PIN from the customer-selected PIN. The modulo 10 subtraction ignores borrows. The rightmost m digits of the offset data form the PIN offset, where m is specified by the PIN check length. Note that n cannot be less than m. To generate a PIN offset for a GBP PIN, m is set to 4 and n is set to 6.

Figure 5 illustrates the PIN offset generation algorithm.

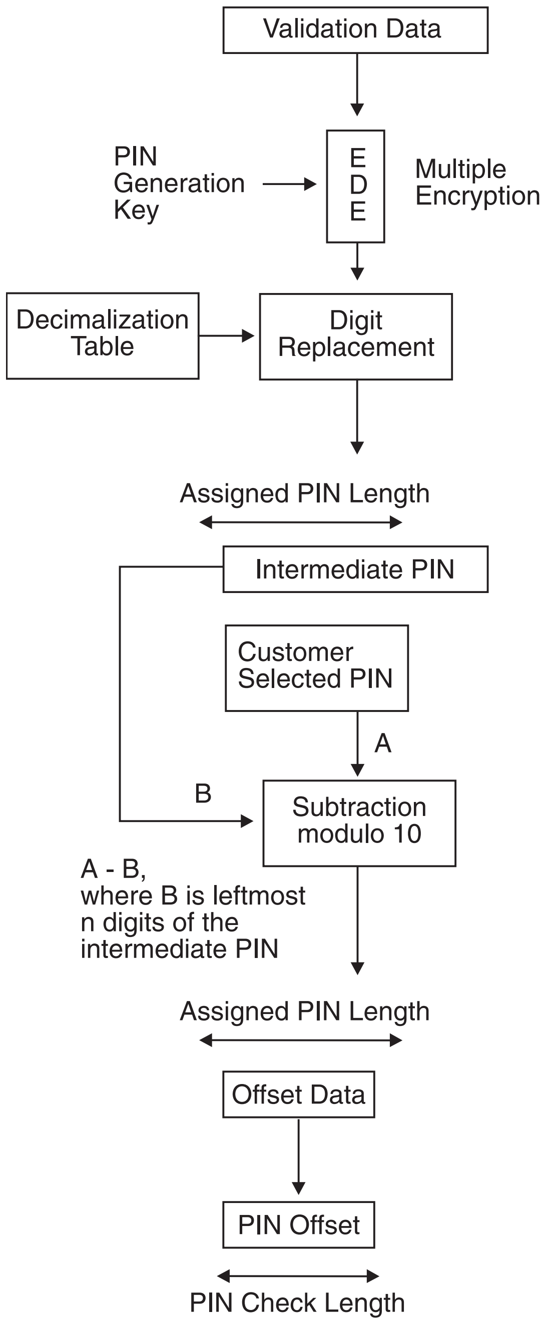


Figure 5. PIN-Offset Generation Algorithm

3624 PIN Verification Algorithm

This algorithm generates an intermediate PIN based on the specified validation data. A part of the intermediate PIN is adjusted by adding an offset data. A part of the result is compared with the corresponding part of the customer-entered PIN.

The algorithm requires the following input parameters:
- A 64-bit validation data
- A 64-bit decimalization table
- A 128-bit PIN-verification key

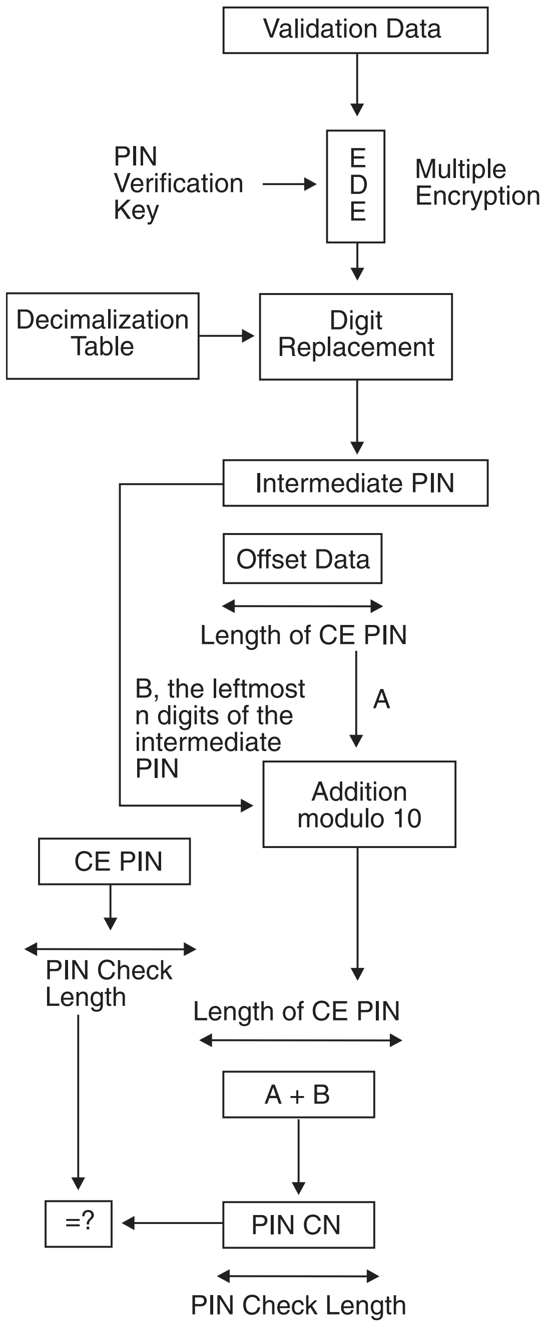
- A 4-bit PIN check length
- An offset data
- A customer-entered PIN

The rightmost m digits of the offset data form the PIN offset, where m is the PIN check length.

1. The validation data is enciphered using the PIN verification key. Each digit of the enciphered validation data is replaced by the digit in the decimalization table whose displacement from the leftmost digit of the table is the same as the value of the digit of enciphered validation data.
2. The leftmost n digits of the result is added (modulo 10) to the offset data value, where n is the length of the customer-entered PIN. The modulo 10 addition ignores carries.
3. The rightmost m digits of the result of the addition operation form the PIN check number. The PIN check number is compared with the rightmost m digits of the customer-entered PIN. If they match, PIN verification is successful; otherwise, verification is unsuccessful.

When a nonzero PIN offset is used, the length of the customer-entered PIN is equal to the assigned PIN length.

Figure 6 illustrates the PIN verification algorithm.



PIN CN: PIN Check Number
CE PIN: Customer-entered PIN

Figure 6. PIN Verification Algorithm

German Banking Pool PIN Verification Algorithm

This algorithm generates an intermediate PIN based on the specified validation data. A part of the intermediate PIN is adjusted by adding an offset data. A part of the result is extracted. The extracted value may or may not be modified before it compares with the customer-entered PIN.

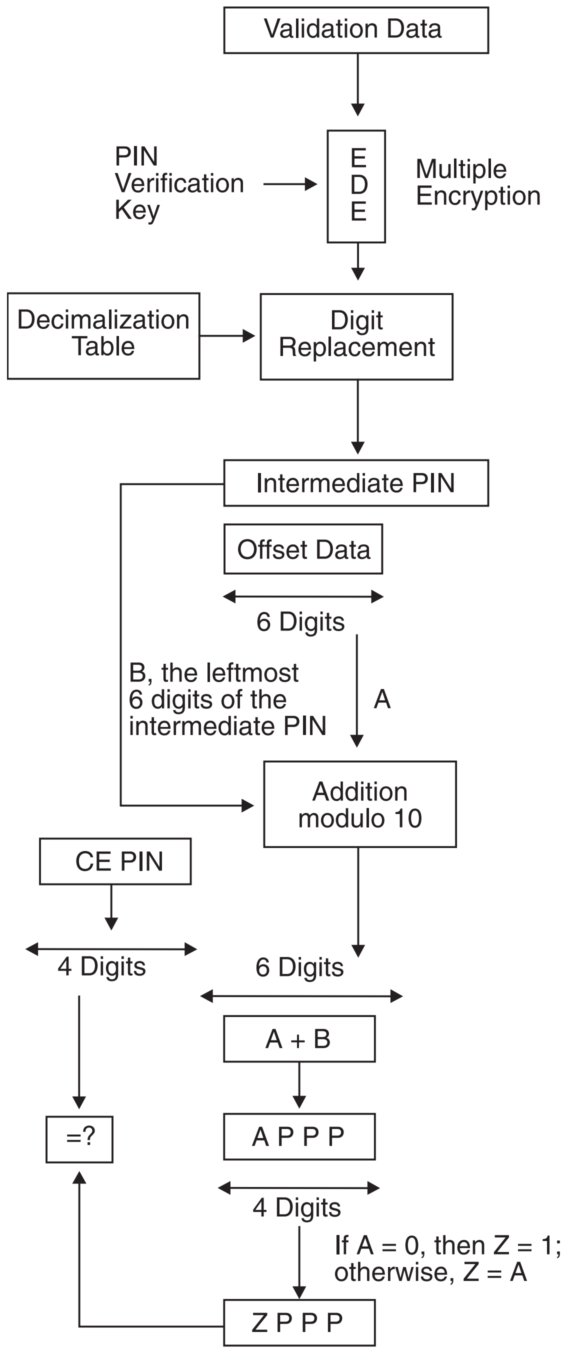
The algorithm requires the following input parameters:

- A 64-bit validation data
- A 64-bit decimalization table
- A 128-bit PIN verification key
- An offset data
- A customer-entered PIN

The rightmost 4 digits of the offset data form the PIN offset.

1. The validation data is enciphered using the PIN verification key. Each digit of the enciphered validation data is replaced by the digit in the decimalization table whose displacement from the leftmost digit of the table is the same as the value of the digit of enciphered validation data.
2. The leftmost 6 digits of the result is added (modulo 10) to the offset data. The modulo 10 addition ignores carries.
3. The rightmost 4 digits of the result of the addition (modulo 10) are extracted.
4. The leftmost digit of the extracted value is checked for zero. If the digit is zero, the digit is set to one; otherwise, the digit remains unchanged. The resulting four digits are compared with the customer-entered PIN. If they match, PIN verification is successful; otherwise, verification is unsuccessful.

Figure 7 illustrates the GBP PIN verification algorithm.



CE PIN: Customer-entered PIN

Figure 7. GBP PIN Verification Algorithm

VISA PIN Algorithms

The VISA PIN verification algorithm performs a multiple encipherment of a value, called the transformed security parameter (TSP), and a extraction of a 4-digit PIN verification value (PVV) from the ciphertext. The calculated PVV is compared with the referenced PVV and stored on the plastic card or data base. If they match, verification is successful.

PVV Generation Algorithm

The algorithm generates a 4-digit PIN verification value (PVV) based on the transformed security parameter (TSP).

The algorithm requires the following input parameters:

- A 64-bit TSP
- A 128-bit PVV generation key

1. A multiple encipherment of the TSP using the double-length PVV generation key is performed.
2. The ciphertext is scanned from left to right. Decimal digits are selected during the scan until four decimal digits are found. Each selected digit is placed from left to right according to the order of selection. If four decimal digits are found, those digits are the PVV.
3. If, at the end of the first scan, less than four decimal digits have been selected, a second scan is performed from left to right. During the second scan, all decimal digits are skipped and only nondecimal digits can be processed. Nondecimal digits are converted to decimal digits by subtracting 10. The process proceeds until four digits of PVV are found.

Figure 8 illustrates the PVV generation algorithm.

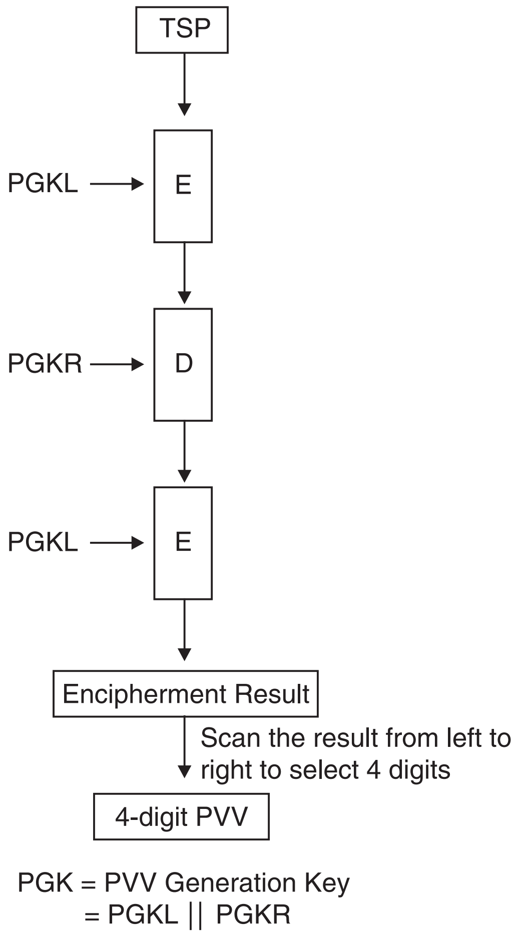


Figure 8. PVV Generation Algorithm

Programming Note: For VISA PVV algorithms, the leftmost 11 digits of the TSP are the personal account number (PAN), the leftmost 12th digit is a key table index to select the PVV generation key, and the rightmost 4 digits are the PIN. The key table index should have a value between 1 and 6, inclusive.

PVV Verification Algorithm

The algorithm requires the following input parameters:

- A 64-bit TSP
- A 16-bit referenced PVV
- A 128-bit PVV verification key

A PVV is generated using the PVV generation algorithm, except a PVV verification key rather than a PVV generation key is used. The generated PVV is compared with the referenced PVV. If they match, verification is successful.

Interbank PIN Generation Algorithm

The Interbank PIN calculation method consists of the following steps:

1. Let X denote the transaction_security parameter element converted to an array of 16 4-bit numeric values. This parameter consists of (in the following sequence) the 11 rightmost digits of the customer PAN (excluding the check digit), a constant of 6, a 1-digit key indicator, and a 3-digit validation field.

2. Encrypt X with the double-length PINGEN (or PINVER) key to get 16 hexadecimal digits (64 bits).
3. Perform decimalization on the result of the previous step by scanning the 16 hexadecimal digits from left to right, skipping any digit greater than X'9' until 4 decimal digits (for example, digits that have values from X'0' to X'9') are found.

   If all digits are scanned but 4 decimal digits are not found, repeat the scanning process, skipping all digits that are X'9' or less and selecting the digits that are greater than X'9'. Subtract 10 (X'A') from each digit selected in this scan.

   If the 4 digits that were found are all zeros, replace the 4 digits with 0100.
4. Concatenate and use the resulting digits for the Interbank PIN. The 4-digit PIN consists of the decimal digits in the sequence in which they are found.

Appendix E. Transform CDMF Key Algorithm

The CDMF key transformation algorithm uses a 64-bit cryptographic key.

1. Set parity bits of the key to zero by ANDing the key with X'FEFEFEFEFEFEFEFE' to produce Kx.
2. Using DES, encipher Kx under the constant K1.
3. XOR this value with Kx to produce Ky.
4. AND Ky with X'0EFE0EFE0EFE0EFE' to produce Kz.
5. Using DES, encipher Kz under K2 to produce eK2(Kz).
6. Adjust eK2(Kz) to odd parity in each byte. The result is the transformed key.

The following figure illustrates these steps. (e indicates DES encryption.)

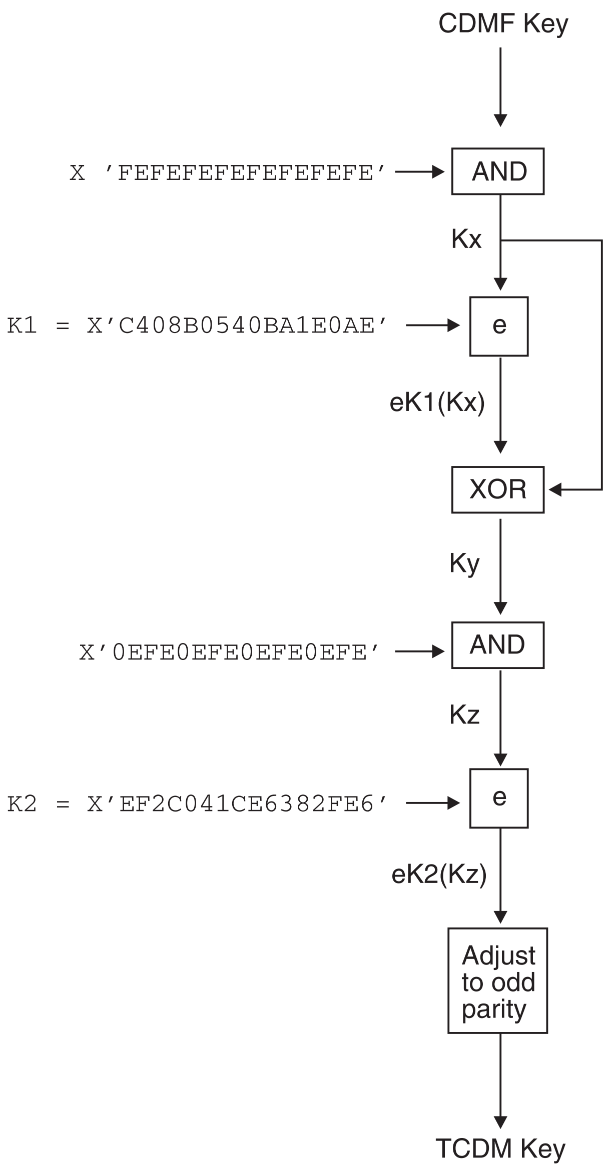


Figure 9. The CDMF Key Transformation Algorithm

Appendix F. Multiple Decipherment and Encipherment

This appendix explains multiple encipherment and decipherment and their equations.

The Integrated Cryptographic Feature uses multiple encipherment whenever it enciphers a key under a key-encrypting key like the master key or the transport key and in triple-DES encipherment for data privacy. Multiple encipherment is superior to single encipherment because multiple encipherment increases the work needed to “break” a key. ICSF provides extra protection for a key by enciphering it under an enciphering key multiple times rather than once. The multiple encipherment method for keys enciphered under a key-encrypting key uses a double-length (128 bit) key split into two 64-bit halves. Like single encipherment, multiple encipherment uses a DES based on the electronic code book (ECB) mode of encipherment.

Keys can either be double-length or single-length depending on the installation and their cryptographic function. When a single-length key is encrypted under a double-length key, multiple encipherment is performed on the key. In the multiple encipherment method, the key is encrypted under the left half of the enciphering key. The result is then decrypted under the right half of the enciphering key. Finally, this result is encrypted under the left half of the enciphering key again.

When a double-length key is encrypted with multiple encipherment, the method is similar, except ICSF uses two enciphering keys. One enciphering key encrypts each half of the double-length key. Double-length keys active on the system have two master key variants used when enciphering them.

Multiple encipherment and decipherment is not only used to protect or retrieve a cryptographic key, but they are also used to protect or retrieve 64-bit data in the area of PIN applications. For example, the following two sections use a double-length *KEK as an example to cipher a single-length key even though the same algorithms apply to cipher 64-bit data by a double-length PIN-related cryptographic key.

ICSF also supports triple-DES encipherment for data privacy using double-length and triple-length DATA keys. For this procedure the data is first enciphered using the first DATA key. The result is then deciphered using the second DATA key. This second result is then enciphered using the third DATA key when a triple-length key is provided, or reusing the first DATA key when a double-length key is provided.

Note that an asterisk (*) preceding the key means that the key is double-length. Notations in this chapter have the following meaning:
- eK(x), where x is enciphered under K
- dK(y) represents plaintext, where K is the key and y is the ciphertext

Therefore, dK(eK(x)) equals x for any 64-bit key K and any 64-bit plaintext x.

When a key (*K) to be protected is double-length, two double-length *KEKs are used. One *KEK is used for protecting the left half of the key (*K); another is for the right half. Multiple encipherment is used with the appropriate *KEK for protecting each half of the key.

Multiple Encipherment of Single-length Keys

The multiple encipherment of a single-length key (K) using a double-length *KEK is defined as follows:

```
e*KEK(K) = eKEKL(dKEKR(eKEKL(K)))
```

where KEKL is the left 64 bits of *KEK and KEKR is the right 64 bits of *KEK.

Figure 10 illustrates the definition.

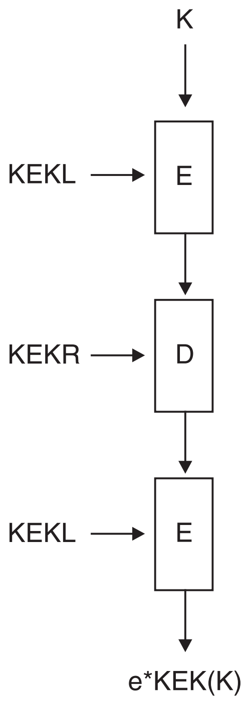


Figure 10. Multiple Encipherment of Single-length Keys

Multiple Decipherment of Single-length Keys

The multiple encipherment of an encrypted single-length key (Y = e*KEK(K)) using a double-length *KEK is defined as follows:

```
d*KEK(Y) = dKEKL(eKEKR(dKEKL(Y)))
         = d*KEK(e*KEK(K))
         = K
```

where KEKL is the left 64 bits of *KEK and KEKR is the right 64 bits of *KEK.

Figure 11 illustrates the definition.

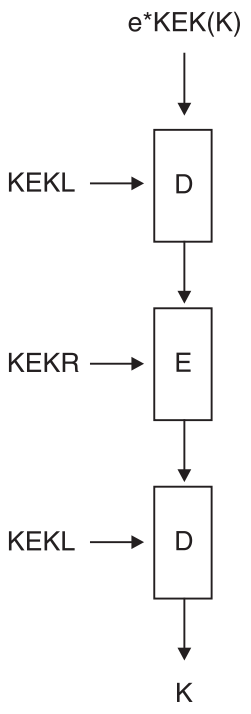


Figure 11. Multiple Decipherment of Single-length Keys

Multiple Encipherment of Double-length Keys

The multiple encipherment of a double-length key (*K) using two double-length *KEKs, *KEKa and *KEKb is defined as follows:

```
e*KEKa(KL) || e*KEKb(KR) =
              eKEKaL(dKEKaR(eKEKaL(KL))) ||
              eKEKbL(dKEKbR(eKEKbL(KR)))
```

where:
- KL is the left 64 bits of *K.
- KR is the right 64 bits of *K.
- KEKaL is the left 64 bits of *KEKa.
- KEKaR is the right 64 bits of *KEKa.
- KEKbL is the left 64 bits of *KEKb.
- KEKbR is the right 64 bits of *KEKb.
- ∥ means concatenation.

Figure 12 illustrates the definition.

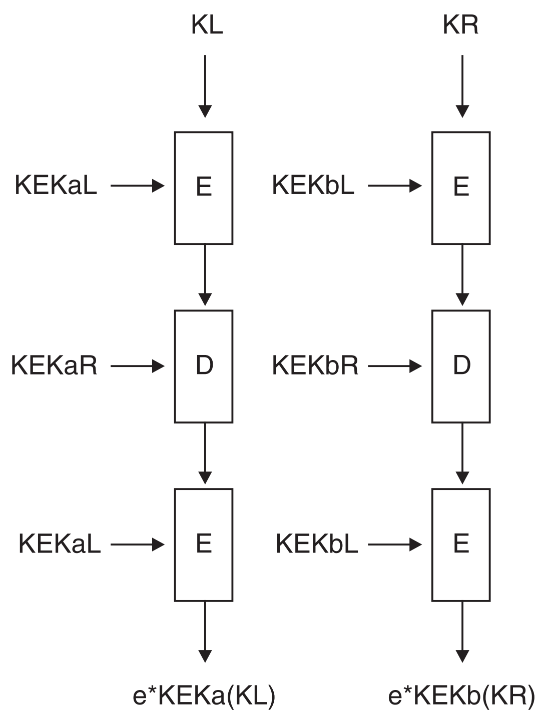


Figure 12. Multiple Encipherment of Double-length Keys

Multiple Decipherment of Double-length Keys

The multiple decipherment of an encrypted double-length key, *Y = e*KEKa(KL) || e*KEKb(KR), using two double-length *KEKs, *KEKa and *KEKb, is defined as follows:

```
D*KEKa(YL) || d*KEKb(YR)
        = dKEKaL(eKEKaR(dKEKaL(YL))) ||
          dKEKbL(eKEKbR(dKEKbL(YR)))
        = d*KEKa(e*KEKa(KL)) ||
          d*KEKb(e*KEKb(KR))
        = *K
```

where
- YL is the left 64 bits of *Y.
- YR is the right 64 bits of *Y.
- KEKaL is the left 64 bits of *KEKa.
- KEKaR is the right 64 bits of *KEKa.
- KEKbL is the left 64 bits of *KEKb.
- KEKbR is the right 64 bits of *KEKb.
- || means concatenation.

Figure 13 illustrates the definition.

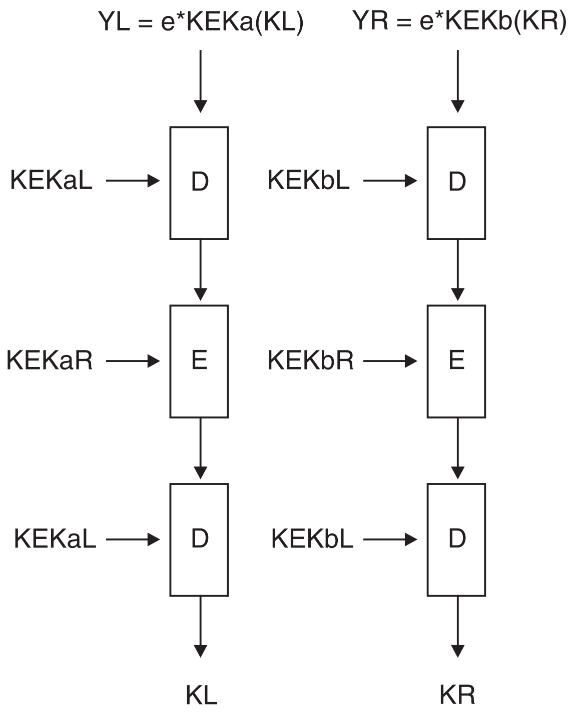


Figure 13. Multiple Decipherment of Double-length Keys

Multiple Encipherment of Triple-length Keys

The multiple encipherment of a triple-length key (**K) using two double-length *KEKs, *KEKa and *KEKb is defined as follows:

```
e*KEKa(KL) || e*KEKb(KM) || e*KEKa(KR) =
    eKEKaL(dKEKaR(eKEKaL(KL))) ||
    eKEKbL(dKEKbR(eKEKbL(KM))) ||
    eKEKaL(dKEKaR(eKEKaL(KR)))
```

where:

- KL is the left 64 bits of **K
- KM is the next 64 bits of **K
- KR is the right 64 bits of **K
- KEKaL is the left 64 bits of *KEKa
- KEKaR is the right 64 bits of *KEKa
- KEKbL is the left 64 bits of *KEKb
- KEKbR is the right 64 bits of *KEKb
- || means concatenation

Figure 14 on page 380 illustrates the definition.

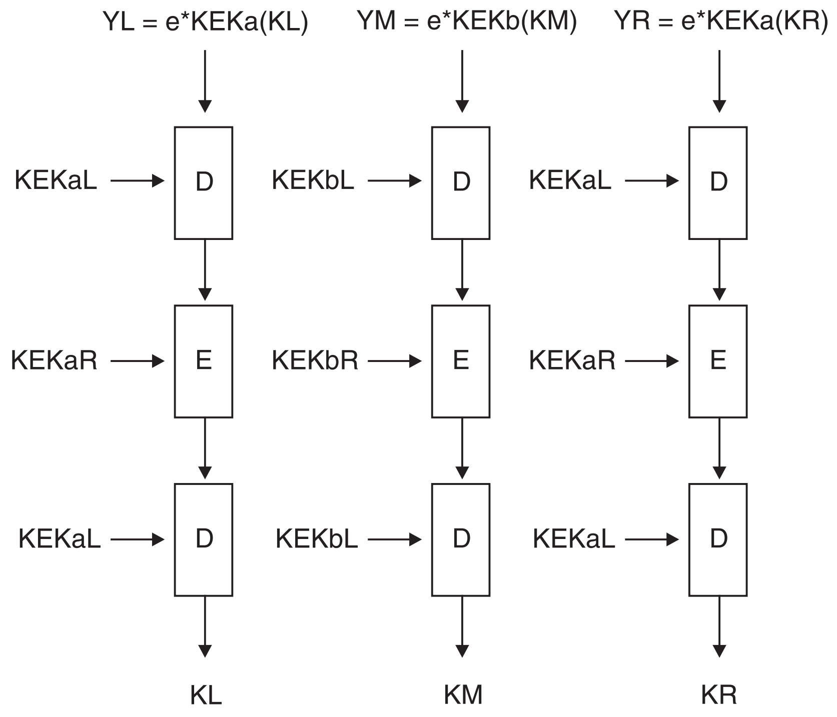


Figure 14. Multiple Encipherment of Triple-length Keys

Multiple Decipherment of Triple-length Keys

The multiple decipherment of an encrypted triple-length key **Y = e*KEKa(KL) || e*KEKb(KM) || e*KEKa(KR), using two double-length *KEKs, *KEKa and *KEKb, is defined as follows:

```
d*KEKa(YL) || d*KEKb(YM) || d*KEKa(YR)
   = dKEKaL(eKEKaR(dKEKaL(YL))) ||
     dKEKbL(eKEKbR(dKEKbL(YM))) ||
     dKEKaL(eKEKaR(dKEKaL(YR)))
   = d*KEKa(e*KEKa(KL)) ||
     d*KEKb(e*KEKb(KM)) ||
     d*KEKa(e*KEKa(KR))
   = **K
```

where:

- YL is the left 64 bits of **Y
- YM is the next 64 bits of **Y
- YR is the right 64 bits of **Y
- KEKaL is the left 64 bits of *KEKa
- KEKaR is the right 64 bits of *KEKa
- KEKbL is the left 64 bits of *KEKb
- KEKbR is the right 64 bits of *KEKb
- || means concatenation

Figure 15 on page 381 illustrates the definition.

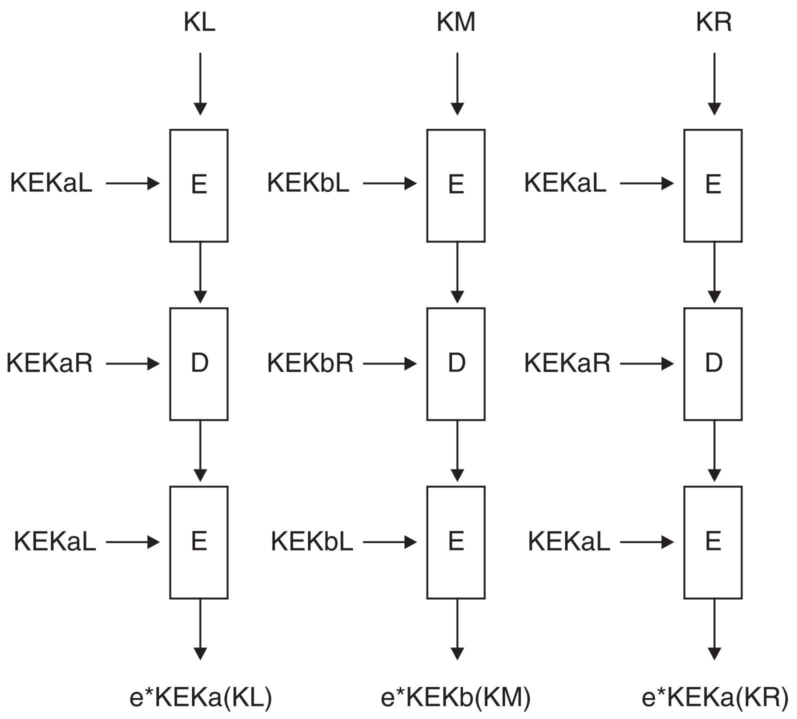


Figure 15. Multiple Decipherment of Triple-length Keys

Appendix G. ANSI X9.17 Partial Notarization Method

The ANSI X9.17 notarization process can be divided into two procedures:

1. *Partial notarization*, in which the ANSI key-encrypting key (AKEK) is cryptographically combined with the origin and destination identifiers.

   Note: IBM defines this step as partial notarization. The ANSI X9.17 standard does not use the term partial notarization.
2. *Offsetting*, in which the result of the first step is exclusive-ORed with a counter value. ICSF performs the offset procedure to complete the notarization process when you use a partially notarized AKEK.

This appendix describes partial notarization for the ANSI X9.17 notarization process.

Partial Notarization

Partial notarization improves performance when you use an AKEK for many cryptographic service messages, each with a different counter value.

This section describes the steps in partial notarization. For more information about partial notarization, see "ANSI X9.17 Key Management Services" on page 14. For a description of the steps ICSF uses to complete the notarization of an AKEK or to notarize a key in one process, see *ANSI X9.17 - 1985, Financial Institution Key Management (Wholesale)*.

Notations Used in the Calculations

***KK**	The 16-byte AKEK to be partially notarized
KKL	The leftmost 8 bytes of *KK
KKR	The rightmost 8 bytes of *KK
KK	The 8-byte AKEK to be partially notarized
KK1	An 8-byte intermediate result
KK2	An 8-byte intermediate result
FMID	The 16-byte origin identifier
FMID1	The leftmost 8 bytes of FMID
FMID2	The rightmost 8 bytes of FMID
TOID	The 16-byte destination identifier
TOID1	The leftmost 8 bytes of TOID
TOID2	The rightmost 8 bytes of TOID
NSL	An 8-byte intermediate result
NSL1	The leftmost 4 bytes of NSL
NSR	An 8-byte intermediate result
NSR2	The rightmost 4 bytes of NSR
***KKNI**	The 16-byte partially notarized AKEK
KKNIL	The leftmost 8 bytes of *KKNI
KKNIR	The rightmost 8 bytes of *KKNI

KKNI	The 8-byte partially notarized AKEK
XOR	Denotes the exclusive-OR operation
TOID1<<1	Denotes the ASCII TOID1 left-shifted one bit
FMID1<<1	Denotes the ASCII FMID1 left-shifted one bit
eK(X)	Denotes DES encryption of plaintext X using key K
‖	Denotes the concatenation operation

Partial Notarization Calculation for a Double-Length AKEK

For a double-length AKEK, the partial notarization calculation consists of the following steps:

1. Set KK1 = KKL XOR TOID1<<1
2. Set KK2 = KKR XOR FMID1<<1
3. Set NSL = eKK2(TOID2)
4. Set NSR = eKK1(FMID2)
5. Set KKNIL = KKL XOR NSL
6. Set KKNIR = KKR XOR NSR
7. Set *KKNI = KKNIL ‖ KKNIR

Partial Notarization Calculation for a Single-Length AKEK

For a single-length AKEK, the partial notarization calculation consists of the following steps:

1. Set KK1 = KK XOR TOID1<<1
2. Set KK2 = KK XOR FMID1<<1
3. Set NSL = eKK2(TOID2)
4. Set NSR = eKK1(FMID2)
5. Set NSL = NSL1 ‖ NSR2
6. Set KKNI = KK XOR NSL

Appendix H. Key Token Formats

For debugging purposes, this appendix provides the formats for DES internal, external, and null key tokens and for PKA key tokens.

Format of the DES Internal Key Token

Table 94 shows the format for a DES internal key token.

Table 94. Internal Key Token Format

Bytes	Description
0	X'01' (flag indicating this is an internal key token)
1–3	Implementation-dependent bytes (X'000000' for ICSF)
4	Key token version number (X'00' or X'01')
5	Reserved (X'00')
6	Flag byte **Bit** **Meaning When Set On** **0** Encrypted key and master key verification pattern (MKVP) are present. **1** Control vector (CV) value in this token has been applied to the key. **2** Key is used for no control vector (NOCV) processing. Valid for transport keys only. **3** Key is an ANSI key-encrypting key (AKEK). **4** AKEK is a double-length key (16 bytes). **Note:** When bit 3 is on and bit 4 is off, AKEK is a single-length key (8 bytes). **5** AKEK is partially notarized. **6** Key is an ANSI partial key. **7** Export prohibited.
7	Reserved (X'00')
8–15	Master key verification pattern (MKVP)
16–23	A single-length key, the left half of a double-length key, or Part A of a triple-length key. The value is encrypted under the master key.
24–31	X'0000000000000000' if a single-length key, or the right half of a double-length operational key, or Part B of a triple-length operational key. The right half of the double-length key or Part B of the triple-length key is encrypted under the master key.
32–39	The control vector (CV) for a single-length key or the left half of the control vector for a double-length key.
40–47	X'0000000000000000' if a single-length key or the right half of the control vector for a double-length operational key.
48–55	X'0000000000000000' if a single-length key or double-length key, or Part C of a triple-length operational key. Part C of a triple-length key is encrypted under the master key.
56-58	Reserved (X'000000')
59 bits 0 and 1	**B'10'** Indicates CDMF DATA or KEK. **B'00'** Indicates DES for DATA keys or the system default algorithm for a KEK. **B'01'** Indicates DES for a KEK.

Table 94. Internal Key Token Format (continued)

Bytes	Description
59 bits 2 and 3	**B'00'** Indicates single-length key (version 0 only). **B'01'** Indicates double-length key (version 1 only). **B'10'** Indicates triple-length key (version 1 only).
59 bits 4 –7	B'0000'
60–63	Token validation value (TVV).

Note: A key token stored in the CKDS will not have an MKVP or TVV. Before such a key token is used, the MKVP is copied from the CKDS header record and the TVV is calculated and placed in the token. See "Token Validation Value" for more information.

Token Validation Value

ICSF uses the *token validation value (TVV)* to verify that a token is valid. The TVV prevents a key token that is not valid or that is overlaid from being accepted by ICSF. It provides a checksum to detect a corruption in the key token.

When an ICSF callable service generates a key token, it generates a TVV and stores the TVV in bytes 60-63 of the key token. When an application program passes a key token to a callable service, ICSF checks the TVV. To generate the TVV, ICSF performs a twos complement ADD operation (ignoring carries and overflow) on the key token, operating on four bytes at a time, starting with bytes 0-3 and ending with bytes 56-59.

DES External Key Token

Table 95 on page 387 shows the format for a DES external key token.

Table 95. Format of External Key Tokens

Bytes	Description
0	X'02' (flag indicating an external key token)
1	Reserved (X'00')
2–3	Implementation-dependent bytes (X'0000' for ICSF)
4	Key token version number (X'00' or X'01')
5	Reserved (X'00')
6	Flag byte **Bit** **Meaning When Set On** **0** Encrypted key is present. **1** Control vector (CV) value has been applied to the key. Other bits are reserved and are binary zeros.
7	Reserved (X'00')
8–15	Reserved (X'0000000000000000')
16–23	Single-length key or left half of a double-length key, or Part A of a triple-length key. The value is encrypted under a transport key.
24–31	X'0000000000000000' if a single-length key or right half of a double-length key, or Part B of a triple-length key. The right half of a double-length key or Part B of a triple-length key is encrypted under a transport (key-encrypting key) for export or import.
32–39	Control vector (CV) for single-length key or left half of CV for double-length key
40–47	X'0000000000000000' if single-length key or right half of CV for double-length key
48–55	X'0000000000000000' if a single-length key, double-length key, or Part C of a triple-length key.
56–58	Reserved (X'000000')
59 bits 0 and 1	B'00'
59 bits 2 and 3	**B'00'** Indicates single-length key (version 0 only). **B'01'** Indicates double-length key (version 1 only). **B'10'** Indicates triple-length key (version 1 only).
59 bits 4–7	B'0000'
60-63	Token validation value (see “Token Validation Value” on page 386 for a description).

DES Null Key Token

Table 96 on page 388 shows the format for a DES null key token.

Table 96. Format of Null Key Tokens

Bytes	Description
0	X'00' (flag indicating this is a null key token).
1–15	Reserved (set to binary zeros).
16–23	Single-length encrypted key, or left half of double-length encrypted key, or Part A of triple-length encrypted key.
24–31	X'0000000000000000' if a single-length encrypted key, the right half of double-length encrypted key, or Part B of triple-length encrypted key.
32–39	X'0000000000000000' if a single-length encrypted key or double-length encrypted key.
40–47	Reserved (set to binary zeros).
48–55	Part C of a triple-length encrypted key.
56–63	Reserved (set to binary zeros).

Format of the RSA Public Key Token

An RSA public key token contains the following sections:

- A required token header, starting with the token identifier X'1E'
- A required RSA public key section, starting with the section identifier X'04'

Table 97 presents the format of an RSA public key token. All length fields are in binary. All binary fields (exponents, lengths, and so on) are stored with the high-order byte first (left, low-address, S/390 format).

Table 97. RSA Public Key Token

Offset (Dec)	Number of Bytes	Description
Token Header (required)		
000	001	Token identifier. X'1E' indicates an external token.
001	001	Version, X'00'.
002	002	Length of the key token structure.
004	004	Ignored. Should be zero.
RSA Public Key Section (required)		
000	001	X'04', section identifier, RSA public key.
001	001	X'00', version.
002	002	Section length, 12+xxx+yyy.
004	002	Reserved field.
006	002	RSA public key exponent field length in bytes, “xxx”.
008	002	Public key modulus length in bits.
010	002	RSA public key modulus field length in bytes, “yyy”.
012	xxx	Public key exponent (this is generally a 1-, 3-, or 64- to 256-byte quantity), e. e must be odd and 1<e<n. (Frequently, the value of e is 2.) ^{16}+1
12+xxx	yyy	Modulus, n.

Format of the DSS Public Key Token

A DSS public key token contains the following sections:

- A required token header, starting with the token identifier X'1E'
- A required DSS public key section, starting with the section identifier X'03'

Table 98 presents the format of a DSS public key token. All length fields are in binary. All binary fields (exponents, lengths, and so on) are stored with the high-order byte first (left, low-address, S/390 format).

Table 98. DSS Public Key Token

Offset (Dec)	Number of Bytes	Description
Token Header (required)		
000	001	Token identifier. X'1E' indicates an external token.
001	001	Version, X'00'.
002	002	Length of the key token structure.
004	004	Ignored. Should be zero.
DSS Public Key Section (required)		
000	001	X'03', section identifier, DSS public key.
001	001	X'00', version.
002	002	Section length, 14+ppp+qqq+ggg+yyy.
004	002	Size of p in bits. The size of p must be one of: 512, 576, 640, 704, 768, 832, 896, 960, or 1024.
006	002	Size of the p field in bytes, “ppp”.
008	002	Size of the q field in bytes, “qqq”.
010	002	Size of the g field in bytes, “ggg”.
012	002	Size of the y field in bytes, “yyy”.
014	ppp	Prime modulus (large public modulus), p.
014 +ppp	qqq	Prime divisor (small public modulus), q. $2^{159}<q<2^{160}$.
014 +ppp +qqq	ggg	Public key generator, g.
014 +ppp +qqq +ggg	yyy	Public key, y. $y=g^x$ mod(p); $1<y<p$.

Format of RSA Private External Key Tokens

An RSA private external key token contains the following sections:

- A required PKA token header starting with the token identifier X'1E'
- A required RSA private key section starting with one of the following section identifiers:
  - X'02' which indicates a modulus-exponent form RSA private key section (not optimized) with modulus length of up to 1024 bits for use with the S/390 Cryptographic Coprocessor Feature or the PCI Cryptographic Coprocessor.
  - X'08' which indicates an optimized Chinese Remainder Theorem form private key section with modulus bit length of up to 2048 bits for use with the PCI Cryptographic Coprocessor
- A required RSA public key section, starting with the section identifier X'04'
- An optional private key name section, starting with the section identifier X'10'

Table 99 presents the basic record format of an RSA private external key token. All length fields are in binary. All binary fields (exponents, lengths, and so on) are stored with the high-order byte first (left, low-address, S/390 format). All binary fields (exponents, modulus, and so on) in the private sections of tokens are right-justified and padded with zeros to the left.

Table 99. RSA Private External Key Token Basic Record Format

Offset (Dec)	Number of Bytes	Description
Token Header (required)		
000	001	Token identifier. X'1E' indicates an external token. The private key is either in cleartext or enciphered with a transport key-encrypting key.
001	001	Version, X'00'.
002	002	Length of the key token structure.
004	004	Ignored. Should be zero.
RSA Private Key Section (required) • For 1024-bit Modulus-Exponent form refer to "RSA Private Key Token, 1024-bit Modulus-Exponent External Form" • For 2048-bit Chinese Remainder Theorem form refer to "RSA Private Key Token, 2048-bit Chinese Remainder Theorem External Form" on page 391		
RSA Public Key Section (required)		
000	001	X'04', section identifier, RSA public key.
001	001	X'00', version.
002	002	Section length, 12+xxx.
004	002	Reserved field.
006	002	RSA public key exponent field length in bytes, "xxx".
008	002	Public key modulus length in bits.
010	002	RSA public key modulus field length in bytes, which is zero for a private token. **Note:** In an RSA private key token, this field should be zero. The RSA private key section contains the modulus.
012	xxx	Public key exponent, e (this is generally a 1-, 3-, or 64- to 256-byte quantity). e must be odd and $1<e<n$. (Frequently, the value of e is $2^{16}+1$ (=65,537).
Private Key Name (optional)		
000	001	X'10', section identifier, private key name.
001	001	X'00', version.
002	002	Section length, X'0044' (68 decimal).
004	064	Private key name (in ASCII), left-justified, padded with space characters (X'20'). An access control system can use the private key name to verify that the calling application is entitled to use the key.

RSA Private Key Token, 1024-bit Modulus-Exponent External Form

This RSA private key token and the external X'02' token is supported on the S/390 Cryptographic Coprocessor Feature and PCI Cryptographic Coprocessor.

Table 100. RSA Private Key Token, 1024-bit Modulus-Exponent External Format

Offset (Dec)	Number of Bytes	Description
000	001	X'02', section identifier, RSA private key, modulus-exponent format (RSA-PRIV)

Table 100. RSA Private Key Token, 1024-bit Modulus-Exponent External Format (continued)

Offset (Dec)	Number of Bytes	Description
001	001	X'00', version.
002	002	Length of the RSA private key section X'016C' (364 decimal).
004	020	SHA-1 hash value of the private key subsection cleartext, offset 28 to the section end. This hash value is checked after an enciphered private key is deciphered for use.
024	004	Reserved; set to binary zero.
028	001	Key format and security: **X'00'** Unencrypted RSA private key subsection identifier. **X'82'** Encrypted RSA private key subsection identifier.
029	001	Reserved, binary zero.
030	020	SHA-1 hash of the optional key-name section. If there is no key-name section, then 20 bytes of X'00'.
050	004	Key use flag bits. **Bit** **Meaning When Set On** **0** Key management usage permitted. **1** Signature usage not permitted. All other bits reserved, set to binary zero.
054	006	Reserved; set to binary zero.
060	024	Reserved; set to binary zero.
084	Start of the optionally-encrypted secure subsection.	
084	024	Random number, confounder.
108	128	Private-key exponent, d. $d=e^{-1} \bmod((p-1)(q-1))$, and $1<d<n$ where e is the public exponent.
	End of the optionally-encrypted subsection; the confounder field and the private-key exponent field are enciphered for key confidentiality when the key format and security flags (offset 28) indicate that the private key is enciphered. They are enciphered under a double-length transport key using the ede2 algorithm.	
236	128	Modulus, n. $n=pq$ where p and q are prime and $1<n<2^{1024}$.

RSA Private Key Token, 2048-bit Chinese Remainder Theorem External Form

This RSA private key token is supported on the PCI Cryptographic Coprocessor.

Table 101. RSA Private Key Token, 2048-bit Chinese Remainder Theorem External Format

Offset (Dec)	Number of Bytes	Description
000	001	X'08', section identifier, RSA private key, CRT format (RSA-CRT)
001	001	X'00', version.
002	002	Length of the RSA private-key section, 132 + ppp + qqq + rrr + sss + uuu + xxx + nnn.
004	020	SHA-1 hash value of the private key subsection cleartext, offset 28 to the end of the modulus.
024	004	Reserved; set to binary zero.

Table 101. RSA Private Key Token, 2048-bit Chinese Remainder Theorem External Format (continued)

Offset (Dec)	Number of Bytes	Description
028	001	Key format and security: **X'40'** Unencrypted RSA private-key subsection identifier, Chinese Remainder form. **X'42'** Encrypted RSA private-key subsection identifier, Chinese Remainder form.
029	001	Reserved; set to binary zero.
030	020	SHA-1 hash of the optional key-name section and any following optional sections. If there are no optional sections, then 20 bytes of X'00'.
050	004	Key use flag bits. **Bit** **Meaning When Set On** **0** Key management usage permitted. **1** Signature usage not permitted. All other bits reserved, set to binary zero.
054	002	Length of prime number, p, in bytes: ppp.
056	002	Length of prime number, q, in bytes: qqq.
058	002	Length of d_p, in bytes: rrr.
060	002	Length of d_q, in bytes: sss.
062	002	Length of U, in bytes: uuu.
064	002	Length of modulus, n, in bytes: nnn.
066	004	Reserved; set to binary zero.
070	002	Length of padding field, in bytes: xxx.
072	004	Reserved, set to binary zero.
076	016	Reserved, set to binary zero.
092	032	Reserved; set to binary zero.
124	Start of the optionally-encrypted secure subsection.	
124	008	Random number, confounder.
132	ppp	Prime number, p.
132 + ppp	qqq	Prime number, q
132 + ppp + qqq	rrr	d_p = d mod(p - 1)
132 + ppp + qqq + rrr	sss	d_q = d mod(q - 1)
132 + ppp + qqq + rrr + sss	uuu	U = q^{-1}mod(p).
132 + ppp + qqq + rrr + sss + uuu	xxx	X'00' padding of length xxx bytes such that the length from the start of the random number above to the end of the padding field is a multiple of eight bytes.
	End of the optionally-encrypted secure subsection; all of the fields starting with the confounder field and ending with the variable length pad field are enciphered for key confidentiality when the key format-and-security flags (offset 28) indicate that the private key is enciphered. They are enciphered under a double-length transport key using the TDES (CBC outer chaining) algorithm.	
132 + ppp + qqq + rrr + sss + uuu + xxx	nnn	Modulus, n. n = pq where p and q are prime and $2^{512}<n<2^{2048}$.

Format of the DSS Private External Key Token

A DSS private external key token contains the following sections:
- A required PKA token header, starting with the token identifier X'1E'
- A required DSS private key section, starting with the section identifier X'01'
- A required DSS public key section, starting with the section identifier X'03'
- An optional private key name section, starting with the section identifier X'10'

Table 102 presents the format of a DSS private external key token. All length fields are in binary. All binary fields (exponents, lengths, and so on) are stored with the high-order byte first (left, low-address, S/390 format). All binary fields (exponents, modulus, and so on) in the private sections of tokens are right-justified and padded with zeros to the left.

Table 102. DSS Private External Key Token

Offset (Dec)	Number of Bytes	Description
Token Header (required)		
000	001	Token identifier. X'1E' indicates an external token. The private key is enciphered with a PKA master key.
001	001	Version, X'00'.
002	002	Length of the key token structure.
004	004	Ignored. Should be zero.
DSS Private Key Section and Secured Subsection (required)		
000	001	X'01', section identifier, DSS private key.
001	001	X'00', version.
002	002	Length of the DSS private key section, 436, X'01B4'.
004	020	SHA-1 hash value of the private key subsection cleartext, offset 28 to the section end. This hash value is checked after an enciphered private key is deciphered for use.
024	004	Reserved; set to binary zero.
028	001	Key security: **X'00'** Unencrypted DSS private key subsection identifier. **X'81'** Encrypted DSS private key subsection identifier.
029	001	Padding, X'00'.
030	020	SHA-1 hash of the key token structure contents that follow the public key section. If no sections follow, this field is set to binary zeros.
050	010	Reserved; set to binary zero.
060	048	Ignored; set to binary zero.
108	128	Public key generator, g. $1<g<p$.
236	128	Prime modulus (large public modulus), p. $2^{L-1}<p<2^{L}$ and L (the modulus length) must be a multiple of 64.
364	020	Prime divisor (small public modulus), q. $2^{159}<q<2^{160}$.
384	004	Reserved; set to binary zero.
388	024	Random number, confounder. **Note:** This field and the next two fields are enciphered for key confidentiality when the key security flag (offset 28) indicates the private key is enciphered.
412	020	Secret DSS key, x; x is random. (See the preceding note.)

Table 102. DSS Private External Key Token (continued)

Offset (Dec)	Number of Bytes	Description
432	004	Random number, generated when the secret key is generated. (See the preceding note.)
DSS Public Key Section (required)		
000	001	X'03', section identifier, DSS public key.
001	001	X'00', version.
002	002	Section length, 14+yyy.
004	002	Size of p in bits. The size of p must be one of: 512, 576, 640, 704, 768, 832, 896, 960, or 1024.
006	002	Size of the p field in bytes, which is zero for a private token.
008	002	Size of the q field in bytes, which is zero for a private token.
010	002	Size of the g field in bytes, which is zero for a private token.
012	002	Size of the y field in bytes, "yyy".
014	yyy	Public key, y. $y=g^x$ mod(p) **Note:** p, q, and y are defined in the DSS public key token.
Private Key Name (optional)		
000	001	X'10', section identifier, private key. name
001	001	X'00', version.
002	002	Section length, X'0044' (68 decimal).
004	064	Private key name (in ASCII), left-justified, padded with space characters (X'20'). An access control system can use the private key name to verify that the calling application is entitled to use the key.

Format of the RSA Private Internal Key Token

An RSA private internal key token contains the following sections:

- A required PKA token header, starting with the token identifier X'1F'
- basic record format of an RSA private internal key token. All length fields are in binary. All binary fields (exponents, lengths, and so on) are stored with the high-order byte first (left, low-address, S/390 format). All binary fields (exponents, modulus, and so on) in the private sections of tokens are right-justified and padded with zeros to the left.

Table 103. RSA Private Internal Key Token Basic Record Format

Offset (Dec)	Number of Bytes	Description
Token Header (required)		
000	001	Token identifier. X'1F' indicates an internal token. The private key is enciphered with a PKA master key.
001	001	Version, X'00'.
002	002	Length of the key token structure excluding the internal information section.
004	004	Ignored; should be zero.

Table 103. RSA Private Internal Key Token Basic Record Format (continued)

Offset (Dec)	Number of Bytes	Description
RSA Private Key Section and Secured Subsection (required) • For 1024-bit X'02' Modulus-Exponent form refer to "RSA Private Key Token, 1024-bit Modulus-Exponent Internal Form for Cryptographic Coprocessor Feature" on page 396 • For 1024-bit X'06' Modulus-Exponent form refer to "RSA Private Key Token, 1024-bit Modulus-Exponent Internal Form for PCI Cryptographic Coprocessor" on page 397 • For 2048-bit X'08' Chinese Remainder Theorem form refer to "RSA Private Key Token, 2048-bit Chinese Remainder Theorem Internal Form" on page 398		
RSA Public Key Section (required)		
000	001	X'04', section identifier, RSA public key.
001	001	X'00', version.
002	002	Section length, 12+xxx.
004	002	Reserved field.
006	002	RSA public key exponent field length in bytes, "xxx".
008	002	Public key modulus length in bits.
010	002	RSA public key modulus field length in bytes, which is zero for a private token.
012	xxx	Public key exponent (this is generally a 1, 3, or 64 to 256-byte quantity), e. e must be odd and 1<e<n. (Frequently, the value of e is 2^{16}+1 (=65,537).
Private Key Name (optional)		
000	001	X'10', section identifier, private key name.
001	001	X'00', version.
002	002	Section length, X'0044' (68 decimal).
004	064	Private key name (in ASCII), left-justified, padded with space characters (X'20'). An access control system can use the private key name to verify that the calling application is entitled to use the key.
Internal Information Section (required)		
000	004	Eye catcher 'PKTN'.
004	004	PKA token type. **Bit** **Meaning When Set On** **0** RSA key. **1** DSS key. **2** Private key. **3** Public key. **4** Private key name section exists. **5** Private key unenciphered. **6** Blinding information present. **7** Retained private key.
008	004	Address of token header.
012	002	Total length of total structure including this information section.
014	002	Count of number of sections.

Table 103. RSA Private Internal Key Token Basic Record Format (continued)

Offset (Dec)	Number of Bytes	Description
016	016	PKA master key hash pattern.
032	001	Domain of retained key.
033	008	Serial number of processor holding retained key.
041	007	Reserved.

RSA Private Key Token, 1024-bit Modulus-Exponent Internal Form for Cryptographic Coprocessor Feature

Table 104. RSA Private Internal Key Token, 1024-bit ME Form for Cryptographic Coprocessor Feature

Offset (Dec)	Number of Bytes	Description
000	001	X'02', section identifier, RSA private key.
001	001	X'00', version.
002	002	Length of the RSA private key section X'016C' (364 decimal).
004	020	SHA-1 hash value of the private key subsection cleartext, offset 28 to the section end. This hash value is checked after an enciphered private key is deciphered for use.
024	004	Reserved; set to binary zero.
028	001	Key format and security: **X'02'** RSA private key.
029	001	Format of external key from which this token was derived: **X'21'** External private key was specified in the clear. **X'22'** External private key was encrypted.
030	020	SHA-1 hash of the key token structure contents that follow the public key section. If no sections follow, this field is set to binary zeros.
050	001	Key use flag bits. **Bit** **Meaning When Set On** **0** Key management usage permitted. **1** Signature usage not permitted. All other bits reserved, set to binary zero.
051	009	Reserved; set to binary zero.
060	048	Object Protection Key (OPK) encrypted under a PKA master key—can be under the Signature Master Key (SMK) or Key Management Master Key (KMMK) depending on key use.
108	128	Secret key exponent d, encrypted under the OPK. $d=e^{-1} \bmod((p-1)(q-1))$
236	128	Modulus, n. n=pq where p and q are prime and $1<n<2^{1024}$.

RSA Private Key Token, 1024-bit Modulus-Exponent Internal Form for PCI Cryptographic Coprocessor

Table 105. RSA Private Internal Key Token, 1024-bit ME Form for PCI Cryptographic Coprocessor

Offset (Dec)	Number of Bytes	Description
000	001	X'06', section identifier, RSA private key modulus-exponent format (RSA-PRIV).
001	001	X'00', version.
002	002	Length of the RSA private key section X'0198' (408 decimal) + rrr + iii + xxx.
004	020	SHA-1 hash value of the private key subsection cleartext, offset 28 to and including the modulus at offset 236.
024	004	Reserved; set to binary zero.
028	001	Key format and security: **X'02'** RSA private key.
029	001	Format of external key from which this token was derived: **X'21'** External private key was specified in the clear. **X'22'** External private key was encrypted. **X'23'** Private key was generated using regeneration data. **X'24'** Private key was randomly generated.
030	020	SHA-1 hash of the optional key-name section and any following optional sections. If there are no optional sections, this field is set to binary zeros.
050	004	Key use flag bits. **Bit** **Meaning When Set On** **0** Key management usage permitted. **1** Signature usage not permitted. All other bits reserved, set to binary zeros.
054	006	Reserved; set to binary zero.
060	048	Object Protection Key (OPK) encrypted under the Asymmetric Keys Master Key using the ede3 algorithm.
108	128	Private key exponent d, encrypted under the OPK using the ede5 algorithm. $d=e^{-1}mod((p-1)(q-1))$, and $1<d<n$ where e is the public exponent.
236	128	Modulus, n. n=pq where p and q are prime and $2^{512}<n<2^{1024}$.
364	016	Asymmetric-Keys Master Key hash pattern.
380	020	SHA-1 hash value of the blinding information subsection cleartext, offset 400 to the end of the section.
400	002	Length of the random number r, in bytes: rrr.
402	002	Length of the random number r^{-1}, in bytes: iii.
404	002	Length of the padding field, in bytes: xxx.
406	002	Reserved; set to binary zeros.
408	Start of the encrypted blinding subsection	
408	rrr	Random number r (used in blinding).
408 + rrr	iii	Random number r^{-1} (used in blinding).

Table 105. RSA Private Internal Key Token, 1024-bit ME Form for PCI Cryptographic Coprocessor (continued)

Offset (Dec)	Number of Bytes	Description
408 + rrr + iii	xxx	X'00' padding of length xxx bytes such that the length from the start of the encrypted blinding subsection to the end of the padding field is a multiple of eight bytes.
	End of the encrypted blinding subsection; all of the fields starting with the random number r and ending with the variable length pad field are encrypted under the OPK using TDES (CBC outer chaining) algorithm.	

RSA Private Key Token, 2048-bit Chinese Remainder Theorem Internal Form

This RSA private key token is supported on the PCI Cryptographic Coprocessor.

Table 106. RSA Private Internal Key Token, 2048-bit Chinese Remainder Theorem External Format

Offset (Dec)	Number of Bytes	Description
000	001	X'08', section identifier, RSA private key, CRT format (RSA-CRT)
001	001	X'00', version.
002	002	Length of the RSA private-key section, 132 + ppp + qqq + rrr + sss + uuu + +ttt + iii + xxx + nnn.
004	020	SHA-1 hash value of the private-key subsection cleartext, offset 28 to the end of the modulus.
024	004	Reserved; set to binary zero.
028	001	Key format and security: **X'08'** Encrypted RSA private-key subsection identifier, Chinese Remainder form.
029	001	Key derivation method: **X'21'** External private key was specified in the clear. **X'22'** External private key was encrypted. **X'23'** Private key was generated using regeneration data. **X'24'** Private key was randomly generated.
030	020	SHA-1 hash of the optional key-name section and any following sections. If there are no optional sections, then 20 bytes of X'00'.
050	004	Key use flag bits: **Bit** **Meaning When Set On** **0** Key management usage permitted. **1** Signature usage not permitted. All other bits reserved, set to binary zero.
054	002	Length of prime number, p, in bytes: ppp.
056	002	Length of prime number, q, in bytes: qqq.
058	002	Length of d_p, in bytes: rrr.
060	002	Length of d_q, in bytes: sss.
062	002	Length of U, in bytes: uuu.
064	002	Length of modulus, n, in bytes: nnn.
066	002	Length of the random number r, in bytes: ttt.
068	002	Length of the random number r^{-1}, in bytes: iii.

Table 106. RSA Private Internal Key Token, 2048-bit Chinese Remainder Theorem External Format (continued)

Offset (Dec)	Number of Bytes	Description
070	002	Length of padding field, in bytes: xxx.
072	004	Reserved, set to binary zero.
076	016	Asymmetric-Keys Master Key hash pattern.
092	032	Object Protection Key (OPK) encrypted under the Asymmetric-Keys Master Key using the TDES (CBC outer chaining) algorithm.
124	Start of the encrypted secure subsection, encrypted under the OPK using TDES (CBC outer chaining).	
124	008	Random number, confounder.
132	ppp	Prime number, p.
132 + ppp	qqq	Prime number, q
132 + ppp + qqq	rrr	d_p = d mod(p - 1)
132 + ppp + qqq + rrr	sss	d_q = d mod(q - 1)
132 + ppp + qqq + rrr + sss	uuu	U = q^{-1}mod(p).
132 + ppp + qqq + rrr + sss + uuu	ttt	Random number r (used in blinding).
132 + ppp + qqq + rrr + sss + uuu + ttt	iii	Random number r^{-1} (used in blinding).
132 + ppp + qqq + rrr + sss + uuu + ttt + iii	xxx	X'00' padding of length xxx bytes such that the length from the start of the confounder at offset 124 to the end of the padding field is a multiple of eight bytes.
	End of the encrypted secure subsection; all of the fields starting with the confounder field and ending with the variable length pad field are encrypted under the OPK using TDES (CBC outer chaining) for key confidentiality.	
132 + ppp + qqq + rrr + sss + uuu + ttt + iii + xxx	nnn	Modulus, n. n = pq where p and q are prime and $2^{512}<n<2^{2048}$.

Format of the DSS Private Internal Key Token

A DSS private internal key token contains the following sections:
- A required PKA token header, starting with the token identifier X'1F'
- A required DSS private key section, starting with the section identifier X'01'
- A required DSS public key section, starting with the section identifier X'03'
- An optional private key name section, starting with the section identifier X'10'
- A required internal information section, starting with the eyecatcher 'PKTN'

Table 107 presents the format of a DSS private internal token. All length fields are in binary. All binary fields (exponents, lengths, and so on) are stored with the high-order byte first (left, low-address, S/390 format). All binary fields (exponents, modulus, and so on) in the private sections of tokens are right-justified and padded with zeros to the left.

Table 107. DSS Private Internal Key Token

Offset (Dec)	Number of Bytes	Description
Token Header (required)		

Table 107. DSS Private Internal Key Token (continued)

Offset (Dec)	Number of Bytes	Description
000	001	Token identifier. X'1F' indicates an internal token. The private key is enciphered with a PKA master key.
001	001	Version, X'00'.
002	002	Length of the key token structure excluding the internal information section.
004	004	Ignored; should be zero.
DSS Private Key Section and Secured Subsection (required)		
000	001	X'01', section identifier, DSS private key.
001	001	X'00', version.
002	002	Length of the DSS private key section, 436, X'01B4'.
004	020	SHA-1 hash value of the private key subsection cleartext, offset 28 to the section end. This hash value is checked after an enciphered private key is deciphered for use.
024	004	Reserved; set to binary zero.
028	001	Key security: X'01' DSS private key.
029	001	Format of external key token: **X'10'** Private key generated on an ICSF host. **X'11'** External private key was specified in the clear. **X'12'** External private key was encrypted.
030	020	SHA-1 hash of the key token structure contents that follow the public key section. If no sections follow, this field is set to binary zeros.
050	010	Reserved; set to binary zero.
060	048	The OPK encrypted under a PKA master key (Signature Master Key (SMK)).
108	128	Public key generator, g. $1<g<p$.
236	128	Prime modulus (large public modulus), p. $2^{L-1}<p<2^{L}$ for $512 \leq L \leq 1024$, and L (the modulus length) must be a multiple of 64.
364	020	Prime divisor (small public modulus), q. $2^{159}<q<2^{160}$.
384	004	Reserved; set to binary zero.
388	024	Random number, confounder. **Note:** This field and the two that follow are enciphered under the OPK.
412	020	Secret DSS key, x. x is random. (See the preceding note.)
432	004	Random number, generated when the secret key is generated. (See the preceding note.)
DSS Public Key Section (required)		
000	001	X'03', section identifier, DSS public key.
001	001	X'00', version.
002	002	Section length, 14+yyy.
004	002	Size of p in bits. The size of p must be one of: 512, 576, 640, 704, 768, 832, 896, 960, or 1024.
006	002	Size of the p field in bytes, which is zero for a private token.
008	002	Size of the q field in bytes, which is zero for a private token.
010	002	Size of the g field in bytes, which is zero for a private token.

Table 107. DSS Private Internal Key Token (continued)

Offset (Dec)	Number of Bytes	Description
012	002	Size of the y field in bytes, “yyy”.
014	yyy	Public key, y. y=g^x mod(p); **Note:** p, g, and y are defined in the DSS public key token.
Private Key Name (optional)		
000	001	X'10', section identifier, private key name.
001	001	X'00', version.
002	002	Section length, X'0044' (68 decimal).
004	064	Private key name (in ASCII), left-justified, padded with space characters (X'20'). An access control system can use the private key name to verify that the calling application is entitled to use the key.
Internal Information Section (required)		
000	004	Eye catcher 'PKTN'.
004	004	PKA token type. **Bit** / **Meaning When Set On**: **0** RSA key. **1** DSS key. **2** Private key. **3** Public key. **4** Private key name section exists.
008	004	Address of token header.
012	002	Length of internal work area.
014	002	Count of number of sections.
016	016	PKA master key hash pattern.
032	016	Reserved.

PKA Null Key Token

Table 108 shows the format for a PKA null key token.

Table 108. Format of PKA Null Key Tokens

Bytes	Description
0	X'00' Token identifier (indicates that this is a null key token).
1	Version, X'00'
2–3	X'0008' Length of the key token structure.
4–7	Ignored (should be zero).

Appendix I. EBCDIC and ASCII Default Conversion Tables

This section presents tables showing EBCDIC to ASCII and ASCII to EBCDIC conversion tables. In the table headers, EBC refers to EBCDIC and ASC refers to ASCII.

Table 109 shows the EBCDIC to ASCII default conversion table.

Table 109. EBCDIC to ASCII Default Conversion Table

EBC	ASC	EBC	ASC	EBC	ASC	EBC	ASC	EBC	ASC	EBC	ASC	EBC	ASC	EBC	ASC
00	00	20	81	40	20	60	2D	80	F8	A0	C8	C0	7B	E0	5C
01	01	21	82	41	A6	61	2F	81	61	A1	7E	C1	41	E1	E7
02	02	22	1C	42	E1	62	DF	82	62	A2	73	C2	42	E2	53
03	03	23	84	43	80	63	DC	83	63	A3	74	C3	43	E3	54
04	CF	24	86	44	EB	64	9A	84	64	A4	75	C4	44	E4	55
05	09	25	0A	45	90	65	DD	85	65	A5	76	C5	45	E5	56
06	D3	26	17	46	9F	66	DE	86	66	A6	77	C6	46	E6	57
07	7F	27	1B	47	E2	67	98	87	67	A7	78	C7	47	E7	58
08	D4	28	89	48	AB	68	9D	88	68	A8	79	C8	48	E8	59
09	D5	29	91	49	8B	69	AC	89	69	A9	7A	C9	49	E9	5A
0A	C3	2A	92	4A	9B	6A	BA	8A	96	AA	EF	CA	CB	EA	A0
0B	0B	2B	95	4B	2E	6B	2C	8B	A4	AB	C0	CB	CA	EB	85
0C	0C	2C	A2	4C	3C	6C	25	8C	F3	AC	DA	CC	BE	EC	8E
0D	0D	2D	05	4D	28	6D	5F	8D	AF	AD	5B	CD	E8	ED	E9
0E	0E	2E	06	4E	2B	6E	3E	8E	AE	AE	F2	CE	EC	EE	E4
0F	0F	2F	07	4F	7C	6F	3F	8F	C5	AF	F9	CF	ED	EF	D1
10	10	30	E0	50	26	70	D7	90	8C	B0	B5	D0	7D	F0	30
11	11	31	EE	51	A9	71	88	91	6A	B1	B6	D1	4A	F1	31
12	12	32	16	52	AA	72	94	92	6B	B2	FD	D2	4B	F2	32
13	13	33	E5	53	9C	73	B0	93	6C	B3	B7	D3	4C	F3	33
14	C7	34	D0	54	DB	74	B1	94	6D	B4	B8	D4	4D	F4	34
15	B4	35	1E	55	A5	75	B2	95	6E	B5	B9	D5	4E	F5	35
16	08	36	EA	56	99	76	FC	96	6F	B6	E6	D6	4F	F6	36
17	C9	37	04	57	E3	77	D6	97	70	B7	BB	D7	50	F7	37
18	18	38	8A	58	A8	78	FB	98	71	B8	BC	D8	51	F8	38
19	19	39	F6	59	9E	79	60	99	72	B9	BD	D9	52	F9	39
1A	CC	3A	C6	5A	21	7A	3A	9A	97	BA	8D	DA	A1	FA	B3
1B	CD	3B	C2	5B	24	7B	23	9B	87	BB	D9	DB	AD	FB	F7
1C	83	3C	14	5C	2A	7C	40	9C	CE	BC	BF	DC	F5	FC	F0
1D	1D	3D	15	5D	29	7D	27	9D	93	BD	5D	DD	F4	FD	FA
1E	D2	3E	C1	5E	3B	7E	3D	9E	F1	BE	D8	DE	A3	FE	A7
1F	1F	3F	1A	5F	5E	7F	22	9F	FE	BF	C4	DF	8F	FF	FF

Table 110 shows the ASCII to EBCDIC default conversion table.

Table 110. ASCII to EBCDIC Default Conversion Table

ASC	EBC	ASC	EBC	ASC	EBC	ASC	EBC	ASC	EBC	ASC	EBC	ASC	EBC	ASC	EBC
00	00	20	40	40	7C	60	79	80	43	A0	EA	C0	AB	E0	30

Table 110. ASCII to EBCDIC Default Conversion Table (continued)

ASC	EBC	ASC	EBC	ASC	EBC	ASC	EBC	ASC	EBC	ASC	EBC	ASC	EBC	ASC	EBC
01	01	21	5A	41	C1	61	81	81	20	A1	DA	C1	3E	E1	42
02	02	22	7F	42	C2	62	82	82	21	A2	2C	C2	3B	E2	47
03	03	23	7B	43	C3	63	83	83	1C	A3	DE	C3	0A	E3	57
04	37	24	5B	44	C4	64	84	84	23	A4	8B	C4	BF	E4	EE
05	2D	25	6C	45	C5	65	85	85	EB	A5	55	C5	8F	E5	33
06	2E	26	50	46	C6	66	86	86	24	A6	41	C6	3A	E6	B6
07	2F	27	7D	47	C7	67	87	87	9B	A7	FE	C7	14	E7	E1
08	16	28	4D	48	C8	68	88	88	71	A8	58	C8	A0	E8	CD
09	05	29	5D	49	C9	69	89	89	28	A9	51	C9	17	E9	ED
0A	25	2A	5C	4A	D1	6A	91	8A	38	AA	52	CA	CB	EA	36
0B	0B	2B	4E	4B	D2	6B	92	8B	49	AB	48	CB	CA	EB	44
0C	0C	2C	6B	4C	D3	6C	93	8C	90	AC	69	CC	1A	EC	CE
0D	0D	2D	60	4D	D4	6D	94	8D	BA	AD	DB	CD	1B	ED	CF
0E	0E	2E	4B	4E	D5	6E	95	8E	EC	AE	8E	CE	9C	EE	31
0F	0F	2F	61	4F	D6	6F	96	8F	DF	AF	8D	CF	04	EF	AA
10	10	30	F0	50	D7	70	97	90	45	B0	73	D0	34	F0	FC
11	11	31	F1	51	D8	71	98	91	29	B1	74	D1	EF	F1	9E
12	12	32	F2	52	D9	72	99	92	2A	B2	75	D2	1E	F2	AE
13	13	33	F3	53	E2	73	A2	93	9D	B3	FA	D3	06	F3	8C
14	3C	34	F4	54	E3	74	A3	94	72	B4	15	D4	08	F4	DD
15	3D	35	F5	55	E4	75	A4	95	2B	B5	B0	D5	09	F5	DC
16	32	36	F6	56	E5	76	A5	96	8A	B6	B1	D6	77	F6	39
17	26	37	F7	57	E6	77	A6	97	9A	B7	B3	D7	70	F7	FB
18	18	38	F8	58	E7	78	A7	98	67	B8	B4	D8	BE	F8	80
19	19	39	F9	59	E8	79	A8	99	56	B9	B5	D9	BB	F9	AF
1A	3F	3A	7A	5A	E9	7A	A9	9A	64	BA	6A	DA	AC	FA	FD
1B	27	3B	5E	5B	AD	7B	C0	9B	4A	BB	B7	DB	54	FB	78
1C	22	3C	4C	5C	E0	7C	4F	9C	53	BC	B8	DC	63	FC	76
1D	1D	3D	7E	5D	BD	7D	D0	9D	68	BD	B9	DD	65	FD	B2
1E	35	3E	6E	5E	5F	7E	A1	9E	59	BE	CC	DE	66	FE	9F
1F	1F	3F	6F	5F	6D	7F	07	9F	46	BF	BC	DF	62	FF	FF

Appendix J. Using BSAFE Applications to Access ICSF Services

ICSF works in conjunction with RSA Security, Inc.'s BSAFE toolkit (BSAFE 3.1 or later). If you are currently using applications developed with BSAFE, you may want to take advantage of the increased security and performance available with the S/390 Cryptographic Coprocessor Feature and ICSF.

Through BSAFE 3.1 you can access the ICSF services to:
- Compute message digests or hashes
- Generate random numbers
- Encipher and decipher data using the DES algorithm
- Generate and verify RSA digital signatures

Some BSAFE Basics

BSAFE has many algorithm information types (called AIs). Many of the AIs can perform several cryptographic functions. For this reason, you must specify the algorithmic method (AM) to be used by supplying a chooser. If the cryptographic function requires a key, you supply key information to the BSAFE application with a key information (KI) type. For the most current information on the BSAFE user interface and a complete description of algorithm information types, algorithm methods, choosers, and key information types, refer to *BSAFE User's Manual* and *BSAFE Library Reference Manual*.

Computing Message Digests and Hashes

MD5 and SHA1 hashing are both available from ICSF via BSAFE. If your BSAFE application uses the AM_MD5 or the AM_SHA algorithm methods, you can add a couple of BSAFE function calls and the application will use ICSF and the S/390 Cryptographic Coprocessor Feature instead of the BSAFE algorithm method.

The following list shows BSAFE AI types with choosers that may include AM_MD5:
- AI_MD5
- AI_MD5_BER
- AI_MD5WithDES_CBCPad
- AI_MD5WithDES_CBCPadBER
- AI_MD5WithRC2_CBCPad
- AI_MD5WithRC2_CBCPadBER
- AI_MD5WithRSAEncryption
- AI_MD5WithRSAEncryptionBER
- AI_MD5WithXOR
- AI_MD5WithXOR_BER

The following list shows BSAFE AI types with choosers that may include AM_SHA:
- AI_SHA1
- AI_SHA1_BER
- AI_SHA1WithDES_CBCPad
- AI_SHA1WithDES_CBCPadBER

Generating Random Numbers

If your BSAFE application uses the algorithm method AM_MD5_RANDOM, you can add a chooser definition containing the algorithm method AM_HW_RANDOM (new with BSAFE 3.1) and a couple of BSAFE function calls and your program can use ICSF and the S/390 Cryptographic Coprocessor Feature to generate random numbers instead of the BSAFE algorithm method.

BSAFE 3.1 provides a new algorithm information type, AI_HWRandom. You need to set your random number generation object with AI_HWRandom, and initialize the object with a chooser containing AM_HW_RANDOM, in order to use ICSF with the S/390 Cryptographic Coprocessor Feature for generating random numbers. You do not, however, have to make a B_RandomUpdate call, since the S/390 cryptographic solution does not require a seed.

The only AI type with choosers that may include AM_HW_RANDOM is AI_HWRandom.

Encrypting and Decrypting with DES

If your BSAFE application uses either the AM_DES_CBC_ENCRYPT or the AM_DES_CBC_DECRYPT algorithm methods, you can add a chooser containing the algorithm methods AM_TOKEN_DES_CBC_ENCRYPT and/or AM_TOKEN_DES_CBC_DECRYPT (both new with BSAFE 3.1) and a couple of BSAFE function calls and your program can use ICSF and the S/390 Cryptographic Coprocessor Feature to encrypt and/or decrypt data using the DES algorithm.

For your encryption or decryption key, you can use either a clear key in the form of a KI_8Byte or KI_DES8 or KI_Item (8 bytes long), or a CCA DES Key Token in the form of a KI_TOKEN (64 bytes long). KI_TOKEN is a new key information type in BSAFE 3.1.

The following list shows BSAFE AI types with choosers that may include either AM_TOKEN_DES_CBC_ENCRYPT, AM_TOKEN_DES_CBC_DECRYPT, or both:
- AI_DES_CBC_BSAFE1
- AI_DES_CBC_IV8
- AI_DES_CBCPadBER
- AI_DES_CBCPadIV8
- AI_DES_CBCPadPEM
- AI_MD5WithDES_CBCPad
- AI_MD5WithDES_CBCPadBER
- AI_SHA1WithDES_CBCPad
- AI_SHA1WithDES_CBCPadBER

Generating and Verifying RSA Digital Signatures

You can use algorithm method AM_TOKEN_RSA_PRV_ENCRYPT with AM_MD5 or AM_SHA to have ICSF and the S/390 Cryptographic Coprocessor Feature generate RSA digital signatures. To verify the RSA digital signature using the S/390 cryptographic solution, you can use AM_TOKEN_RSA_PUB_DECRYPT (with AM_MD5 or AM_SHA). Your BSAFE application must contain a couple of new BSAFE function calls to access the S/390 services. AM_TOKEN_RSA_PRV_ENCRYPT and AM_TOKEN_RSA_PUB_DECRYPT are new in BSAFE 3.1. For more information, see “Using the New Function Calls in Your BSAFE Application” on page 407.

For signature generation, you can use either a clear private key in the form of a KI_PKCS_RSAPrivate or a CCA RSA private key token in the form of a KI_TOKEN. For signature verification, you can use either a public RSA key in the form of a KI_RSAPublic or a CCA RSA public key token in the form of a KI_TOKEN.

KI_TOKEN is a new key information type in BSAFE. For more information about KI_TOKEN, see “Using the BSAFE KI_TOKEN” on page 409.

The following list shows BSAFE AI types with choosers that may include AM_TOKEN_RSA_PRV_ENCRYPT:
- AI_MD5WithRSAEncryption
- AI_MD5WithRSAEncryptionBER
- AI_SHA1WithRSAEncryption
- AI_SHA1WithRSAEncryptionBER

The following list shows BSAFE AI types with choosers that may include AM_TOKEN_RSA_PUB_DECRYPT:
- AI_MD5WithRSAEncryption
- AI_SHA1WithRSAEncryption

Encrypting and Decrypting with RSA

You can use algorithm method AM_TOKEN_RSA_ENCRYPT to have ICSF encrypt a symmetric key (or other string of 48 bytes or fewer). To decrypt the string using ICSF, you can use AM_TOKEN_RSA_CRT_DECRYPT. You’ll need a couple of new BSAFE function calls to access the S/390 services (see “Using the New Function Calls in Your BSAFE Application”.

To encrypt a string, you can use either a public key in the form KI_RSAPublic or a CCA RSA public key token in the form of a KI_TOKEN.

To decrypt a string, you can use either a private key in the form KI_PKCS_RSAPrivate or a CCA RSA private key token in the form of a KI_TOKEN.

Using the New Function Calls in Your BSAFE Application

To have your BSAFE application access the ICSF and S/390 Cryptographic Coprocessor Feature services, you need to add several new elements to your program. These elements are explained with examples in the steps that follow.

1. At the beginning of your program, declare one or more session choosers and also the hardware table list. For information about choosers and the hardware table list, see *BSAFE User’s Manual*.

```
/*-------------------------------------------------------------*
 * SESSION_CHOOSER will replace OLD_CHOOSER.                   *
 *-------------------------------------------------------------*/
B_ALGORITHM_METHOD **SESSION_CHOOSER = NULL_PTR;


/*-------------------------------------------------------------*
 * CCA_VTABLE is a vector table of functions that will be      *
 * substituted for BSAFE equivalents.  It is supplied by IBM   *
 * and will be loaded into your application when you invoke    *
 * QueryCrypto.                                                *
 *-------------------------------------------------------------*/
HW_TABLE_LIST CCA_VTABLE = (HW_TABLE_LIST)NULL_PTR;
```

2. Declare a tag list. The content of the tag list is supplied by BSAFE at the B_CreateSessionChooser call, which is discussed in a later step.

```
unsigned char **taglist = (unsigned char **)NULL_PTR;
```

3. For random number generation, DES encryption or decryption or RSA encryption or decryption, you need to define and declare an additional chooser

wherever your current chooser is defined and declared. For instance, suppose your application is doing an RSA encryption, and OLD_CHOOSER is defined as follows:

```
/*------------------------------------------------------------*
 * OLD_CHOOSER is used for this application when ICSF and      *
 * the crypto hardware is not available.                       *
 *------------------------------------------------------------*/
B_ALGORITHM_METHOD *OLD_CHOOSER[] = {
  &AM_SHA,
  &AM_RSA_ENCRYT,
  (B_ALGORITHM_METHOD *)NULL_PTR
};

/*------------------------------------------------------------*
 * ICSF_CHOOSER is a 'skeleton' for SESSION_CHOOSER.           *
 * SESSION_CHOOSER will be used for this application if        *
 * ICSF and the crypto hardware are not available.             *
 *------------------------------------------------------------*/
B_ALGORITHM_METHOD *ICSF_CHOOSER[]  = {
  &AM_SHA,
  &AM_TOKEN_RSA_PUB_ENCRYPT,
  (B_ALGORITHM_METHOD *)NULL_PTR
};
```

4. At the beginning of the main function in your application, add a call to the ICSF QueryCrypto function followed by a conditional call to the BSAFE B_CreateSessionChooser function.

```
/*------------------------------------------------------------*
 * Check for the existence of crypto hardware.  If it's there, *
 * QueryCrypto will supply CCA_VTABLE                          *
 *------------------------------------------------------------*/
if ((status = QueryCrypto(CRYPTO_Q_DES_AND_RSA,&CCA_VTABLE)) == 0)
/*-------------------------------------------*
                 * B_CreateSessionChooser will replace the     *
                 * BSAFE software functions with their CCA     *
                 * hardware equivalents.                       *
                 *                                             *
                 * Note that the last three parameters are not *
                 * used with CCA                               *
                 *---------------------------------------------*/
  if ((status = B_CreateSessionChooser(ICSF_CHOOSER,
                                      &SESSION_CHOOSER,
                                       CCA_VTABLE,
                                       (ITEM *)NULL_PTR,
                                       (POINTER *)NULL_PTR,
                                         &taglist)) != 0)
    break;
```

5. Set up the conditions under which any alternate choosers are used to initialize the appropriate algorithm object. For information about initializing algorithm objects, see *BSAFE User's Manual*.

```
/*-----------------------------------------------------*
 * Initialize the algorithm object with the appropriate  *
 * chooser.                                              *
 *------------------------------------------------------*/
if (SESSION_CHOOSER != NULL_PTR)
  if ((status = B_xxxxxxInit
       (xxxxxxObject,SESSION_CHOOSER,
        (A_SURRENDER_CTX *)NULL_PTR)) != 0)
    break;
  else ;
else
  if ((status = B_xxxxxxInit
          (xxxxxxObject,OLD_CHOOSER,
           (A_SURRENDER_CTX *)NULL_PTR)) != 0)
       break;
     else ;
```

6. When your application no longer needs the session chooser, program a call to the BSAFE B_FreeSessionChooser function.

   ```
   if (SESSION_CHOOSER != NULL_PTR)
     B_FreeSessionChooser(&SESSION_CHOOSER,&taglist);
   ```

Using the BSAFE KI_TOKEN

Those ICSF functions that require a key, like encipher and decipher, expect the key in the form of a CCA token. If you already have a CCA token, perform the following steps before you try to set your algorithm object. For information about how to perform the following tasks, see *BSAFE User's Manual* and *BSAFE Library Reference Manual*.

1. Create a key object.
2. Declare a KEY_TOKEN_INFO and fill it in.

   KEY_TOKEN_INFO is defined as follows in the *BSAFE User's Manual*:

   ```
   typedef struct {
     ITEM manufacturerID;
     ITEM internalKeyInfo;
   } KEY_TOKEN_INFO;
   ```

   The first ITEM is the address and length of one of the following three strings, depending on the CCA key token type you are using:

   - com.ibm.CCADES
   - com.ibm.CCARSAPublic
   - com.ibm.CCARSAPrivate

   The second ITEM is the address and length of your CCA key token.
3. Set the key information (B_SetKeyInfo) into the key object using the item and a key information type of KI_TOKEN as input.

If you don't already have a CCA token, you can supply a clear key to the function using one of the key information types mentioned in the section discussing the function you are using. BSAFE will convert the key to a CCA token. If you supply a clear BSAFE KI type to one of the ICSF functions, and the function is performed successfully, you can retrieve the key as a CCA token by invoking B_GetKeyInfo with KI_TOKEN as the key information type. A KEY_TOKEN_INFO struct is returned.

ICSF Triple DES via BSAFE

ICSF performs single, double, or triple DES depending on the length of the DES key; if you're using BSAFE to access ICSF triple DES, you should use the algorithm methods AM_TOKEN_DES_CBC_ENCRYPT and AM_TOKEN_DES_CBC_DECRYPT.

If you've already have an ICSF token, follow the instructions in the section titled "Using the BSAFE KI_TOKEN".

If you're using a clear key, follow the same procedure, except use your clear key padded on the right with binary zeroes to a length of 64 as the internalKeyInfo part of your KI_TOKEN_INFO. ICSF will convert your clear key to an internal ICSF key token.

Here's an example:

```
B_KEY_OBJ desKey = (B_KEY_OBJ)NULL_PTR;
KEY_TOKEN_INFO myTokenInfo;
unsigned char myToken[64] = {0};
unsigned char * myTokenP;
unsigned char myDoubleKey[16];   /* Input to this function  *
unsigned char mfgID[] = "com.ibm.CCADES";
unsigned char * mfgIDP;
    .
    .
    .
myTokenP = myToken;
mfgIDP = mfgID;
T_memcpy(myToken,myDoubleKey,sizeof(myDoubleKey));
myTokenInfo.manufacturerID.len = strlen(mfgID);
myTokenInfo.manufacturerID.data = mfgIDP;
myTokenInfo.internalKeyInfo.len = sizeof(myToken);
myTokenInfo.internalKeyInfo.data = myTokenP;

/*  Create a key object. */
if ((status = B_CreateKeyObject (&desKey)) != 0)
   break;

/*  Set the key object.  */
if ((status = B_SetKeyInfo
   (desKey, KI_TOKEN, myTokenInfo )) != 0)
  break;
    .
    .
    .
```

Retrieving ICSF Error Information

When using the ICSF and S/390 Cryptographic Coprocessor Feature, Init, Update, and Final calls can result in BSAFE returning a status of BE_HARDWARE (0x020B). When this occurs, you can derive the ICSF return and reason codes by using a new BSAFE operation, B_GetExtendedErrorInfo. For an explanation of the return codes and reason codes, see "Appendix A. ICSF and TSS Return and Reason Codes" on page 319.

A coding example follows.

```
    .
    .
#include "balg.h"
#include "algobj.h"
#include "cca.h"
    .
    .
{
    .
    .
    .
  B_ALGORITHM_OBJECT * aop;
  ITEM * errp;
  unsigned char * algorithmMethod;
  CCA_ERROR_DATA * edp;
  unsigned int CCAreturnCode=0;
```

```
   unsigned int CCAreasonCode=0;
   unsigned char algorithmName[40]={0x00};
     .
     .
     .
   if (status==BE_HARDWARE) {
     B_GetExtendedErrorInfo(aop,errp,algorithmMethod);
     edp = errp->data;
     CCAreturnCode = (unsigned int) edp->returnCode;
     CCAreasonCode = (unsigned int) edp->reasonCode;
   }
     .
     .
  }
```

The prototype for B_GetExtendedErrorInfo is in balg.h, as shown in the example that follows.

```
B_GetExtendedErrorInfo (
B_ALGORITHM_OBJ algorithmObject,  /* in--algorithm object  */
ITEM * errorData,                 /* out--address and length of error data */
POINTER algorithmMethod           /* out--address of faulting AM  */
);
```

Appendix K. Control Vector Table

Note: The Control Vectors used in ICSF are exactly the same as documented in CCA and the TSS manuals.

The master key enciphers all keys operational on your system. A transport key enciphers keys that are distributed off your system. Before a master key or transport key enciphers a key, ICSF exclusive ORs both halves of the master key or transport key with a control vector. The same control vector is exclusive ORed to the left and right half of a master key or transport key.

Also, if you are entering a key part, ICSF exclusive ORs each half of the key part with a control vector before placing the key part into the CKDS.

Each type of key on ICSF (except the master key) has either one or two unique control vectors associated with it. The control vector that ICSF exclusive ORs the master key or transport key with depends on the type of key the master key or transport key is enciphering. For double-length keys, a unique control vector exists for each half of a specific key type. For example, there is a control vector for the left half of an input PIN-encrypting key, and a control vector for the right half of an input PIN-encrypting key.

If you are entering a key part into the CKDS, ICSF exclusive ORs the key part with the unique control vector(s) associated with the key type. ICSF also enciphers the key part with two master key variants for a key part. One master key variant enciphers the left half of the key part, and another master key variant enciphers the right half of the key part. ICSF creates the master key variants for a key part by exclusive ORing the master key with the control vectors for key parts. These procedures protect key separation.

| Table 111 displays the default value of the control vector that is associated with each type of key. For keys that are double-length, ICSF enciphers a unique control vector on each half. Control vectors indicated with an ″*″ are supported by the Cryptographic Coprocessor Feature.

Table 111. Control Vector Table

Key Type	Control Vector Value (Hex)
*ANSI key-encrypting key	00 00 00 00 00 00 00 00
CIPHER	00 03 71 00 03 00 00 00
CVARDEC	00 3F 42 00 03 00 00 00
CVARENC	00 3F 48 00 03 00 00 00
CVARPINE	00 3F 41 00 03 00 00 00
CVARXCVL	00 3F 44 00 03 00 00 00
CVARXCVR	00 3F 47 00 03 00 00 00
DATAC (left half)	00 00 71 00 03 41 00 00
DATAC (right half)	00 00 71 00 03 21 00 00
*Data-encrypting key	00 00 00 00 00 00 00 00
*DATAM key (left and right half) - internal	00 05 4D 00 03 00 00 00
*DATAM generation key (left half) - external	00 00 4D 00 03 41 00 00
*DATAM generation key (right half) - external	00 00 4D 00 03 21 00 00

Table 111. Control Vector Table (continued)

Key Type	**Control Vector Value (Hex)**
*DATAMV MAC verification key (left and right half) - internal	00 05 44 00 03 00 00 00
*DATAMV MAC verification key (left half) - external	00 00 44 00 03 41 00 00
*DATAMV MAC verification key (right half) - external	00 00 44 00 03 21 00 00
*Data-translation key	00 06 71 00 03 00 00 00
DECIPHER	00 03 50 00 03 00 00 00
ENCIPHER	00 03 60 00 03 00 00 00
*MAC generation key	00 05 4D 00 03 00 00 00
*MAC verification key	00 05 44 00 03 00 00 00
IKEYXLAT (left half)	00 42 42 00 03 41 00 00
IKEYXLAT (right half)	00 42 42 00 03 21 00 00
OKEYXLAT (left half)	00 41 42 00 03 41 00 00
OKEYXLAT (right half)	00 41 42 00 03 21 00 00
*Input PIN-encrypting key (left half)	00 21 5F 00 03 41 00 00
*Input PIN-encrypting key (right half)	00 21 5F 00 03 21 00 00
*Output PIN-encrypting key (left half)	00 24 77 00 03 41 00 00
*Output PIN-encrypting key (right half)	00 24 77 00 03 21 00 00
*PIN generation key (left half)	00 22 7E 00 03 41 00 00
*PIN generation key (right half)	00 22 7E 00 03 21 00 00
*PIN verification key (left half)	00 22 42 00 03 41 00 00
*PIN verification key (right half)	00 22 42 00 03 21 00 00
*Export key-encrypting key (left half)	00 41 7D 00 03 41 00 00
*Export key-encrypting key (right half)	00 41 7D 00 03 21 00 00
*Import key-encrypting key (left half)	00 42 7D 00 03 41 00 00
*Import key-encrypting key (right half)	00 42 7D 00 03 21 00 00
*Key part (left half)	00 FF 41 00 03 48 00 00
*Key part (right half)	00 FF 41 00 03 28 00 00
*Intermediate MAC	00 11 41 00 03 00 00 00
*Compatibility importer	22 22 22 22 22 22 22 22
*Compatibility exporter	88 88 88 88 88 88 88 88
*PKA importer key (left half)	00 42 05 00 03 41 00 00
*PKA importer key (right half)	00 42 05 00 03 21 00 00

Note: The external control vectors for DATAC, DATAM MAC generation and DATAMV MAC verification keys are also referred to as data compatibility control vectors.

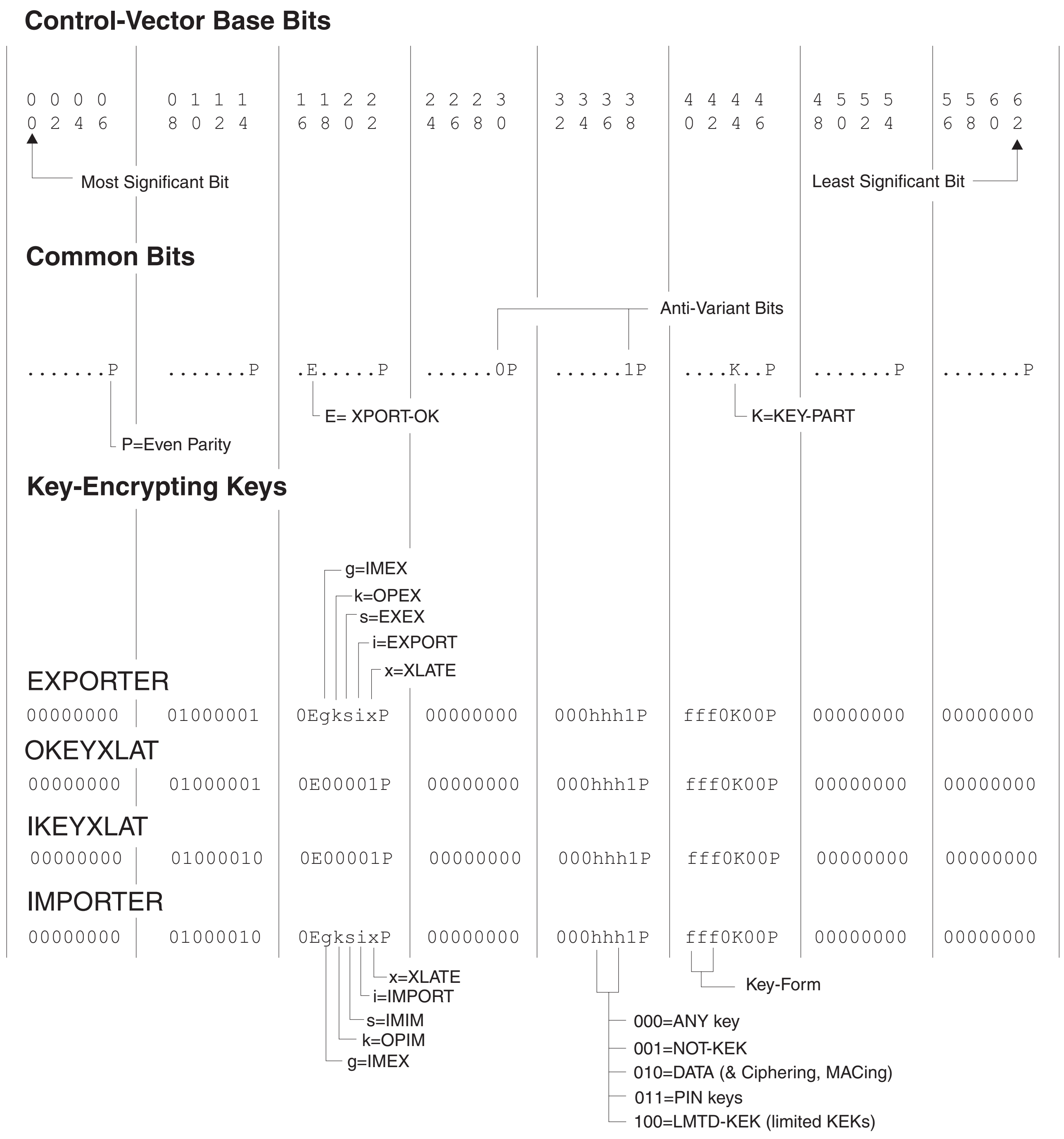


Figure 16. Control Vector Base Bit Map (Common Bits and Key-Encrypting Keys)

Control-Vector Base Bits

	0 0 0 0	0 1 1 1	1 1 2 2	2 2 2 3	3 3 3 3	4 4 4 4	4 5 5 5	5 5 6 6
	0 2 4 6	8 0 2 4	6 8 0 2	4 6 8 0	2 4 6 8	0 2 4 6	8 0 2 4	6 8 0 2
	Most Significant Bit							Least Significant Bit
Data Operation Keys								
DATA	00000000	00000000	0Eedmv0P	00000000	00000011	fff0K00P	00000000	00000000
DATAC	00000000	00000000	0E11000P	00000000	00000011	fff0K00P	00000000	00000000
DATAM	00000000	00000000	0E00110P	00000000	00000011	fff0K00P	00000000	00000000
DATAMV	00000000	00000000	0E00010P	00000000	00000011	fff0K00P	00000000	00000000
CIPHER	00000000	00000011	0E11000P	00000000	00000011	fff0K00P	00000000	00000000
DECIPHER	00000000	00000011	0E01000P	00000000	00000011	fff0K00P	00000000	00000000
ENCIPHER	00000000	00000011	0E10000P	00000000	00000011	fff0K00P	00000000	00000000
MAC	cccc0000	00000101	0E00110P	00000000	00000011	fff0K00P	00000000	00000000
MACVER	cccc0000	00000101	0E00010P	00000000	00000011	fff0K00P	00000000	00000000

cccc:
- 0000 ANY
- 0001 ANSI X9.9
- 0010 CVV KEY-A
- 0011 CVV KEY-B

fff: Key-Form

Figure 17. Control Vector Base Bit Map (Data Operation Keys)

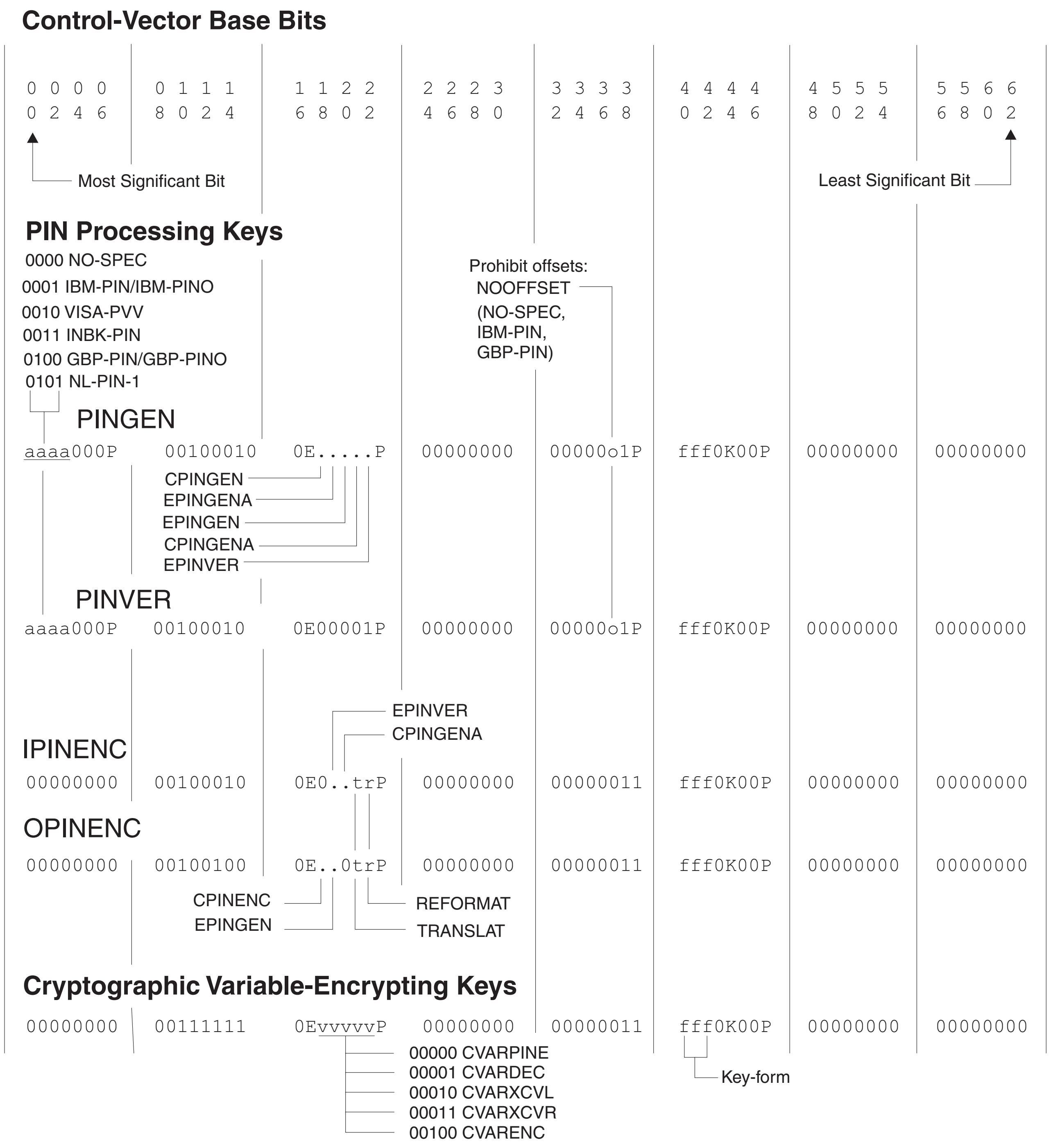


Figure 18. Control Vector Base Bit Map (PIN Processing Keys and Cryptographic Variable-Encrypting Keys)

Key Form Bits, 'fff' - The key form bits, 40-42, and for a double-length key, bits 104-106, are designated 'fff' in the preceding illustration. These bits can have these values:

000	Single length key
010	Double length key, left half
001	Double length key. right half

The following values may exist in some CCA implementations:

110	Double-length key, left half, halves guaranteed unique
101	Double-length key, right half, halves guaranteed unique

Specifying a Control-Vector-Base Value

You can determine the value of a control vector by working through the following series of questions:

1. Begin with a field of 64 bits (eight bytes) set to B'0'. The most significant bit is referred to as bit 0. Define the key type and subtype (bits 8 to 14), as follows:
   - The main key type bits (bits 8 to 11). Set bits 8 to 11 to one of the following values:

Bits 8 to 11	Main Key Type
0000	Data operation keys
0010	PIN keys
0011	Cryptographic variable-encrypting keys
0100	Key-encrypting keys
0101	Key-generating keys

   - The key subtype bits (bits 12 to 14). Set bits 12 to 14 to one of the following values:

Bits 12 to 14	Key Subtype
Data Operation Keys	
000	Compatibility key (DATA)
001	Confidentiality key (CIPHER, DECIPHER, or ENCIPHER)
010	MAC key (MAC or MACVER)
Key-Encrypting Keys	
000	Transport-sending keys (EXPORTER and OKEYXLAT)
001	Transport-receiving keys (IMPORTER and IKEYXLAT)
PIN Keys	
001	PIN-generating key (PINGEN, PINVER)
000	Inbound PIN-block decrypting key (IPINENC)
010	Outbound PIN-block encrypting key (OPINENC)
Cryptographic Variable-Encrypting Keys	
111	Cryptographic variable-encrypting key (CVAR....)

2. For key-encrypting keys, set the following bits:
   - The key-generating usage bits (gks, bits 18 to 20). Set the gks bits to B'111' to indicate that the Key Generate callable service can use the associated key-encrypting key to encipher generated keys when the Key Generate callable service is generating various key-pair key-form combinations (see the Key-Encrypting Keys section of Figure 16). Without any of the gks bits set to 1, the Key Generate callable service cannot use the associated key-encrypting key. The Key Token Build callable service can set the gks bits to 1 when you supply the **OPIM, IMEX, IMIM, OPEX**, and **EXEX** keywords.
   - The IMPORT and EXPORT bit and the XLATE bit (ix, bits 21 and 22). If the 'i' bit is set to 1, the associated key-encrypting key can be used in the Data Key

Import, Key Import, Data Key Export, and Key Export callable services. If the 'x' bit is set to 1, the associated key-encrypting key can be used in the Key Translate callable service.

- The key-form bits (fff, bits 40 to 42). The key-form bits indicate how the key was generated and how the control vector participates in multiple-enciphering. To indicate that the parts can be the same value, set these bits to B'010'. For information about the value of the key-form bits in the right half of a control vector, see Step 8.

3. For MAC and MACVER keys, set the following bits:
   - The MAC control bits (bits 20 and 21). For a MAC-generate key, set bits 20 and 21 to B'11'. For a MAC-verify key, set bits 20 and 21 to B'01'.
   - The key-form bits (fff, bits 40 to 42). For a single-length key, set the bits to B'000'. For a double-length key, set the bits to B'010'.
4. For PINGEN and PINVER keys, set the following bits:
   - The PIN calculation method bits (aaaa, bits 0 to 3). Set these bits to one of the following values:

Bits 0 to 3	Calculation Method Keyword	Description
0000	NO-SPEC	A key with this control vector can be used with any PIN calculation method.
0001	IBM-PIN or IBM-PINO	A key with this control vector can be used only with the IBM PIN or PIN Offset calculation method.
0010	VISA-PVV	A key with this control vector can be used only with the VISA-PVV calculation method.
0100	GBP-PIN or GBP-PINO	A key with this control vector can be used only with the German Banking Pool PIN or PIN Offset calculation method.
0011	INBK-PIN	A key with this control vector can be used only with the Interbank PIN calculation method.
0101	NL-PIN-1	A key with this control vector can be used only with the NL-PIN-1, Netherlands PIN calculation method.

   - The prohibit-offset bit (o, bit 37) to restrict operations to the PIN value. If set to 1, this bit prevents operation with the IBM 3624 PIN Offset calculation method and the IBM German Bank Pool PIN Offset calculation method.
5. For PINGEN, IPINENC, and OPINENC keys, set bits 18 to 22 to indicate whether the key can be used with the following callable services

Service Allowed	Bit Name	Bit
Clear PIN Generate	CPINGEN	18
Encrypted PIN Generate Alternate	EPINGENA	19
Encrypted PIN Generate	EPINGEN	20 for PINGEN 19 for OPINENC
Clear PIN Generate Alternate	CPINGENA	21 for PINGEN 20 for IPINENC

Service Allowed	Bit Name	Bit
Encrypted Pin Verify	EPINVER	19
Clear PIN Encrypt	CPINENC	18

6. For the IPINENC (inbound) and OPINENC (outbound) PIN-block ciphering keys, do the following:
   - Set the TRANSLAT bit (t, bit 21) to 1 to permit the key to be used in the PIN Translate callable service. The Control Vector Generate callable service can set the TRANSLAT bit to 1 when you supply the **TRANSLAT** keyword.
   - Set the REFORMAT bit (r, bit 22) to 1 to permit the key to be used in the PIN Translate callable service. The Control Vector Generate callable service can set the REFORMAT bit and the TRANSLAT bit to 1 when you supply the **REFORMAT** keyword.
7. For the cryptographic variable-encrypting keys (bits 18 to 22), set the variable-type bits (bits 18 to 22) to one of the following values:

Bits 18 to 22	Generic Key Type	Description
00000	CVARPINE	Used in the Encrypted PIN Generate Alternate service to encrypt a clear PIN.
00010	CVARXCVL	Used in the Control Vector Translate callable service to decrypt the left mask array.
00011	CVARXCVR	Used in the Control Vector Translate callable service to decrypt the right mask array.
00100	CVARENC	Used in the Cryptographic Variable Encipher callable service to encrypt an unformatted PIN.

8. For all keys, set the following bits:
   - The export bit (E, bit 17). If set to 0, the export bit prevents a key from being exported. By setting this bit to 0, you can prevent the receiver of a key from exporting or translating the key for use in another cryptographic subsystem. Once this bit is set to 0, it cannot be set to 1 by any service other than Control Vector Translate. The Prohibit Export callable service can reset the export bit.
   - The key-part bit (K, bit 44). Set the key-part bit to 1 in a control vector associated with a key part. When the final key part is combined with previously accumulated key parts, the key-part bit in the control vector for the final key part is set to 0. The Control Vector Generate callable service can set the key-part bit to 1 when you supply the **KEY-PART** keyword.
   - The anti-variant bits (bit 30 and bit 38). Set bit 30 to 0 and bit 38 to 1. Many cryptographic systems have implemented a system of variants where a 7-bit value is exclusive-ORed with each 7-bit group of a key-encrypting key before enciphering the target key. By setting bits 30 and 38 to opposite values, control vectors do not produce patterns that can occur in variant-based systems.
   - Control vector bits 64 to 127. If bits 40 to 42 are B'000' (single-length key), set bits 64 to 127 to 0. Otherwise, copy bits 0 to 63 into bits 64 to 127 and set bits 105 and 106 to B'01'.
   - Set the parity bits (low-order bit of each byte, bits 7, 15, ..., 127). These bits contain the parity bits (P) of the control vector. Set the parity bit of each byte so the number of zero-value bits in the byte is an even number.

Appendix L. PKA92 Key Format and Encryption Process

The PKA Symmetric Key Generate and the PKA Symmetric Key Import callable services optionally support a **PKA92** method of encrypting a DES or CDMF key with an RSA public key. This format is adapted from the IBM Transaction Security System (TSS) 4753 and 4755 product's implementation of "PKA92". The callable services do not create or accept the complete PKA92 AS key token as defined for the TSS products. Rather, the callable services only support the actual RSA-encrypted portion of a TSS PKA92 key token, the *AS External Key Block*.

Forming an External Key Block - The PKA96 implementation forms an AS External Key Block by RSA-encrypting a key block using a public key. The key block is formed by padding the key record detailed in Table 112 with zero bits on the left, high-order end of the key record. The process completes the key block with three sub-processes: masking, overwriting, and RSA encrypting.

Table 112. PKA96 Clear DES Key Record

Offset (Bytes)	Length (Bytes)	Description
Zero-bit padding to form a structure as long as the length of the public key modulus. The implementation constrains the public key modulus to a multiple of 64 bits in the range of 512 to 1024 bits. Note that government export or import regulations can impose limits on the modulus length. The maximum length is validated by a check against a value in the Function Control Vector.		
000	005	Header and flags: X'01 0000 0000'
005	016	Environment Identifier (EID), encoded in ASCII
021	008	Control vector base for the DES key
029	008	Repeat of the CV data at offset 021
037	008	The single-length DES key or the left half of a double-length DES key
045	008	The right half of a double-length DES key or a random number. This value is locally designated ″K.″
053	008	Random number, ″IV″
061	001	Ending byte, X'00'

Masking Sub-process - Create a mask by CBC encrypting a multiple of 8 bytes of binary zeros using K as the key and IV as the initialization vector as defined in the key record at offsets 45 and 53. Exclusive-OR the mask with the key record and call the result PKR.

Overwriting Sub-process - Set the high-order bits of PKR to B'01', and set the low-order bits to B'0110'.

Exclusive-OR K and IV and write the result at offset 45 in PKR.

Write IV at offset 53 in PKR. This causes the masked and overwritten PKR to have IV at its original position.

Encrypting Sub-process - RSA encrypt the overwritten PKR masked key record using the public key of the receiving node.

Recovering a Key from an External Key Block - Recover the encrypted DES key from an AS External Key Block by performing decrypting, validating, unmasking, and extraction sub-processes.

Decrypting Sub-process - RSA decrypt the AS External Key Block using an RSA private key and call the result of the decryption PKR. The private key must be usable for key management purposes.

Validating Sub-process - Verify that the high-order two bits of the PKR record are valued to B'01' and that the low-order four bits of the PKR record are valued to B'0110'.

Unmasking Sub-process - Set IV to the value of the 8 bytes at offset 53 of the PKR record. Note that there is a variable quantity of padding prior to offset 0. See Table 112 on page 421.

Set K to the exclusive-OR of IV and the value of the 8 bytes at offset 45 of the PKR record.

Create a mask that is equal in length to the PKR record by CBC encrypting a multiple of 8 bytes of binary zeros using K as the key and IV as the initialization vector. Exclusive-OR the mask with PKR and call the result the key record.

Copy K to offset 45 in the PKR record.

Extraction Sub-process. Confirm that:
- The four bytes at offset 1 in the key record are valued to X'0000 0000'
- The two control vector fields at offsets 21 and 29 are identical
- If the control vector is an IMPORTER or EXPORTER key class, that the EID in the key record is not the same as the EID stored in the cryptographic engine.

The control vector base of the recovered key is the value at offset 21. If the control vector base bits 40 to 42 are valued to B'010' or B'110', the key is double length. Set the right half of the received key's control vector equal to the left half and reverse bits 41 and 42 in the right half.

The recovered key is at offset 37 and is either 8 or 16 bytes long based on the control vector base bits 40 to 42. If these bits are valued to B'000', the key is single length. If these bits are valued to B'010' or B'110', the key is double length.

Appendix M. Changing Control Vectors with the Control Vector Translate Callable Service

Do the following when using the Control Vector Translate callable service:

- Provide the control information for testing the control vectors of the source, target, and key-encrypting keys to ensure that only sanctioned changes can be performed
- Select the key-half processing mode.

Providing the Control Information for Testing the Control Vectors

To minimize your security exposure, the Control Vector Translate callable service requires control information (*mask array* information) to limit the range of allowable control vector changes. To ensure that this service is used only for authorized purposes, the source-key control vector, target-key control vector, and key-encrypting key (KEK) control vector must pass specific tests. The tests on the control vectors are performed within the secured cryptographic engine.

The tests consist of evaluating four logic expressions, the results of which must be a string of binary zeros. The expressions operate bitwise on information that is contained in the mask arrays and in the portions of the control vectors associated with the key or key-half that is being processed. If any of the expression evaluations do not result in all zero bits, the callable service is ended with a *control vector violation* return and reason code (8/39). See Figure 19. Only the 56 bit positions that are associated with a key value are evaluated. The low-order bit that is associated with key parity in each key byte is not evaluated.

Mask Array Preparation

A mask array consists of seven 8-byte elements: A_1, B_1, A_2, B_2, A_3, B_3, and B_4. You choose the values of the array elements such that each of the following four expressions evaluates to a string of binary zeros. (See Figure 19 on page 425.) Set the **A** bits to the value that you require for the corresponding control vector bits. In expressions 1 through 3, set the **B** bits to select the control vector bits to be evaluated. In expression 4, set the **B** bits to select the source and target control vector bits to be evaluated. Also, use the following control vector information:

C_1 is the control vector associated with the left half of the KEK.

C_2 is the control vector associated with the source key, or selected source-key half/halves.

C_3 is the control vector associated with the target key or selected target-key half/halves.

1. (C_1 exclusive-OR A_1) logical-AND B_1

   This expression tests whether the KEK used to encipher the key meets your criteria for the desired translation.
2. (C_2 exclusive-OR A_2) logical-AND B_2

   This expression tests whether the control vector associated with the source key meets your criteria for the desired translation.
3. (C_3 exclusive-OR A_3) logical-AND B_3

   This expression tests whether the control vector associated with the target key meets your criteria for the desired translation.
4. (C_2 exclusive-OR C_3) logical-AND B_4

This expression tests whether the control vectors associated with the source key and the target key meet your criteria for the desired translation.

Encipher two copies of the mask array, each under a different cryptographic-variable key (key type CVARENC). To encipher each copy of the mask array, use the Cryptographic Variable Encipher callable service. Use two different keys so that the enciphered-array copies are unique values. When using the Control Vector Translate callable service, the *mask_array_left* parameter and the *mask_array_right* parameter identify the enciphered mask arrays. The *array_key_left* parameter and the *array_key_right* parameter identify the internal keys for deciphering the mask arrays. The *array_key_left* key must have a key type of CVARXCVL and the array_key_right key must have a key type of CVARXCVR. The cryptographic process deciphers the arrays and compares the results; for the service to continue, the deciphered arrays must be equal. If the results are not equal, the service returns the return and reason code for data that is not valid (8/385).

Use the Key Generate callable service to create the key pairs CVARENC-CVARXCVL and CVARENC-CVARXCVR. Each key in the key pair must be generated for a different node. The CVARENC keys are generated for, or imported into, the node where the mask array will be enciphered. After enciphering the mask array, you should destroy the enciphering key. The CVARXCVL and CVARXCVR keys are generated for, or imported into, the node where the Control Vector Translate callable service will be performed.

If using the **BOTH** keyword to process both halves of a double-length key, remember that bits 41, 42, 104, and 105 are different in the left and right halves of the CCA control vector and must be ignored in your mask-array tests (that is, make the corresponding $\mathbf{B_2}$ and/or $\mathbf{B_3}$ bits equal to zero).

When the control vectors pass the masking tests, the verb does the following:

- Deciphers the source key. In the decipher process, the service uses a key that is formed by the exclusive-OR of the KEK and the control vector in the key token variable the *source_key_token* parameter identifies.
- Enciphers the deciphered source key. In the encipher process, the service uses a key that is formed by the exclusive-OR of the KEK and the control vector in the key token variable the *target_key_token* parameter identifies.
- Places the enciphered key in the key field in the key token variable the *target_key_token* parameter identifies.

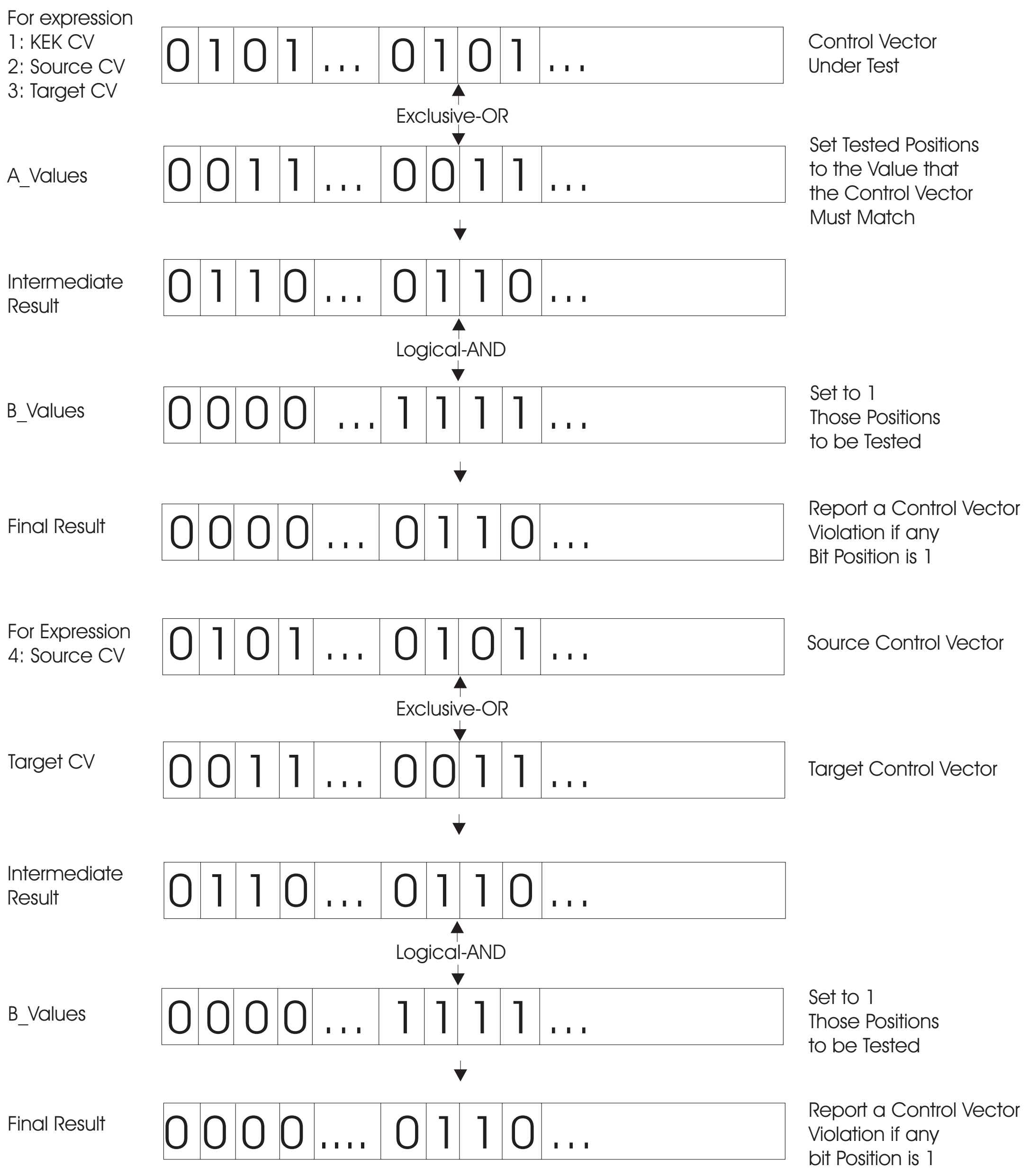


Figure 19. Control Vector Translate Callable Service Mask_Array Processing

Selecting the Key-Half Processing Mode

Use the Control Vector Translate callable service to change a control vector associated with a key. Rule-array keywords determine which key halves are processed in the call, as shown in Figure 20 on page 426.

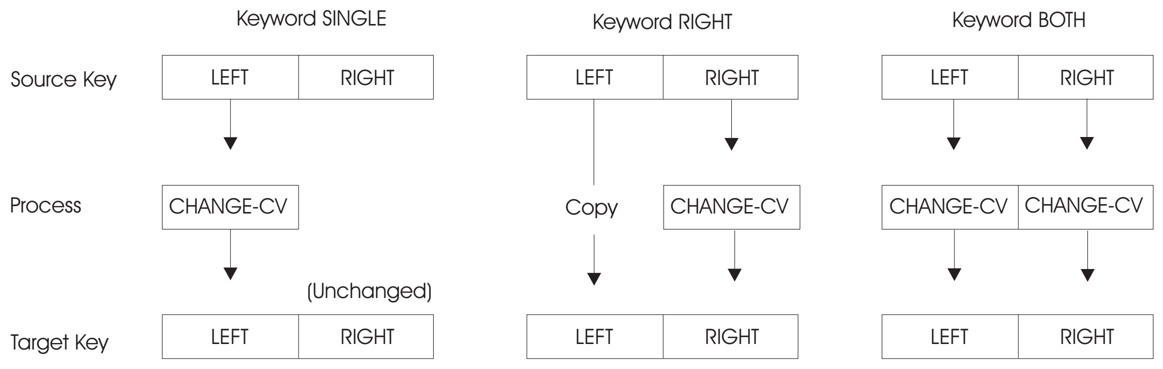


Figure 20. Control Vector Translate Callable Service.. In this figure, CHANGE-CV means the requested control vector translation change; LEFT and RIGHT mean the left and right halves of a key and its control vector.

Keyword	**Meaning**
SINGLE	This keyword causes the control vector of the left half of the source key to be changed. The updated key half is placed into the left half of the target key in the target key token. The right half of the target key is unchanged. The **SINGLE** keyword is useful when processing a single-length key, or when first processing the left half of a double-length key (to be followed by processing the right half).
RIGHT	This keyword causes the control vector of the right half of the source key to be changed. The updated key half is placed into the right half of the target key of the target key token. The left half of the source key is copied unchanged into the left half of the target key in the target key token.
BOTH	This keyword causes the control vector of both halves of the source key to be changed. The updated key is placed into the target key in the target key token. A single set of control information must permit the control vector changes applied to each key half. Normally, control vector bit positions 41, 42, 105, and 106 are different for each key half. Therefore, set bits 41 and 42 to B'00' in mask array elements B_1, B_2, and B_3. You can verify that the source and target key tokens have control vectors with matching bits in bit positions 40-42 and 104-106, the “form field” bits. Ensure that bits 40-42 of mask array B_4 are set to B'111'.
LEFT	This keyword enables you to supply a single-length key and obtain a double-length key. The source key token must contain: • The KEK-enciphered single-length key • The control vector for the single-length key (often this is a null value) • A control vector, stored in the source token where the right-half control vector is normally stored, used in decrypting the single-length source key when the key is being processed for the target right half of the key. The service first processes the source and target tokens as with the **SINGLE** keyword. Then the source token is processed using the

single-length enciphered key and the source token right-half control vector to obtain the actual key value. The key value is then enciphered using the KEK and the control vector in the target token for the right-half of the key.

This approach is frequently of use when you must obtain a double-length CCA key from a system that only supports a single-length key, for example when processing PIN keys or key-encrypting keys received from non-CCA systems.

To prevent the service from ensuring that each key byte has odd parity, you can specify the **NOADJUST** keyword. If you do not specify the **NOADJUST** keyword, or if you specify the **ADJUST** keyword, the service ensures that each byte of the target key has odd parity.

When the Target Key-Token CV Is Null

When you use any of the **LEFT**, **BOTH**, or **RIGHT** keywords, and when the control vector in the target key token is null (all B'0'), then bit 0 in byte 59 will be set to B'1' to indicate that this is a double-length DATA key.

Control Vector Translate Example

As an example, consider the case of receiving a single-length PIN-block encrypting key from a non-CCA system. Often such a key will be encrypted by an unmodified transport key (no control vector or variant is used). In a CCA system, an inbound PIN encrypting key is double-length.

First use the Key Token Build callable service to insert the single-length key value into the left-half key-space in a key token. Specify **USE-CV** as a key type and a control vector value set to 16 bytes of X'00'. Also specify **EXTERNAL**, **KEY**, and **CV** keywords in the rule array. This key token will be the source key key-token.

Second, the target key token can also be created using the Key Token Build callable service. Specify a key type of **IPINENC** and the **NO-EXPORT** rule array keyword.

Then call the Control Vector Translate callable service and specify a rule-array keyword of **LEFT**. The mask arrays can be constructed as follows:

- A_1 is set to the value of the KEK’s control vector, most likely the value of an IMPORTER key, perhaps with the NO-EXPORT bit set. B_1 is set to eight bytes of X'FF' so that all bits of the KEK’s control vector will be tested.
- A_2 is set to eight bytes of X'00', the (null) value of the source key control vector. B_2 is set to eight bytes of X'FF' so that all bits of the source-key “control vector” will be tested.
- A_3 is set to the value of the target key’s left-half control vector. B_3 is set to X'FFFF FFFF FF9F FFFF'. This will cause all bits of the control vector to be tested except for the two (“fff”) bits used to distinguish between the left-half and right-half target-key control vector.
- B_4 is set to eight bytes of X'00' so that no comparison is made between the source and target control vectors.

|

Appendix N. Notices

This information was developed for products and services offered in the USA. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
USA

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs

© Copyright IBM Corp. 1997, 2000

and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Mail Station P300
2455 South Road
Poughkeepsie, NY 12601-5400
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Programming Interface Information

This book documents intended Programming Interfaces that allow the customer to write programs to obtain the services of OS/390 Integrated Cryptographic Service Facility.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

AIX
CICS
ES/3090
ES/9000
IBM
IBMLink
Multiprise

MVS/ESA
MVS/SP
OS/390
Parallel Sysplex
Personal Security
Processor Resource/Systems Manager
PR/SM
RACF
RMF
S/370
S/390
S/390 Parallel Enterprise Server
System/390
VTAM
3090

The following terms are trademarks of other companies:

BSAFE	RSA Data Security, Incorporated
MasterCard	MasterCard International, Incorporated
Netscape	Netscape Communications Corporation
SET	SET Secure Electronic Transaction, LLC
VISA	VISA International Service Association

Other company, product, and service names may be trademarks or service marks of others.

Glossary

This glossary defines terms and abbreviations used in Integrated Cryptographic Service Facility (ICSF). If you do not find the term you are looking for, refer to the index of the appropriate Integrated Cryptographic Service Facility manual or view *IBM Dictionary of Computing* located at: http://www.ibm.com/networking/nsg/nsgmain.htm

This glossary includes terms and definitions from:

- *IBM Dictionary of Computing*. Definitions are identified by the symbol (D) after the definition.
- The *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies can be purchased from the American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Definitions are identified by the symbol (A) after the definition.
- The *Information Technology Vocabulary*, developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions of published parts of this vocabulary are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.

Definitions specific to the Integrated Cryptographic Services Facility are labeled “In ICSF.”

A

access method services (AMS). The facility used to define and reproduce VSAM key-sequenced data sets (KSDS). (D)

American National Standard Code for Information Interchange (ASCII). The standard code using a coded character set consisting of 7-bit characters (8 bits including parity check) that is used for information exchange among data processing systems, data communication systems, and associated equipment. The ASCII set consists of control characters and graphic characters.

ANSI key-encrypting key (AKEK). A 64- or 128-bit key used exclusively in ANSI X9.17 key management applications to protect data keys exchanged between systems.

ANSI X9.17. An ANSI standard that specifies algorithms and messages for DES key distribution.

ANSI X9.19. An ANSI standard that specifies an optional double-MAC procedure which requires a double-length MAC key.

application program. (1) A program written for or by a user that applies to the user’s work, such as a program that does inventory control or payroll. (2) A program used to connect and communicate with stations in a network, enabling users to perform application-oriented activities. (D)

application program interface (API). (1) A functional interface supplied by the operating system or by a separately orderable licensed program that allows an application program written in a high-level language to use specific data or functions of the operating system or the licensed program. (D) (2) In ICSF, a callable service.

asymmetric cryptography. Synonym for public key cryptography. (D)

authentication pattern. An 8-byte pattern that ICSF calculates from the master key when initializing the cryptographic key data set. ICSF places the value of the authentication pattern in the header record of the cryptographic key data set.

authorized program facility (APF). A facility that permits identification of programs authorized to use restricted functions. (D)

C

callable service. A predefined sequence of instructions invoked from an application program, using a CALL instruction. In ICSF, callable services perform cryptographic functions and utilities.

CBC. Cipher block chaining.

| **CCA.** Common Cryptographic Architecture.

| **CCF.** Cryptographic Coprocessor Feature.

CDMF. Commercial Data Masking Facility.

CEDA. A CICS transaction that defines resources online. Using CEDA, you can update both the CICS system definition data set (CSD) and the running CICS system.

checksum. (1) The sum of a group of data associated with the group and used for checking purposes. (T) (2) In ICSF, the data used is a key part. The resulting checksum is a two-digit value you enter when you use the key-entry unit to enter a master key part or a clear key part into the key-storage unit.

Chinese Remainder Theorem (CRT). A mathematical theorem that defines a format for the RSA private key that improves performance.

CICS. Customer Information Control System.

cipher block chaining (CBC). A mode of encryption that uses the data encryption algorithm and requires an initial chaining vector. For encipher, it exclusively ORs the initial block of data with the initial control vector and then enciphers it. This process results in the encryption both of the input block and of the initial control vector that it uses on the next input block as the process repeats. A comparable chaining process works for decipher.

ciphertext. (1) In computer security, text produced by encryption. (2) Synonym for enciphered data. (D)

CKDS. Cryptographic Key Data Set.

clear key. Any type of encryption key not protected by encryption under another key.

CMOS. Complementary metal oxide semiconductor.

coexistence mode. An ICSF method of operation during which CUSP or PCF can run independently and simultaneously on the same ICSF system. A CUSP or PCF application program can run on ICSF in this mode if the application program has been reassembled.

Commercial Data Masking Facility (CDMF). A data-masking algorithm using a DES-based kernel and a key that is shortened to an effective key length of 40 DES key-bits. Because CDMF is not as strong as DES, it is called a masking algorithm rather than an encryption algorithm. Implementations of CDMF, when used for data confidentiality, are generally exportable from the USA and Canada.

Common Cryptographic Architecture: Cryptographic Application Programming Interface. Defines a set of cryptographic functions, external interfaces, and a set of key management rules that provide a consistent, end-to-end cryptographic architecture across different IBM platforms.

compatibility mode. An ICSF method of operation during which a CUSP or PCF application program can run on ICSF without recompiling it. In this mode, ICSF cannot run simultaneously with CUSP or PCF.

complementary keys. A pair of keys that have the same clear key value, are different but complementary types, and usually exist on different systems.

console. A part of a computer used for communication between the operator or maintenance engineer and the computer. (A)

control-area split. In systems with VSAM, the movement of the contents of some of the control intervals in a control area to a newly created control area in order to facilitate insertion or lengthening of a data record when there are no remaining free control intervals in the original control area. (D)

control block. (1) A storage area used by a computer program to hold control information. (I) Synonymous with control area. (2) The circuitry that performs the control functions such as decoding microinstructions and generating the internal control signals that perform the operations requested. (A)

control interval. A fixed-length area of direct-access storage in which VSAM stores records and creates distributed free space. Also, in a key-sequenced data set or file, the set of records pointed to by an entry in the sequence-set index record. The control interval is the unit of information that VSAM transmits to or from direct access storage. A control interval always comprises an integral number of physical records. (D)

control interval split. In systems with VSAM, the movement of some of the stored records in a control interval to a free control interval to facilitate insertion or lengthening of a record that does not fit in the original control interval. (D)

control statement input data set. A key generator utility program data set containing control statements that a particular key generator utility program job will process.

control statement output data set. A key generator utility program data set containing control statements to create the complements of keys created by the key generator utility program.

control vector. In ICSF, a mask that is exclusive ORed with a master key or a transport key before ICSF uses that key to encrypt another key. Control vectors ensure that keys used on the system and keys distributed to other systems are used for only the cryptographic functions for which they were intended.

cross memory mode. Synchronous communication between programs in different address spaces that permits a program residing in one address space to access the same or other address spaces. This synchronous transfer of control is accomplished by a calling linkage and a return linkage.

CRT. Chinese Remainder Theorem.

cryptographic adapter (4755 or 4758). An expansion board that provides a comprehensive set of cryptographic functions for the network security processor and the workstation in the TSS family of products.

| **cryptographic coprocessor.** A microprocessor that adds cryptographic processing functions to specific S/390 G3, or higher, Enterprise Servers and S/390 Multiprise Servers and higher processors. The Cryptographic Coprocessor Feature is a tamper-resistant chip built into the processor board. The combination of the Cryptographic Coprocessor Feature and ICSF Version 2 Release 1, or higher, provides secure high-speed cryptographic services in the OS/390 environment.

cryptographic key data set (CKDS). (1) A data set that contains the encrypting keys used by an installation. (D) (2) In ICSF, a VSAM data set that contains all the cryptographic keys. Besides the encrypted key value, an entry in the cryptographic key data set contains information about the key.

cryptography. (1) The transformation of data to conceal its meaning. (2) In computer security, the principles, means, and methods for encrypting plaintext and decrypting ciphertext. (D) (3) In ICSF, the use of cryptography is extended to include the generation and verification of MACs, the generation of MDCs and other one-way hashes, the generation and verification of PINs, and the generation and verification of digital signatures.

CUSP (Cryptographic Unit Support Program). The IBM cryptographic offering, program product 5740-XY6, using the channel-attached 3848.

CUSP/PCF conversion program. A program, for use during migration from CUSP or PCF to ICSF, that converts a CUSP or PCF cryptographic key data set into a ICSF cryptographic key data set.

Customer Information Control System (CICS). An IBM licensed program that enables transactions entered at remote terminals to be processed concurrently by user written application programs. It includes facilities for building, using, and maintaining databases.

CVC. Card verification code used by MasterCard.

CVV. Card verification value used by VISA.

D

data encryption algorithm (DEA). In computer security, a 64-bit block cipher that uses a 64-bit key, of which 56 bits are used to control the cryptographic process and 8 bits are used for parity checking to ensure that the key is transmitted properly. (D)

data encryption standard (DES). In computer security, the National Institute of Standards and Technology (NIST) Data Encryption Standard, adopted by the U.S. government as Federal Information Processing Standard (FIPS) Publication 46, which allows only hardware implementations of the data encryption algorithm. (D)

data key or data-encrypting key. (1) A key used to encipher, decipher, or authenticate data. (D) (2) In ICSF, a 64-bit encryption key used to protect data privacy using the DES algorithm or the CDMF algorithm.

data set. The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access. (D)

data-translation key. A 64-bit key that protects data transmitted through intermediate systems when the originator and receiver do not share the same key.

DEA. Data encryption algorithm.

decipher. (1) To convert enciphered data in order to restore the original data. (T) (2) In computer security, to convert ciphertext into plaintext by means of a cipher system. (3) To convert enciphered data into clear data. Contrast with encipher. Synonymous with decrypt. (D)

decode. (1) To convert data by reversing the effect of some previous encoding. (I) (A) (2) In ICSF, to decipher data by use of a clear key.

decrypt. See decipher.

DES. Data Encryption Standard.

diagnostics data set. A key generator utility program data set containing a copy of each input control statement followed by a diagnostic message generated for each control statement.

digital signature. In public key cryptography, information created by using a private key and verified by using a public key. A digital signature provides data integrity and source nonrepudiation.

| **Digital Signature Standard (DSS).** A standard describing the use of algoritms for digital signature purposes. The algorithm specified is DSA (Digital Signature Algorithm).

domain. (1) That part of a network in which the data processing resources are under common control. (T) (2) In ICSF, an index into a set of master key registers.

double-length key. A key that is 128 bits long. A key can be either double- or single-length. A single-length key is 64 bits long.

| **DSA.** Digital Signature Algorithm.

DSS. Digital Signature Standard.

E

ECB. Electronic codebook.

ECI. Eurochèque International S.C., a financial institution consortium that has defined three PIN block formats.

| **EID.** Environment Identification.

electronic codebook (ECB) operation. (1) A mode of operation used with block cipher cryptographic algorithms in which plaintext or ciphertext is placed in the input to the algorithm and the result is contained in the output of the algorithm. (D) (2) A mode of encryption using the data encryption algorithm, in which each block of data is enciphered or deciphered without an initial chaining vector. It is used for key management functions and the encode and decode callable services.

electronic funds transfer system (EFTS). A computerized payment and withdrawal system used to transfer funds from one account to another and to obtain related financial data. (D)

encipher. (1) To scramble data or to convert data to a secret code that masks the meaning of the data to any unauthorized recipient. Synonymous with encrypt. (2) Contrast with decipher. (D)

enciphered data. Data whose meaning is concealed from unauthorized users or observers. (D)

encode. (1) To convert data by the use of a code in such a manner that reconversion to the original form is possible. (T) (2) In computer security, to convert plaintext into an unintelligible form by means of a code system. (D) (3) In ICSF, to encipher data by use of a clear key.

encrypt. See encipher.

exit. (1) To execute an instruction within a portion of a computer program in order to terminate the execution of that portion. Such portions of computer programs include loops, subroutines, modules, and so on. (T) (2) In ICSF, a user-written routine that receives control from the system during a certain point in processing—for example, after an operator issues the START command.

exportable form. A condition a key is in when enciphered under an exporter key-encrypting key. In this form, a key can be sent outside the system to another system. A key in exportable form cannot be used in a cryptographic function.

exporter key-encrypting key. A 128-bit key used to protect keys sent to another system. A type of transport key.

F

file. A named set of records stored or processed as a unit. (T)

G

GBP. German Bank Pool.

German Bank Pool (GBP). A German financial institution consortium that defines specific methods of PIN calculation.

H

hashing. An operation that uses a one-way (irreversible) function on data, usually to reduce the length of the data and to provide a verifiable authentication value (checksum) for the hashed data.

header record. A record containing common, constant, or identifying information for a group of records that follows. (D)

I

ICSF. Integrated Cryptographic Service Facility.

importable form. A condition a key is in when it is enciphered under an importer key-encrypting key. A key is received from another system in this form. A key in importable form cannot be used in a cryptographic function.

importer key-encrypting key. A 128-bit key used to protect keys received from another system. A type of transport key.

initial chaining vector (ICV). A 64-bit random or pseudo-random value used in the cipher block chaining mode of encryption with the data encryption algorithm.

initial program load (IPL). (1) The initialization procedure that causes an operating system to commence operation. (2) The process by which a configuration image is loaded into storage at the beginning of a work day or after a system malfunction. (3) The process of loading system programs and preparing a system to run jobs. (D)

input PIN-encrypting key. A 128-bit key used to protect a PIN block sent to another system or to translate a PIN block from one format to another.

installation exit. See exit.

Integrated Cryptographic Service Facility (ICSF). A licensed program that runs under MVS/System Product 3.1.3, or higher, or OS/390 Release 1, or higher, and provides access to the hardware cryptographic feature for programming applications. The combination of the hardware cryptographic feature and ICSF provides secure high-speed cryptographic services.

International Organization for Standardization. An organization of national standards bodies from many countries, established to promote the development of standards to facilitate the international exchange of goods and services and to develop cooperation in intellectual, scientific, technological, and economic activity. ISO has defined certain standards relating to cryptography and has defined two PIN block formats.

ISO. International Organization for Standardization.

J

job control language (JCL). A control language used to identify a job to an operating system and to describe the job's requirements. (D)

K

key-encrypting key (KEK). (1) In computer security, a key used for encryption and decryption of other keys. (D) (2) In ICSF, a master key or transport key.

key generator utility program (KGUP). A program that processes control statements for generating and maintaining keys in the cryptographic key data set.

key output data set. A key generator utility program data set containing information about each key that the key generator utility program generates except an importer key for file encryption.

key part. A 32-digit hexadecimal value that you enter for ICSF to combine with other values to create a master key or clear key.

key part register. A register in the key storage unit that stores a key part while you enter the key part.

L

linkage. The coding that passes control and parameters between two routines.

load module. All or part of a computer program in a form suitable for loading into main storage for execution. A load module is usually the output of a linkage editor. (T)

LPAR mode. The central processor mode that enables the operator to allocate the hardware resources among several logical partitions.

M

MAC generation key. A 64-bit or 128-bit key used by a message originator to generate a message authentication code sent with the message to the message receiver.

MAC verification key. A 64-bit or 128-bit key used by a message receiver to verify a message authentication code received with a message.

magnetic tape. A tape with a magnetizable layer on which data can be stored. (T)

master key. (1) In computer security, the top-level key
| in a hierarchy of key-encrypting keys. (2) In ICSF, there
| are three types of master keys on the Cryptographic
| Coprocessor Feature: the 128-bit DES master key, the
| 192-bit signature master key, and the 192-bit key
| management master key. On the PCI Cryptographic
| Coprocessor there are two types of master keys: the
| 192-bit Symmetric master key and the 192-bit
| Asymmetric master key. Master keys are known only to
| the ICSF hardware and maintained in the cryptographic
| enclosure in a secure fashion. All keys in operational
| form in the system are enciphered under a master key.
| Master keys are used only to encrypt other keys.

master key concept. The idea of using a single cryptographic key, the master key, to encrypt all other keys on the system.

master key register. A register in the Cryptographic Coprocessor Feature that stores the master key that is active on the system.

master key variant. A key derived from the master key by use of a control vector. It is used to force separation by type of keys on the system.

MD4. Message Digest 4. A hash algorithm.

MD5. Message Digest 5. A hash algorithm.

message authentication code (MAC). (1) The cryptographic result of block cipher operations on text or data using the cipher block chain (CBC) mode of operation. (D) (2) In ICSF, a MAC is used to authenticate the source of the message, and verify that the message was not altered during transmission or storage.

modification detection code (MDC). (1) A 128-bit value that interrelates all bits of a data stream so that the modification of any bit in the data stream results in a new MDC. (2) In ICSF, an MDC is used to verify that a message or stored data has not been altered.

multiple encipherment. The method of encrypting a key under a double-length key-encrypting key.

N

new master key register. A register in the key storage unit that stores a master key before you make it active on the system.

NIST. U.S. National Institute of Science and Technology.

NOCV processing. Process by which the key generator utility program or an application program encrypts a key under a transport key itself rather than a transport key variant.

noncompatibility mode. An ICSF method of operation during which CUSP or PCF can run independently and simultaneously on the same OS/390 or MVS system. You cannot run a CUSP or PCF application program on ICSF in this mode.

nonrepudiation. A method of ensuring that a message was sent by the appropriate individual.

notarization. The ANSI X9.17 process involving the coupling of an ANSI key-encrypting key (AKEK) with ASCII character strings containing origin and destination identifiers and then exclusive ORing (or offsetting) the result with a binary counter.

O

OAEP. Optimal asymmetric encryption padding.

offset. The process of exclusively ORing a counter to a key.

old master key register. A register in the key storage unit that stores a master key that you replaced with a new master key.

operational form. The condition of a key when it is encrypted under the master key so that it is active on the system.

output PIN-encrypting key. A 128-bit key used to protect a PIN block received from another system or to translate a PIN block from one format to another.

P

PAN. Personal Account Number.

parameter. Data passed between programs or procedures. (D)

parmlib. A system parameter library, either SYS1.PARMLIB or an installation-supplied library.

partial notarization. The ANSI X9.17 standard does not use the term partial notarization. IBM has divided the notarization process into two steps and defined the term partial notarization as a process during which only the first step of the two-step ANSI X9.17 notarization process is performed. This step involves the coupling of an ANSI key-encrypting key (AKEK) with ASCII character strings containing origin and destination identifiers.

partitioned data set (PDS). A data set in direct access storage that is divided into partitions, called members, each of which can contain a program, part of a program, or data. (D)

Personal Account Number (PAN). A Personal Account Number identifies an individual and relates that individual to an account at a financial institution. It consists of an issuer identification number, customer account number, and one check digit.

| **PCI Cryptographic Coprocessor.** The 4758 model 2
| standard PCI-bus card supported on the field upgraded
| IBM S/390 Parallel Enterprise Server - Generation 5
| and the IBM S/390 Parallel Enterprise Server -
| Generation 6.

PCICC. PCI Cryptographic Coprocessor.

personal identification number (PIN). The 4- to 12-digit number entered at an automatic teller machine to identify and validate the requester of an automatic teller machine service. Personal identification numbers are always enciphered at the device where they are entered, and are manipulated in a secure fashion.

Personal Security card. An ISO-standard “smart card” with a microprocessor that enables it to perform a variety of functions such as identifying and verifying users, and determining which functions each user can perform.

PIN block. A 64-bit block of data in a certain PIN block format. A PIN block contains both a PIN and other data.

PIN generation key. A 128-bit key used to generate PINs or PIN offsets algorithmically.

PIN key. A 128-bit key used in cryptographic functions to generate, transform, and verify the personal identification numbers.

PIN offset. For 3624, the difference between a customer-selected PIN and an institution-assigned PIN. For German Bank Pool, the difference between an institution PIN (generated with an institution PIN key) and a pool PIN (generated with a pool PIN key).

PIN verification key. A 128-bit key used to verify PINs algorithmically.

PKA. Public Key Algorithm.

PKCS. Public Key Cryptographic Standards (RSA Data Security, Inc.)

PKDS. Public key data set (PKA cryptographic key data set).

plaintext. Data in normal, readable form.

primary space allocation. An area of direct access storage space initially allocated to a particular data set or file when the data set or file is defined. See also secondary space allocation. (D)

private key. In computer security, a key that is known only to the owner and used with a public key algorithm to decrypt data or generate digital signatures. The data is encrypted and the digital signature is verified using the related public key.

processor complex. A configuration that consists of all the machines required for operation.

Processor Resource/Systems Manager. Enables logical partitioning of the processor complex, may provide additional byte-multiplexer channel capability, and supports the VM/XA System Product enhancement for Multiple Preferred Guests.

Programmed Cryptographic Facility (PCF). (1) An IBM licensed program that provides facilities for enciphering and deciphering data and for creating, maintaining, and managing cryptographic keys. (D) (2) The IBM cryptographic offering, program product 5740-XY5, using software only for encryption and decryption.

PR/SM. Processor Resource/Systems Manager.

public key. In computer security, a key made available to anyone who wants to encrypt information using the public key algorithm or verify a digital signature generated with the related private key. The encrypted data can be decrypted only by use of the related private key.

public key algorithm (PKA). In computer security, an asymmetric cryptographic process in which a public key is used for encryption and digital signature verification and a private key is used for decryption and digital signature generation.

public key cryptography. In computer security, cryptography in which a public key is used for encryption and a private key is used for decryption. Synonymous with asymmetric cryptography.

R

RDO. Resource definition online.

record chaining. When there are multiple cipher requests and the output chaining vector (OCV) from the previous encipher request is used as the input chaining vector (ICV) for the next encipher request.

Resource Access Control Facility (RACF). An IBM licensed program that provides for access control by identifying and verifying the users to the system, authorizing access to protected resources, logging the detected unauthorized attempts to enter the system, and logging the detected accesses to protected resources. (D)

retained key. A private key that is generated and retained within the secure boundary of the PCI Cryptographic Coprocessor.

return code. (1) A code used to influence the execution of succeeding instructions. (A) (2) A value returned to a program to indicate the results of an operation requested by that program. (D)

Rivest-Shamir-Adleman (RSA) algorithm. A process for public key cryptography that was developed by R. Rivest, A. Shamir, and L. Adleman.

RMI. Resource Manager Interface (CICS).

RSA. Rivest-Shamir-Adleman.

S

| **SAF.** Security Authorization Facility.

save area. Area of main storage in which contents of registers are saved. (A)

secondary space allocation. In systems with VSAM, area of direct access storage space allocated after primary space originally allocated is exhausted. See also primary space allocation. (D)

Secure Electronic Transaction. A standard created by Visa International and MasterCard for safe-guarding payment card purchases made over open networks.

Secure Sockets Layer. A security protocol that provides communications privacy over the Internet by allowing client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

sequential data set. A data set whose records are organized on the basis of their successive physical positions, such as on magnetic tape. (D)

SET. Secure Electronic Transaction.

SHA-1. Secure Hash Algorithm 1, a hash algorithm required for use with the Digital Signature Standard.

single-length key. A key that is 64 bits long. A key can be single- or double-length. A double-length key is 128 bits long.

special secure mode. An alternative form of security that allows you to enter clear keys with the key generator utility program or generate clear PINs.

SSL. Secure Sockets Layer.

supervisor state. A state during which a processing unit can execute input/output and other privileged instructions. (D)

System Authorization Facility (SAF). An interface to a system security system like the Resource Access Control Facility (RACF).

system key. A key that ICSF creates and uses for internal processing.

System Management Facilities (SMF). An optional control program feature of OS/VS that provides the means for gathering and recording information that can be used to evaluate system usage. (D)

T

| **TDEA.** Triple Data Encryption Algorithm.

TKE. Trusted key entry.

Transaction Security System. An IBM product offering including both hardware and supporting software that provides access control and basic cryptographic key-management functions in a network environment. In the workstation environment, this includes the 4755 Cryptographic Adapter, the Personal Security Card, the 4754 Security Interface Unit, the Signature Verification feature, the Workstation Security Services Program, and the AIX Security Services Program/6000. In the host environment, this includes the 4753 Network Security Processor and the 4753 Network Security Processor MVS Support Program.

transport key. A 128-bit key used to protect keys distributed from one system to another. A transport key can either be an exporter key-encrypting key, an importer key-encrypting key, or an ANSI key-encrypting key.

transport key variant. A key derived from a transport key by use of a control vector. It is used to force separation by type for keys sent between systems.

TRUE. Task-related User Exit (CICS). The CICS-ICSF Attachment Facility provides a CSFATRUE and CSFATREN routine.

U

| **UAT.** UDX Authority Table.

UDF. User-defined function.

UDK. User-derived key.

| **UDP.** User Developed Program.

| **UDX.** User Defined Extension.

V

verification pattern. An 8-byte pattern that ICSF calculates from the key parts you enter when you enter a master key or clear key. You can use the verification pattern to verify that you have entered the key parts correctly and specified a certain type of key.

Virtual Storage Access Method (VSAM). (1) An IBM licensed program that controls communication and the flow of data in an SNA network. It provides single-domain, multiple-domain, and interconnected network capability. (D) (2) An access method for indexed or sequential processing of fixed and variable-length records on direct-access devices. The records in a VSAM data set or file can be organized in logical sequence by means of a key field (key sequence), in the physical sequence in which they are written on the data set or file (entry-sequence), or by means of relative-record number.

VISA. A financial institution consortium that has defined four PIN block formats and a method for PIN verification.

VISA PIN Verification Value (VISA PVV). An input to the VISA PIN verification process that, in practice, works similarly to a PIN offset.

Numerics

3621. A model of an IBM Automatic Teller Machine that has a defined PIN block format.

3624. A model of an IBM Automatic Teller Machine that has a defined PIN block format and methods of PIN calculation.

| **4753.** The Network Security processor. The IBM 4753
| is a processor that uses the Data Encryption Algorithm
| and the RSA algorithm to provide cryptograpic support
| for systems requiring secure transaction processing
| (and other cryptographic services) at the host computer.
| The NSP includes a 4755 cryptographic adapter in a
| workstation which is channel attached to a S/390 host
| computer.

| **4758.** The IBM PCI Cryptographic processor provides
| a secure programming and hardware environment
| where DES and RSA processes are performed.

Index

Numerics

3621 PIN block format 173, 360
3624 PIN block format 173, 360
4700-PAD processing rule 127, 133
4704-EPP PIN block format 173

A

accessing
  callable service 29
  invocation requirements 29
affinity (IEAAFFN callable service) 29
AKEK key type 8
ALET (alternate entry point)
  format 24
algorithm 16
  3624 PIN generation 362
  3624 PIN verification 365
  DES 3, 16
  GBP-PIN 193
  GBP PIN generation 363
  GBP PIN verification 367
  GBP-PINO 193
  IBM-PIN 193
  IBM-PINO 193
  PIN, detailed 362
  PIN, general 19
  PIN offset generation 364
  PVV generation 370
  PVV verification 371
  VISA PIN 370
  VISA-PVV 189, 193
ANSI 9.9-1 algorithm 145
ANSI key-encrypting key (AKEK) 8
ANSI X3.106 processing rule 355
ANSI X9.17 EDC generate callable service (CSNAEGN)
  format 103
  overview 15
  parameters 103
  syntax 103
ANSI X9.17 key-encrypting key 7
ANSI X9.17 key export callable service (CSNAKEX)
  format 105
  overview 15
  parameters 105
  syntax 105
ANSI X9.17 key import callable service (CSNAKIM)
  format 110
  overview 15
  parameters 110
  syntax 110
ANSI X9.17 key management 103
  overview 14
ANSI X9.17 key translate callable service (CSNAKTR)
  format 114
  overview 15
  parameters 114
  syntax 114
ANSI X9.17 transport key partial notarize callable service (CSNATKN)
  overview 16
ANSI X9.17 transport key partial notorize (CSNATKN)
  format 119
  parameters 119
  syntax 119
ANSI X9.19 optional double MAC procedure 145
ANSI X9.23 processing rule 122, 127, 133, 355
ANSI X9.8 202
ANSI X9.8 PIN block format 359
ASCII to EBCDIC conversion
  table 403
authenticating messages 145

C

c-variable encrypting key identifier parameter
  cryptographic variable encipher callable service 212
call
  successful 45
  unsuccessful 46
callable service
  ANSI X9.17 EDC generate (CSNAEGN) 15, 103
  ANSI X9.17 key export (CSNAKEX) 15, 105
  ANSI X9.17 key import (CSNAKIM) 15, 110
  ANSI X9.17 key translate (CSNAKTR) 15, 114
  ANSI X9.17 transport key partial notarize (CSNATKN) 16
  ANSI X9.17 transport key partial notorize (CSNATKN) 119
  character/nibble conversion (CSNBXBC and CSNBXCB) 220
  ciphertext 44
  ciphertext translate (CSNBCTT or CSNBCTT1) 141
  clear key import (CSNBCKI) 11, 49
  clear PIN encrypt (CSNBCPE) 20, 183
  clear PIN generate (CSNBPGN) 20, 175
  clear PIN generate alternate (CSNBCPA) 20, 186
  code conversion (CSNBXAE) 21
  code conversion (CSNBXBC) 22
  code conversion (CSNBXCB) 22
  code conversion (CSNBXEA) 21
  code conversion (CSNBXEA and CSNBXAE) 218
  coding examples 343
    Assembler H 347
    C 343
    COBOL 345
    PL/1 349
  control vector generate (CSNBCVG) 21, 213
  control vector translate callable service (CSNBCVT) 21, 215
  cryptographic variable encipher (CSNBCVE) 21, 211
  CSFxxxx format 23
  CSNBxxxx format 23
  data key export (CSNBDKX) 11, 54
  data key import (CSNBDKM) 11, 53

callable service *(continued)*
  decipher (CSNBDEC or CSNBDEC1) 130
  decode (CSNBDCO) 137
  definition 3, 23
  digital signature generate (CSNDDSG) 235, 247
  digital signature verify (CSNDDSV) 235, 251
  encipher (CSNBENC or CSNBENC1) 123
  encode (CSNBECO) 135
  encrypted PIN generate (CSNBEPG) 20, 179
  encrypted PIN translate (CSNBPTR) 20, 197
  encrypted PIN verification (CSNBPVR) 20, 191
  format 225, 229
  IEAAFFN (affinity) 29
  installation-defined 3
  invoking a 23
  key export (CSNBKEX) 11, 56
  key generate (CSNBKGN) 10, 40, 48, 63
  key import (CSNBKIM) 11, 74
  key part import (CSNBKPI) 11, 79
  key record create (CSNBKRC) 12, 92
  key record delete (CSNBKRD) 13, 93
  key record read (CSNBKRR) 13, 95
  key record write (CSNBKRW) 12, 96
  key test (CSNBKYT and CSNBKYTX) 12, 88
  key token build (CSNBKTB) 21, 203
  key translate (CSNBKTR) 10, 73
  link edit step 38
  MAC generation (CSNBMGN or CSNBMGN1) 17, 147
  MAC verification (CSNBMVR or CSNBMVR1) 18, 152
  MDC generation (CSNBMDG or CSNBMDG1) 18, 156
  multiple clear key import (CSNBCKM) 11, 50
  multiple secure key import (CSNBSKM) 12, 84
  non-key management 36
  one-way hash generate (CSNBOWH and CSNBOWH1) 18, 160
  overview 23
  PCI interface (CSFPCI) 225
  PKA decrypt (CSNDPKD) 238
  PKA encrypt (CSNDPKE) 238
  PKA key generate (CSNDPKG) 235, 297
  PKA key import (CSNDPKI) 235, 300
  PKA key token build (CSNDPKB) 238, 287
  PKA public key extract (CSNDPKX) 236, 303
  PKDS record create (CSNDKRC) 305
  PKDS record delete (CSNDKRD) 310
  PKDS record read (CSNDKRR) 308
  PKDS record write (CSNDKRW) 306
  PKSC interface (CSFPKSC) 229
  prohibit export (CSNBPEX) 11, 60
  prohibit export extended (CSNBPEXX) 11, 48, 62
  random number generate (CSNBRNG) 16, 139
  retained key delete (CSNDRKD) 314
  retained key list (CSNDRKL) 312
  secure key import (CSNBSKI) 11, 81
  security considerations 29
  sequences 38
  SET block compose (CSNDSBC) 238, 267
  SET block decompose (CSNDSBD) 238, 272

callable service *(continued)*
  symmetric key export (CSNDSYX) 237, 262
  symmetric key generate (CSNDSYG) 237, 255
  symmetric key import (CSNDSYI) 237, 259
  syntax 23
  transform CDMF key (CSNBTCK) 14, 97
  translating ciphertext 16
  User derived key (CSFUDK) 99
  using key types and key forms 35
  VISA CVV service generate (CSNBCSG) 163
  VISA CVV service verify (CSNBCSV) 166
  with ALETs (alternate entry point) 24
  X9.9 data editing (CSNB9ED) 22, 222
CBC processing rule 122, 127, 133
CDMF
  overview 13
CDMF key, transforming
  algorithm 373
  callable service 97
chaining vector length parameter
  one-way hash generate callable service 162
chaining vector parameter
  decipher callable service 134
  encipher callable service 128
  MAC generation callable service 150
  MAC verification callable service 155
  MDC generation callable service 159
  one-way hash generate callable service 162
changing control vectors 423
character/nibble conversion callable service (CSNBXBC and CSNBXCB)
  format 220
  parameters 220
  syntax 220
character/nibble conversion callable services (CSNBXBC and CSNBXCB)
  overview 22
choosing between
  CSNBCTT and CSNBCTT1 141
  CSNBDEC and CSNBDEC1 131
  CSNBENC and CSNBENC1 124
  CSNBMDG and CSNBMDG1 156
  CSNBMGN and CSNBMGN1 148
  CSNBMVR and CSNBMVR1 152
cipher block chaining (CBC) 121
ciphertext
  cryptographic variable encipher callable service 213
  deciphering 16, 121
  encoding 135
  field 129, 135
  translating 16, 141
ciphertext id parameter
  decipher callable service 135
  encipher callable service 129
ciphertext parameter
  decipher callable service 133
  decode callable service 138
  encipher callable service 129
  encode callable service 137

ciphertext translate callable service (CSNBCTT or CSNBCTT1)
  format 141
  parameters 142
  syntax 141
  using 44
clear key
  deciphering data with 137
  definition 8
  enciphering 81
  enciphering data with 135
  encoding and decoding data with 16
  protecting 121
clear key import callable service (CSNBCKI)
  format 49
  overview 11
  parameters 49
  syntax 49
clear key length parameter
  multiple clear key import callable service 52, 86
clear key parameter
  clear key import callable service 50
  decode callable service 138
  encode callable service 136
  multiple clear key import callable service 52, 86
  secure key import callable service 82
clear PIN encrypt callable service (CSNBCPE)
  format 183
  syntax 183
clear PIN encrypt service (CSNBCPE)
  parameters 183
clear PIN generate alternate callable service (CSNBCPA)
  format 186
  overview 20
  parameters 186
  syntax 186
clear PIN generate callable service (CSNBPGN)
  format 176
  parameters 176
  syntax 176
clear PIN generate key identifier parameter 187
  clear PIN generate callable service 176
clear text id parameter
  decipher callable service 135
  encipher callable service 129
clear text parameter
  decipher callable service 135
  decode callable service 138
  encipher callable service 126
  encode callable service 137
code conversion callable service (CSNBXEA and CSNBXAE)
  format 218
  parameters 218
  syntax 218
code conversion callable services (CSNBXEA and CSNBXAE)
  overview 21
code table parameter
  character/nibble conversion callable service 222
code table parameter *(continued)*
  code conversion callable service 220
coding examples 343
  Assembler H 347
  C 343
  COBOL 345
  PL/1 349
Commercial Data Masking Facility (CDMF) 121
control information
  for digital signature generate 249
  for digital signature verify 252
  for key test 90
  for key token build 206
  for MAC generation 150
  for MAC verification 154
  for MDC generation 159
  for multiple clear key import 52
  for multiple secure key import 86
  for one-way hash generate 162
  for PKA key token build 288
  for symmetric key generate 256
  for symmetric key import 260
  for user derived key 101
control vector
  description 413
  value 413
control vector, description of 4, 5
control vector generate (CSNBCVG)
  parameters 214
control vector generate callable service (CSNBCVG)
  format 213
  overview 21
  syntax 213
control vector parameter
  control vector generate callable service 215
control vector translate callable service (CSNBCVT)
  format 216
  overview 21
  parameters 216
  syntax 216
control vectors, changing 423
cryptographic feature
  description xxi
cryptographic key data set (CKDS)
  held keys 7
  storing keys 10, 12, 47
cryptographic variable encipher (CSNBCVE)
  parameters 212
cryptographic variable encipher callable service (CSNBCVE)
  format 212
  overview 21
  syntax 212
CSFPCI callable service 225
CSFPKSC callable service 229
CSFUDK callable service 99
CSFxxxx format 23
CSNAEGN callable service 103
CSNAKEX callable service 105, 110
CSNAKTR callable service 114
CSNATKN callable service 119

CSNB9ED callable service 222
CSNBCKI callable service 49
CSNBCKM callable service 50
CSNBCPA callable service 186
CSNBCPE callable service 183
CSNBCSG callable service 163
CSNBCSV callable service 166
CSNBCTT or CSNBCTT1 callable service 141
CSNBCVE callable service 211
CSNBCVG callable service 213
CSNBCVT callable service 215
CSNBDCO callable service 137
CSNBDEC or CSNBDEC1 callable service 130
CSNBDKM callable service 53
CSNBDKX callable service 54
CSNBECO callable service 135
CSNBENC or CSNBENC1 callable service 123
CSNBEPG callable service 179
CSNBKEX callable service 56
CSNBKGN callable service 63
CSNBKIM callable service 74
CSNBKPI callable service 79
CSNBKRC callable service 92
CSNBKRD callable service 93
CSNBKRR callable service 95
CSNBKRW callable service 96
CSNBKTB callable service 203
CSNBKTR callable service 73
CSNBKYT callable service 88
CSNBKYTX callable service 88
CSNBMDG or CSNBMDG1 callable service 156
CSNBMGN or CSNBMGN1 callable service 147
CSNBMVR or CSNBMVR1 callable service 152
CSNBOWH and CSNBOWH1 callable services 160
CSNBPEX callable service 60
CSNBPEXX callable service 62
CSNBPGN callable service 175
CSNBPTR callable service 197
CSNBPVR callable service 191
CSNBRNG callable service 139
CSNBSKI callable service 81
CSNBSKM callable service 84
CSNBTCK callable service 97
CSNBXAE callable service 218
CSNBXBC callable service 220
CSNBXCB callable service 220
CSNBXEA callable service 218
CSNBxxxx format 23
CSNDDSG callable service 247
CSNDDSV callable service 251
CSNDKRC callable service 305
CSNDKRD callable service 310
CSNDKRR callable service 308
CSNDKRW callable service 306
CSNDPKB callable service 287
CSNDPKD callable service 282
CSNDPKE callable service 279
CSNDPKG callable service 297
CSNDPKI callable service 300
CSNDPKX callable service 303
CSNDRKD callable service 314
CSNDRKL callable service 312
CSNDSBC callable service 267
CSNDSBD callable service 272
CSNDSYG callable service 255
CSNDSYI callable service 259
CSNDSYX callable service 262
CUSP/IPS processing rule 122
CUSP/PCF
  key separation 4
  keys 6
  macros 26
  migration consideration 26
CUSP processing rule 127, 133, 356

D

data
  deciphering 130
  enciphering 123
  enciphering and deciphering 16
  encoding and decoding 16
  length, determining 124
  protecting 121
data array parameter
  clear PIN generate alternate callable service 189
  clear PIN generate callable service 177
  encrypted PIN generate callable service 181
  encrypted PIN verification callable service 195
data-encrypting key 5
data integrity
  ensuring 16
  verifying 145
data key
  exporting 54
  importing 49
  reenciphering 54
data key export callable service (CSNBDKX)
  format 54
  overview 11
  parameters 54
  syntax 54
data key import callable service (CSNBDKM)
  format 53
  overview 11
  parameters 53
  syntax 53
DATA key type 8
data space
  callable services that use data in data spaces 24
data-translation key 6, 141
DATAM key type 8
DATAMV key type 8
DATAXLAT key type 8
decipher callable service (CSNBDEC or CSNBDEC1)
  format 131
  syntax 131
deciphering
  data 121, 130
  data with clear key 137
  multiple 375
decode callable service (CSNBDCO)
  format 137

decode callable service (CSNBDCO) *(continued)*
  parameters 137
  syntax 137
DES algorithm 3, 16, 121
DES enciphered key token parameter 258
DES external key token format 386
DES internal key token format 385
destination identifier 15
digital signature generate callable service (CSNDDSG)
  format 247
  overview 235
  parameters 247
  syntax 247
digital signature verify callable service (CSNDDSV)
  format 251
  overview 235
  parameters 251
  syntax 251
double-length key
  key length 66
  multiple decipherment 378
  multiple encipherment 377
  using 6
DSS private external key token 393
DSS private internal key token 399
DSS public token 389
dynamic CKDS update callable services
  description 12

E

EBCDIC to ASCII conversion
  table 403
ECI-1 202
ECI-2 PIN block format 173, 361
ECI-3 PIN block format 173, 361
ECI-4 202
EDC
  generating 103
electronic code book (ECB) 121
encipher callable service (CSNBENC or CSNBENC1)
  format 125
  parameters 125
  syntax 125
enciphered
  key 63, 84, 121
  under master key 74
enciphering
  data 121, 123
  multiple 375
  string with clear key 135
encode callable service (CSNBECO)
  format 135
  parameters 135
  syntax 135
encrypted PIN block parameter
  clear PIN generate alternate callable service 188
  encrypted PIN verification callable service 193
encrypted PIN generate callable service (CSNBEPG)
  format 179
  syntax 179
encrypted PIN generate service (CSNBEPG)
  parameters 179
encrypted PIN translate callable service (CSNBPTR) 197
  extraction rules 361
  format 197
  parameters 198
  syntax 197
encrypted PIN verification callable service (CSNBPVR)
  extraction rules 361
  format 191
  parameters 191
  syntax 191
ensuring data integrity and authenticity 16
error detection code (EDC)
  generating 103
EX key form 40
examples of callable services 343
EXEX key form 43
exit, installation 27
exit data 27
exit data length 27
export, prohibiting 48
exportable key form 5
  definition 35
  generating 38
  value 64
exporter key-encrypting key 6
  any DES key 56
  enciphering data key 54
exporter key identifier parameter
  data key export callable service 56
  key export callable service 59
EXPORTER key type 8
external key token 27, 29, 243
  DES 386
  PKA 245
    DSS private 393
    RSA private 390
extraction rules, PIN 361

F

FEATURE=CRYPTO keyword
  SCHEDULE macro 29
form parameter
  random number generate callable service 140
format control 174
formats, PIN 19
functions of
  cryptographic keys 3
  ICSF 3

G

GBP-PIN algorithm 193
GBP-PINO algorithm 193
generated key identifier 1 parameter
  key generate callable service 70
generated key identifier 2 parameter
  key generate callable service 70
generating an error detection code (EDC) 103

generating encrypted keys 63
German Banking Pool PIN algorithm 363

H

hash length parameter
  digital signature generate callable service 249
  digital signature verify callable service 253
  one-way hash generate callable service 163
hash parameter
  digital signature generate callable service 250
  digital signature verify callable service 253
  one-way hash generate callable service 163
high-level languages 23

I

IBM 3624 175, 191
IBM-4700 PIN block format 360
IBM 4700 processing rule 122, 355
IBM GBP 175, 191
IBM-PIN algorithm 193
IBM-PINO algorithm 193
ICSF
  functions 3
  overview 3
IEAAFFN callable service (affinity) 29
IM key form 40
IMEX key form 43
IMIM key form 40
importable key form 5
  definition 35
  generating 37
  value 64
imported key identifier length parameter
  multiple secure key import callable service 88
imported key identifier parameter
  multiple secure key import callable service 88
importer key-encrypting key 6
  enciphering clear key 81, 84
importer key identifier parameter
  key import callable service 77
  PKA key import callable service 302
  secure key import callable service 84
IMPORTER key type 8
importing a non-exportable key 62
improving performance using partial notarization 383
INBK PIN 172, 175
INBK-PIN 191
initial chaining vector (ICV)
  description 121, 355
initialization vector in parameter
  ciphertext translate callable service 143
initialization vector out parameter
  ciphertext translate callable service 143
initialization vector parameter
  cryptographic variable encipher callable service 213
  decipher callable service 133
  encipher callable service 126
  key token build callable service 208
input data transport key 141
input KEK key identifier parameter
  key translate callable service 74
input PIN-encrypting key identifier parameter
  encrypted PIN translate callable service 198
  encrypted PIN verification callable service 192
input PIN profile parameter
  clear PIN generate alternate callable service 187
  encrypted PIN translate callable service 198
  encrypted PIN verification callable service 192
installation-defined callable service 3
installation exit
  post-processing 27
  preprocessing 27
Integrated Cryptographic Service Facility (ICSF)
  description xxi
Interbank PIN 33, 172, 175, 191
internal key token 27, 28, 243, 244
  DES 385
  PKA
    DSS private 399
    RSA private 394, 396, 397
invocation requirements 29
IPINENC key type 8, 198
IPS processing rule 127, 133, 357
ISO-0 PIN block format 173
ISO-1 PIN block format 173, 360
ISO-2 PIN block format 360

J

JCL statements, sample 38

K

KEK key identifer parameter
  control vector translate callable service 216
KEK key identifier 1 parameter
  key generate callable service 69
KEK key identifier 2 parameter
  key generate callable service 69
KEK key identifier parameter
  key test callable service 91
  prohibit export extended callable service 63
  transform CDMF key callable service 99
key array parameter
  control vector translate callable service 217
key array right parameter
  control vector translate callable service 217
key-encrypting key 6
  definition 4
  description 6
  exporter 54, 56
  importer 81
key encrypting key identifier parameter 257
key export callable service (CSNBKEX)
  format 56
  overview 11
  parameters 56
  syntax 56
key flow 36
key form
  combinations for a key pair 71
  combinations with key type 71
  definition 5

key form *(continued)*
  exportable 5, 35
  importable 5, 35
  operational 5, 35
  value 64
key form parameter
  key generate callable service 64
  secure key import callable service 83
key generate callable service (CSNBKGN)
  format 63
  overview 10
  parameters 63
  syntax 63
  using 40, 48
key generator utility program (KGUP)
  description 10
  generating keys 47
  panels 47
key identifier 27
  PKA keys 243
key identifier in parameter
  ciphertext translate callable service 142
key identifier length parameter
  multiple clear key import callable service 52
key identifier out parameter
  ciphertext translate callable service 143
key identifier parameter
  clear key import callable service 50
  decipher callable service 132
  encipher callable service 126
  key test callable service 91
  MAC generation callable service 149, 153
  multiple clear key import callable service 52
  secure key import callable service 84
key import callable service (CSNBKIM)
  format 74
  overview 11
  parameters 74
  syntax 74
key label 27, 244
  security considerations 29
key length parameter
  key generate callable service 65
key management
  ANSI X9.17 standard 103
key pair 71
key part import callable service (CSNBKPI)
  format 79
  overview 11
  parameters 79
  syntax 79
key record create callable service (CSNBKRC)
  format 92
  overview 12
  parameters 92
  syntax 92
key record delete callable service (CSNBKRD)
  format 93
  overview 13
  parameters 93
  syntax 93
key record read callable service (CSNBKRR)
  format 95
  overview 13
  parameters 95
  syntax 95
key record write callable service (CSNBKRW)
  format 96
  overview 12
  parameters 96
  syntax 96
key test callable service (CSNBKYT and CSNBKYTX)
  format 88
  overview 12
  parameters 88
  syntax 88
key token 28, 244
  DES
    external 386
    internal 385
    null 387
  DES internal 385
  external 29
  internal 28, 244
  null 29
  PKA 241
    DSS private external 393
    DSS private internal 399
    DSS public 389
    null 401
    RSA 1024-bit modulus-exponent private external 390
    RSA 1024-bit private internal 396, 397
    RSA 2048-bit Chinese remainder theorem private external 391
    RSA 2048-bit Chinese remainder theorem private internal 398
    RSA private external 390
    RSA private internal 394
    RSA public 388
  PKA external 245
key token build callable service (CSNBKTB)
  format 203
  overview 21
  parameters 203
  syntax 203
key translate (CSNBKTR)
  parameters 73
key translate callable service (CSNBKTR)
  format 73
  overview 10
  syntax 73
key type 1 40, 41, 43
key type 1 parameter
  key generate callable service 67
key type 2 40, 41, 43
key type 2 parameter
  key generate callable service 67
key type parameter
  key export callable service 57
  key import callable service 75
  key token build callable service 204

key type parameter *(continued)*
  secure key import callable service 83
  user derived key callable service 100
key value structure length parameter 289
key value structure parameter 289
keys
  ANSI X9.17 key-encrypting 7
  changing CDMF DATA key to transformed shortened DES 97
  clear 8, 81
  control vector 4, 5
  creating 35, 36, 48
  cryptographic, functions of 3
  data-encrypting 5
  data key
    exporting 54
    importing 49
    reenciphering 54
  data-translation 6
  double-length 41, 43
  enciphered 84
  exporter key-encrypting 6
  forms 35
  generating
    encrypted 63
    values for keys 16
  held in applications 7
  held in CKDS 7
  importer key-encrypting 6
  key-encrypting 6
  list of types 8
  MAC 6
  managing 47
  master, DES 5
  master key variant 4
  multiple decipherment/encipherment 375
  pair 40, 41, 43
  parity 49
  PIN 6
  PIN-encrypting key 197
  PKA master 233
    Key Management Master Key (KMMK) 233
    Signature Master Key (SMK) 233
  possible forms 10
  protecting 121
  reenciphered 74
  reenciphering 56
  separation 3
  single-length 40
  transport 6
  transport key variant 4
  types of 5
  using 35
  VISA PVV
    generating 186

L

languages, high-level 23
large data object 356
length of data 124
linking callable services 38

M

MAC
  generation callable service 17
  keys 6
  length keywords 150, 154
  managing 17
  verification callable service 18
MAC generation callable service (CSNBMGN or CSNBMGN1)
  format 148
  parameters 148
  syntax 148
MAC key type 8
mac parameter
  MAC generation callable service 151
  MAC verification callable service 155
MAC verification callable service (CSNBMVR or CSNBMVR1)
  format 152
  parameters 153
  syntax 152
MACVER key type 8
managing keys 47
mask array left parameter
  control vector translate callable service 217
mask array preparation 423
mask array right parameter
  control vector translate callable service 217
master key
  changing
    possible effect on internal key tokens 28
  enciphered key 74
master key, DES 5
master key variant 4
MAXLEN keyword 124, 126, 132, 143
MDC
  generate callable service 18
  length keywords 159
  managing 18
mdc parameter
  MDC generation callable service 159
message authentication
  definition 17
message authentication code (MAC)
  description 145
  generating 145, 147
  verifying 145, 152
messages
  authenticating 145
migration consideration
  return codes from CUSP/PCF macros 26
mode, special secure 9
modes of operation 121
modification detection
  definition 18
modification detection code (MDC)
  generating 146, 156
  verifying 146
multiple
  decipherment 375

multiple *(continued)*
  encipherment 375
multiple clear key import callable service (CSNBCKM) 50
  format 51
  overview 11
  parameters 51
  syntax 51
multiple node network 141
multiple secure key import callable service (CSNBSKM) 84
  format 85
  overview 12
  parameters 85
  syntax 85

N
notarization 15
Notices 429
null key token 29
  format 387, 401
number, generated 139

O
offsetting 15, 383
one-way hash generate callable service (CSNBOWH and CSNBOWH1)
  format 160
  overview 18
  parameters 160
  syntax 160
OP key form 40
operational key form 5
  definition 35
  generating 37
  value 64
OPEX key form 41
OPIM key form 40
OPINENC key type 8, 198
OPOP key form 40
origin identifier 15
output chaining vector (OCV)
  description 122, 355
output data transport key 141
output KEK key identifier parameter
  key translate callable service 74
output PIN-encrypt translation key identifier parameter
  encrypted PIN translate callable service 198
output PIN profile parameter
  encrypted PIN translate callable service 201
overview of callable services 23

P
pad character parameter
  encipher callable service 128
  key token build callable service 208
pad digit 175
  format 174
padding schemes 124, 131
pair of keys 40, 41, 43
PAN data in parameter
  encrypted PIN translate callable service 199
PAN data out parameter
  encrypted PIN translate callable service 201
PAN data parameter
  clear PIN encrypt callable service 185
  clear PIN generate alternate callable service 187
  encrypted PIN generate callable service 182
  encrypted PIN verification callable service 193
parameter
  attribute definitions 24
  definitions 26
  direction 25
  exit data 27
  exit data length 27
  reason code 26
  return code 26
  type 25
parity of key 49, 81
  adjusting 90
  EVEN 140
  ODD 140
partial notarization 15, 383
  calculation for a double-length AKEK 384
  calculation for a single-length AKEK 384
PCI interface callable service (CSFPCI)
  parameters 225
  syntax 225
performance considerations 29
personal account number (PAN)
  for encrypted PIN translate 199
  for encrypted PIN verification 193
personal authentication
  definition 19
personal identification number (PIN)
  3624 PIN generation algorithm 362
  3624 PIN verification algorithm 365
  algorithm value 189, 193
  algorithms 19, 172, 175
  block format 172, 197
  clear PIN encrypt callable service 20
  clear PIN generate alternate callable service 20, 186
  definition 19
  description 171
  detailed algorithms 362
  encrypted generation callable service 20
  encrypting key 173, 197
  extraction rules 361
  formats 19
  GBP PIN verification algorithm 367
  generating 172, 175
    from encrypted PIN block 172
  generation callable service 20, 175
  German Banking Pool PIN algorithm 363
  keys 6
  managing 19
  PIN offset generation algorithm 364
  PVV generation algorithm 370

personal identification number (PIN) *(continued)*
  PVV verification algorithm 371
  translating 172
  translation callable service 20, 197
  translation of, in networks 171
  using 171
  verification callable service 20, 191
  verifying 172, 191
  VISA PIN algorithm 370
PIN block format
  3621 360
  3624 360
  additional names 202
  ANSI X9.8 359
  changing 199
  detail 359
  ECI-2 361
  ECI-3 361
  format values 173
  IBM-4700 360
  ISO-1 360
  ISO-2 360
  VISA-2 360
  VISA-3 360
PIN block in parameter
  encrypted PIN translate callable service 199
PIN block out parameter
  encrypted PIN translate callable service 202
PIN block variant constant (PBVC)
  description 174, 190
  for clear PIN generate alternate 190
  for encrypted PIN translation 202
  for PIN verification 196
PIN check length parameter
  c 189
  clear PIN encrypt callable service 185
  clear PIN generate callable service 177
  PIN verification callable service 195
PIN-encrypting key
  changing 199
PIN encryption key identifier parameter 187
PIN encryting key identifier parameter
  clear PIN encrypt callable service 184
PIN generating key identifier parameter
  encrypted PIN generate callable service 180
PIN keys 6
PIN length parameter
  clear PIN generate callable service 177, 185
  encrypted PIN generate callable service 181
PIN notation 359
PIN profile 173
  description 192, 199
PIN profile parameter 187
  encrypted PIN generate callable service 182
PIN validation value (PVV) 175
PIN verifying key identifier parameter
  encrypted PIN verification callable service 192
PINGEN key type 8
PINVER key type 8
PKA decrypt callable service (CSNDPKD)
  overview 238
PKA decrypt callable servicec 282
PKA encrypt callable service (CSNDPKE)
  overview 238
PKA encrypt callable servicec 279
PKA external key token 245
PKA key generate callable service (CSNDPKG)
  format 297
  parameters 297
  syntax 297
PKA key import callable service (CSNDPKI)
  format 300
  overview 235
  parameters 300
  syntax 300
PKA key token 241
  external 245
  record format
    DSS private external 393
    DSS private internal 399
    DSS public 389
    RSA 1024-bit modulus-exponent private external 390
    RSA 1024-bit private internal 396, 397
    RSA 2048-bit Chinese remainder theorem private external 391
    RSA 2048-bit Chinese remainder theorem private internal 398
    RSA private external 390
    RSA private internal 394
    RSA public 388
PKA key token build callable service (CSNDPKB)
  format 287
  overview 238
  parameters 287
  syntax 287
PKA master key 234
PKA private key identifier length parameter 249
PKA private key identifier parameter 249
PKA public key extract callable service (CSNDPKX)
  format 303
  overview 236
  parameters 303
  syntax 303
PKA public key identifier length parameter 252
PKA public key identifier parameter 253
PKA92 key format and encryption process 421
PKDS record create callable service (CSNDKRC) 305
  format 305
  parameters 305
  syntax 305
PKDS record delete callable service (CSNDKRD) 310
  format 310
  parameters 310
  syntax 310
PKDS record read callable service (CSNDKRR) 308
  format 309
  parameters 309
  syntax 309
PKDS record write callable service (CSNDKRW) 306
  format 307
  parameters 307

PKDS record write callable service (CSNDKRW) 306
(continued)
syntax 307
PKSC interface 229
PKSC interface callable service (CSFPKSC)
parameters 229
syntax 229
plaintext
enciphering 121
encoding 135
field 129, 135
plaintext parameter
cryptographic variable encipher callable service 213
post-processing exit 27
preprocessing exit 27
privacy 16
private external key token
DSS 393
RSA 390
private internal key token
DSS 399
RSA 394, 396, 397
private key name length parameter 293
private key name parameter 294
processing rule
4700-PAD 127, 133
ANSI X3.106 355
ANSI X9.23 122, 127, 133, 355
CBC 122, 127, 133
cipher 355
cipher last block 356
CUSP 356
CUSP/IPS 122, 127, 133
decipher 133
description 122
encipher 127
GBP-PIN 177
GBP-PINO 177
IBM 4700 122, 355
IBM-PIN 177
IBM-PINO 177
INBK-PIN 177
IPS 357
recommendations for encipher 128
REFORMAT keyword 199
segmenting 356
TRANSLAT keyword 199
VISA-PVV 177
prohibit export (CSNBPEX) 61
prohibit export callable service (CSNBPEX)
format 61
overview 11
syntax 61
prohibit export extended callable service (CSNBPEXX)
format 62
overview 11
parameters 62
syntax 62
using 48
protecting data and keys 121
public key token
DSS 389
RSA 388

R

RACF authorization 29
random number generate callable service (CSNBRNG)
format 139
overview 16
parameters 139
syntax 139
random number parameter
key test callable service 91
random number generate callable service 140
reason codes 26, 46
reason codes for ICSF
for return code 0 (0) 320
for return code 10 (16) 335
for return code 4 (4) 320
for return code 8 (8) 321
for return code C (12) 332
reason codes for TSS
for return code 10 (16) 342
for return code 4 (4) 336
for return code 8 (8) 337
for return code C (12) 341
recommendations for encipher processing rules 128
record chaining 122, 357
reenciphered
key 74
reenciphering
data-encrypting key 54
PIN block 197
REFORMAT keyword 199
reserved parameter
control vector generate callable service 74, 215
retained key delete callable service (CSNDRKD)
format 314
overview 237
parameters 314
syntax 314
retained key list callable service (CSNDRKL)
format 312
overview 237
parameters 312
syntax 312
retained private keys
overview 236
return codes 26, 46
from CUSP and PCF macros
migration consideration 26
return codes for ICSF
description 319
return codes for TSS
description 336
returned PVV parameter 190
returned result parameter
clear PIN generate callable service 178
Rivest-Shamir-Adleman (RSA) algorithm 233
RSA 1024-bit private internal key token 396, 397

RSA algorithm 233
RSA enciphered key length parameter
  symmetric key generate callable service 258
  symmetric key import callable service 261
RSA enciphered key parameter
  symmetric key generate callable service 258
  symmetric key import callable service 261
RSA private external Chinese remainder theorem key token 391
RSA private external key token 390
RSA private external modulus-exponent key token 390
RSA private internal key token 394
RSA private internall Chinese remainder theorem key token 398
RSA private key identifier 261
RSA private key identifier length 261
RSA public key identifier length parameter
  for symmetric key generate 257
RSA public key identifier parameter 257
RSA public token 388
rule array count parameter
  clear PIN encrypt callable service 184
  Clear PIN encrypt callable service 180, 217
  clear PIN generate alternate callable service 188
  clear PIN generate callable service 177
  control vector translate callable service 217
  decipher callable service 133
  digital signature generate callable service 249
  digital signature verify callable service 252
  encipher callable service 126
  encrypted PIN translate callable service 199
  encrypted PIN verification callable service 193
  key test callable service 90
  key token build callable service 205
  MAC generation callable service 149, 154
  MDC generation callable service 158
  one-way hash generate callable service 161
  PKA key generate callable service 298
  PKA key import callable service 302
  PKA key token build callable service 288
  PKA public key extract callable service 304
  symmetric key export callable service 263
  symmetric key generate callable service 256
  symmetric key import callable service 260
  transform CDMF key callable service 98
  user derived key callable service 101
rule array parameter
  clear PIN encrypt callable service 184
  clear PIN generate alternate callable service 188
  clear PIN generate callable service 177
  control vector generate callable service 214
  control vector translate callable service 217
  decipher callable service 133
  digital signature generate callable service 249
  digital signature verify callable service 252
  encipher callable service 127
  encrypted PIN generate callable service 180
  encrypted PIN translate callable service 199
  encrypted PIN verification callable service 193
  key test callable service 90
  key token build callable service 206
rule array parameter *(continued)*
  MAC generation callable service 149, 154
  MDC generation callable service 158
  one-way hash generate callable service 162
  PKA key generate callable service 299
  PKA key import callable service 302
  PKA key token build callable service 288
  PKA public key extract callable service 304
  symmetric key export callable service 264
  symmetric key generate callable service 256
  symmetric key import callable service 260
  transform CDMF key callable service 98
  user derived key callable service 101

S

sample JCL statements 38
SCHEDULE macro
  FEATURE=CRYPTO keyword 29
SCSFMOD0 module 38
secure key import callable service (CSNBSKI)
  format 81
  overview 11
  parameters 81
  syntax 81
Secure Sockets Layer (SSL) 238
security considerations 29
segmenting
  control keywords 150, 154, 159
  definition 356
  rule, large data object 356
sequence number parameter
  encrypted PIN translate callable service 202
sequences of callable service 38
SET
  overview 267
SET block compose callable service (CSNDSBC) 267
  format 268
  overview 238
  parameters 268
  syntax 268
SET block decompose callable service (CSNDSBD) 272
  format 273
  overview 238
  paramters 273
  syntax 273
SET protocol 237
SET Secure Electonic Transaction 267
SET Secure Electronic Transaction 237
short blocks 124
signature bit length parameter 250
signature field length parameter
  digital signature generate callable service 250
  digital signature verify callable service 253
signature field parameter
  digital signature generate callable service 250
  digital signature verify callable service 253
single-length key
  key length 66
  multiple decipherment 376

single-length key *(continued)*
multiple encipherment 376
purpose 40
using 6
source key identifier length parameter
PKA key import callable service 302
PKA public key extract callable service 304
source key identifier parameter
data key export callable service 55
key export callable service 59
key import callable service 77
PKA key import callable service 302
PKA public key extract callable service 304
transform CDMF key callable service 99
source key token length parameter
prohibit export extended callable service 63
source text parameter
character/nibble conversion callable service 221
code conversion callable service 220
X9.9 data editing callable service 223
special secure mode 9
SRB, scheduling 29
SSL support 238
symmetric key export callable service (CSNDSYX)
format 262
overview 237
parameters 262
syntax 262
symmetric key generate callable service (CSNDSYG)
format 255
overview 237
parameters 255
syntax 255
symmetric key import callable service (CSNDSYI)
format 259
overview 237
parameters 259
syntax 259
syntax for callable service 23

T

target key identifier length parameter 302
target key identifier parameter 302
data key export callable service 56
key export callable service 59
key import callable service 78
symmetric key import callable service 261
transform CDMF key callable service 99
target key token parameter
encrypted PIN generate callable service 218
target public key token length parameter 304
target public key token parameter 305
target text parameter
character/nibble conversion callable service 222
code conversion callable service 220
X9.9 data editing callable service 224
text, translating 141
text id in parameter
ciphertext translate callable service 143
MAC generation callable service 151
MAC verification callable service 155

text id in parameter *(continued)*
MDC generation callable service 160
one-way hash generate callable service 163
text id out parameter
ciphertext translate callable service 143
text in parameter
ciphertext translate callable service 143
text length parameter
character/nibble conversion callable service 221
ciphertext translate callable service 143
code conversion callable service 219
cryptographic variable encipher callable service 212
decipher callable service 132
encipher callable service 126
MAC generation callable service 149, 154
MDC generation callable service 158
one-way hash generate callable service 162
X9.9 data editing callable service 223
text out parameter
ciphertext translate callable service 143
text parameter
MAC generation callable service 149, 154
MDC generation callable service 158
one-way hash generate callable service 162
TKE
overview 21
token validation value (TVV) 386
trailing short blocks 124
transform CDMF key algorithm 373
transform CDMF key callable service (CSNBTCK)
format 97
overview 14
parameters 97
syntax 97
transformed shortened DES key 97
TRANSLAT keyword 199
transport key 6
transport key variant 4
triple-length key
key length 66
triple-length keys
multiple encipherment 379
mutiple decipherment 380
Trusted Key Entry
overview 21
types of keys 5

U

user derived key
generating 99
processing rules 101
utilities
character/nibble conversion 220
code conversion 218
key token build 203
PKA key token build 287
X9.9 data editing 222

V

verification pattern, generating and verifying 88
verification pattern parameter 91
verifying data integrity and authenticity 145
VISA-1 202
VISA-2 PIN block format 173, 360
VISA-3 PIN block format 173, 360
VISA-4 PIN block format 173
VISA CVV service generate callable service (CSNBCSG) 163
  format 164
  parameters 164
  syntax 164
VISA CVV service verify callable service (CSNBCSV) 166
  format 167
  parameters 167
  syntax 167
VISA PVV 175
  generating 186
VISA-PVV algorithm 189, 193

X

X9.9-1 keyword 150, 154
X9.9 data editing callable service (CSNB9ED)
  format 222
  overview 22
  parameters 222
  syntax 222

Readers' Comments — We'd Like to Hear from You

OS/390
Integrated Cryptographic Service Facility
Application Programmer's Guide

Publication No. SC23-3976-07

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

Phone No.

Readers' Comments — We'd Like to Hear from You
SC23-3976-07

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Department 55JA, Mail Station P384
2455 South Road
Poughkeepsie, NY
12601-5400

Fold and Tape **Please do not staple** Fold and Tape

SC23-3976-07

Cut or Fold
Along Line

Program Number: 5647-A01

Printed in the United States of America on recycled paper containing 10% recovered post-consumer fiber.

SC23-3976-07