Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0970-V2-2018

for

KC 1000 SC series, JK-A01xxyy-z-Z-, FW-Version: 2.0.0, HW-Version: /01

from

Cherry GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0970-V2-2018 (*)

Digital signature: Smart Card Readers

KC 1000 SC series
JK-A01xxyy-z-Z-, FW-Version: 2.0.0, HW-Version: /01

from Cherry GmbH

PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, AGD_OPE.1, AGD_PRE.1, ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_CMC.3, ALC_CMS.3, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2, AVA_VAN.3

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 4

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2

Bonn, 26 January 2018

For the Federal Office for Information Security

Joachim Weber
Head of Branch

L.S.

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Contents

This page is intentionally left blank.

A. Certification

1. Preliminary Remarks

Under the BSIG1 Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

2 Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

3 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045.
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogisportal.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2+ ALC_FLR components.

[4] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product KC 1000 SC series, JK-A01xxyy-z-Z-, FW-Version: 2.0.0, HW-Version: /01 has undergone the certification procedure at BSI.

The evaluation of the product KC 1000 SC series, JK-A01xxyy-z-Z-, FW-Version: 2.0.0, HW-Version: /01 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 12 January 2018. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Cherry GmbH.

The product was developed by: Cherry GmbH.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 26 January 2018 is valid until 25. January 2023. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

[5] Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product KC 1000 SC series, JK-A01xxyy-z-Z-, FW-Version: 2.0.0, HW-Version: /01 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Cherry GmbH
Cherrystraße
91275 Auerbach/Opf
Deutschland

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is the product “KC 1000 SC series with firmware version 2.0.0 and the hardware version /01", produced by Cherry GmbH. The TOE is a computer keyboard with an integrated smart card reader that conforms to the USB classes "Human Interface Device" (HID) and "Smart Card" (CCID). The keyboard is intended for use in a non-public environment.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, AGD_OPE.1, AGD_PRE.1, ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_CMC.3, ALC_CMS.3, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2, AVA_VAN.3.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
SF.1: Secure PIN entry	The PIN which identifies the user to the smartcard is entered on the keyboard. The TOE ensures that the PIN is only communicated to the smartcard, but not to other parties, e.g. software on the PC connected to the TOE. The TOE signals to the user by lighting a dedicated LED when it is secure to enter the PIN on the keyboard.
SF.2: Memory reprocessing	The TOE ensures that no information about the PIN remain in the TOE after it has been transmitted to the smartcard.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.2. Based on these assets the TOE Security Problem is defined in terms of Assumptions and Threats. This is outlined in the Security Target [6], chapters 3.1 and 3.4.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this

certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

KC 1000 SC series, JK-A01xxyy-z-Z-, FW-Version: 2.0.0, HW-Version: /01

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery[7]
1	HW/FW	Cherry KC 1000 SC JK-A01xxyy-z-Z- /01[8] with firmware version 2.0.0	01	By distributor or by special agreement with Cherry GmbH, see notes below
2	DOC	Quick Start Guide CHERRY KC1000SC – Corded Smartcard Keyboard; 6440639-03 [9]	Jul 2017	Electronic
3	DOC	Operating Instruction CHERRY KC1000SC – Corded Smartcard Keyboard; 6440640-00 [10]	Nov 2017	Electronic
4	DOC	CHERRY KC 1000 SC Software Developer Guide; 64410018-01 [11]	September 2017	Electronic

Table 2: Deliverables of the TOE

The TOE is a hardware device with associated guidance documents. The TOE is intended to be used with driver software which is not in the scope of this evaluation.

The Quick Start Guide [9], the detailed Operating Instruction [10] and the Software Developer's Guide [11] are supplied to the user in electronic form. The documents are signed with a qualified electronic signature and are available from the Cherry Support website https://www.cherry.de/cid/download.php[9].

An authentic TOE must fulfil all of the following criteria:

- It is marked "CHERRY KC 100 SC" on the top of the casing in abrasion-proof inscription.
- It has an engraved part number ("P/N") on the bottom of the casing, which is one of the following (see also section 8 for further details[10]):
  - JK-A0100BE-0-Z- /01 JK-A0100BE-2-Z- /01
    JK-A0100BR-0-Z- /01 JK-A0100BR-2-Z- /01
    JK-A0100CH-0-Z- /01 JK-A0100CH-2-Z- /01
    JK-A0100DE-0-Z- /01 JK-A0100DE-2-Z- /01
    JK-A0100EE-0-Z- /01 JK-A0100EE-2-Z- /01
    JK-A0100ES-0-Z- /01 JK-A0100ES-2-Z- /01
    JK-A0100EU-0-Z- /01 JK-A0100EU-2-Z- /01

[7] As ALC_DEL has been excluded, the delivery procedure was not in the scope of this evaluation. The form of delivery is nevertheless described informally.

[8] The part number reflects the packaging version (JK-A0100 means single, JK-A0150 bulk packaging), the national keyboard layout (e.g. DE=German) and the casing color (0=gray, 2=black).

[9] Optionally, the documents can also be enclosed on CD with the delivery. However, only the electronically signed versions distributed via the Cherry website are part of the evaluated configuration.

[10]The TOE has only a single configuration, which cannot be changed. There are only variations e.g in casing colour (grey, black) or national keyboard layout. However, this has no impact on the security functionality.

JK-A0100FR-0-Z- /01 JK-A0100FR-2-Z- /01
JK-A0100GB-0-Z- /01 JK-A0100GB-2-Z- /01
JK-A0100IT-0-Z- /01 JK-A0100IT-2-Z- /01
JK-A0100PN-0-Z- /01 JK-A0100PN-2-Z- /01
JK-A0100PO-0-Z- /01 JK-A0100PO-2-Z- /01
JK-A0100US-0-Z- /01 JK-A0100US-2-Z- /01

- JK-A0150BE-0-Z- /01 JK-A0150BE-2-Z- /01
  JK-A0150BR-0-Z- /01 JK-A0150BR-2-Z- /01
  JK-A0150CH-0-Z- /01 JK-A0150CH-2-Z- /01
  JK-A0150DE-0-Z- /01 JK-A0150DE-2-Z- /01
  JK-A0150EE-0-Z- /01 JK-A0150EE-2-Z- /01
  JK-A0150ES-0-Z- /01 JK-A0150ES-2-Z- /01
  JK-A0150EU-0-Z- /01 JK-A0150EU-2-Z- /01
  JK-A0150FR-0-Z- /01 JK-A0150FR-2-Z- /01
  JK-A0150GB-0-Z- /01 JK-A0150GB-2-Z- /01
  JK-A0150IT-0-Z- /01 JK-A0150IT-2-Z- /01
  JK-A0150PN-0-Z- /01 JK-A0150PN-2-Z- /01
  JK-A0150PO-0-Z- /01 JK-A0150PO-2-Z- /01
  JK-A0150US-0-Z- /01 JK-A0150US-2-Z- /01

- It has four intact security seals with a lock symbol (two on the back, one each left and right) that match the description in the user guidance [10], sec. 5 "Sicherheitssiegel".
- Due to the fact, that the Common Criteria component ALC_DEL.1 is not part of the certification, the security review ends with the packaging process at the production line. The delivery of the TOE to the secure environment in which the TOE will be used must be negotiated individually with every single customer. Direct delivery to the user or administrator is preferred.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- User data protection: Access control, Residual information protection
- Identification and authentication: Protected authentication feedback
- TOE access: Default TOE access banner
- Protection of the TSF: TOE emanation, Passive detection of physical attack

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- The TOE must be used as a smartcard keyboard for the non-public environment.
- The user must check the integrity of the security seal and the TOE.
- The user must follow the security advice of the card issuer.

- While entering the PIN, the user must check the status of the LED to ensure that the secure PIN entry mode is active.
- The user must only use processor cards which satisfy the [12] and [13] specifications.

Details can be found in the Security Target [6], chapter 4.2.

5. Architectural Information

The functionality of the TOE is mainly provided by the firmware of the TOE's microcontroller. The firmware consists of two subsystems; the CCID Subsystem and the Misc Subsystem. The Misc Subsystem comprises basic hardware management as well as the TOE's functionality as a regular USB keyboard. The CCID subsystem contains all components providing security relevant services. The subsystems are further divided into modules.

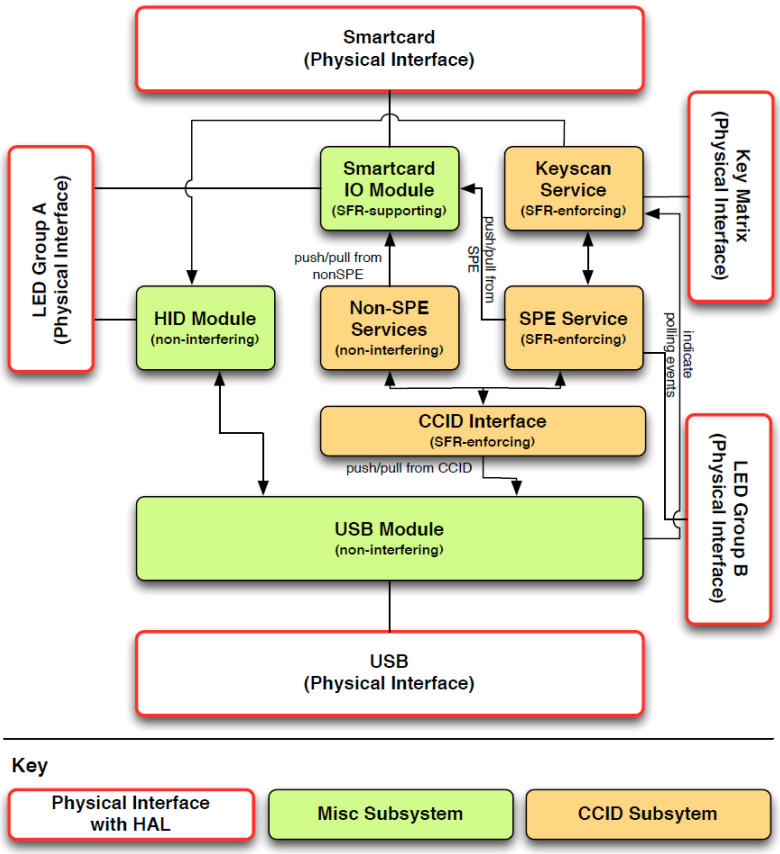

Figure 1: Architecture of the TOE

The modules shown in Figure 1 provide the following functionality:

- Misc Subsystem
  - USB Module: Basic USB functions, distribution of USB messages to the HID (keyboard) or CCID (card reader) functionality
  - HID Module: Keyboard functionality, including Caps-Lock and Num-Lock LEDs
  - Smartcard IO Module: Access to the card reader, control of the Data LED

  - Hardware Abstraction (HAL): Access to physical hardware features, i.e. keyboard and LEDs
- CCID Subsystem
  - CCID Interface: Interpretation of CCID class USB messages
  - SPE Service: Implementation of the Secure PIN Entry (SPE) functionality, including control of the SPE LED
  - Non-SPE Services: Implementation of all other card reader functionality
  - Keyscan Service: Handling of key presses either in SPE or regular mode

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

7.1. Developer Testing

Test Environment

The tests are performed on an actual TOE that is connected as a USB device to a virtual machine (VM) (operating on a notebook) running the test scripts. User key presses are simulated by an automatic keyboard tester operating the key matrix directly.

The test environment, under control of a test script, operates the USB interface and the key matrix and checks the state of the SPE LED. Removal and insertion of test smartcards has to be done by the test operator as prompted by the test script. The tested smart card echoes back the data it received from the TOE, so the test script can check it against the expected values.

The developer tests cover the following areas:

- Physical interfaces: USB, smart card, SPE LED
- USB HID class commands for non-interference with the smartcard reader functionality
- USB CCID class commands (transmission modes, functionality, PIN formats)
- SPE functionality

Test Depth and Result

The topics covered by the tests can be summarized as follows

- Misc Subsystem
  - Identification of the TOE
  - Reporting of capabilities (e.g. firmware version)
  - HID functionality

- CCID Subsystem
  - SPE operations
  - Other CCID operations
  - Error handling
  - State of the SPE LED
  - (Non-)reporting of key presses
  - Functionality of the smartcard interface

The focus of the tests for the CCID subsystem was naturally on the SPE functionality. The purpose of the majority of the tests is dedicated to SPE operations, covering all possible combinations of features.

The tests are executed against the TSFIs. The more complex TSFIs adhere to universal, well-documented standards, the others have a very limited range of possible values.

The evaluator deems the testing approach of the developer as appropriate. Especially the systematic testing of the SPE functionality supports the confidence that the TOE's behaviour conforms to the specifications.

The tests were reproducible and the results were in accordance with the ST and could be matched to the expected values in the test plan.

7.2. Independent Evaluator Testing

Overview

The independent testing was performed using the developer’s testing environment, operated by the evaluator at the evaluation lab's premises.

The overall test result is that no deviations were found between the expected and the actual test results.

Test Configurations

The test environment provided by the developer consisted of the following items:

- Virtual Machine with all software necessary to execute the test scripts of the developer
- Test scripts of the developer
- Key Tester device to operate keyboard TFSI
- TOE prepared with adapter circuit board for use with Key Tester for fully automatic testing
- Unmodified TOE for testing with manual interaction by the test operator.

Comparing the configuration of the unique reference of the TOE under testing with the configuration of the TOE being under evaluation the evaluators verified that the configuration of the samples are consistent to the configuration as stated in the ST and with the TOE reference as managed by the CM.

Test Approach

Secure PIN Entry is the primary security feature of the TOE, so the evaluator chose for his test subset the developer tests for this feature. All tests regarding the SPE feature that could be executed automatically (644 tests in total) were repeated.

Additionally, the evaluator devised a set of tests that verifies the TOE behaviour for the following cases:

- Legal alphanumeric PIN is entered
- Illegal alphanumeric PIN is entered
- Unsuitable encoding for alphanumeric PIN is used

The SFRs FDP_ACC.1, FDP_ACF.1, FDP_RIP.1 and FTA_TAB.1 are tested directly by tests included in the evaluator subset; for FIA_UAU.7 the evaluator checked that there is at least one test in the developer test suite. FPT_EMS.1 and FPT_PHP.1 do not directly concern TOE behaviour that is visible at the TSFIs and are therefore addressed in the vulnerability assessment (AVA_VAN).

Summary

The evaluator test subset covers all SFR-enforcing and SFR-supporting TSFI in a way that would expose incorrect behaviour of the TOE.

For the independent testing the overall test result is that no deviations were found between the expected and the actual test results. For all test cases, the actual test results are consistent with the expected test results.

7.3. Vulnerability Assessment

The evaluator performed a focused vulnerability assessment analysing all developer evidences provided for evaluation and taking in consideration publicly available information about potential vulnerabilities.

The SFR FPT_PHP.1 was tested as part of the vulnerability assessment. Penetration tests of the security seals were performed using operational samples of the TOE. Since there are no different configurations of the TOE, the configuration under test was consistent with the version under evaluation.

The remaining SFRs were analysed, but not tested through penetration due to non-exploitability of the related attack scenarios in the TOE's operational environment.

The overall penetration test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential enhanced basic was actually successful.

Since the Common Criteria assurance component ALC_DEL.1 was not part of the assurance activities it cannot be excluded that potential vulnerabilities in this life cycle phase of the TOE exist. Please see the respective obligation in Chapter 10.

8. Evaluated Configuration

This certification covers the following configurations of the TOE: The TOE, the smartcard keyboard KC 1000 SC, features a USB keyboard with an integrated Class 2 reader that is able to read processor smartcards in line with ISO 7816 [12] and EMV 2000 [13] via various application interfaces. The keyboard works with all smartcard data transfer protocols according to ISO 7816 [12].

The TOE has only a single configuration, which cannot be changed. There are variations in casing colour (grey, black) and national keyboard layout. However, this has no impact on the security functionality. The exact product variant can be seen from the Cherry part number printed on the bottom of the TOE which takes the form JK-A01xxyy-z-Z- /01, where yy stands for the country code of the keyboard layout and z for 0 (grey) or 2 (black). xx is the packaging version[11] (00=single, 50=bulk). The uppercase "Z" at the end of the part number distinguishes the TOE from a similar Cherry smartcard keyboard that is not in scope of this evaluation.

Country Code (yy)	Country	Country Code (yy)	Country
DE	Germany	EU	U.S.A. (with € symbol)
GB	Great Britain	ES	Spain
US	U.S.A. (without € symbol)	CH	Switzerland
BE	Belgium	BR	Brazil
IT	Italy	EE	Estonia
FR	France	PN	Scandinavian (Pan Nordic)
PO	Portugal		

Table 3: Localized Keyboard Layouts

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components claimed in the Security Target [6], chapter 2.3 and defined in the CC (see also part C of this report). Informally, this component claim corresponds to the assurance level EAL 3 augmented by the components ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1 and AVA.VAN.3 and reduced by the component ALC_DEL.1.

The evaluation has confirmed:

- PP Conformance: None [8]
- for the Functionality: Product specific Security Target
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, AGD_OPE.1, AGD_PRE.1, ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_CMC.3, ALC_CMS.3, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2, AVA_VAN.3

[11] This is not a variant of the TOE itself, but only of the packaging.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The TOE does not include cryptographic mechanisms. Thus, no such mechanisms were part of the assessment.

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

In addition, the following aspects need to be fulfilled when using the TOE:

- The delivery procedures (aspect ALC_DEL) have not been evaluated. The user must therefore assess whether the form of delivery offered by the developer and the possibilities to check the integrity and authenticity of the received product is adequate to their security needs.
- Furthermore the user has to follow the security requirements stated in the user guidance, especially in [10], section 4, of which the main points are summarized here:
  - The TOE must be used in a non-public environment.
  - The TOE environment must be protected against installation of audio and video recording equipment.
  - The smartcard and the PIN must be kept confidential. The security advice of the card issuer must be followed.
  - The integrity and authenticity of the TOE must be verified before use by inspecting the security seals.
  - During PIN entry the user must not be observed and the Secure PIN Entry LED must be on.
  - The user must only use processor cards which satisfy the [12] and [13] specifications.

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Definitions

12.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCID	Chip Card Interface Device, an USB protocol
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
DRNG	Deterministic Random Number Generator
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable ROM
ETR	Evaluation Technical Report
HID	Human Interface Device, an USB protocol
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LED	Light Emitting Diode
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SPE	Secure PIN Entry
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

13. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012,
Part 2: Security functional components, Revision 4, September 2012,
Part 3: Security assurance components, Revision 4, September 2012,
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4,September 2012,
http://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[12]
https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-0970-V2-2018, Version 1.06, 19.12.2017, Security Target for KC 1000 SC, Cherry GmbH

[7] Evaluation Technical Report, Version 1.2, 09.01.2018, SRC Security Research & Consulting, (confidential document)

[8] Configuration list for the TOE, Version 1.05, 19.12.2017, Konfigurationsliste KC1000SC, (confidential document)

[12]specifically

- AIS 1, Version 13, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 48, Version 1, Anforderungen an die Prüfung von Sicherheitsetiketten

[9] Guidance documentation for the TOE, Quick Start Guide CHERRY KC1000SC – Corded Smartcard Keyboard, 6440639-03, Jul 2017

[10] Guidance documentation for the TOE, Cherry KC 1000 SC Corded Smartcard Keyboard Betriebsdokumentation, 6440640-00, Nov 2017

[11] Guidance documentation for the TOE, CHERRY KC 1000 SC Software Developer's Guide, 64410018-01, September 2017

[12] DIN ISO 7816 - 1 Identification cards - Integrated circuit(s) cards with contacts – Physical Characteristics
DIN ISO 7816 – 2 Identification cards - Integrated circuit(s) cards with contacts - Dimensions and locations of the contacts
DIN ISO 7816 – 3 Identification cards - Integrated circuit(s) cards with contacts - electrical characteristics and transmission protocols
DIN ISO 7816 – 4 Information technology - Identification cards - Integrated circuit(s) cards with contacts - Inter - industry commands for interchange
DIN ISO 7816 – 8 Identification cards – Integrated circuit(s) cards with contacts – Security related interindustry commands

[13] EMV 2000 Book 1 - Application independent ICC to Terminal Interface requirements, Version 4.0, December 2000

This page is intentionally left blank.

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailled definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at http://www.commoncriteriaportal.org/cc/

This page is intentionally left blank.

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report