# Oracle Key Manager

## Systems Assurance Guide

Oracle Key Manager: Systems Assurance Guide

316194806 Revision: D

# Summary of Changes

| EC Number | Date | Revision | Description |
|-----------|------|----------|-------------|
| EC000227 | February 2008 | A | Initial release. |
| EC000496 | May 2008 | B | Refer to this revision for the list of changes (included T9840D tape drives) |
| EC000594 | June 2008 | BA | Refer to this revision for the list of changes (included HP LTO 4 tape drives) |
| EC001009 | February 2009 | BB | Refer to this revision for the list of changes (included X2200 server, FIPS-compliant, IPv6, T10000B) |
| EC001402 | November 2009 | BC | Refer to this revision for the list of changes (KMS 2.2, IBM LTO4, IBM ICSF) |
| 316194806 | April 2010 | C | Refer to this revision for the list of changes (Oracle branding, updated marketing/order numbers) |
| 316194806 | November 2010 | D | This revision includes:<br>■ Product Name Change<br>From: Crypto Key Management System (KMS)<br>To: **Oracle Key Manager (OKM)**<br>■ Added new server: X4170 M2 content<br>■ Added new tape drive: LTO5 content<br>■ Added new platforms (SL24 and SL48)<br>■ Added engineering updates |

**Note –** Change bars are included in this revision.

# Contents

# Preface

This guide is intended for service representatives, customers, partners, and anyone responsible for planning the installation of the Oracle Key Manager (OKM) encryption solution.

**Note –** The customer must have a copy of the *Administration Guide* and the *Customer Virtual Operator Panel Guide* to complete the installation.

**Make sure these guides are available to the customer at the time of the installation.** Go to: http://docs.sun.com/app/docs/prod/stortek.crypto.keymgmt20

# Related Information

These publications contain the additional information mentioned in this guide:

| Publication Description | Part Number |
| --- | --- |
| Important Safety Information for Hardware Systems | 816-7190-xx |
| *SunFire X2100 Server Installation Guide* | 819-6589-xx |
| *SunFire X2200 Server Installation Guide* | 819-6596-xx |
| *SunFire X4170 Server Installation Guide* | 821-0481-xx |
| *Embedded Lights Out Manager Administration Guide* | 819-6588-xx |
| *T10000 Tape Drive Installation Manual* | 96173 |
| *T9x40 Tape Drive Installation Manual* | 95879 |
| *SL8500 Modular Library System Installation Manual* | 96138 |
| *SL3000 Modular Library System Installation Manual* | 316194201 |
| *SL500 Modular Library System Installation Manual* | 96114 |
| *L700/1400 Library Installation Manual* | 95843 |
| *9310 PowderHorn Library Installation Manual* | 9314 |
| *Virtual Operator Panel—Service* | 96180 |

| Publication Description | Part Number |
|---|---|
| *Virtual Operator Panel*—Customer | 96179 |
| *Oracle Key Manager Installation and Service Manual* | 3161949xx |
| *Oracle Key Manager Administration Guide* | 3161951xx |
| *Oracle Key Manager Disaster Recovery Guide* | 3161971xx |
| *Storage Regulatory and Safety Compliance Manual* | 820-5506-xx |

# Documentation, Support, and Training

| Function | URL | Description |
|---|---|---|
| Web Site | http://www.oracle.com/index.html | General information and links. |
| Documentation<br>■ Customer:<br>■ Employee:<br>■ Partner: | http://docs.sun.com<br>http://docs.sfbay.sun.com/<br>https://spe.sun.com/spx/control/Login | Search for technical documentation.<br>Download PDF/HTML documents.<br>Order printed documents. |
| Downloads<br>■ Customer:<br>■ Employee: | http://www.sun.com/download/index.jsp<br>http://dlrequest.sfbay.sun.com:88/usr/login | Download firmware and graphical user interfaces, patches, and features. |
| Support | http://www.sun.com/support/ | Obtain and escalate support. |
| Training | http://www.sun.com/training/ | Access training resources. |

# Oracle Welcomes Your Comments

Oracle is interested in improving its documentation and welcomes your comments and suggestions. Submit your comments by clicking the Feedback [+] link at:

http://docs.sun.com

Please include the title and part number of your document with your feedback:

*Oracle Key Manager, Systems Assurance Guide*, PN: 3161948xx

# Introduction

Encryption is based on the science of **cryptography**, which is one of the most effective ways to achieve data security today. To read an encrypted file, you must have access to the key that will enable you to decipher the file.

This chapter introduces you to Oracle's Key Manager (OKM) and the components for encryption.

# Planning for Encryption

Are your customer accounts concerned with:
  – **Data security?**
  – **Data protection and sensitive information?**
  – **Government regulations and retention?**

■ Data security is a major concern for IT professionals today—what happens if and when data falls into the wrong hands?

■ Access to sensitive data can happen when it is:

  ■ Sent over networks

  ■ Written on disk or tape

  ■ Stored in archives

■ Your customers may also be required to take measures to protect their data because of government regulations or contractual obligations with business partners. A number of regulations require organizations to *encrypt* their data.

Encryption can occur during three points in the life of the data. When data is:

■ Created (host-based)

■ Transported (appliance-based)

■ Stored (device-based)

Oracle offers **device-based** implementations, for a "**data-at-rest**" encryption solution. This offering provides an excellent solution for mixed environments with a variety of operating system types—both enterprise and open systems platforms.

Choosing device-based encryption is the **least disruptive** to an existing system infrastructure because the encryption functionality is built directly in to the tape drive, so there is no need to maintain special software specifically for encrypted data.

# Encryption Standards

Oracle's encryption solutions are based on the most current advanced industry standards and functionality, including:

- Federal Information Processing Standards
  - **FIPS PUB 140-2**, Security Requirements for Cryptographic Modules
  - **FIPS PUB 46-3**, Data Encryption Standard
  - **FIPS PUB 171**, Key Management

  FIPS are standards and guidelines adopted and declared under the provisions of Section 5131 of the Information Technology Management Reform Act of 1996. FIPS defines four levels of security.

  **Level 1** – The basic level with production-grade requirements.
  **Level 2** – Adds requirements for physical tamper evidence and role-based authentication. Built on a validated operating platform.
  **Level 3** – Adds requirements for physical tamper resistance and identity-based authentication. Requires additional physical or logical separations.
  **Level 4** – Makes the physical security requirements more stringent and requires robustness against environmental attacks.

- **National Institute of Standards and Technology** (**NIST**) AES-standard defining a cryptographic cipher using the Rijndael symmetric block cipher algorithm.

  **NIST 800-57 Part 1**, Recommendations for Key Management

- Institute of Electrical and Electronics Engineers **IEEE 1619**, working groups:

  1619.1 Standard for Tape Encryption—complete
  1619.2 Standard for Disk Encryption—in process
  1619.3 Standard for Key Management—in process

- **Common Criteria** (CC), an International Consortium sponsored by the National Security Agency (**NSA**) that sets requirements for IT security.

- International Standard Organization **ISO/IEC 1779** Security Techniques

- CCM–AES-256 encryption

  **CCM** = "Counter with CBC-MAC," is a mode of encryption that provides for both a strong form of privacy (security) and efficient authentication.
  **CBC–MAC =**"Cipher Block Chaining–Message Authentication Code," a message integrity method in which each block of plain text is encrypted with a cipher.
  **AES** = "**Advanced Encryption Standard**," a block cipher encryption algorithm that uses both cryptographic techniques, Counter mode and CBC-MAC (CCM).

- **Symmetric encryption,** uses one key to both encrypt and decrypt data.

- **Nonce,** a non-repeating number that is incorporated into the mode of operation to ensure that repetitive plaintext does not result in repetitive ciphertext.

- **Cipher-suite**
  - TLS 1.0 = Transport layer security
  - RSA = A 2048-bit key encryption algorithm
  - SHA1 = A widely used and secure hash algorithm
  - HMAC = Hash message authentication code (Hash-MAC)

# Components

The Oracle Key Manager is a **device-based** encryption solution that uses:

- An appliance (server) called the Key Management Appliance or KMA.
- Network connectivity* (a clean gigabit Ethernet connection).
- StorageTek automated libraries for automated cartridge tape handling.
- StorageTek tape drives (T-Series and LTO) as the agents for encryption.

Components for the OKM Version 2.3 and above encryption solution consists of:

| | |
|---|---|
| **Key Management Appliance** (KMA) | The KMA is a SunFire$^{TM}$ server (such as the 2100, 2200, and 4170) for the hardware platform. This server:<br>■ Runs the key manager application on a specialized, pre-loaded version of the Solaris$^{TM}$ 10 operating system.<br>■ Delivers a policy-based key manager and provisioning services.<br>■ Generates the raw keys for encryption |
| **SCA**6000 card | An *optional* Sun Cryptographic Accelerator (SCA6000) card for cryptographic processing and administrative functions is provided for customers that require FIPS-compliance.<br>**Note:** This is a FIPS 140-2 Level 3 hardware security module. |
| **OKM Manager** or **OKM Manager GUI** | The manager is a client-side software component with a graphical user interface (GUI).<br>**Note:** The OKM Manager must be installed on a *customer-provided*, network-attached, PC, server, or workstation running Windows XP, Vista, 2003 Server, or running Solaris x86 or Solaris SPARC. |
| **OKM CLI** | A command line interface to assist with automation of management tasks such as backup and reporting. |
| **OKM Cluster** | A full set of KMAs in a system. All of the KMAs are aware of each other, and replicate information to each other.<br>**Note:** *There must be a minimum of 2 servers in a cluster.* |
| **Agent** | Agents are devices (currently tape drives) that are authenticated with the Key Manager and obtain key material over a "secure" (TLS) session.<br>**Note:** Agents should *not* be on public networks. |
| **Data Unit ID** | A unique ID assigned by the OKM to each individual data cartridge. |
| **Key Groups** | Provide organization for keys and associates them to a Key Policy.<br>Key Groups are used by the OKM to enforce access to the key material by the Encryption Agents (tape drives). |
| **Network connections** | Each key management appliance has four network connections:<br>LAN 0 = Management network<br>LAN 1 = Embedded or Internal Lights Out Manager (ELOM/ILOM)<br>LAN 2 = Service network, connection to the tape drives<br>LAN 3 = Additional aggregated service port (*optional*) |

**\* Note:** For additional security and to isolate LAN traffic, the customer may want to consider using Virtual Local Area Networks* (VLANs) when connecting to the management network.
**\* VLANs** are broadcast domains that exist within a defined set of switches. Ports on these switches can be grouped together to provide a logical network to provide the services traditionally created by traditional routers in network configurations.

**Important:**
Key management appliances *should be* installed in **pairs** as shown in the configuration drawings FIGURE 1-1 through FIGURE 1-4. Some key points include:

- Multiple KMAs are clustered on a **dedicated**, private, local, or wide area network.
- The servers in a OKM Cluster provide data replication so there is redundancy. This allows each key management appliance to serve as backups to others.
- Tape drives, called Agents, must remain connected to the network in the event an encryption key is needed.
- Any KMA in the cluster can service any tape drive on the network provided there is an Ethernet connection between the two.
- KMAs and agents can be logically "group" to create a site, where agents preference KMAs within the site to which they are assigned.
- By default, Agents are serviced by the local KMAs if available.
- Any KMA can be used for administration functions.
- All changes to any KMA are replicated to all other KMAs in the cluster:
  - New keys generated at any site are replicated to all other KMAs in the cluster.
  - All administrative changes are propagated to all other KMAs in the cluster.

# Encryption Hardware Kits

Encryption hardware kits come complete with Ethernet switches, cables, power distribution units, and mounting hardware for connection of the tape drives in either a **library** or standalone **rack** configuration.

The type of configuration determines how the tape drives are installed, **each configuration has its own kit**, see Chapter 4, "Components" for more information.

Refer to the *Oracle Key Manager: Installation and Service Manual* and the individual *product installation manuals* for specific installation instructions.

# Key Manager Configurations

Multiple KMAs[1] (two or more) must be installed together to create a cluster[2]. Clusters of KMAs are able to fully replicate their data to each other KMA.
**Note:** Cluster size should be strongly considered when designing the system for maximum availability.

The following figures show examples of Version 2.x configurations for the key management appliance:

- FIGURE 1-1 Single site – local area network
- FIGURE 1-2 Multiple sites – wide area network
- FIGURE 1-3 Multiple sites with disaster recovery – wide area network
- FIGURE 1-4 Disaster Recovery Configuration

---

1. **Multiple KMAs**: Exceptions to this standard configuration *must* be made with the approval of Encryption Engineering, Professional Services, and Support Services.

2. A **Cluster** is a group of linked appliances that work together, so that in many respects they form a single component.

**FIGURE 1-1**  Single Site Configuration

This example uses a *single site* with a local area network for the management link.
The service network for the tape drives shows all of the supported tape drives (Agents)
Agents include T-Series (T10000 A and B, T9840D) and LTO (generations 4 and 5) tape drives.
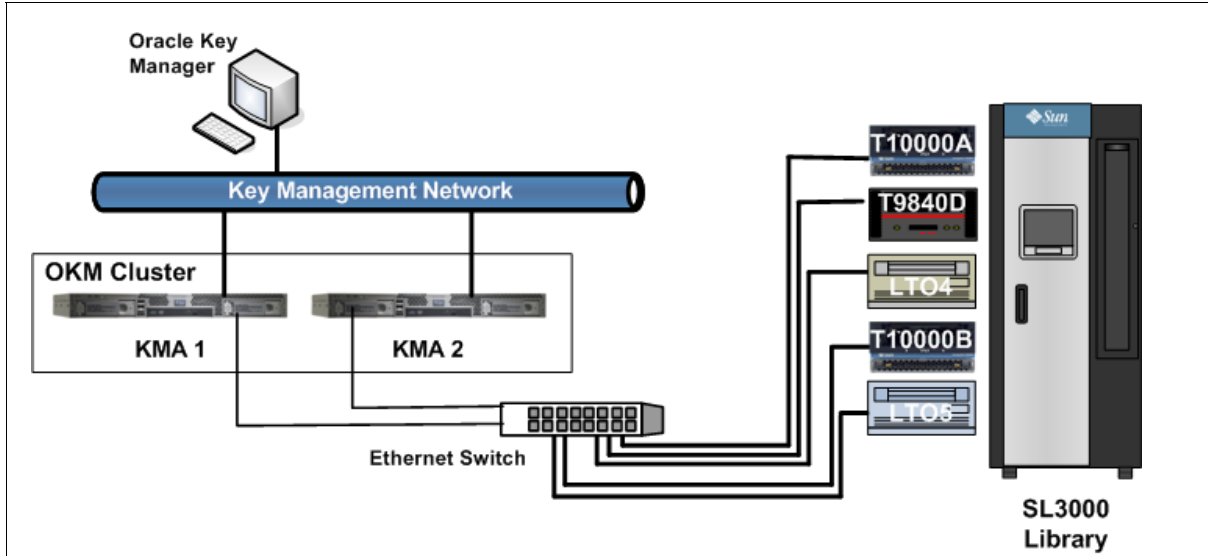


**FIGURE 1-2**  Dual Site Configuration

In this example, the KMAs are managed over a wide area network.
All four KMAs belong in the same OKM cluster.
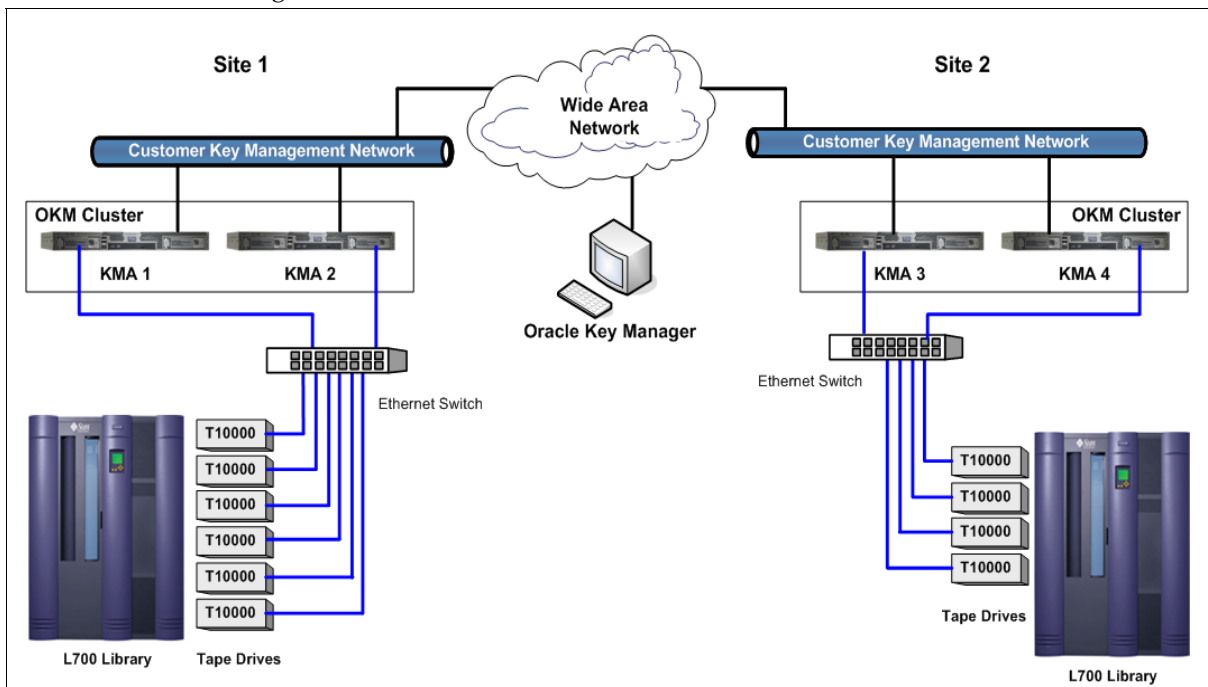


*Note:* LTO encryption-capable tape drives are not supported in L-Series libraries.

**FIGURE 1-3** Multiple Site Configuration

This example uses two remote sites and a local (main) site within one OKM cluster.
The main site contains a partitioned SL8500 library with specific key groups that provides
backup facilities for all the KMAs (1–6) and media within the entire OKM cluster.
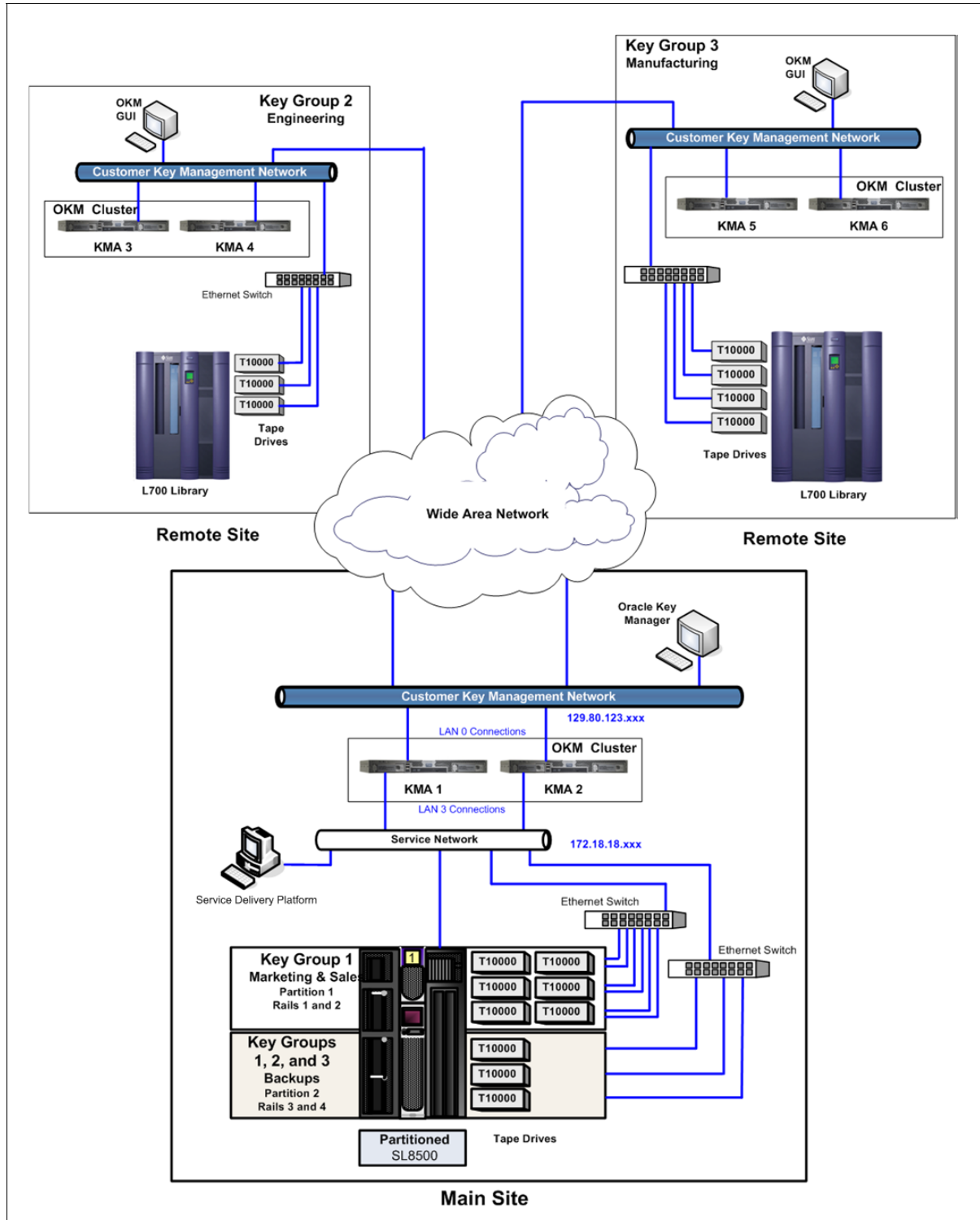
**FIGURE 1-4** Disaster Recovery Configuration

In this example there are two wide area networks; one for management and one for service.
- The OKM communicates with all four KMAs in the cluster.
- The service network consists of two interface ports, LAN 2 and LAN 3.
  The KMA aggregates LAN2 with LAN 3 into an aggregated service port.
- The service wide area network allows any KMA at either site to communicate with the agents.
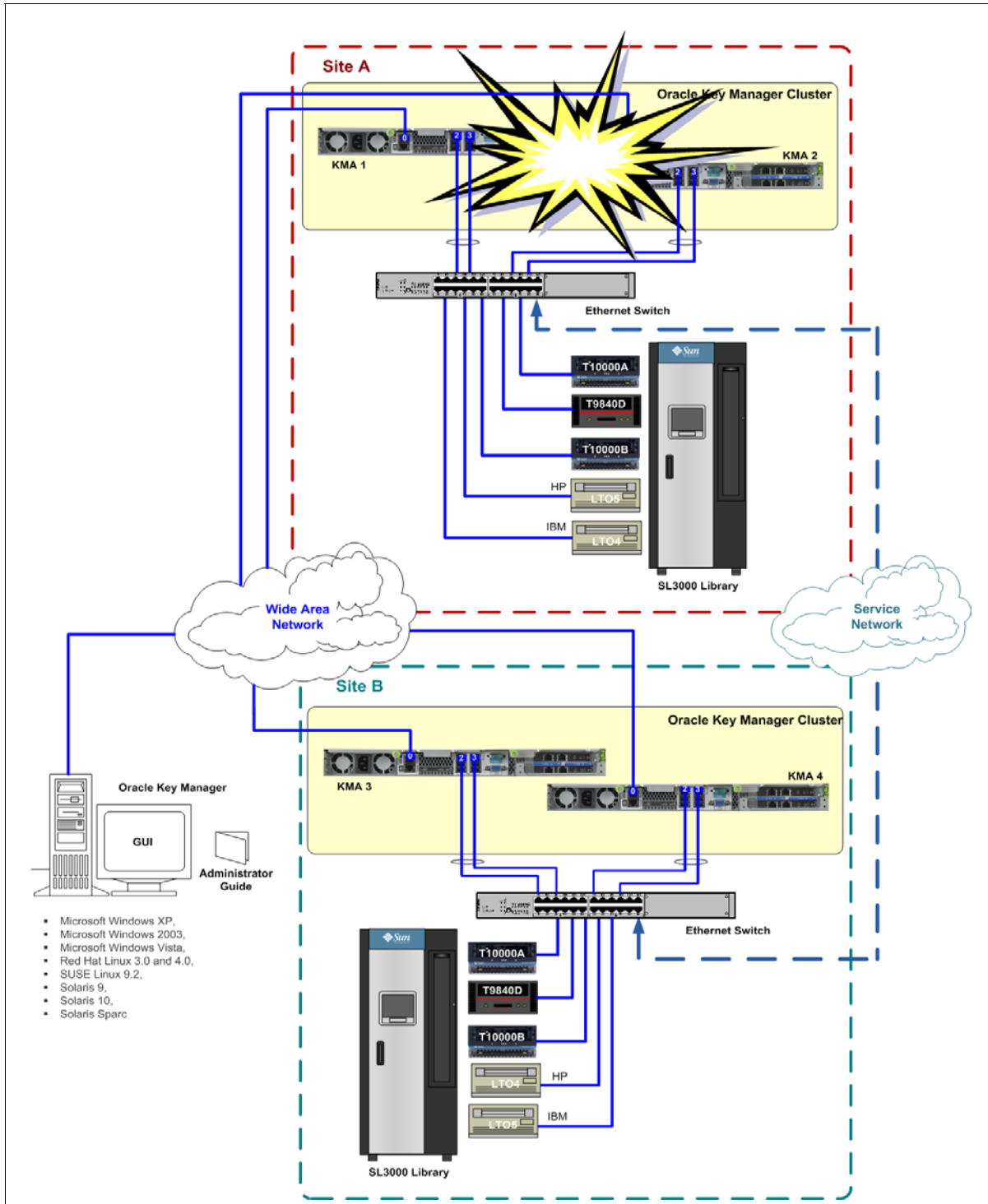
# Key Management Appliance

There are three types of servers for the Key Management Appliance (KMA)

- SunFire X2100 servers (original)
- SunFire X2200 servers (upgrade)
- SunFire 4170 M2 servers (current)

All three servers are functionally equivalent.

**Notes:**

- Subsequent releases of the OKM appliance may use different server hardware but are guaranteed to be interoperable with other deployed KMAs.
- An OKM may consist of a mix of SunFire X2100s, X2200s, and X4170s as systems are upgraded, scaled, or as replacements to failed units.

## SunFire 4170 Server

FIGURE 1-5 shows a rear view of the Sun Fire X4170 M2 server.

FIGURE 1-6 shows a front view of the Sun Fire X4170 M2 server.

TABLE 1-1 lists the specifications for the Sun Fire X4170 M2 server.

**FIGURE 1-5** Key Management Appliance—4170 Rear Panel



1. AC Power connectors
2. Serial Management (SER MGT) RJ-45 serial port
3. Service Processor (NET MGT) port
4. Ethernet ports (0, 1, 2, 3) , from left to right these ports are labeled "Net0" thru "Net3".
5. USB ports (0, 1)
6. Video connector (VGA)
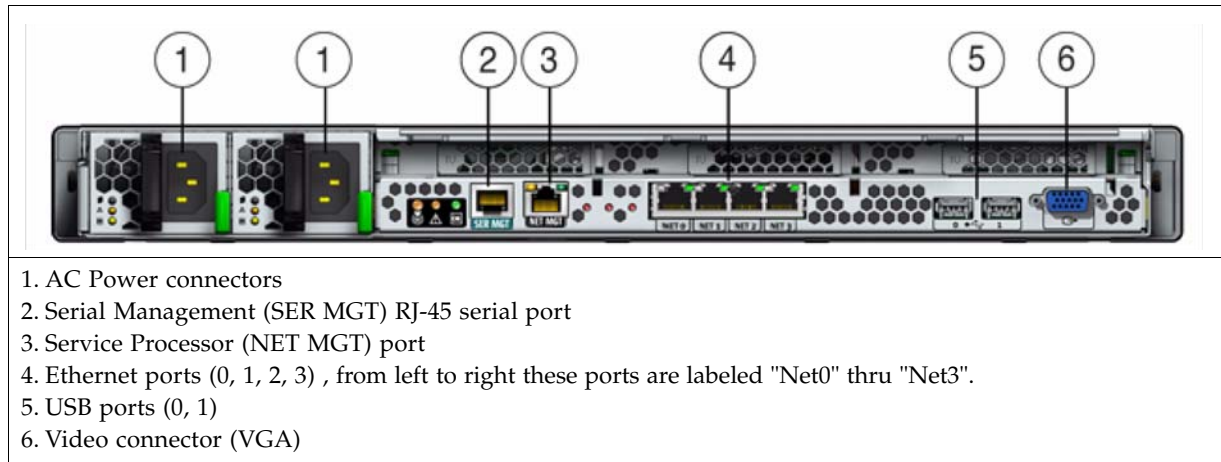
**FIGURE 1-6** Key Management Appliance—4170 Front Panel



1. Power /OK LED
2. Power button
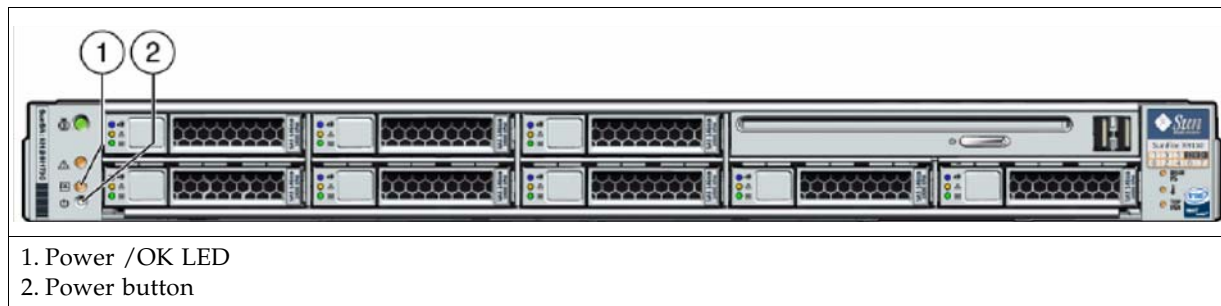
## 4170 Component Specifications

lists the specifications for the Sun Fire X4170 M2 server.

**TABLE 1-1** Specifications

| Specification | |
|---|---|
| Processor | One or two quad-core (2.4-GHz) |
| Memory | Nine DDR3 DIMMs per processor |
| Management Software | Service processor standard Integrated Lights Out Manager (ILOM) |
| Mass storage | One SATA disk drive |
| PCI Slots | Two PCI-Express slots (PCIe) PCIe-0 contains the Sun Crypto Accelerator (SCA6000) if installed |
| Networking | Four USB 2.0 connectors on the rear panel Two USB 2.0 connectors on the front panel VGA with DB-15 connectors Four 10/100/1000 Base-T Ethernet ports |
| **Dimensions** | |
| Height | 4.34 cm (1.71 in.) |
| Width | 42.5 cm (16.75 in.) |
| Depth | 68.58 cm (27.0 in.) |
| Weight | 16.36 kg (36 lb) |
| **Environmental** | |
| Operating temperature | 5° C to 35° C (41° F to 95° F) |
| Non-operating temperature | -40° C to 70° C (-40° F to 158° F) |
| Operating humidity | 10% to 90% relative humidity, non-condensing |
| Non-operating humidity | Up to 93% relative humidity, non-condensing |
| Altitude (operating) | Up to 3000 m, maximum ambient temperature is degraded by 1 degree C per 300 m above 900 m |
| Altitude (non-operating) | Up to 12,000 m |

# SunFire 2100 and 2200 Servers

FIGURE 1-7 shows a rear view of the Sun Fire X2100/2200 M2 server.

FIGURE 1-8 shows a front view of the Sun Fire X2100/2200 M2 server.

TABLE 1-2 lists the specifications for the Sun Fire X2100 M2 server.

TABLE 1-3 lists the specifications for the Sun Fire X2200 M2 server.

**FIGURE 1-7** Key Management Appliance—2100/2200 Front Panel



| | |
|---|---|
| 1. System identification button/LED | 5. Optional hard disk drive bay (0) |
| 2. Fault LED | 6. USB 2.0 connectors (2) |
| 3. Power/OK LED | 7. CD/DVD drive (not populated) |
| 4. Power button | 8. Optional hard disk drive bay (1) |
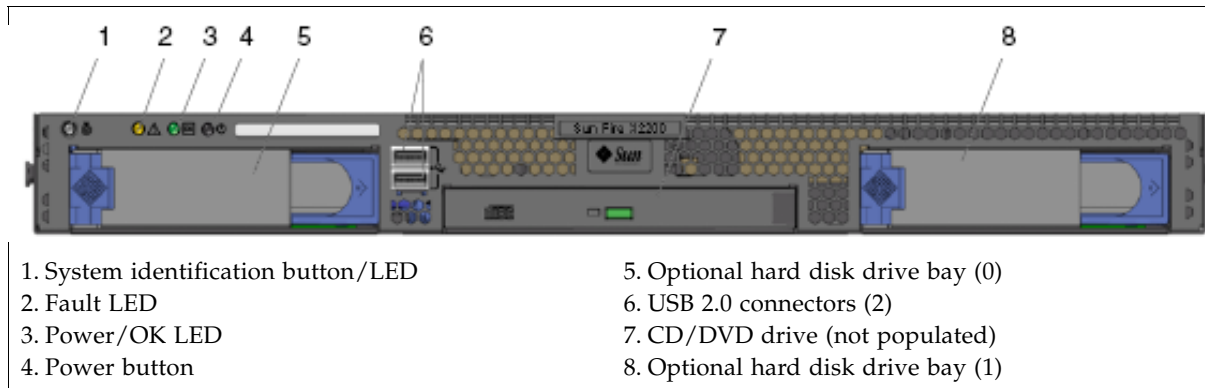
**FIGURE 1-8** Key Management Appliance—2100/2200 Rear Panel



| | |
|---|---|
| 1. Power connector | 7. Serial port (DB9, RS232) |
| 2. Ethernet connectors (2) | 8. PCIe slots (2) |
|    Top = KMA Management Network (LAN 0) |    Top = SCA6000 card (not shown) |
|    Bottom = Embedded Lights Out Manager (ELOM) |    Bottom = Blank (empty) |
| 3. System Identification LED | 9. VGA connector (if using a monitor/keyboard for |
| 4. Fault LED |    the initial configuration) |
| 5. Power LED | 10.USB 2.0 ports (4) |
| 6. Ethernet Service Network connections (2) | |
|    Left = Service network (LAN 2) | |
|    Right = Aggregated service network (LAN 3) | |

# SunFire X2100 Server

TABLE 1-2 lists the specifications for the SunFire X2100 server.

**TABLE 1-2** SunFire X2100 Specifications

| Specification | |
|---|---|
| **Processor** | ■ One dual-core AMD Operton processor<br>■ Processor frequencies: 2.2 GHz<br>■ Up to 1 MB level 2 cache |
| **Memory** | ■ Four DIMM slots (up to 4 gigabytes)<br>■ Unbuffered ECC memory |
| **IPMI 2.0** | ■ Service processor standard<br>■ embedded Lights Out Manager |
| **Mass storage** | One SATA disk drive |
| **PCI Slots** | Two PCI-Express slots (PCIe)<br>PCIe-0 contains the Sun Crypto Accelerator 6000 (SCA6000) |
| **Networking** | ■ Four USB 2.0 connectors on the rear panel<br>■ Two USB 2.0 connectors on the front panel<br>■ Two ports: Serial port with DB-9; VGA with DB-15<br>■ Four 10/100/1000 Base-T Ethernet ports |
| **Dimensions:** | |
| Height | 43 mm (1.7 in.) |
| Width | 425.5mm (16.8 in.) |
| Depth | 550 mm (21.68 in.) |
| Weight (maximum) | 10.7 kg (23.45 lb) |
| Mounting options | 19-inch rackmount kit; Compact 1 rack-unit (1.75 in.) |
| **Environmental parameters:** | |
| Temperature | 5°C to 35°C (41°F to 95°F) |
| Relative humidity | 27°C (80°F) max wet bulb |
| Altitude | Up to 3,000 m (9,000 ft) |
| Power supply | 90 – 2640 VAC, 47 – 63 Hz<br>One 6.5 Amp non-redundant power supply at 345 Watts<br>Heat output is about 850 BTU/hour |
| **Regulations meets or exceeds the following requirements:** | |
| Acoustic Noise Emissions declared in accordance with ISO 9296 | |
| Safety IEC 60950, UL/CSA60950, EN60950, CB scheme | |
| RFI/EMI FCC Class A, Part 15 47 CFR, EN55022, CISPR 22, EN300-386:v1.31, ICES-003 | |
| Immunity: EN55024, EN300-386:v1.3.2 | |
| Certifications: Safety CE Mark, GOST, GS Mark, cULus Mark, CB scheme, CCC, S Mark | |
| EMC CE Mark, Emissions and Immunity Class A Emissions Levels:<br>FCC, C-Tick, MIC, CCC, GOST, BSMI, ESTI, DOC, S Mark | |

# SunFire X2200 Server

TABLE 1-3 lists the specifications for the SunFire X2200 server.

**TABLE 1-3** SunFire X2200 Specifications

| Specification | |
|---|---|
| **Processor** | ■ Two Quad core AMD Opteron processors<br>■ Processor frequencies: 2.3Ghz |
| **Memory** | ■ 8 GB of RAM, installed as 4, 2 GB Dimms |
| **IPMI 2.0** | ■ Service processor standard<br>■ embedded Lights Out Manager |
| **Mass storage** | One SATA disk drive<br>250 GB capacity |
| **PCI Slots** | Two PCI-Express slots (PCIe)<br>PCIe-0 contains the Sun Crypto Accelerator 6000 (SCA6000) |
| **Networking** | ■ Four USB 2.0 connectors on the rear panel<br>■ Two USB 2.0 connectors on the front panel<br>■ Two ports: Serial port with DB-9; VGA with DB-15<br>■ Four 10/100/1000 Base-T Ethernet ports |
| **Dimensions:** | |
| Height | 43 mm (1.69 in.) |
| Width | 425.5 mm (16.75 in.) |
| Depth | 633.7 mm (25 in.) |
| Weight | 1.6 kg (24.64 lb.) |
| Mounting options | 19-inch rackmount kit; Compact 1 rack-unit (1.75 in.) |
| **Environmental parameters:** | |
| Temperature | 5°C to 35°C (41°F to 95°F) |
| Relative humidity | 27°C (80°F) max wet bulb |
| Altitude | Up to 3,000 m (9,000 ft) |
| Power supply | 100 – 240 VAC, 47 – 63 Hz<br>One 8 Amps non-redundant power supply at 500 Watts<br>Heat output is about 850 BTU/hour |
| **Regulations meets or exceeds the following requirements:** | |
| Safety: CE, CB Scheme, UL, CSA, CCC, BSMI, AR-S, GOST-R | |
| EMC: CE, FCC, VCCI, ICES, BSMI, CCC, MIC, C-Tick, AR-S, GOST-R | |
| Other: RoHS-compliant labeled, per WEEE (Waste Electrical and Electronics Equipment) Directive (2002/95/EC) | |

# Network Considerations

Oracle and StorageTek recommends that *customers supply* a *managed switch* for connecting KMAs to the tape drives on **private service networks**. Managed switches then would supply connectivity to the supplied unmanaged tape drive switches as well as any connectivity to customer supplied routers for wide area service network.

The following managed switches have been tested and are recommended by engineering:

■ 3COM Switch 4500G 24-Port (3CR17761-91)

■ Extreme Networks Summit X150-24t Switch

Other managed switches can be used; however, there is only configuration guidance on the above listed switches.

Managed switches are recommended for the following reasons:

■ Improved serviceability through better switch diagnostics and service network trouble shooting

■ Potential for minimizing single points of failure on the service network through use of redundant connections and spanning tree protocol.

■ Support for aggreation of the KMA service network interfaces to minimize single point of failure on the KMA's service interface.

provides an example of a managed switch configuration. In this example, if either KMA or either managed switch should fail, the drives still have a path from which they can communicate with the other KMA.

## Management Network

The OKM network should use a clean gigabit Ethernet connection for optimal replication and performance.

## ELOM and ILOM

An ELOM or ILOM networks should have spanning tree turned off or disabled.

# KMA Service Port Aggregation

Beginning with Version 2.1 it is possible to aggregate physical Ethernet interfaces (LAN 2 and LAN 3) into a single virtual interface. Additional availability is achieved by aggregating these ports; if a failure occurs with either port, the other port maintains connectivity.

Make sure the Ethernet switch ports have the correct configuration.
For example, switch ports should be:

■ Set to auto negotiate settings for duplex (should be full duplex).

■ Set to auto negotiate speed settings, the KMA ports are capable of gigabit speeds.

■ Using identical speeds, such as: both set to 100 Mbps (auto speed negotiating may work fine).

**FIGURE 1-9** Managed Switch Configuration

In this example the service network consists of two *customer-provided* managed switches that are cabled to three unmanaged switches, which contains redundant paths that require a spanning tree configuration. This example may be easily scaled for larger SL8500 drive configurations by adding additional KMAs, switch hardware, and tape drives.

■ Managed switches *must* be enabled for Spanning Tree whenever the cabling includes redundancy.
■ Unmanaged switches have two paths to the managed switches for redundancy.
■ Unmanaged switches are then cabled for connectivity to the tape drives (agents)
■ Each unmanaged switch connects 16 drives. Cabled in groups of four. Ports 1–4, 6–9, 11–14, and 16–19.
■ Service Delivery Platform (**SDP**) connects to each Managed Switch at Port 1.

Each key management appliance has four network connections. These include:

- LAN 0 = Management network (Net0)
- LAN 1 = Service Processor (either ELOM, or ILOM) network (Net1)
- LAN 2 = Service network (Net2)
- LAN 3 = Aggregated service network (Net3)

**TABLE 1-4** KMA Network Connections

| LAN 0 | This is a *required* connection.<br>This network is called the "**Management Network**" and interconnects with the Key Management Appliances and management clients hosting the GUI or CLI. This network can be local, remote, or a combination of both.<br>**Note – Customers are expected to provide this network and connection.** |
|---|---|
| LAN 1* | This connection is called the "**NET MGT ELOM**" and provides a network connection for the Embedded Lights Out Manager. The KMA console can be remotely launched and accessed over this interface. |
| LAN 2 | This is normally a *required* connection for the tape drives.<br>This network is called the "**Service Network**" and connects to the tape drives, either directly or through Ethernet switches to create the network. |
| LAN 3 | This is an *optional* connection with version 2.1 and requires a managed switch. LAN 3 provides an additional service network interface that the KMA aggregates with LAN2 into an aggregated service port.<br>Aggregation or IEEE 802.1AX-2008, is a networking term that describes the use of multiple network cables and ports in parallel to increase the link speed and redundancy for higher availability. |
| **\*Note –** The ELOM IP address is most easily configured using a serial connection. Initially, connect a DB9-to-DB9 serial null modem cable from a laptop PC serial port to the serial port on the server. | |

The initial setup of a KMA requires a terminal emulator on a laptop or monitor/keyboard assembly to access the Embedded Lights Out Manager (ELOM). The ELOM is a remote console function that requires a network connection and IP address to use these functions.

# Key Management Appliance Physical Connections

All of the physical connections are from the rear of the KMA.

**FIGURE 1-10** Key Management Appliance—Rear Panel Connections
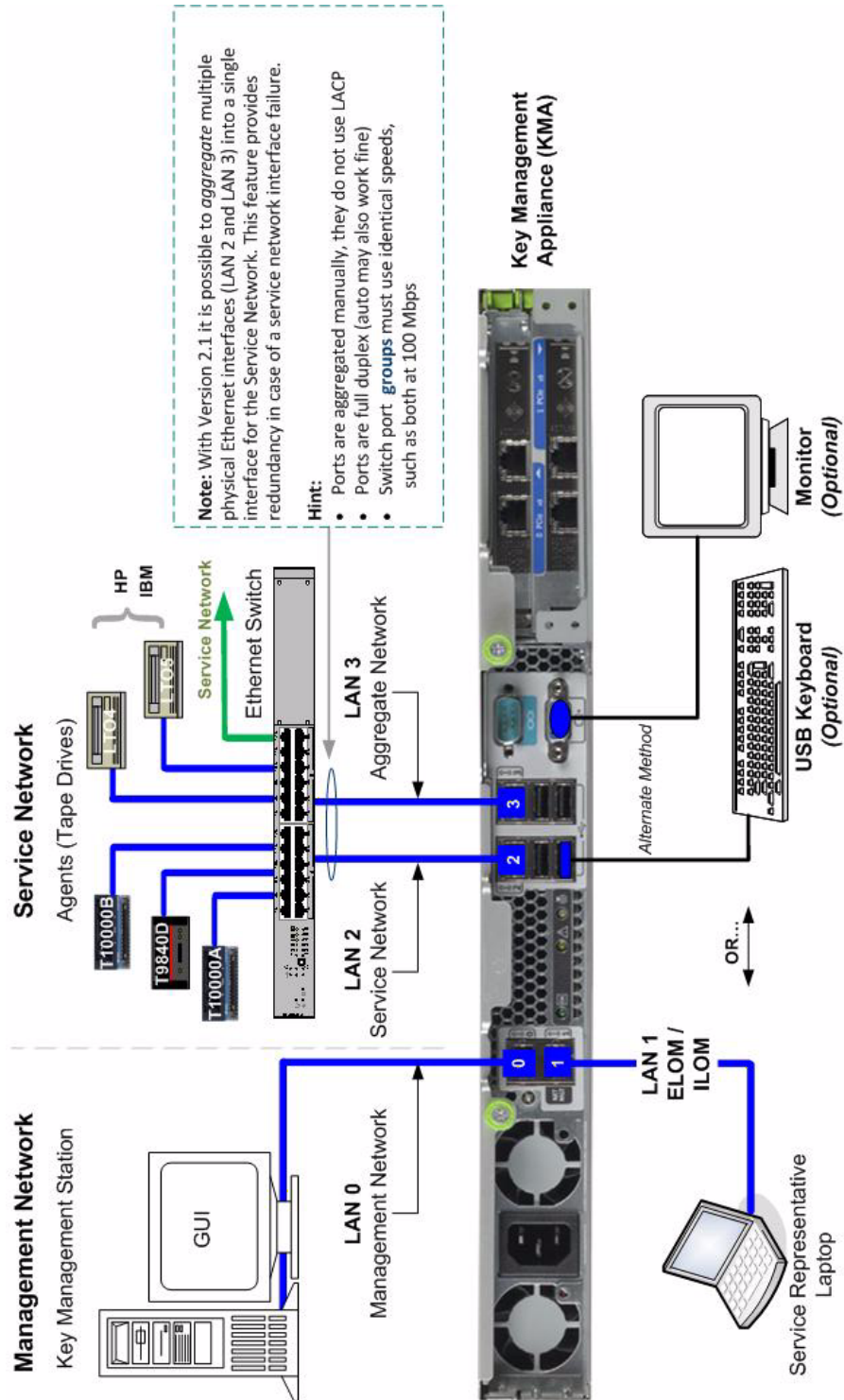
# Internet Protocol Versions

Enhancements made to Version 2.1 included support for the newest implementation of the Internet Protocol Suite, or IP.

- The current version—IPv4—uses a 32-bit number written as four groups of three numbers separated by periods. Each group can be from 0 to 255, for example, 129.80.180.234.

  Within these four groups are two identifiers, the network address and the host address. The first two groups (129.80) identify the network address, the second two groups (180.234) identify the host.

- The new generation—**IPv6—**uses a 128-bit value written as eight groups of four hexadecimal characters separated by colons, for example,
  2001:0db8:85a3:0000:0000:8a2e:0370:7334
  2001:0db8:85a3:::8a2e:0370:7334 (means the same as above)

  IPv6 addresses are typically composed of two logical parts: a 64-bit network prefix, and a 64-bit host address, which is either automatically generated or assigned.

**Important:**
The Key Manager supports a "dual stack" implementation where both protocols are used within the system. However, not all applications use IPv6, for example, Domain Name System (DNS); therefore, IPv4 is still necessary.

# Automated Tape Libraries

Because every customer has different needs and requirements, Oracle's StorageTek automated tape libraries provides a variety of libraries to meet these customers demands.

**TABLE 1-5** Tape Libraries

| Tape Libraries | L700 | L1400 | 9310 | SL24 | SL48 | SL500 | SL3000 | SL8500 |
|---|---|---|---|---|---|---|---|---|
| Minimum slots | 216 | 200 | 2,000 | 1 | 1 | 30 or 50 | 200 | 1,448 |
| Maximum slots | 1,344 | 1,344 | 6,000 | 24 | 48 | 440 to 575 | 5,925 | 10,000 |
| Complex/ACS | No | No | 144,000 | No | No | No | No | 100,000 |
| Mixed-media | Yes | Yes | Yes | No | No | Yes | Yes | Yes |
| Pass-thru ports | Yes (1) | Yes (1) | Yes | No | No | No | No | Yes |
| Maximum drives | 24, 40 | 24, 40 | 80, 960 | 1 | 2 | 2, 18 | 56 | 64, 640 |
| CAP size | 20–80 | 20–80 | 21 or 80 | Mailslots | Mailslots | 5–45 | 26 | 39 |
| Number of CAPs | 1–4 | 1–4 | 4x20 | 0–1 | 1–3 | 1–5 | 10[1] | 2 |
| Interface type | SCSI, FC | SCSI, FC | TCP/IP | SCSI, FC, SAS | SCSI, FC, SAS | SCSI, FC | SCSI, FC | TCP/IP |
| **Tape Technology (Encryption-capable Tape Drives Only)** | | | | | | | | |
| T9840D (StorageTek) | Yes | Yes | Yes | No | No | No | Yes | Yes |
| T10000A (StorageTek) | Yes | Yes | Yes | No | No | No | Yes | Yes |
| T10000B (StorageTek) | Yes | Yes | Yes | No | No | No | Yes | Yes |
| LTO4 (HP and IBM) | No | No | No | Verify Support | | Yes | Yes | Yes |
| LTO5 (HP and IBM) | No | No | No | Yes | Yes | Yes | Yes | Yes |
| 1. Access expansion modules provide bulk cartridge loading capabilities from 234 to 468 cartridges (one or two AEMs) | | | | | | | | |

# Tape Drives

Well known for its *state-of-the-art* tape technology, StorageTek has numerous years of experience and leadership in tape and tape automation. Today, StorageTek, with its proven technology, continues to provide storage solutions for:

■ Small to large businesses and organizations

■ Enterprise and client-server platforms

■ Stand-alone and automated tape environments

There are seven tape drive models to choose from:

■ StorageTek T10000A

■ StorageTek T10000B

■ StorageTek T9840 Model D only

■ Hewlett Packard (HP) Linear Tape-Open (LTO) Generations 4 and 5

■ International Business Machines (IBM) Linear Tape-Open (LTO) Generations 4 and 5

## FIPS Compliant Tape Drives

Beginning with Version 2.1 and the latest tape drive firmware, the following drives are FIPS[3] compliant.

**TABLE 1-6** FIPS 140-2 Compliant Tape Drives

| Tape Drive | FIPS 140-2 Level |
|---|---|
| T10000A | 1 |
| T10000B | 2 |
| T9840D | 1 |
| LTO4 (HP and IBM) | No plans for FIPS* |
| LTO5 (HP and IBM) | No plans for FIPS* |
| * LTO drives may be FIPS validated in its basic form but not necessarily in specific encryption applications. | |

FIPS 140-2 levels of security for the above tape drives includes Levels 1 and 2.

> **Level 1** – The basic level with production-grade requirements.

> **Level 2** – Adds requirements for physical tamper evidence and role-based authentication. Built on a validated operating platform.

This selection provides a higher level of security for the KMAs and tape drives.

---

3. **FIPS 140-2** = is a U.S. government computer security standard used to accredit cryptographic modules.Federal Information Processing Standards are publicly announced standards and guidelines developed by the United States Federal government. Many FIPS standards are modified versions of standards used in the wider community (ANSI, NIST, IEEE, ISO, etc.).

# About the StorageTek T10000 Tape Drive

The StorageTek T10000 tape drives are modular, high-performance tape drives designed for high-capacity storage.

There are two models of the T10000 that support encryption:

- T10000A
- T10000B

**Dimensions:** The tape drive is:

- 8.89 cm (3.5 in.) high
- 14.6 cm (5.75 in.) wide
- 42.5 cm (16.75 in.) deep.

**Capacity:**

- T10000A = 500 gigabytes (GB) of uncompressed data
- T10000B = 1 terabyte (TB) of uncompressed data[4]

# About the StorageTek T9840D Tape Drive

The StorageTek T9840D tape drive is a small, high-performance, **access-centric** tape drive that has an average access time of just 8 seconds.

This drive obtains its high-performance by using a unique *dual-hub* cartridge design with midpoint load technology. This enables fast access and reduces latency by positioning the read/write head in the middle of the tape.

There are four models of the T9840; however, only the T9840D supports encryption.

**Dimensions:** The tape drive is:

- 8.25 cm (3.25 in.) high
- 14.6 cm (5.75 in.) wide
- 38.1 cm (15 in.) deep

**Capacity:**
T9840D = 75 gigabytes (GB) of uncompressed data

For a variety of operating system platforms:

- Enterprise mainframes (z/OS and OS/390)
- Open system platforms (Windows, UNIX, and Linux)

---

4. **Capacity:** To get an idea of the capacity of a terabyte, consider the common megabyte (MB). Just over thousand megabytes equals one gigabyte, and just over one million megabytes equals a terabyte.
1,024 megabytes = 1 gigabyte
1,024 gigabytes = 1 terabyte
1,048,576 ($1,024^2$) megabytes = 1 terabyte

# About the LTO Tape Drives

**Overview**

Linear Tape-Open (LTO) tape drives are a high-performance, high-capacity, data-storage device that is designed for backup and restore applications in both enterprise mainframe and open systems environments.

Both HP and IBM offer a fourth- and fifth-generation, Ultrium series of linear tape-open products called the LTO4 and LTO5 tape drives.

*Note:* Currently, only the LTO4 and LTO5 tape drives are capable of supporting tape- or device-based encryption.

**Encryption Capable**

Both the HP and IBM LTO drives support write encryption and read decryption when integrated into a secure encryption system, such as Oracle's Key Manager.

Key management is essential to ensure that what is written on tape can be read in the future.

Being able to manage the "Keys to Encryption" requires a special, custom-designed, Ethernet **adapter card** mounted inside the drive tray. This adapter card provides a means for the LTO drives to connect to and interface with the Oracle Key Manager. Each vendor has their own unique version of an adapter card:
- HP LTO4 = Dione card (external)
- HP LTO5 = Embedded (no adpater card required)
- IBM = Belisarius card (external)

With this connection, the LTO drives are capable of communicating with the OKM to transfer encryption keys over the secure network.

*Note:* Currently the LTO drives can only use *one encryption key at a time.* During a read operation, if another encryption key is found on the tape, the adapter card requests the key directly from the OKM.

**Media** (Native capacity)

LTO5 tape drives use a 1.5 TB Data Cratridge and LTO4 tape drives use an 800 GB Data Cartridge, both are compatible with other vendor cartridges and other generations of LTO tape drives.
The drive performs the following functions:
- Reads/Writes LTO5 cartridges in Ultrium 5 format, including WORM
- Reads/Writes LTO4 cartridges in Ultrium 4 format, including WORM

LTO5 and LTO4 tape drives also support Write Once, Read Many (WORM) secure media. This non-erasable, non-rewritable media complies with regulations such as HIPAA, Sarbanes-Oxley, and SEC 17A-4.

**Interfaces**

LTO drives come with a Fibre Channel interface (FC), in either a single or dual port configuration.

The HP LTO tape drives also supports:
- Ultra 320 Small Computer System Interface (SCSI)
-

# Tape Drive Comparisons

**TABLE 0-1** Tape Drive Comparison

| Specification | StorageTek | | | | HP | | IBM | |
|---|---|---|---|---|---|---|---|---|
| | **T10K A** | **T10K B** | **T9840C** | **T9840D** | **LTO4** | **LTO5** | **LTO4** | **LTO5** |
| Capacity (native) | 500 GB | 1 TB | 40 GB | 75 GB | 800 GB | 1.5 TB | 800 GB | 1.5 TB |
| Transfer rates (native) | 120 MB/s | 120 MB/s | 30 MB/s | 30 MB/s | 120 MB/s | 140 MB/s | 120 MB/s | 140 MB/s |
| Buffer size | 256 MB | 256 MB | 64 MB | 64 MB | 256 MB | 256 MB | 256 MB | 256 MB |
| Load Time (seconds) | 16 sec | 16 sec | 6.5 sec | 8.5 sec | 19 sec | 12 sec | 15 sec | 12 sec |
| Access (seconds) | 46 sec | 46 | 8 sec | 8 sec | 72 sec | 60 sec | 46 sec | 60 sec |
| Tape speed (m/s) | 2–4.95 | 2–3.74 | 3.295 | 3.4 | 7.0 | — | 7.0 | — |
| Rewind time (seconds) | 90 | 90 | 16 / 8 | 16 / 8 | 106/54 sec | 96/ 78 sec | 106/54 sec | 96/ 78 sec |
| Unload Time | 23 sec | 23 sec | 11.5 sec | 12 sec | 22 sec | 17 sec | 22 sec | 17 sec |
| **Interfaces** | | | | | | | | |
| Fibre Channel | 2 & 4 Gb/s | 4 Gb/s | 2 Gb/s | 4 Gb/s | 4 Gb/s | 8 Gb/s | 4 Gb/s | 8 Gb/s |
| SCSI / SAS | no | no | no | no | Ultra-320 | 6 Gb SAS | Ultra-320 | 6 Gb SAS |
| FICON | 2 Gb/s | 2 Gb/s | 2 Gb/s | 2 Gb/s | Not Supported | | Not Supported | |
| ESCON | 2 Gb/s | 2 Gb/s | 18 MB/s | 2 Gb/s | | | | |
| **Compatibility** | | | | | | | | |
| Availability (MTBF) | 290,000 hrs | | 290,000 hrs | | 250,000 hrs | | 250,000 hrs | |
| Tracks | 768 | 1152 | 288 | 576 | 896 | 1280 | 896 | 1280 |
| Length–usable | 855 m (2805 ft) | 855 m (2805 ft) | 251 m (889 ft) | 251 m (889 ft) | 820 m (2690 ft) | 850 m (2789 ft) | 820 m (2690 ft) | 850 m (2789 ft) |
| VolSafe—WORM | yes | yes | yes | yes | yes | yes | yes | yes |

For your information, the following tables provide tape drive and media comparisons.

# StorageTek T-Series Tape Drives

TABLE 1-7 shows the media compatibilities for the T-Series (T10000 and T9840) drives:

- Encryption-capable T-Series tape drives
- Non-encryption T-Series tape drives

**TABLE 1-7** T-Series Tape Drive Media Compatibilities

| Task | Enrolled for Encryption | Not Enrolled for Encryption |
|------|-------------------------|------------------------------|
| Write new data encrypted | Yes | No |
| Write new data not encrypted | No | Yes |
| Read encrypted data with key available | Yes | No |
| Read non-encrypted data | Yes | Yes |
| Append non-encrypted data to encrypted tape | No | No |

TABLE 1-8 shows a comparison between:

- Encryption-enabled and non-encrypted tape drives
- Encrypted and non-encrypted media

**TABLE 1-8** T-Series Tape Drive and Media Support

| Tape Drive Types | Media Types | |
|------------------|-------------|--|
| | **Non-encrypted Tapes** | **Encrypted Tapes** |
| **Standard drive** (non-encrypted) | ■ Fully compatible<br>■ Read, write, and append | ■ **Not capable** of reading, writing to or appending to this tape<br>■ Can re-write from the beginning of tape (BOT) |
| **Encryption-capable drive** | ■ **Read** capability only<br>■ Not capable of appending to this tape<br>■ Can re-write from the beginning-of-tape (BOT) | ■ Fully compatible<br>■ Read with correct keys<br>■ Write with current write key |

## LTO Tape Drives

**Notes:** Both HP and IBM LTO tape drives are:

■ Specified to interchange with un-encrypted data cartridges from other tape drives that comply to the LTO U-28, U-316 and U-416 specifications.

■ Capable of interchanging encrypted data cartridges provided the correct encryption key is available.

### Future compatibility:

In the future, LTO drives will be capable of:

■ Reading and writing tapes from the current generation

■ Reading and writing tapes from *one* earlier generation

■ Reading tapes from *two* earlier generations

**Note –** Encryption is only supported with LTO4 and LTO5 Data Cartridges on LTO4 and LTO5 tape drives. To avoid problems, these drives will not write in normal or native modes once the drive is enabled for encryption.

## LTO Encryption Behavior

When LTO encryption is controlled by the Oracle Key Manager, the LTO drives can behave differently from StorageTek T-Series drives. There can also be slight differences between the HP and IBM drives from each other. These differences arise from specific aspects of the IBM and HP drive architecture.

TABLE 1-9 lists the various scenarios and how HP and IBM drives behave.

**TABLE 1-9** LTO4 Encryption Behavior

| LTO4 Drive Performance | HP Implementation | IBM Implementation |
|---|---|---|
| **Not Enrolled for Encryption** | | |
| Read LTO4 non-encrypted data | OK non-encrypted | OK non-encrypted |
| Read LTO4 encrypted data | Error | Error |
| Write LTO4 from BOT | OK non-encrypted | OK non-encrypted |
| Read LTO3 tape | OK non-encrypted | OK non-encrypted |
| LTO4 append write to non-encrypted data (Space EOD and write) | OK non-encrypted | OK non-encrypted |
| LTO4 append write to non-encrypted data (Read to EOD and write) | OK non-encrypted | OK non-encrypted |
| LTO4 append write to encrypted data (Space EOD and write) | OK non-encrypted (Note 1) | OK non-encrypted (Note 1) |
| LTO4 append write to encrypted data (Read to EOD and write) | Error | Error |

**TABLE 1-9** LTO4 Encryption Behavior  (Continued)

| LTO4 Drive Performance | HP Implementation | IBM Implementation |
| --- | --- | --- |
| **Enrolled for Encryption** | | |
| Read LTO4 non-encrypted data | OK non-encrypted | OK - non-encrypted |
| Read LTO4 encrypted data | OK* encrypted | OK* encrypted |
| Write LTO4 from BOT | OK* encrypted | OK* encrypted |
| LTO4 append write to encrypted data | OK* encrypted | OK* encrypted |
| Write LTO3 tape | OK non-encrypted (Note 5) | Error (Note 6) |
| Read LTO3 tape | OK non-encrypted | OK non-encrypted |
| LTO4 append write to non-encrypted data (Space EOD and write) | OK* encrypted (Note 2) | Error (Note 3) |
| LTO4 append write to non-encrypted data (Read to EOD and write) | OK* encrypted (Note2) | Error (Note 3) |
| LTO4 append write to encrypted data (Space EOD and write) | OK* encrypted | OK* encrypted |
| LTO4 append write to encrypted data (Read to EOD and write) | OK* encrypted | OK* encrypted – but with prior read key (Note 4) |
| * If the correct key is available. | | |

| | |
| --- | --- |
| **Note 1** | Enterprise drives do not allow the mixing of encrypted and non-encrypted data on a single tape. |
| **Note 2** | While this scenario allows appending encrypted data behind non-encrypted data, this has an operational benefit since it allows tapes pre-labeled with non-encrypted data to be used in an HP LTO drives in the encrypting environment without having to re-label them. |
| **Note 3** | In this scenario, unlike HP drives, IBM drives will error in this scenario. |
| **Note 4** |  In this scenario, IBM drives will write encrypted data but will use the same key as it used to read the prior encrypted data on tape. The drive will not request a new key from the OKM when the write command is issued and this will ignore the Key Expiration Policy set by the OKM. |
| **Note 5** | HP drives will write tapes in non-encrypted mode. The LTO3 format does not support encryption and this could be considered a security violation since an HP LTO4/LTO5 drives can be made to write non-encrypted data simply by inserting a LTO3 cartridge. |
| **Note 6** | IBM drives will report an error if an attempt is made to write LTO3 tapes. |

# Systems Assurance

This chapter contains information about the systems assurance process.

The system assurance process is the exchange of information among team members to ensure that no aspects of the sale, order, installation and implementation for the Oracle Key Manager are overlooked. This process promotes an error-free installation and contributes to the overall customer satisfaction.

The system assurance team members (customer and Oracle/StorageTek) ensure that all aspects of the process are planned carefully and performed efficiently. This process begins when the customer accepts the sales proposal. At this time, a representative schedules the system assurance planning meetings.

# Planning Meetings

The purpose of the system assurance planning meetings is to:

- Introduce the customer to Oracle's encryption products
- Explain the system assurance process and establish the team
- Identify and define the customer requirements
- Identify any additional items needed (such as cables, tokens, and switches)
- Prepare for the installation and implementation
- Schedule and track the entire process

**TABLE 2-1** System Assurance Task Checklist

| Task | Completed? |
|---|---|
| Introduce the team members to the customer.<br>Complete the Team Member Contact sheets.<br>Make copies as necessary. | Yes ❑   No ❑ |
| Explain the encryption solutions to the customer.<br>See Chapter 1, "Introduction" for topics and information. | Yes ❑   No ❑ |
| Use Chapter 2, "Systems Assurance" to help define the customer requirements. | Yes ❑   No ❑ |
| Complete the Team Member Contact sheets. | Yes ❑   No ❑ |
| Review and complete Chapter 3, "Site Preparation".<br>*Comments:* | Yes ❑   No ❑ |
| Review and identify "User Roles Work Sheet".<br>*Comments:* | Yes ❑   No ❑ |
| Review Chapter 4, "Components".<br>*Comments:* | Yes ❑   No ❑ |
| Review "Supported Configurations".<br>*Comments:* | Yes ❑   No ❑ |
| Determine the installation schedule:<br><br>**Date:** _____<br><br>**Time:** _____ | Yes ❑   No ❑ |
| Download and provide the customer with a copy of the:<br>*Administrator's Guide* PN 316195101.<br>*Virtual Operator Panel—Customer* PN: 96179<br>http://docs.sun.com/app/docs/prod/stortek.crypto.keymgmt | Yes ❑   No ❑ |

# Customer Team Member Contact Sheet

Complete the following information for the customer team members:

**Name:**

Title:

Telephone Number:

FAX Number:

Cell Phone / Pager:

E-mail Address:

**Name:**

Title:

Telephone Number:

FAX Number:

Cell Phone / Pager:

E-mail Address:

**Name:**

Title:

Telephone Number:

FAX Number:

Cell Phone / Pager:

E-mail Address:

**Name:**

Title:

Telephone Number:

FAX Number:

Cell Phone / Pager:

E-mail Address:

**Note –** Customer representatives may include: security officers, finance managers, IT managers, network administrators, systems administrators, site planning managers, and anyone else involved in installations.

# Oracle Team Member Contact Sheet

Complete the following information for the Oracle team members:

**Name:** _____

Title: _____

Telephone Number: _____

FAX Number: _____

Cell Phone / Pager: _____

E-mail Address: _____


**Name:** _____

Title: _____

Telephone Number: _____

FAX Number: _____

Cell Phone / Pager: _____

E-mail Address: _____


**Name:** _____

Title: _____

Telephone Number: _____

FAX Number: _____

Cell Phone / Pager: _____

E-mail Address: _____


**Name:** _____

Title: _____

Telephone Number: _____

FAX Number: _____

Cell Phone / Pager: _____

E-mail Address: _____


**Note –** Representatives may include: marketing, sales, and account representative, systems engineers (SEs), Professional Services (PS), installation coordinators, and trained services personnel.

# Configuration Planning

Complete the following checklist and make a conceptual drawing to help with the installation. Provide this information and drawing to the installers.

Use this checklist for each Key Manager the customer is considering. This checklist is geared towards planning a single Oracle Key Manager system, with up to 20 OKMs.

**TABLE 2-2** Solution Planning Checklist

| Question | Selection / Comments | Quantity |
|---|---|---|
| What type of configuration does the customer want?<br>**Notes:**<br>■ The maximum number of sites with KMAs is 20.<br> It is possible to have sites without KMAs connected across a customer supplied wide area network.<br>■ Also, the 20 site limit is within a single cluster.<br> The customer may choose to have multiple clusters; however, KMAs in one clusters are unaware of KMAs in other clusters. | ❏ Single site<br><br>❏ Multiple sites<br><br>❏ Disaster recovery site | How many:<br>_____<br><br>_____<br><br>_____ |
| How many appliances (KMAs) are needed?<br>■ The maximum number of KMAs is 20.<br>■ The minimum OKM size is 2*.<br>■ The recommendation is at least 2 (assuming sites are geographically dispersed)<br><br>* The exception to this standard configuration (single-node site) must be made with the approval of Encryption Engineering, Professional Services, and Support Services. | | How many:<br>_____ |
| What type of encryption **hardware kits** are needed?<br><br>How many encryption hardware kits are needed? | ❏ SL8500<br>❏ SL3000<br>❏ SL500<br>❏ 9310 / 9741E<br>❏ L-Series<br>❏ Rackmount | How many:<br>_____<br>_____<br>_____<br>_____<br>_____<br>_____ |
| How many and of what type of encryption-capable tape drives are needed? | ❏ T10000A<br>❏ T10000B<br>❏ T9840D<br>❏ HP LTO 4 or 5<br>❏ IBM LTO 4 or 5 | How many:<br>_____<br>_____<br>_____<br>_____<br>_____ |
| Are external (standalone) Racks required?<br>Type? | ❏ Yes<br>❏ No | How many:<br>_____ |
| Identify customer requirements and expectations. | | |

The following page provides space to help sketch a drawing of the configuration.

# Site Preparation

Use this chapter and checklists to prepare for the installation.

- *"Site Planning Checklist"*

There are a few things to be aware of to install encryption hardware into a supported configuration, such as:

- *"Rack Specifications"*
- *"Service Delivery Platform"*
- *"Content Management"*
  - *Capacity on Demand*
  - *RealTime Growth Technology*
  - *Partitioning*
  - *Planning the Data Path*
  - *Planning Tasks*
- *"Required Tools"*
- *"Supported Platforms and Web Browsers"*
- *"Firmware Levels"*
- *"Role-Based Operations"*

# Site Planning Checklist

Use the following checklist to ensure that the customer is ready to receive the Key Management System and to ensure that you are ready to start the installation.

**TABLE 3-1** Site Planning Checklist

| Question | Completed? | Comments: |
|---|---|---|
| **Delivery and Handling** | | |
| **Important:** The Oracle Key Manager and appliances are considered "secure" items. Follow the customers security guidelines during delivery and installation. | | |
| Does the customer have a delivery dock? If *no*, where will the equipment be delivered? If a delivery dock *is* available, what are the hours of operation? | Yes ❏   No ❏ | |
| Are there street or alley limitations that might hinder delivery? | Yes ❏   No ❏ | |
| Will authorized personnel be available to handle and accept the delivery? | Yes ❏   No ❏ | |
| Is the delivery location close to the computer room where the equipment will be installed? | Yes ❏   No ❏ | |
| Is an elevator available to move the equipment to the appropriate floors? | Yes ❏   No ❏ | |
| Is there a staging area where the equipment can be placed close to the installation site? | Yes ❏   No ❏ | |
| Are there special requirements to dispose of or *recycle* packing material? Pallets, plastic, and cardboard? | Yes ❏   No ❏ | |
| **Environmental Planning** | | |
| Does the site meet the environmental requirements for temperature, humidity, and cooling? | Yes ❏   No ❏ | See Key Management Appliance for the appliance specifications. |

**TABLE 3-1** Site Planning Checklist  (Continued)

| Question | Completed? | Comments: |
|---|---|---|
| **Power Requirements** | | |
| Does the intended site meet the power requirements? | Yes ❑   No ❑ | See Key Management Appliance for the appliance specifications. **KMA:** 90 to 132 VAC \| 180 to 264 VAC 57 to 63 Hz \| 47 to 53 Hz 2.3 to 4.6 Amps Maximum continuous power is 150 W |
| Has the customer identified the circuit breakers locations and ratings? | Yes ❑   No ❑ | |
| Does the customer want redundant power options? If so, an additional APC power switch is required to create an uninterrupted power configuration. | Yes ❑   No ❑ | Check for updated model and part numbers. (Part number #419951602) |
| Are there any power cable routing requirements and concerns? | Yes ❑   No ❑ | See Power Cables for more information. |
| **Personnel:** | | |
| Are there trained/qualified Oracle representatives locally to install and maintain the encryption equipment? | Yes ❑   No ❑ | **Names:** |
| **Connectivity:** Cabling is *very important* to establish a reliable network between the OKM, KMAs, Ethernet switches, and tape drives. | | |
| Does this customer support **IPv6** implementations? | Yes ❑   No ❑ | |
| Does the customer intend on using **Managed** switches for LANs 2 and 3? | Yes ❑   No ❑ | Cable considerations are impacted by the decision to use a managed switch and the corresponding topology of the service network. |
| Is a **Wide Area Service Network** being considered? | Yes ❑   No ❑ | Designing the service network across a WAN to remote sites adds additional failover capability to the agents and can facilitate disaster recovery scenarios. |
| Does the customer want to **aggregate** the service ports (LAN 2 and LAN 3)? | Yes ❑   No ❑ | Requires additional cables and compatible port configuration on a customer supplied managed switch. |
| Does the customer plan to use a private network for the agents (tape drives)? | Yes ❑   No ❑ | Removes contention for the tape drives. |

**TABLE 3-1** Site Planning Checklist  (Continued)

| Question | Completed? | Comments: |
|---|---|---|
| **Connectivity** (continued) | | |
| Will there be a Service Delivery Platform (**SDP**) installed at this site? | Yes ❏   No ❏ | See SDP on page 44 for information. |
| Will the customer be monitoring the OKM using **SNMP**? | Yes ❏   No ❏ | SNMP v3 recommended<br>SNMP v2 supported |
| Are there considerations for monitoring of **ELOM/ILOM** using the LAN 1 port? | Yes ❏   No ❏ | Refer to the SunFire X2100/2200 ELOM Administration Guide, or X4170 ILOM Supplement Guides for information. |
| Have you and the customer completed a:<br>■ Cable plan?<br>■ Do the agents have private network?<br>■ Configuration drawing?<br>    A drawing can help determine the number of and length of the cables required. | Yes ❏   No ❏<br>Yes ❏   No ❏<br>Yes ❏   No ❏ | |
| Have you determined the type and number of Ethernet cables required?<br>*Customer supplied:*<br>■ OKM to the network<br>■ Encryption Network to the KMAs (LAN 0)<br>■ ELOM/ILOM monitoring (LAN 1)<br>■ Service network to agents (LAN 2 & 3)<br><br>*Supplied in the encryption kits:*<br>■ Switch to tape drives | Yes ❏   No ❏ | **Note:**<br>■ Ethernet cables are shipped with kits.<br>■ Lengths are dependant on the location of the switches and devices.<br><br>**Note:** A onfiguration drawing will help identify the cables needed. |
| **Configurations** | | |
| Does the customer have adequate rack space to hold the KMAs and Ethernet switches? | Yes ❏   No ❏ | See "Rack Specifications" on page 38 |
| What type of support configurations does the customer want or need?<br><br>❏ Existing configuration<br><br>❏ New configuration | Configuration<br>❏ SL8500<br>❏ SL3000<br>❏ SL500<br>❏ 9310/9741e<br>❏ L-Series<br>❏ SL24/48<br>❏ Rackmount | Encryption-capable Drives:<br>T-Series & LTO drives<br>T-Series & LTO drives<br>LTO only<br>T-Series only<br>T-Series only<br>LTO only<br>T-Series only |
| Does the customer have existing tape drives they want to upgrade to encryption-capable?<br><br>Are these drives already installed in a library? | Yes ❏   No ❏<br><br><br>Yes ❏   No ❏ | See Chapter 4, "Components" for x-options (conversion bills). |

**TABLE 3-1** Site Planning Checklist  (Continued)

| Question | Completed? | Comments: |
|---|---|---|
| **Drive types?**<br><br>Check current and required firmware versions. | ❏ T10000A<br>❏ T10000B<br>❏ T9840D<br>❏ HP LTO4<br>❏ IBM LTO4<br>❏ HP LTO5<br>❏ IBM LTO5 | <br><br><br>Requires drive tray and Dione card<br>Requires drive tray and Belisarius card<br><br>Requires drive tray and Belisarius card |
| **Configurations** (continued) | | |
| Does the customer need to order more drives?<br>■ Tape drive type:<br><br>■ Interface types?<br>  ■ (FC) Fibre Channel (all tape drives)<br>  ■ (FI) FICON (T-Series only)<br>  ■ (ES) ESCON (T9840D)<br>  ■ SCSI (SL500 library and LTO drive only) | Yes ❏   No ❏<br><br>❏ T10000A<br>❏ T10000B<br>❏ T9840D<br>❏ HP LTO4<br>❏ IBM LTO4<br>❏ HP LTO5<br>❏ IBM LTO5 | How many tape drives? |
| Are additional cartridges required?<br>■ Data cartridge<br>■ Cleaning cartridges<br>■ VolSafe cartridges<br>■ Labels<br><br>■ Type: _____<br><br>■ Quantity: _____ | <br>Yes ❏   No ❏<br>Yes ❏   No ❏<br>Yes ❏   No ❏<br>Yes ❏   No ❏ | **Note:**<br>All versions of encryption tape drives use different, unique cartridges.<br>■ T9840 = 9840 cartridges<br>■ T10000 = T10000 cartridges<br>■ LTO4 = LTO4 cartridges.<br>■ LTO5 = LTO5 cartridges.<br>All versions of each cartridge-type are supported, for example: standard, sport, VolSafe, and WORM. |
| | | |
| **Notes:** | | |
| **Configurations:** | | |
| **Tape Drives and Media:** | | |

# Rack Specifications

The KMAs can be installed in standard, RETMA[1] 19-inch, four post racks or cabinets. Note: Two-post racks are *not* supported.

The slide rails are compatible for a wide range of racks with the following standards:

- Horizontal opening and unit vertical pitch conforming to ANSI/EIA 310-D-1992 or IEC 60927 standards.
- Distance between front and rear mounting planes between 610 mm and 915 mm (24 in. to 36 in.).
- Clearance depth to a front cabinet door must be at least 25.4 mm (1 in.).
- Clearance depth to a rear cabinet door at least 800 mm (31.5 in.) to incorporate cable management or 700 mm (27.5 in.) without cable management.
- Clearance width between structural supports and cable troughs and between front and rear mounting planes is at least 456 mm (18 in.).

## SL8500 Rack Guidelines

An SL8500 library can have up to 4 *optional* accessory racks, (PN XSL8500-RACK-Z). If the customer wants power redundancy, a minimum of 2 racks are required.

Each rack can hold up to 6 units, called Us[2], of equipment, such as the key management appliances and the Ethernet switches. Each rack has a six-connector power distribution unit (PDU) that provides power and two cooling fans that provides additional air flow. Table 3-2 lists the rack guidelines.

**TABLE 3-2** SL8500 Accessory Rack Guidelines

| Guideline | Descriptions |
| --- | --- |
| **Rack numbering** | Rack numbering is top-down from 1 to 4.<br>Rack 1 is on the top; Rack 4 is on the bottom. |
| **Rack mounting** | Components must be able to function in a vertical orientation. |
| **Dimensional restrictions** | Rack module depth is 72 cm (28 in.).<br>Recommended safe length is 66 cm (26 in.). |
| **Equipment weight** | The accessory rack itself is mounted on slides rated for 80 kg (175 lb).<br>The recommended safe load is 64 kg (140 lb).<br>The KMA is 10.7 kg (23.45 lb), the Ethernet switch is 1.5 kg (3.1 lb) |
| **Power consumption** | Per rack module is 4 Amps (maximum). Per outlet strip is 200–240 VAC, 50–60 Hz.<br>The KMA is 185 W, the Ethernet Switch is 20 W. |
| **Power cord** | Power plug to connect to the rack PDU is: IEC320 C13 shrouded male plug.<br>Minimum cord length is component *plus* 46 cm (18 in.) for a service loop. |
| **Thermal requirements** | Maximum power dissipation is 880 watts (3,000 Btu/hr) per rack module. |
| **Regulatory compliance** | Minimum requirements are: Safety—UL or CSA certification and Electromagnetic—Class A certification from agencies such as FCC or BSMI. |

1. **RETMA** = Radio Electronics Television Manufacturers Association.

2. **U** stands for rack units. One unit is equal to 4.4 cm (1.75 in.).

# Network Considerations

StorageTek engineering recommends that *customers supply* a **managed switch** for connecting KMAs to the tape drives on their service network. Managed switches would then supply connectivity to the StorageTek-supplied unmanaged switches as well as any connectivity to customer supplied routers for wide area service network.

The following managed switches have been tested and are recommended:

- 3COM Switch 4500G 24-Port (3CR17761-91)
- Extreme Networks Summit X150-24t Switch

Other managed switches can be used but engineering only provides configuration guidance on the above listed switches.

Managed switches are recommended for the following reasons:

- Improved serviceability through better switch diagnostics and service network trouble shooting
- Potential for minimizing single points of failure on the service network through use of redundant connections and spanning tree protocol.
- Support for aggreation of the KMA service network interfaces to minimize single point of failure on the KMA's service interface.

FIGURE 3-1 provides an example of a managed switch configuration. In this example, if either KMA or either managed switch should fail, the drives still have a path from which they can communicate with the other KMA.

# KMA Service Port Aggregation

It is possible to aggregate physical Ethernet interfaces (LAN 2 and LAN 3) into a single virtual interface. Additional availability is achieved by aggregating these ports; if a failure occurs with either port, the other port maintains connectivity.

Make sure the Ethernet switch ports have the correct configuration. For example, Switch ports should be:

- Set to auto negotiate settings for duplex (should be full duplex).
- Set to auto negotiate speed settings, the KMA ports are capable of gigabit speeds.
- Using identical speeds, such as: both set to 100 Mbps (auto speed negotiating may work fine).

## Aggregated Service Network Switch Configuration

To provide redundancy in case of a service network interface failure, the LAN 2 port may now be aggregated with the LAN 3 port. To use the port aggregation feature, you need to configure the switches for link aggregation. The Solaris port selection policy on the KMA is address based. Here is some information about the service port aggregation that may be needed to configure the switch:

- Ports are aggregated manually, meaning they do not use LACP
- Ports are full duplex (auto may work fine)

- Switch ports used for aggregation groups must be identical speed, for example, both ports are set to 100 Mbps (auto speed negotiating may work fine)

**Notes:**

- There may be an order or connection dependency. Create the aggregation group on the switch *before* connecting the KMAs service port.
- If the aggregated IP address (IPv4 or IPv6) is not responding, reboot the KMA.

A System Dump using the Management GUI will contain display aggregated port information. The information is gathered using dladm commands.

*Extreme Network Switch Configuration*

To configure aggregated ports on an Extreme Ethernet switch

1. Login to the switch using telnet.

2. Enter the following CLI commands:

```
show port sharing
enable sharing <b> port></b> grouping <b> portlist</b>
algorithm address-based L3_L4
```

Port specifies the master port for a load sharing group.

Portlist specifies one or more ports or slots and ports to be grouped to the master port. On a stand-alone switch (this is what is normally supplied), can be one or more port numbers. May be in the form 1, 2, 3, 4, 5.
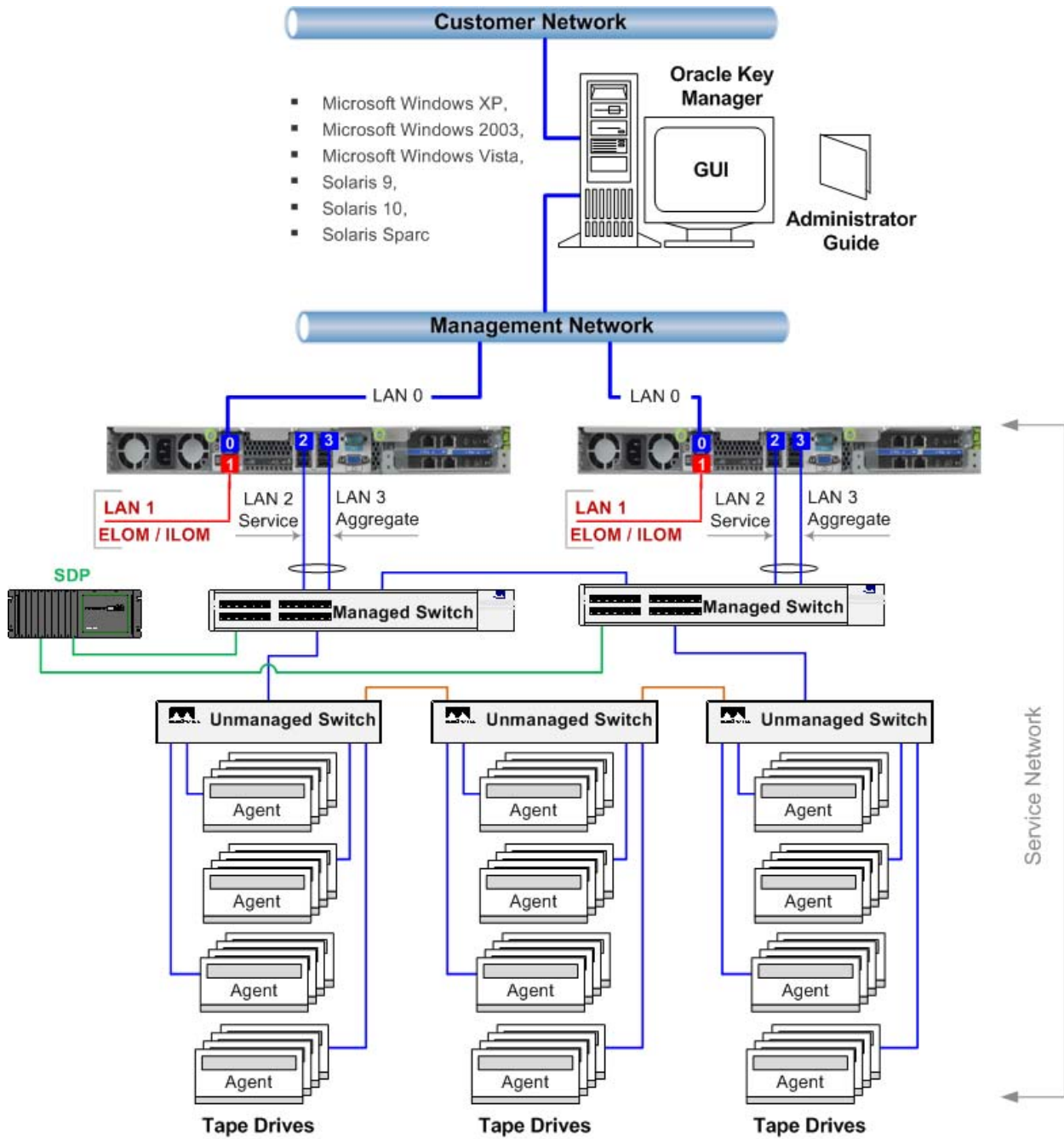
*3COM Network Switch Configuration*

1. Use a Web browser to connect to the switch IP.

2. Select port and then link aggregation from the menu.

From the subsequent dialog you can use the Create tab to create a new port grouping.

**FIGURE 3-1** Managed Switch Configuration (Example)

In this example the service network consists of two *customer-provided* managed switches that are cabled to three unmanaged switches, which contains redundant paths that require a spanning tree configuration. This example may be easily scaled for larger SL8500 drive configurations by adding additional KMAs, switch hardware, and tape drives.

■ Managed switches *must* be enabled for Spanning Tree whenever the cabling includes redundancy.
■ Unmanaged switches have two paths to the managed switches for redundancy.
■ Unmanaged switches are then cabled for connectivity to the tape drives (agents)
■ Each unmanaged switch connects 16 drives. Cabled in groups of four. Ports 1–4, 6–9, 11–14, and 16–19.
■ Service Delivery Platform (SDP) connects to each Managed Switch at Port 1.

# Network Routing Configuration

The following information is useful for customers and Oracle service representatives when setting-up and installing multi-site clusters.

Initially it is not advisable to begin with a multi-site network topology for the tape drives. A simple strategy may be best. Do not configure service network routes between sites so drives are restricted to just local KMAs within their site. After gaining confidence with the system the service network configuration can be extended to other sites using the KMA console menu option for networking.

**NOTE –** Even without a multi-site routed service network, use of default gateway settings can affect failover performance.  Understanding the following information is important for configuring the KMA network.

## Cluster Discovery, Load Balancing, and Failover

The cluster provides tape drives with a capbility to select KMAs for retrieval of key material. To maximize the performance of tape drives with a robust, highly available network is essential. The topology of the network is an important planning and configuration task. The following is some information about how a tape drive utilizes the services of the cluster for retrieval of keys.

**Discovery:** Tape drives (agents) utilize the discovery service of the KMAs to maintain knowledge about the cluster. This information includes the following properties for *each* KMA:

- IP address (both IPv4 and IPv6 addresses)
- Site Name
- KMA ID
- KMA Name
- KMA Version – Helps determine FIPS support for supported tape drives

The following dynamic properties are also provided to tape drives when they issue a *discover* cluster request:

- **Responding** – indicates if the KMA is responding on the network
- **Locked** – indicates if the KMA is currently locked

The tape drives periodically retrieve this information as part of a tape operation (not when the tape drive is idle) and always request it as part of enrollment and whenever the drive is IPLed. The KMA that receives the discover cluster request provides this information for each KMA that is accessible over the service network. This is where the network planning and configuration exercise becomes important.

**Load Balancing:** During normal tape drive operations, the drives use their local table of cluster information to select a KMA for key retrieval.

The drives use an algorithm to pick a random KMA from the cluster of KMAs within:

- the same site as the drive and
- that are unlocked and responding.

If all KMAs within a site are either locked or not responding then the tape drive attempts to access a KMA from another site.

Presumably this is a remote site with a network response time that may be higher than other the KMAs within the same site as the tape drive.

What is important is that the KMAs from other sites can be reached by the tape drive or the attempt to retrieve keys will timeout forcing a failover.

**Failover:** Whenever a tape drive's attempt to communicate with a KMA fails the drive tries to select another KMA for failover. Tape drives attempt a failover up to three (3) times before giving up and returning an error to the host tape application.

For each failover attempt, a similar selection algorithm is used for failovers as for Load Balancing. Consequently, the drive's information about the cluster state is used again (and may even be refreshed if it is time to refresh the information about the cluster).

Sometimes a drive chooses a non-responding KMA during a failover attempt if all other KMAs are non-responding. This is not ideal but because information about the cluster may be stale, there is a chance that a KMA has come back online and will respond. Whenever the drive discovers a new response state for a KMA, it updates the cluster information to mark a KMA as responding, or not responding, however the case may be.

## KMA Routing Configuration and Discovery

The routing configuration of a KMA has an effect on responses to tape drive discovery requests. Mistakes in the routing configuration can lead to erroneous cluster information being provided to tape drives. This could cause drives to attempt communication with KMAs that they cannot reach over the network.

Customers need to consider the network topology they want for their tape drives. The ability for tape drives to failover to remote sites can improve drive reliability and availability when local KMAs are down or slow to respond (such as timeout situations because of heavy workloads).

**Note:** Providing the ability to failover to remote sites is something that needs to be planned for and should involve customer network engineers.

For drives on the service network a route must be configured between sites and the KMA console network menu option should be used. The common mistake to avoid is configuring a default route.

provides an example for a Multi-Site Routed Service Network.

# Service Delivery Platform

The Service Delivery Platform (SDP) is a support solution for StorageTek's libraries and tape drives (T-Series only) that consists of a smart appliance and a dedicated network.

The SDP appliance can be configured to use the Dynamic Host Configuration Protocol (DHCP) to automate the assignment of IP addresses for device connections. Optionally, the SDP can be used as the DHCP server for the KMAs service network IP address.

## Oracle Key Manager and the SDP

Beginning with new deployments of SDP and the Oracle Key Manager the configuration was changed to strengthen security. The SDP product team recommends a firewall between the KMAs, switches, and tape drives on the service network because of the connectivity of KMAs to the customer's network. Refer to the *Service Delivery Platform Security White Paper*, May 2008 and the Optional Firewall.

When planning for a multi-site service network the subnet addressing scheme for the KMA service ports and drives needs to be determined.  Use of duplicate network addresses must be avoided.  For example, the use of 172.18.18.x networks (a common convention) need to be avoided.

KMAs will typically be connected to the customer's network for any of the following reasons:

- Administrative access to the KMAs using the Oracle Key Manager GUI hosted in the customer network
- Cluster replication between KMAs
- KMA access to the customer's NTP server
- KMA access to customer's SNMP Managers
- Customer access to the KMA's service processor (ELOM or ILOM)

Similarly, with Oracle Key Manager's support for a routable, multi-site service network, customer supplied routers and networking equipment will be required to connect the various sites comprising the key management cluster.

Because of this connectivity into the customer's network, SDP security policy dictates that a firewall must be present between the devices connecting to a KMA and the SDP. This "customer firewall" is the firewall attached to Port2 of the SDP appliance in the following diagram. The firewall will need to be configured so that SDP can monitor the tape drives in the customer controlled portion of the service network.

DMZ in the diagram refers to the secure network architecture of SDP that secures the network traffic between the SDP onset unit and the Oracle network.

This firewall effectively partitions the service network in two: the Oracle controlled service network and the customer controlled service network.   The *Service Delivery Platform Security White Paper*, May 2008 describes this network as the "Service Network interface". The Oracle Service Network interface is the connection between the SDP site unit and storage devices, this is the Port1 connection in the diagram. The Customer Network interface is the connection between SDP and Oracle storage devices

connected to the customer operations center LAN that is attached to the customer network, Port 2 in the diagram. These devices include the tape drives and switches connected to the KMAs.

The "customer firewall" prevents this connection from having access to the customer's network and only to the devices that SDP can monitor.

Oracle service personnel still need to service equipment in both partitions of the service network and coordinate with SDP engineers for planning and configuration.

**FIGURE 3-2** SDP Connectivity Example
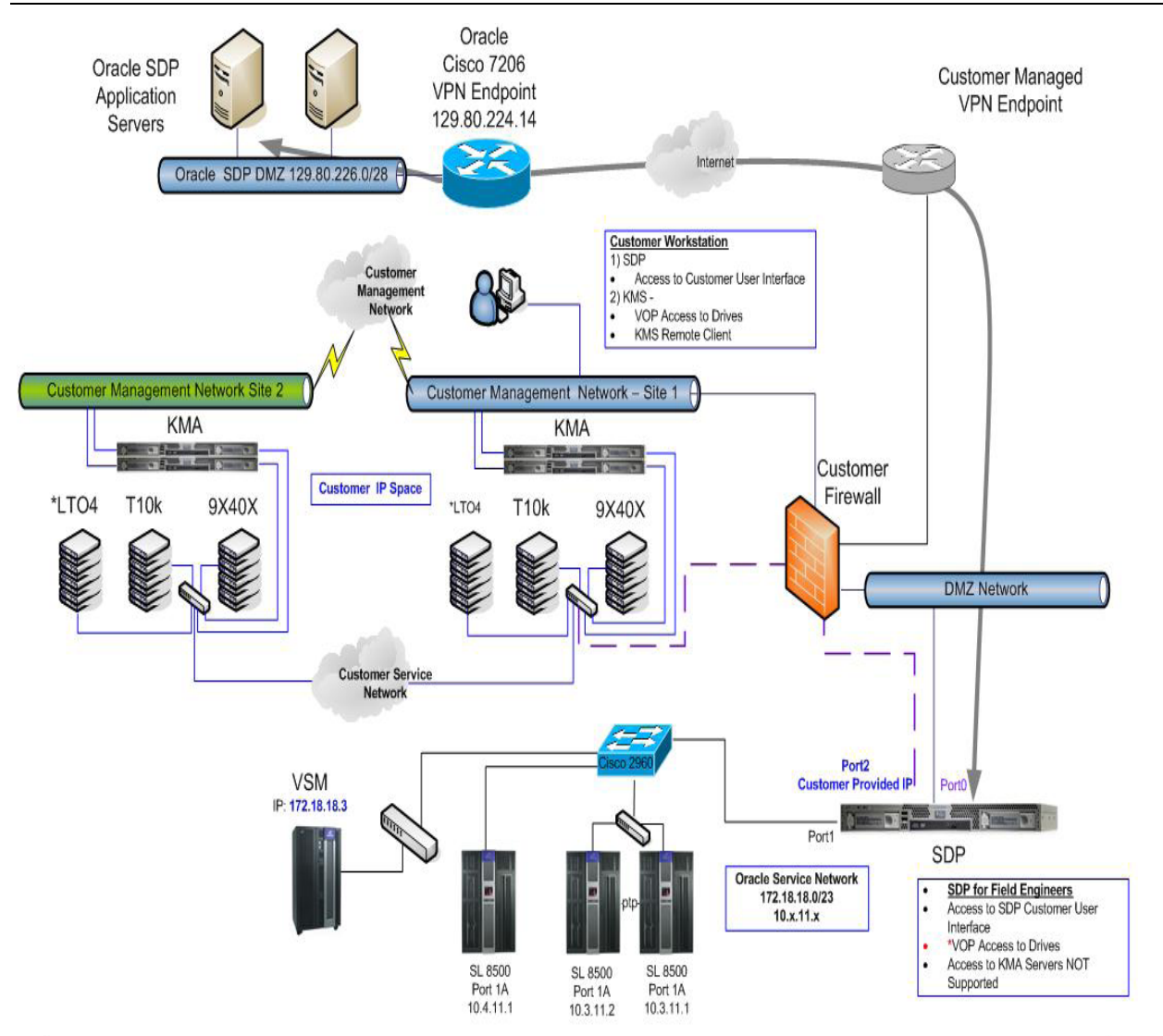
# Content Management

Encryption-capable tape drives add another element to the design for content management in an SL8500, SL3000, and SL500 library installation. All three libraries have a different design that share similar elements, considerations include:

**TABLE 3-3** Content Management Planning

| Element | SL8500 | SL3000 | SL500 |
|---|---|---|---|
| Drive Quantity | You may need to order multiple kits or additional Ethernet switches to support all the encryption-capable tape drives in a library. | | |
| | ■ Single: **1** to **64** drives<br>■ 10 library complex:<br>  up to 640 drives | ■ **1** to **56** tape drives | ■ **1** to **18** tape drives |
| Encryption Drives Supported | ■ T10000 A and B<br>■ T9840D<br>■ LTO 4 and 5 | ■ T10000 A and B<br>■ T9840D<br>■ LTO 4 and 5 | ■ LTO 4 and 5 only (HP, IBM) |
| Non-encryption Drives Supported | ■ T10000 A&B<br>■ T9840 A, B, & C<br>■ LTO 3, 4, 5 | ■ T10000 A&B<br>■ T9840 C<br>■ LTO 3 4, 5 | ■ LTO 2, 3, 4, 5 (HP, IBM)<br>■ SDLT 600<br>■ DLT-S4 |
| Interfaces: | Note: The library interface and tape drive interfaces may be different. | | |
| ■ Libraries | ■ TCP/IP only | ■ TCP/IP<br>■ Fibre Channel | ■ TCP/IP<br>■ Fibre Channel |
| ■ Tape Drives | T10000 A&B FC and FICON<br>T9840D FC, FICON, ESCON<br>LTO 4 & 5 FC only | T10000 A&B FC and FICON<br>T9840D FC, FICON, ESCON<br>LTO 4 & 5 FC only | LTO4, 5Fibre Channel<br>LTO4 SCSI (check availability) |
| Media* | All libraries support true-mixed media—Any Cartridge, Any Slot™ | | |
| | ■ T10000 (Std, Sport, VolSafe)<br>■ 9840 (Std and VolSafe)<br>■ LTO 2, 3, 4, 5 & T-WORM<br>■ DLTtape III<br>■ Super DLTtape I & II | ■ T10000 (Std, Sport, VolSafe)<br>■ 9840 (Std and VolSafe)<br>■ LTO 2, 3, 4, 5 & T-WORM | ■ LTO 1, 2, 3, 4, 5 & T-WORM<br>■ DLTtape III<br>■ Super DLTtape I & II |
| Partitioning | Yes | Yes | Yes |
| SNMP | Yes | Yes | Yes |
| SDP | Yes | Yes | No |
| Power Redundancy | Yes | Yes | No |
| Operating Systems | Enterprise and Open Systems | Enterprise and Open Systems | Open systems only |
| Library Management | ■ ACSLS<br>■ HSC | ■ ACSLS<br>■ HSC<br>■ ISV | ■ ACSLS<br>■ ISV |
| FC = Fibre Channel<br>FICON = IBMs fiber connection<br>SNMP = Simple Network Management Protocol<br>SDP = Service Delivery Platform | | ACSLS = Automated Cartridge System Library Software<br>HSC = Host Software Component<br>ISV = Independent Software Vendor (Symantec, Legato, TSM) | |
| **\*Important:** Only LTO4 media—LTO4 and LTO4-WORM—are encryption-capable on the LTO4 tape drives. | | | |

When planning for content, the most important aspect is to evaluate *content* (tape drives and data cartridges) with respect to the *physical structure* of the library.

These libraries provide several ways to accommodate growing data storage needs:

- Addition of library modules—to the front, to the left or right, or up and down.
- Capacity on Demand
    - Activation of slots without service representative involvement
    - Requires the installation of slots or modules up front
- Flexible partitions
- Ease to re-allocate resources as needs change
- Real-Time Growth
- Disaster recovery scenario's

# Capacity on Demand

Capacity on Demand is a *non-disruptive* optional feature that allows the customer to add capacity to the library using *previously installed*, yet inactive slots.

The installed physical capacity is separate from the activated capacity. The advantage of Capacity on Demand is that the customer only buys the storage that they need and not all the storage that is installed.

Activated capacity can be purchased in multiple increments.

When a customer purchases a hardware activation key to use more physical storage an encrypted *key file* is sent through e-mail. The file is then loaded into the library using the Storage Library Console (SLC).

# RealTime Growth Technology

Because the physical and the activated slot capacities are separate, the customer has the option of installing physical capacity in advance before they are ready to use these slots.

The advantage of installing physical capacity in advance is that now, scaling the library is non-disruptive, quick, and easy to accomplish.

For example: Whenever building a library configuration, there are two basic slot capacity questions you need to answer:

1. How many slots does the customer need to use?

2. How many cartridge slots does the customer want to physically install?

# Partitioning

The definition of a partition is to divide into parts or shares.

**Benefits:** Partitioning a library means the customer can have:

- Multiple libraries from one physical piece of hardware.
- More than one operating system and application manage the library.
- An improvement in the protection or isolation of files.
- An increase in system and library performance.
- An increase in user efficiency.

**Customized fit:**
Partitions may be customized to fit different requirements, such as:

- Separating different encryption key groups.
- Isolating clients as service centers.
- Dedicating partitions for special tasks.
- Giving multiple departments, organizations, and companies access to appropriate sized library resources.

**Tip:**
When using encryption-capable tape drives, partitions can add an additional layer to data security. Customers can assign partitions that limit the access to the tape drives and data cartridges.

Ideally, you would want to set up partitions that allow for future. Allowing room for growth allows the customer to activate slots within a partition using Capacity on Demand. This is the easiest and least disruptive growth path:

1. Install extra physical capacity.
2. Define partitions large enough to accommodate future growth.
3. Adjust the library capacity to meet current demands.

Essential guidelines for understanding partitions are:

- Clear communication between the system programmers, network administrators, library software representatives and administrators, and service representatives.
- Knowing what partitions exist, their boundaries, and who has access to the specific partitions that are configured.
- Setting up a partition requires some important considerations:
  - Slots and tape drives are allocated to a specific partition and cannot be shared across other partitions.
  - Partition users must anticipate how much storage is needed for their resident data cartridges and the amount of free slots required for both current use and potential growth.
- Remember:
  - Each partition acts as an independent library.
  - One partition will not recognize another partition within the library.

# Disaster Recovery

Disaster recovery is a subset of a larger process known as **business continuity planning** (BCP), which should include replacing hardware, re-establishing networks, resuming applications, and restoring data.

Disaster recovery is the process, policies, and procedures that relate to preparing for recovery or continuation of business critical information to an organization after a natural or human-induced disaster. This includes:

- **Recovery Point Objective** (RPO): The point in time to recover data as defined by a business continuity plan. This is generally a definition of what the business determines is an "acceptable loss" in a disaster situation. This could be in hours, days, or even weeks.

- **Recovery Time Objective** (RTO): The duration of time that a business process must be "restored" after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. This could be minutes when using a combined service network.

The OKM uses a cluster design that requires at least two key management appliances. This design helps reduce the risk of disrupting business continuity. Clustering KMAs allows for replication of database entries and workload balancing. In the unlikely event that a component should fail, it can be easily replaced and restored to operation.

An OKM can span multiple, geographically-separated sites. This highly reduces the risk of a disaster destroying the entire cluster. Clustering KMAs allows for replication of database entries and workload balancing. Although unlikely, that an entire cluster needs to be recreated, most of the key data can be recovered by recreating the OKM 2.x environment from a recent database backup.

While designing an encryption and archive strategy, an important design guideline is to make sure that critical data generated at any site is replicated and vaulted off-site. Many companies employ the services of a third-party disaster recovery (DR) site to allow them to restart their business operations as quickly as possible.

Refer to *Disaster Recovery Reference Guide* PN 31619710x for more information.

# Planning the Data Path

When planning for partitions, you also need to be aware of the location, quantity, type, and need for the tape drives and media.

In addition, an understanding about how to logically group and install the tape drives and locate the media for the different hosts, control data sets, interface types, and partitions is necessary. When planing for partitions:

- Make sure the tape drive interface supports that operating system.
  - Open system platforms do not support ESCON or FICON interfaces.
  - Not all mainframes support Fibre Channel interfaces or LTO tape drives.
- Make sure the media types match the application.
- Install tape drives that use the same media types in the same partition.
- Make sure there are enough scratch cartridges and free slots to support the application and workload.

## Planning Tasks

One essential message for content management and partitioning is **planning**. Items to plan for include:

**TABLE 3-4** Steps and Tasks for Partitioning

| ✓ | Item | Task | Responsibility* |
|---|------|------|-----------------|
| ❏ | **1. Team** | Create a Team.<br>When planning for content, data and partitions, use a process similar to that of the system assurance process; which is the exchange of information among team members to ensure all aspects of the implementation are planned carefully and performed efficiently. Team members should include representatives from both the customer. | ■ Customer<br>■ Administrators<br>■ Operators<br><br>■ SE, PS<br>■ Svc Rep |
| ❏ | **2. Codes** | Review the software and firmware requirements.<br>Update as required. | ■ Customer<br>■ SE, PS<br>■ Svc Rep |
| ❏ | **3. Planning** | ■ Define the customer expectations<br>■ Complete the assessment<br>■ Identify the configurations<br>■ Complete the planning diagrams (include network planning)<br>■ Service Delivery Platform (SDP) | ■ Customer<br>■ Administrators<br>■ SE, PS<br>■ Svc Rep |
| ❏ | **4. Encryption** | ■ Complete an encryption survey (PS)<br>■ Select the type of tape drive, interface, and library configuration<br>■ Select location<br>■ Ensure there is adequate media | ■ Customer<br>■ SE, PS<br>■ Svc Rep |
| ❏ | **5. Disaster Recovery** | ■ Develop a business continuity and disaster recovery plan<br>■ Select a backup site<br>■ Determine network configurations (LAN, WAN, aggregation) | ■ Customer<br>■ SE, PS<br>■ Svc Rep |
| ❏ | **6. Media** | ■ Verify the distribution of cartridges and required tape drives are available and ready. | ■ Customer<br>■ Operators |
| ❏ | **7. Library** | ■ Install and configure a library (if necessary). | ■ Svc Rep |
| ❏ | **8. Activation** | ■ Activate the required features:<br>  ■ Library<br>  ■ Tape drives | ■ Customer<br>■ Administrators<br>■ Svc Rep |
| ❏ | **9. Partitions** | ■ Create partitions. | ■ Customer<br>■ Administrators<br>■ Operators |
| ❏ | **10.Hosts** | ■ Momentarily stop all host activity if currently connected. | ■ Customer |
| ❏ | **11.Use** | Instruct the customer how to:<br>■ Use and manage the library<br>■ Use the OKM GUI | ■ Customer<br>■ SE, PS<br>■ Svc Rep |
| ❏ | **12.Reference** | Make sure the customer has access to the appropriate documents. | ■ Customer<br>■ SE, PS<br>■ Svc Rep |
| ■ SE = Systems engineer<br>■ PS = Professional services representative<br>■ Service = Customer services representative (Svc Rep)<br>■ Customer = System administrators, network administrators, system programmers, operators | | | |

# Oracle Key Manager Interface

The manager graphical user interface (GUI) consists of a three-paned display:

1. On the left is a navigational pane or tree.

2. In the center is an operations detail pane for the appropriate selection on the left.

3. On the bottom is a session events pane.

**TABLE 3-5** Manager Display
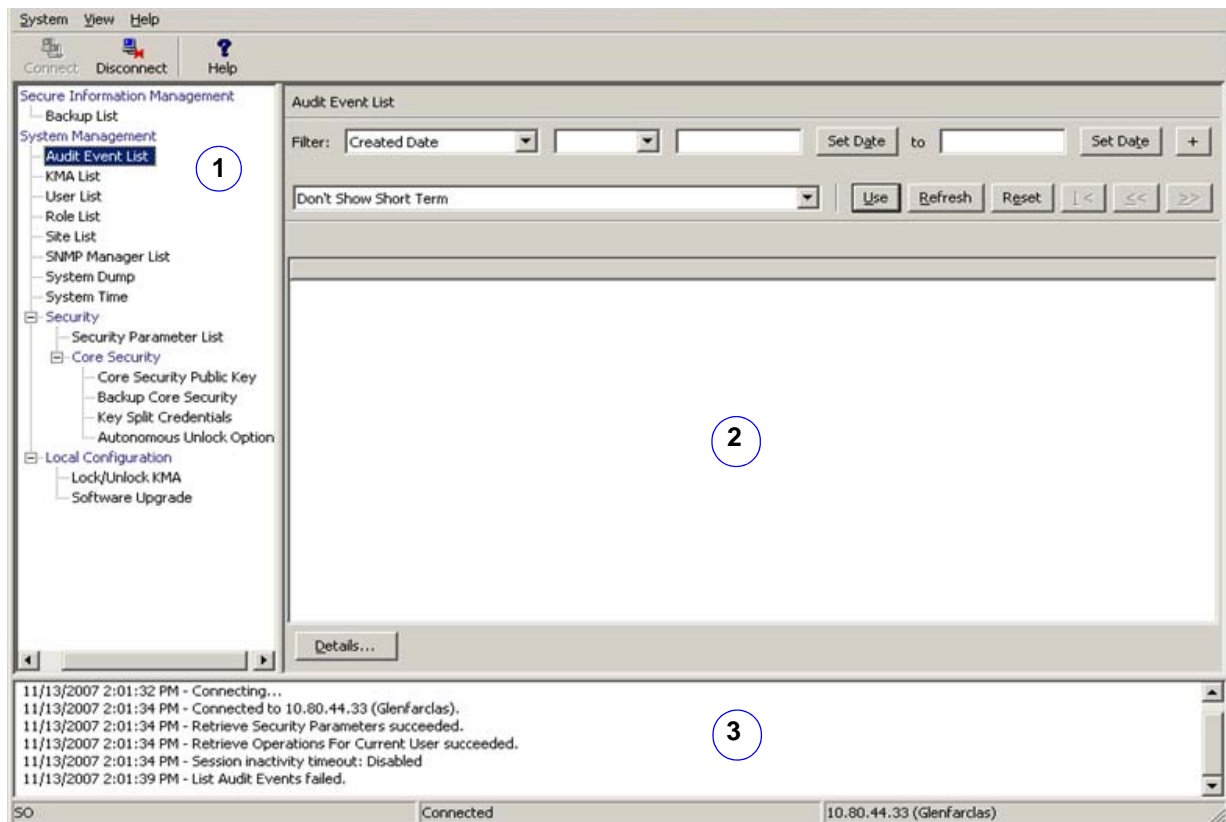


The manager is an easy-to-use graphical user interface that allows users to configure functions of the KMAs depending on the roles that user is assigned (see "Role-Based Operations" on page 52).

The manager contains System, View, and Help menus in the upper left corner of the display with toolbar buttons that provide shortcuts to several menu options.

# Role-Based Operations

The manager defines and uses the following roles. Completing and assigning roles is a customer task, service representatives should only advise.

| ■ **Auditor** | Views information about the Cluster. |
|---|---|
| ■ **Backup Operator** | Performs backups. |
| ■ **Compliance Officer** | Manages *key policies* and *key groups*. Determines which Agents and Transfer Partners can use key groups. |
| ■ **Operator** | Manages Agents, Data Units, and Keys. |
| ■ **Quorum Member** | Views and approves pending quorum operations. |
| ■ **Security Officer** | Full authority to view, modify, create, and delete Sites, KMAs, Users, and Transfer Partners. |

👉 **Note:** Each person or user may fulfill one or more of these roles.

FIGURE 3-3 shows an example of the Users Detail screen.
Use TABLE 3-7 on page 57 to help prepare for the assignments.

**FIGURE 3-3** User Roles Detail Screen



1. Enter a User ID
   Between 1 and 64 characters
2. Provide a description
   Between 1 and 64 characters

3. Click the Passphrase tab and
   Enter a Passphrase—twice

   Passphrases must use:
   ■ 8 to 64 characters
   ■ 3 of 4 classes
     (upper case, lower case, numbers, and symbols)
   ■ do not include the users name

The KMA verifies that the requesting user has permission to execute an operation based on the user's roles. Unavailable operations typically indicate the wrong role.

There are four basic operations a user/role can have: Create, Delete, Modify, and View. TABLE 3-6 on page 53 shows the system entities and functions that each user role can perform. In the "Roles" columns:

■ **Yes** indicates that the role is allowed to perform the operation.
■ **Quorum** indicates that the role is allowed but must belong to a quorum.
■ **Blank** indicates that the role is not allowed to perform the operation.

**TABLE 3-6** System Operations and User Roles  (Sheet 1 of 4)

| Operation | Roles | | | | | |
|---|---|---|---|---|---|---|
| | Security Officer | Compliance Officer | Operator | Backup Operator | Auditor | Quorum Member |
| **Console** | | | | | | |
| Log In | Yes | Yes | Yes | Yes | Yes | Yes |
| Set KMA Locale | Yes | | | | | |
| Set KMA IP Address | Yes | | | | | |
| Enable Tech Support | Yes | | | | | |
| Disable Tech Support | Yes | | Yes | | | |
| Enable Primary Administrator | Yes | | | | | |
| Disable Primary Administrator | Yes | | Yes | | | |
| Restart KMA | | | Yes | | | |
| Shutdown KMA | | | Yes | | | |
| Log into Cluster | Quorum | | | | | |
| Set User's Passphrase | Yes | | | | | |
| Reset KMA | Yes | | | | | |
| Zeroize KMA | Yes | | | | | |
| Logout | Yes | Yes | Yes | Yes | Yes | Yes |
| **Connect** | | | | | | |
| Log In | Yes | Yes | Yes | Yes | Yes | Yes |
| Create Profile | Yes | Yes | Yes | Yes | Yes | Yes |
| Delete Profile | Yes | Yes | Yes | Yes | Yes | Yes |
| Set Config Settings | Yes | Yes | Yes | Yes | Yes | Yes |
| Disconnect | Yes | Yes | Yes | Yes | Yes | Yes |
| **Key Split Credentials** | | | | | | |
| List | Yes | | | | | |
| Modify | Quorum | | | | | |
| **Autonomous Unlock** | | | | | | |
| List | Yes | | | | | |
| Modify | Quorum | | | | | |
| **Lock/Unlock KMA** | | | | | | |
| List Status | Yes | Yes | Yes | Yes | Yes | |
| Lock | Yes | | | | | |
| Unlock | Quorum | | | | | |

**TABLE 3-6** System Operations and User Roles  (Sheet 2 of 4)

| Operation | Roles | | | | | |
|---|---|---|---|---|---|---|
| | Security Officer | Compliance Officer | Operator | Backup Operator | Auditor | Quorum Member |
| **Site** | | | | | | |
| Create | Yes | | | | | |
| List | Yes | | Yes | | | |
| Modify | Yes | | | | | |
| Delete | Yes | | | | | |
| **Security Parameters** | | | | | | |
| List | Yes | Yes | Yes | Yes | Yes | |
| Modify | Yes | | | | | |
| **KMA** | | | | | | |
| Create | Yes | | | | | |
| List | Yes | | Yes | | | |
| Modify | Yes | | | | | |
| Delete | Yes | | | | | |
| **User** | | | | | | |
| Create | Yes | | | | | |
| List | Yes | | | | | |
| Modify | Yes | | | | | |
| Modify Passphrase | Yes | | | | | |
| Delete | Yes | | | | | |
| **Role** | | | | | | |
| List | Yes | | | | | |
| **Key Policy** | | | | | | |
| Create | | Yes | | | | |
| List | | Yes | | | | |
| Modify | | Yes | | | | |
| Delete | | Yes | | | | |
| **Key Group** | | | | | | |
| Create | | Yes | | | | |
| List | | Yes | Yes | | | |
| List Data Units | | Yes | Yes | | | |
| List Agents | | Yes | Yes | | | |
| Modify | | Yes | | | | |
| Delete | | Yes | | | | |

**TABLE 3-6** System Operations and User Roles  (Sheet 3 of 4)

| Operation | Roles | | | | | |
|---|---|---|---|---|---|---|
| | Security Officer | Compliance Officer | Operator | Backup Operator | Auditor | Quorum Member |
| **Agent** | | | | | | |
| Create | | | Yes | | | |
| List | | Yes | Yes | | | |
| Modify | | | Yes | | | |
| Modify Passphrase | | | Yes | | | |
| Delete | | | Yes | | | |
| **Agent/Key Group Assignment** | | | | | | |
| List | | Yes | Yes | | | |
| Modify | | Yes | | | | |
| **Data Unit** | | | | | | |
| Create | | | | | | |
| List | | Yes | Yes | | | |
| Modify | | | Yes | | | |
| Modify Key Group | | Yes | | | | |
| Delete | | | | | | |
| **Keys** | | | | | | |
| List Data Unit Keys | | Yes | Yes | | | |
| Destroy | | | Yes | | | |
| Compromise | | Yes | | | | |
| **Transfer Partners** | | | | | | |
| Configure | Quorum | | | | | |
| List | Yes | Yes | Yes | | | |
| Modify | Quorum | | | | | |
| Delete | Yes | | | | | |
| **Key Transfer Keys** | | | | | | |
| List | Yes | | | | | |
| Update | Yes | | | | | |
| **Transfer Partner Key Group Assignments** | | | | | | |
| List | | Yes | Yes | | | |
| Modify | | Yes | | | | |
| **Backup** | | | | | | |
| Create | | | | Yes | | |
| List | Yes | Yes | Yes | Yes | | |
| List Backups & Destroyed Keys | | Yes | Yes | | | |

**TABLE 3-6** System Operations and User Roles  (Sheet 4 of 4)

| Operation | Roles | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| | Security Officer | Compliance Officer | Operator | Backup Operator | Auditor | Quorum Member |
| Restore | Quorum | | | | | |
| Confirm Destruction | | | | Yes | | |
| **Core Security Backup** | | | | | | |
| Create | Yes | | | | | |
| **SNMP Manager** | | | | | | |
| Create | Yes | | | | | |
| List | Yes | | Yes | | | |
| Modify | Yes | | | | | |
| Delete | Yes | | | | | |
| **Audit Event** | | | | | | |
| View | Yes | Yes | Yes | Yes | Yes | |
| View Agent History | | Yes | Yes | | | |
| View Data Unit History | | Yes | Yes | | | |
| View Data Unit Key History | | Yes | Yes | | | |
| **System Dump** | | | | | | |
| Create | Yes | | Yes | | | |
| **System Time** | | | | | | |
| List | Yes | Yes | Yes | Yes | Yes | |
| Modify | Yes | | | | | |
| **NTP Server** | | | | | | |
| List | Yes | Yes | Yes | Yes | Yes | |
| Modify | Yes | | | | | |
| **Software Version** | | | | | | |
| List | Yes | Yes | Yes | Yes | Yes | |
| Upgrade | | | Yes | | | |
| **Network Configuration** | | | | | | |
| Display | Yes | Yes | Yes | Yes | Yes | |
| **Pending Quorum Operation** | | | | | | |
| Approve | | | | | | Quorum |
| Delete | Yes | | | | | |

**TABLE 3-7** User Roles Work Sheet

| User ID | Description | Passphrase ** (Confidential password) | Roles | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | **Security Officer** | **Compliance Officer** | **Operator** | **Backup Operator** | **Auditor** | **Quorum Member** |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

**Note:** The Passphrase should not be recorded here for security reasons.
This column is provided as a reminder that as User IDs are entered, the person with that ID will be required to enter a passphrase.

# Preparing the Tape Drives

The tape drives should be installed and tested in their appropriate configuration before adding the encryption capability to them. Each drive-type has its own requirements.

## T-Series Drive Data Preparation

To obtain the drive data for *each* T-Series (T10000 and T9840) tape drive:

1. Using the Virtual Operator Panel, connect to each tape drive and record the last *eight* digits of the tape drive serial number.
   - Select: File ➪ Connect to Drive
   - Select: Retrieve ➪ View Drive Data ➪ Manufacturing

**FIGURE 3-4** Tape Drive Serial Number—VOP
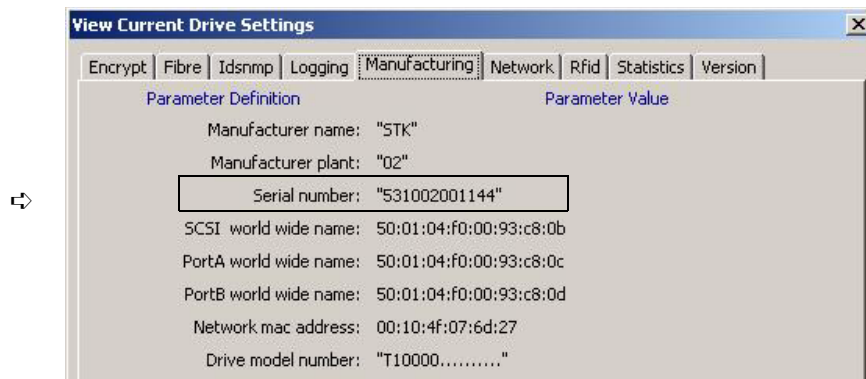


2. Use the Tape Drives Work Sheet to build information about the tape drives. You will find this information helpful during the installation, activation, and enrollment process for the tape drives (agents).

3. Request an Encryption Key File:

   a. Log in to the Applications Web site at: http://crcapplications/keyswebapp/

   b. Select Request an Encryption key

**FIGURE 3-5** Request an Encryption Key Application

☞ **Access is Restricted:** You must be an employee, complete the encryption training courses, and include the name of the employee on the Request Encryption Key list.

4. Complete the Encryption Request form.

   a. First name, last name, and e-mail address are automatically included.

   b. Provide a site ID and order number.

   c. Select the tape drive type (T10000A, T10000B, or T9840D).

   d. Complete the serial number for the selected tape drive.

   e. Add any optional remarks and click Request Key File.
      After submitting the Encryption File Request you will be prompted to download the file. This file contains the drive data you need to enable and enroll the drive.

**FIGURE 3-6** Encryption File Request for Drive Data



Family serial numbers start with:
   T10000A = 5310 xxxxxxxx
   T10000B = 5720 xxxxxxxx
   T9840D  = 5700 xxxxxxxx

When selecting the drive family-type, the first four numbers of the serial number are automatically filled in.

5. Continue with this process until you obtain all the drive data files for each tape drive you are going to enable.

# Create a Drive Data File Structure

When enabling multiple drives, it is best to create a file structure where each tape drive has its own folder. For example:

1. FIGURE 3-7 uses a top-level folder name of **crypto_drvs** placed on the Desktop. (This is only for grouping of the other folders.)

2. Under crypto_drvs are the folders for each tape drive using the serial numbers.

3. In each serial number folder is the drive data file for that specific tape drive.

**FIGURE 3-7** Drive Data File Structure
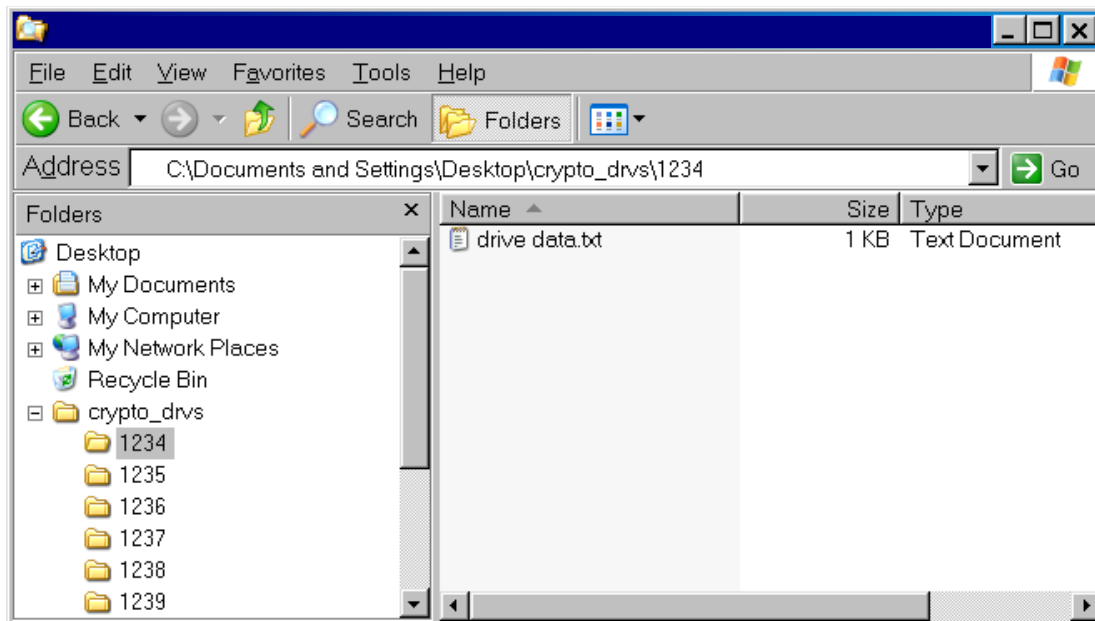


When activating the tape drives, the VOP requests a download location.

4. Complete the Agent Enrollment Work Sheet to help with the activation and enrollment of the tape drives. What you need to know before beginning:
   - What is the drive number (serial or system) and IP address?
   - What are the Agent IDs and Passphrases?
   - Is this drive going to use **tokens** (Version 1.x) to get media keys (OKT)? Or use the **appliance** (KMA Version 2.x) to get the encryption keys?
   - Does the customer want this drive to remain in encryption mode? Or do they want the ability to switch encryption on and off?

5. Make copies of this page as necessary.

**Notes:**
   - Agent names (IDs) cannot be changed; however, an agent can be deleted and re-enrolled with a different name.
   - If you replace the agent, you can reuse the name; however, passphrases can only be used once, you will need to give the agent a new passphrase.
   - Which means, the replacement drive will need to be enrolled using the existing name and a new passphrase.

## LTO Tape Drive Preparation

No enablement requirements or drive data is required for the LTO tape drives. The only preparation is to make sure the customer has the information to assign the IP addresses and Agent names for the tape drives in the OKM manager.

**Note –** The Virtual Operator Panel must be at:
■ Version 1.0.12 and higher to provide support for the HP LTO tape drives.
■ Version 1.0.14 and higher to provide support for the IBM LTO tape drives.

To use the VOP for LTO tape drives, you need to launch a special file:

■ **Windows:** Launch the batch file (**ltoVOP.bat**)

FIGURE 3-8 shows an example of the VOP 1.0.12 download contents.

**FIGURE 3-8** VOP LTO Files
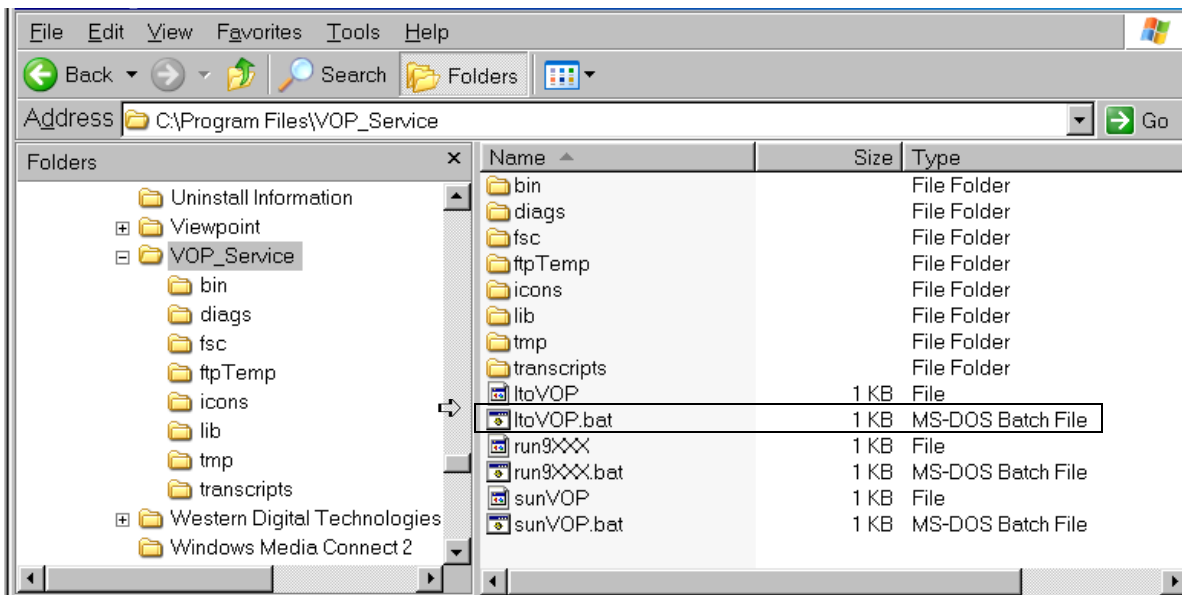
# Required Tools

The required tools to install and initially configure the KMAs are:

- Standard field service tool kit, including both standard and Phillips screwdrivers, Torx driver and bits, and other tools necessary to mount the servers in a rack
- Serial or null modem cable (P/N 24100134) with DB-9 connector
- Adapter (P/N 10402019)
- Straight Ethernet cable (P/N 24100216) 10-ft
- Cross-over Ethernet cable (P/N 24100163) 10-ft
- Service laptop (or personal computer)
- Virtual Operator Panel (VOP) at Version 1.0.11 or higher for T-Series tape drives
- Virtual Operator Panel for HP LTO tape drives at Version 1.0.12 or higher
- Virtual Operator Panel for IBM LTO tape drives at Version 1.0.14 or higher
- Virtual Operator Panel for LTO5 tape drives at Version 1.0.16 or higher
- Multi-Drive Virtual Operator Panel (MD-VOP) Version 1.1 or higher

# Supported Platforms and Web Browsers

The manager (graphical user interface—GUI) must be installed on either a Windows XP or Solaris platforms.

**Web Browsers:**
The Embedded Lights Out Manager is sensitive to Web browser and Java versions. Refer to the *Embedded Lights Out Manager Administration Guide* PN: 819-6588-xx for more information and Web browsers.

TABLE 3-8 lists the supported operating systems and Web browsers:

**TABLE 3-8** Operating Systems and Web Browsers

| Client OS | Supports these Web browsers | Java Runtime Environment Including Java Web Start |
|---|---|---|
| ■ Microsoft Windows XP<br>■ Microsoft Windows 2003<br>■ Microsoft Windows Vista | ■ Internet Explorer 6.0 and later Mozilla 1.7.5 or later<br>■ Mozilla Firefox 1.0 | JRE 1.5<br>(Java 5.0 Update 7 or later) |
| ■ Red Hat Linux 3.0 and 4.0 | ■ Mozilla 1.7.5 or later<br>■ Mozilla Firefox 1.0 | JRE 1.5<br>(Java 5.0 Update 7 or later) |
| ■ Solaris 9<br>■ Solaris 10<br>■ Solaris Sparc<br>■ SUSE Linux 9.2 | ■ Mozilla 1.7.5 | JRE 1.5<br>(Java 5.0 Update 7 or later) |
| You can download the Java 1.5 runtime environment at: http://java.com<br>The current version of the ELOM guide is located at: http://dlc.sun.com/ | | |

# Firmware Levels

The *minimum* firmware requirements include:

**TABLE 3-9** Firmware Compatibilities

| Component | Version | Version | Version | Version |
|---|---|---|---|---|
| Version 2.x | 2.02 | 2.1 | 2.2 | 2.3 |

**Library Management**

| | |
|---|---|
| ACSLS | 7.1 and 7.1.1 with PUT0701, or 7.2, 7.3, and 8.0 |
| HSC | 6.1 or 6.2 |
| VSM | 6.1 or 6.2 (includes VTCS and VTSS) |
| VTL models | 1.0 or 2.0 |

| Tape Drives | SL8500 | SL3000 | Lxxx | 9310 | SL500 | SL24 | SL48 | VOP |
|---|---|---|---|---|---|---|---|---|
| T10000A FC | FRS_3.11 D–137113 | L-FRS_2.0 D–137113 | L–3.17.03 D–137113 | L–4.4.08 D–137113 | n/a | n/a | n/a | 1.0.11 |
| T10000A FICON | L–3.11c D–137114 | L-FRS_2.0 D–137114 | L–3.17.03 D–137114 | L–4.4.08 D–137114 | n/a | n/a | n/a | 1.0.11 |
| T10000B FC | L–3.98b D–138x07 | L-FRS_2.0 D–138x07 | L–3.17.03 D–138x07 | n/a | n/a | n/a | n/a | 1.0.12 |
| T10000B FICON | L–3.98b D–138x09 | L-FRS_2.0 D–138x09 | L–3.17.03 D–138x09 | n/a | n/a | n/a | n/a | 1.0.12 |
| T9840D FC | L–3.98 D–142x07 | L-FRS_2.0 D–142x07 | L–3.17.03 D–142x07 | L–4.4.08 D–142x07 | n/a | n/a | n/a | 1.0.12 |
| T9840D FICON & ESCON | L–3.98 D–142x07 | L-FRS_2.0 D–142x07 | L–3.17.03 D–142x07 | L–4.4.08 D–142x07 | n/a | n/a | n/a | 1.0.12 |
| HP LTO LTO4 LTO5 | L–3.98B D–H58s F D-I2DS F | FRS_2.0 5 D–H58s F D-I2DS F | n/a | n/a | L–i17 D–H58s F D-I2DS F | L-D.90 D-I2DS F | L-G.20 D-I2DS F | 1.0.12 1.0.16 |
| IBM LTO LTO4 LTO5 | FRS_4.70 D–94D7 F D-A232 F | FRS_2.30 D–94D7 F D-A232 F | n/a | n/a | L–i17 D–94D7 F D-A232 F | L-D.90 D-A232 F | L-G.20 D-A232 F | 1.0.14 1.0.16 |

**Legend:**

L–Library firmware level
D–Drive firmware level
H58s F = Fibre Channel firmware (HP LTO4)
B57s S = SCSI firmware (HP LTO4)

F/FC = Fibre Channel
SPS = Special firmware. Requires approval.
n/a = Not supported. Not applicable.
FRS_ = Library firmware level

Firmware Levels

# Components

This chapter contains descriptions for the components in an Oracle Key Manager encryption solution.

## Supported Configurations

The following components can be ordered to support customer requirements and configurations for an Oracle Key Manager encryption solution:

- "Key Management Appliance"
  This is a *require*d component for key creation, management, and assignments.

When implementing an encryption solution using one of Oracle's StorageTek libraries, review the following:

- "SL8500 Modular Library System"
- "SL3000 Modular Library System"
- "SL500 Modular Library System"
- "9310 Automated Cartridge System"
- "L-Series Libraries"
- "SL24 Autoloader and SL48 Library"
- "Rack Mount"

## Supported Tape Drives

Customers have a choice in the type of tape drive they want to use for encryption:

- T10000A and/or T10000B
- T9840D
- HP LTO4 and/or LTO5
- IBM LTO4 and/or LTO5

See "Firmware Levels" for the supported tape drive firmware versions.

# Key Management Appliance

The current key management appliance is a Sun Fire X4170 M2 server.

- Rack-mountable Key Management Appliance (KMA); order: **CRYPTO-KMA-23**
- If a SCA6000 card is required; order: **CRYPTO-SCA6000**
  This card provides FIPS 140-2 level 3-compliance for the encryption keys.

This server comes with a pre-loaded Solaris 10 operating system and special key management system software.

**FIGURE 4-1** Key Management Appliance—4170 Rear Panel



1. AC Power connectors
2. Serial Management (SER MGT) RJ-45 serial port
3. Service network (NET MGT) port
4. Ethernet ports (0, 1, 2, 3)
5. USB ports (0, 1)
6. Video connector (VGA)
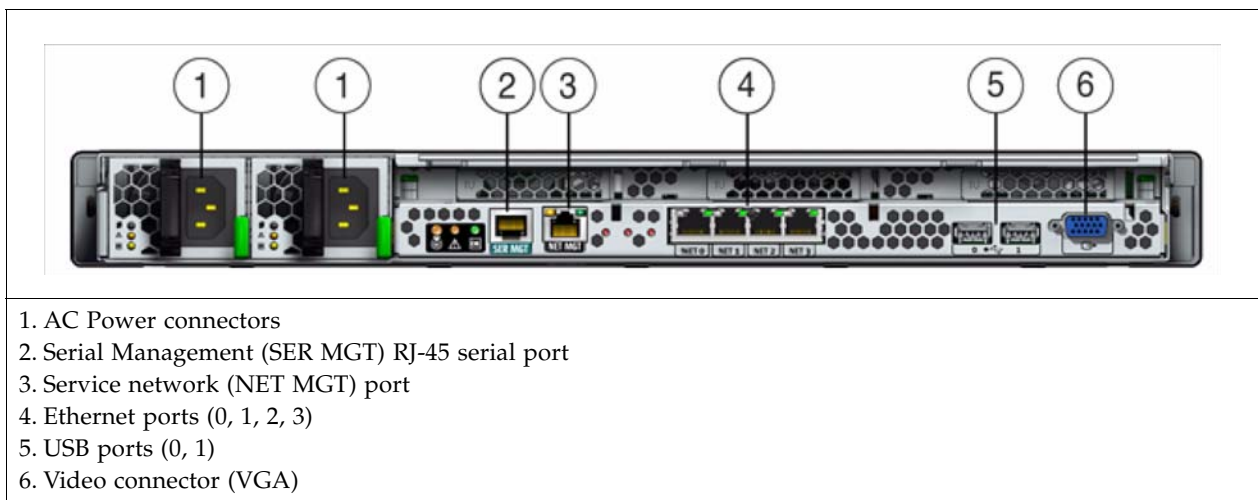
**FIGURE 4-2** Key Management Appliance—4170 Front Panel



1. Power /OK LED
2. Power button
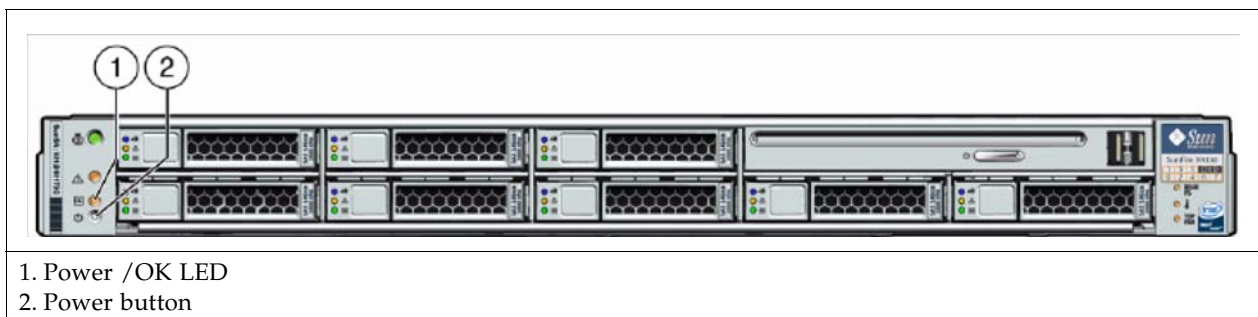
**Note —** **CRYPTO-1XTO23UP** is an upgrade kit of KMA 1.x to version 2.3.

# SL8500 Modular Library System

**FIGURE 4-3** SL8500 Modular Library System Requirements

**High-level Description:**
A single SL8500 library can store up to:
■ 1,448 to 10,000 tape cartridges
■ 64 tape drives.

An SL8500 Library Complex of 10 libraries can store:
■ Up to 100,000 tape cartridges
■ With 640 tape drives

**Operating System Support:**
The SL8500 supports all major operating systems:
enterprise *and* open systems.

**Host-to-Library Interface:**
■ Single Ethernet* (TCP/IP) 1x
■ Dual TCP/IP* (optional feature) 2x
■ Multi-host (optional feature) 4x

This library supports **Partitioning** with up to
4 partitions using the rail boundaries.

| Order Number | Description |
|---|---|
| CRYPTO-2X-SL8500-N | Sun StorageTek crypto kit for use with SL8500 libraries. A 24-port ethernet switch, cables, and rack mount HW for installation within SL8500 library |
| XSL8500-ETHRNT-Z | PUE Ethernet card/switch (PN: 419951602) |

**Firmware Levels**

| | |
|---|---|
| Library | FRS_3.72 (FRS_3.98 or higher is recommended and to support LTO4) FRS_4.70 (current) FRS_6.02 (redundant electronics feature) |
| StreamLine Library Console | FRS_4.00 |
| Tape Drives:<br>■ T10000A<br>■ T10000B<br>■ T9840D<br>■ HP LTO4<br>■ HP LTO5<br>■ IBM LTO4<br>■ IBM LTO5 | 1.34.208 or higher<br>1.38.x07 or higher<br>1.42.104 or higher<br>H58S Fibre Channel<br>I2DS Fibre Channel<br>94D7 Fibre Channel<br>A232 Fibre Channel |
| Virtual Operator Panel (VOP) | Version 1.0.14 or higher to support LTO4 Version 1.0.16 (current) |

# SL3000 Modular Library System

**FIGURE 4-4** SL3000 Modular Library System Requirements



**High-level Description:**
The SL3000 library offers customers the benefits of:
■ Scalability in storage capacity from 200 to 5800 slots
■ Performance from 1 to 56 tape drives
■ Heterogeneous attachments using standard interfaces (Ethernet and Fibre Channel)
■ Multiple library management software options

**Operating System Support:**
The SL3000 supports all major operating systems: enterprise *and* open systems.
**Host-to-Library Interface:**
■ Single Ethernet* (TCP/IP) 1x
■ Dual TCP/IP* (optional feature) 2x
■ Fibre Channel* (dual port optional feature) 2x
* Supports Partitioning

| Order Number | Description |
|---|---|
| ■ SL3000 Kit 1 XSL3000-ETHRNT1-N<br>■ SL3000 Kit 2 XSL3000-ETHRNT2-N<br>■ SL3000 Kit 3 XSL3000-ETHRNT3-N<br>■ SL3000 Kit 4 XSL3000-ETHRNT4-N | The SL3000 uses four different part numbers for Ethernet switches and cables to 1 to 56 tape drives.<br>**Note:**<br>The SL3000 has limited internal rack space. Depending on the number of drives, customers may need to order an external rack. |

**Firmware Levels**

| Library | FRS_2.0.2, FRS_2.30, FRS_2.8x |
|---|---|
| StreamLine Library Console | FRS_4.0 |
| Tape Drives:<br>■ T10000A<br>■ T10000B<br>■ T9840D<br>■ HP LTO4<br>■ HP LTO5<br>■ IBM LTO4<br>■ IBM LTO5 | <br>1.34.208 or higher<br>1.38.x07 or higher<br>1.42.104 or higher<br>H58S Fibre Channel<br>I2DS Fibre Channel<br>94D7 Fibre Channel<br>A232 Fibre Channel |
| Virtual Operator Panel (VOP) | Version 1.0.14 or higher<br>Version 1.0.16 |

# SL500 Modular Library System

**FIGURE 4-5** SL500 Modular Library System Requirements

**High-level Description:**
The SL500 library is a self contained, fully automated, cartridge tape storage system that is scalable and mounts into a standard 483 mm (19 in.) rack or cabinet. The library can consist of 1 to 5 modules (one base and up to four expansion modules). Because of the scalability, the capacity of an SL500 library can store:
■ From: 2 tape drives with 530 data cartridge slots
■ To: 18 tape drives with 395 data cartridge slots
■ A cartridge access port that holds 5 to 45 slots (depending on the number of modules)
With a variety of tape drives and cartridges slots in-between.

**Operating System Support:**
The SL500 supports all major operating systems; enterprise *and* open systems.

**Host-to-Library Interface:**
■ Single Ethernet* (TCP/IP) 1x
■ Fibre Channel
* Supports Partitioning

**Note:** Encryption hardware can be installed in the same rack as the library; depending on the number of modules installed.

| Order Number | Description |
|---|---|
| CRYPTO-2X-SL500B-N | Base module *(required)* Crypto kit for use with SL500 library base. Ethernet switch and cables for installation within SL500 library. In addition, one expansion module kit CRYPTO-2X-SL500X-N for each Drive Expansion Module is required. |
| CRYPTO-2X-SL500X-N | Expansion module *(optional)* crypto kit for use with SL500 library expansion. Ethernet cables for installation within SL500 library. Up to 4 additional expansion modules may be added. **Note:** The SL500 is a rack-installed library. ■ With 3 or fewer expansion modules, encryption hardware can be installed in the same rack. |

**Firmware Levels**

| Library | i15 — 1300, i16 — 1373, i17 — 139x, **i18** — 1407 |
|---|---|
| Tape Drives:<br>■ HP LTO4<br>■ HP LTO5<br>■ IBM LTO4<br>■ IBM LTO5 | H58S Fibre Channel (SCSI: B57S)<br>I2DS Fibre Channel<br>94D7 Fibre Channel<br>A232 Fibre Channel |
| Virtual Operator Panel (VOP) | Version 1.0.14 or higher for LTO4<br>Version 1.0.16 |

# 9310 Automated Cartridge System

**FIGURE 4-6** 9310 Automated Cartridge System Requirements

**High-level Description:**
The 9310—also called PowderHorn—can store:
- From 2,000 up to 6,000 tape cartridges
- Up to **4** drive cabinets with space for up to
  **20** drives per cabinet (80 drives total)

**Operating System Support:**
The 9310 library supports all major operating
systems; enterprise *and* open systems.

**Host-to-Library Interface:**
- TCP/IP

The 9310 requires additional hardware consisting
of Ethernet switches and 19-inch rack.

| Order Number | Description |
|---|---|
| CRYPTO-2X-9310-Z-N | Sun StorageTek crypto kit for use with 9310 libraries. A 24-port ethernet switch and cables for installation in 9310 plus 16-port ethernet switch and cables for connection to KMA externally. Rack mounting HW |
| 9310 libraries require: CRYPTO-2X-9741E-N | Sun StorageTek crypto kit for use with 9310 libraries. A 24-port ethernet switch, cables, and rack mount HW for installation within 9741E cabinet. One required for each additional 9741E cabinet used for crypto. RoHS 5 compliant. **Note:** Each 9741E cabinet may contain up to 20 tape drives and requires the use of a 24-port Ethernet switch. |
| **Firmware Levels** | Firmware Level or Higher |
| Library Prerequisites | The 9310 requires upgrades to support the T10000 tape drive. |
| Feature Codes: | 93T1—LSM upgrade (firmware and hardware) 93T1—LMU upgrade (firmware only) XT10—Hardware kit upgrade (9741E cabinet) |
| Library Firmware (minimum) | 9311: 4.4.06 9330: TCP/IP - 2.1.02 code 9330: 3270 - 1.9.73 code |
| Tape Drives: ■ T10000A ■ T10000B ■ T9840D | 1.34.208 or higher 1.38.x07 or higher 1.42.104 or higher |
| Virtual Operator Panel (VOP) | Version 1.0.11 or higher Version 1.0.16 |

# L-Series Libraries

**Note –** The L-Series libraries (L700 and L1400) *do not* support LTO tape drives for the Oracle Key Manager encryption solution.

**FIGURE 4-7** L-Series Library Requirements

**High-level Description:**
L700 and L1400 libraries support two models:
- *Single frame* libraries can hold:
    - From 678 tape cartridges and
    - Up to **12** tape drives.
- *Dual frame* libraries holds
    - From 1,344 tape cartridges and
    - Up to **24** tape drives.

**Operating System Support:**
Supports open system platforms, such as UNIX, Windows NT, Novel, and Linux.

**Host-to-Library Interface:**
- LVD or HVD SCSI
- Fibre Channel option

The L700e/L1400M libraries have internal rack space for the encryption hardware.

| Order Number | Description |
|---|---|
| CRYPTO-2X-L7/14-N | Sun StorageTek crypto kit for use with L180/700/1400 libraries. A 16-port ethernet switch, cables, and mounting HW for installation within L-series libraries. |

| Firmware Levels | Firmware Level or Higher |
|---|---|
| Library (minimum)<br>■ L700e / L1400 | 3.11.02 or higher |
| Tape Drives:<br>■ T10000A<br>■ T10000B<br>■ T9840D | 1.34.208 or higher<br>1.38.x07 or higher<br>1.42.104 or higher |
| Virtual Operator Panel (VOP) | Version 1.0.14 or higher<br>Version 1.0.16 |

# SL24 Autoloader and SL48 Library

**Note –** The SL24 and SL48 libraries *do not* support T-Series tape drives for the Oracle Key Manager encryption solution.

**FIGURE 4-8** SL24 Autoloader and SL48 Library Requirements

**High-level Description:**
Oracle's **StorageTek SL24 tape autoloader** provides high-capacity automated backup and recovery in a space-efficient, highly manageable product.

With one drive this autoloader includes *two* removable 12-slot magazines with one mail slot dedicated to import and export of data cartridges.

Oracle's **StorageTek SL48 tape library** can meet the data storage demands—including unattended backup, archiving, and disaster recovery.

The SL48 tape library is a 4-U form factor product. With one drive, this library includes *four* removable 12-slot magazines with three mail slots dedicated to the import and export of data cartridges.

**Operating System Support:**
Supports a broad variety of servers, operating systems, and ISV packages.

**Host-to-Library Interface:**
Both products provide SCSI, SAS, and FC interfaces for flexible integration into any storage environment.

**SL24 Autoloader**

Native capacity of 36 TB with a StorageTek LTO5 tape drives

**SL48 Library**

Native capacity of 72 TB with a StorageTek LTO5 tape drives

| Order Number | Description |
|---|---|
| LTO-ENCRYPT-ACTIVE | LTO5 encryption-capable tape drives |

**Firmware Levels**

| | |
|---|---|
| Library (minimum)<br>■ SL24 autoloader<br>■ SL48 library | <br>D.90/3.00e<br>G.20/3.00e |
| Encryption-capable Tape Drives:<br>■ HP LTO5<br>■ IBM LTO5 | <br>I2DS<br>A232 |
| Virtual Operator Panel (VOP) | Version 1.0.16 for the LTO5 tape drives<br>MD-VOP 1.x |

# Rack Mount

**FIGURE 4-9** Rackmount Requirements

The StorageTek rack can hold up to **12** manual-mount tape drives in 6 trays.

This figure shows the T10000 rack module.
■ The top (A) operator panel works with the drive on the left.
■ The bottom (B) operator panel works with the drive on the right.
When only one drive is installed, it must be installed on the left.

**Recommendation:**
The customer should purchase a CBNT42U cabinet with this configuration.



T105_006

| Order Number | Description |
| --- | --- |
| CRYPTO-2X-RACK-Z-N | StorageTek rack mount kit. Include 16-port switch and cabling. |

**Firmware Levels**

| Tape Drives: | |
| --- | --- |
| ■ T10000A | 1.34.208 or higher |
| ■ T10000B | 1.38.x07 or higher |
| ■ T9840D | 1.42.104 or higher |
| Virtual Operator Panel (VOP) | Version 1.0.11 or higher |

# Tape Drive Instructions

See the specific tape drive Systems Assurance Guides for information.

**TABLE 4-1** Tape Drive Ordering Instructions

| Publication Description | Part Number |
|---|---|
| T10000 Tape Drive Systems Assurance Guide | StorageTek: TM0002 |
| T9x40 Tape Drive Systems Assurance Guide | StorageTek: MT5003 |
| Service Delivery Platform Systems Assurance Guide | StorageTek: 11042004 |

# Library Instructions

See the specific library Systems Assurance Guides for information.

**TABLE 4-2** Library Ordering Instructions

| Publication Description | Part Number |
|---|---|
| SL8500 Modular Library Systems Assurance Guide | StorageTek: MT9229 |
| SL3000 Modular Library Systems Assurance Guide | StorageTek: 316194101 |
| SL500 Modular Library Systems Assurance Guide | StorageTek: MT9212 |
| L700/1400 Library Ordering and Configuration Guide | StorageTek: MT9112 |
| L180 Library Ordering and Configuration Guide | StorageTek: MT9112 |
| 9310 PowderHorn Library Systems Assurance Guide | StorageTek: ML6500 |

# Power Cables

For more information and additional part numbers, go to:
http://scss280r1.singapore.sun.com/handbook_internal/Devices/AC_Power/ACPO
WER_AC_Power_Cords.html

| ATO Power Cord | PTO Equivalent | Description | Amps | Voltage | Cable |
|---|---|---|---|---|---|
| 333A-25-10-AR | X312F-N | Pwrcord, Argentina,2.5m, IRAM2073,10A,C13 | 10 | 250 | 180-1999-02 |
| 333A-25-10-AU | X386L-N | Pwrcord, Australian,2.5m, SA3112,10A,C13 | 10 | 250 | 180-1998-02 |
| 333A-25-10-BR | X333A-25-10-BR-N | Pwrcord, Brazil,2.5m,NBR14136,10A,C13 | 10 | 250 | 180-2296-01 |
| 333A-25-10-CH | X314L-N | Pwrcord, Swiss,2.5m,SEV1011, 10A,C13 | 10 | 250 | 180-1994-02 |
| 333A-25-10-CN | X328L | Pwrcord, China,2.5m,GB2099, 10A,C13 | 10 | 250 | 180-1982-02 |
| 333A-25-10-DK | X383L-N | Pwrcord, Denmark,2.5m, DEMKO107,10A,C13 | 10 | 250 | 180-1995-02 |
| 333A-25-10-EURO | X312L-N | Pwrcord, Euro,2.5m,CEE7/VII, 10A,C13 | 10 | 250 | 180-1993-02 |
| 333A-25-10-IL | X333A-25-10-IL-N | Pwrcord, Israel,2.5m,SI-32, 10A,C13 | 10 | 250 | 180-2130-02 |
| 333A-25-10-IN | X333A-25-10-IN-N | Pwrcord, India,2.5m,IS1293,10A,C13 | 10 | 250 | 180-2449-01 |
| 333A-25-10-IT | X384L-N | Pwrcord, Italian,2.5m,CEI23, 10A,C13 | 10 | 250 | 180-1996-02 |
| 333A-25-10-KR | X312G-N | Pwrcord, Korea,2.5m,KSC8305, 10A,C13 | 10 | 250 | 180-1662-03 |
| 333A-25-10-TW | X332A-N | Pwrcord, Taiwan,2.5m, CNS10917,10A,C13 | 10 | 125 | 180-2121-02 |
| 333A-25-10-UK | X317L-N | Pwrcord, UK,2.5m,BS1363A, 10A,C13 | 10 | 250 | 180-1997-02 |
| 333A-25-10-ZA | X333A-25-10-ZA-N | Pwrcord, South Africa,2.5m,SANS164,10A,C13 | 10 | 250 | 180-2298-01 |
| 333A-25-15-JP | X333A-25-15-JP-N | Pwrcord, Japan,2.5m,PSE5-15, 15A,C13 | 15 | 125 | 180-2243-01 |
| 333A-25-15-NEMA | X311L | Pwrcord, N.A./Asia,2.5m, 5-15P,15A,C13 | 15 | 125 | 180-1097-02 |
| 333A-25-15-TW | X333A-25-15-TW-N | Pwrcord, Taiwan,2.5M, CNS10917,15A,C13 | 15 | 125 | 180-2333-01 |
| 333F-20-10-NEMA | X320A-N | Pwrcord, N.A./Asia,2.0m, 6-15P,10A,C13 | 10 | 250 | 180-2164-01 |
| 333F-25-15-JP | X333F-25-15-JP-N | Pwrcord, Japan,2.5m,PSE6-15, 15A,C13 | 15 | 250 | 180-2244-01 |
| 333J-40-15-NEMA | X336L | Pwrcord, N.A./Asia,4.0m, L6-20P,15A,C13 | 15 | 250 | 180-2070-01 |
| 333R-40-10-309 | X332T | Pwrcord, INTL,4.0m, IEC309-IP44,10A,C13 | 10 | 250 | 180-2071-01 |
| For use in non Sun Racks | | | | | |
| 333V-20-15-C14 | X333V-20-15-C14-N | Pwrcord, Jmpr,Straight,2.0m,C14,15A,C13 | 15 | 250 | 180-2442-01 |
| 333V-30-15-C14 | X333V-30-15-C14-N | Pwrcord, Jmpr,Straight,3.0m,C14,15A,C13 | 15 | 250 | 180-2443-01 |
| For use in Sun Rack (NGR) | | | | | |
| 333W-10-13-C14RA | X9237-1-A-N | Pwrcord, Jmpr,1.0m,C14RA,13A,C13 | 13 | 250 | 180-2082-01 |
| 333W-25-13-C14RA | X9238-1-A-N | Pwrcord, Jmpr,2.5m,C14RA,13A,C13 | 13 | 250 | 180-2085-01 |
| For use in Sun Rack II (Redwood) | | | | | |
| SR-JUMP-1MC13 | XSR-JUMP-1MC13-N | Pwrcord, Jmpr,SR2,1.0m,C14RA,13A,C13 | 13 | 250 | 180-2379-01 |
| SR-JUMP-2MC13 | XSR-JUMP-2MC13-N | Pwrcord, Jmpr,SR2,2.0m,C14RA,13A,C13 | 13 | 250 | 180-2380-01 |

# ATO Bill of Materials

**TABLE 4-3** ATO Bill of Materials Part NUmbers and Descriptions

| Order Number | Description |
|---|---|
| CRYPTO-2X-SL8500-N | Sun StorageTek crypto kit for use with SL8500 libraries. A 24-port ethernet switch, cables, and rack mount HW for installation within SL8500 library |
| CRYPTO-2X-9310-Z-N | Sun StorageTek crypto kit for use with 9310 libraries. A 24-port ethernet switch and cables for installation in 9310 plus 16-port ethernet switch and cables for connection to KMA externally. Rack mounting HW |
| CRYPTO-2X-9741E-N | Sun StorageTek crypto kit for use with 9310 libraries. A 24-port ethernet switch, cables, and rack mount HW for installation within 9741E cabinet. One required for each additional 9741E cabinet used for crypto. RoHS 5 compliant. |
| CRYPTO-2X-L7/14-N | Sun StorageTek crypto kit for use with L180/700/1400 libraries. A 16-port ethernet switch, cables, and mounting HW for installation within L-series libraries. |
| CRYPTO-2X-SL500X-N | (expansion module)   Sun StorageTek crypto kit for use with SL500 library expansion. Ethernet cables for installation within SL500 library |
| CRYPTO-2X-SL500B-N | (base module) Sun StorageTek crypto kit for use with SL500 library base. Ethernet switch and cables for installation within SL500 library. Note: An encryption capable SL500 requires one base library accessory kit CRYPTO-2X-SL500B-N. In addition, one expansion module accessory kit CRYPTO-2X-SL500X-N for each Drive Expansion Module is required. |
| XSL3000-ETHRNT1-N | StorageTek SL3000 X-Option, Ethernet Switch for Tape Drives, Includes cable harness for 8 drives, Supports 1st Drive Array in BM or DEM, Needed for SDP and Encryption, Includes Power Cable, Includes Ethernet Switch Harness |
| XSL3000-ETHRNT2-N | StorageTek SL3000 X-Option, 8 Drive Ethernet Cable Harness, Requires XSL3000-ETHRNT1-Z, Supports 2nd Drive Array in BM or DEM, Needed for SDP and Encryption, Includes Power Cable and Switch Harness B/C, |
| XSL3000-ETHRNT3-N | StorageTek SL3000 X-Option, Ethernet Switch for Tape Drives, Includes cable harness for 8 drives, Supports 3rd Drive Array in BM or DEM, Needed for SDP and Encryption, Includes Power Cable and Switch Harness A/C |
| XSL3000-ETHRNT4-N | StorageTek SL3000 X-Option, 8 Drive Ethernet Cable Harness, Requires XSL3000-ETHRNT4-Z, Supports 4th Drive Array in DEM, Needed for SDP and Encryption, Includes Power Cable, Includes Ethernet Switch Harness C/C. Note:   SL3000 released it's own kits for encryption. There are 4 parts - I think the cabling is just different but not sure.   How many and which depends on the number of encryption ready drives to be supported |
| CRYPTO-2X-RACK-Z-N | Sun StorageTek 16-port ethernet switches and rack mounting HW for use with the Oracle Key Manager in redundancy configuration (For rackmount tape) |
| **Additional switch option:** | |
| CRYPTO-X-24PT-Z-N | Sun StorageTek 24PT ethernet switch. No mounting HW or cables. |

# IBM ICSF Integration

This appendix provides an overview about the IBM® Integrated Cryptography Service Facility (ICSF)[1]. For more information, refer to:

■ *Oracle Key Manager: ICSF Integration Guide* PN: 31619810x
■ *Oracle Key Manager: Administration Guide* PN: 31619510x

# System Requirements

Both the IBM mainframe and the OKM Cluster have system requirements for this solution.

## IBM Mainframe

The IBM z/OS mainframe must be running ICSF HCR-7740 or higher.

With the Enterprise Library Software (ELS 7.0) or Nearline Control Software (NCS 6.2) along with any associated PTFs.

A Cryptographic Express2 coprocessor (CEX2C) card must also be installed on the IBM mainframe.

## OKM

The OKM must be running Version 2.2 or higher.

---

1. ICSF is a software component of z/OS providing cryptographic support either in its own software routines or through access to external cryptographic hardware, such as the Oracle Key Manager.

# Understanding the Solution

The IBM Integrated Cryptography Service Facility (ICSF) is an encryption solution where the external key store resides in an IBM mainframe and is accessed using a TLS/XML protocol. This protocol is supported in the IBM mainframe with the keys stored in a Token Data Set in the IBM Integrated Cryptography Service Facility.

FIGURE A-1 shows a typical configuration.

**FIGURE A-1** ICSF Site Configuration
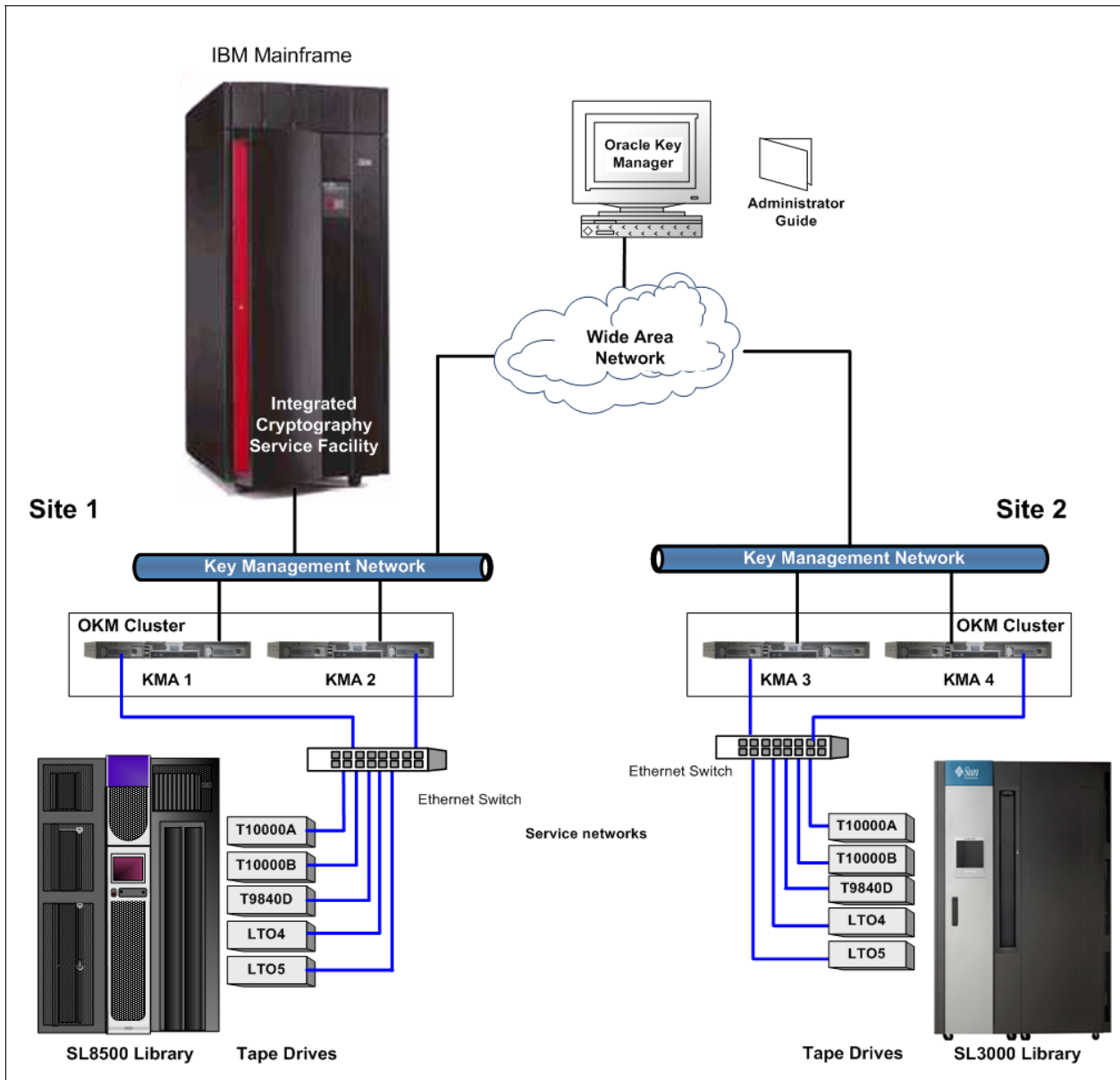
## Site Configurations

The cluster periodically issues requests to the IBM mainframe to create new master keys (referred to as *application keys* in ICSF).

The KMAs then use these new master keys to derive new tape encryption keys.

**Note –** The mainframe where Common Cryptographic Architecture (CCA/ICSF) resides.

# Key Stores and Master Key Mode

In version 2.x, the KMAs generate their own keys using their Cryptographic Accelerator (SCA6000) cards. Some customers may prefer to have the KMAs use master keys that are created and stored in an external key store contained in an IBM mainframe.

Version 2.2 introduces a Master Key Mode feature. When this feature is enabled, the OKM derives tape encryption keys from a set of master keys. The master keys are created and stored in an external key store.

Full disaster recovery is possible with just the tapes, the master keys, and factory default equipment.

## IBM Mainframe

Various steps are required to configure a z/OS system to be used as an external key store for an OKM cluster.

## Updating Information

After the IBM mainframe has been configured, the z/OS systems programmer must provide the following information to the administrator of an OKM:
- Host name or IP address of the mainframe
- Port number (such as 9889)
- Web application path (such as "/cgi/smcgcsf")
- File containing the client "user certificate" (exported and transferred off of the mainframe)
- File containing the client private key (exported and transferred off of the mainframe)
- Password that was used when the client private key was created
- File containing the Root CA certificate (exported and transferred off of the mainframe)

The administrator of an Oracle Key Manager enters this information as the Master Key Provider settings in the Security Parameters panel of the OKM Manager GUI.

After the administrator saves these settings, the OKM cluster begins to issue requests to the Proxy on the IBM mainframe.

The client "user certificate" and the client private key might appear in the same file when they are exported from the IBM mainframe. If so, then the administrator should specify the same file in the OKM Certificate File Name and OKM Private Key File Name fields in the Master Key Provider settings.

# Work Sheets

The following pages contain work sheets that can help prepare for the installation of a Oracle encryption solution.

These work sheets include:

- "Site Log"
- "Obtaining Support"
    - Make several copies and give them to the customer.
    - Explain how to use them.
- "Initial Configuration Work Sheet"
- "User Roles Work Sheet"
- "Tape Drives Work Sheet"
- "Agent Enrollment Work Sheet"

**Make copies as necessary.**

# Site Log

| Account Name: | |
|---|---|

| KMA | | | |
|---|---|---|---|
| Site Location: | KMA S/N: | KMA Name: | KMA Firmware Level: |
| KMA Number: | | Number of KMAs in Cluster: | |
| KMA IP Address: | | Service Network IP: | |
| Oracle Manager IP: | | ELOM / ILOM IP: | |
| IPv6 \| ❏ Yes ❏ No: | | DR Site \| ❏ Yes ❏ No: | |
| NTP \| ❏ Yes ❏ No: | | DHCP \| ❏ Yes ❏ No: | |
| Gateway \| ❏ Yes ❏ No: | | DNS \| ❏ Yes ❏ No: | |
| KMA Location: | | | |
| Oracle Manager Location: | | | |
| Configuration Types: | ❏ SL8500 library<br>❏ SL3000 library<br>❏ SL500 library<br>❏ 9310 library<br>❏ L-Series<br>❏ SL24/SL48 | Tape Drive Types:<br><br>How many? _____ | ❏ T10000A tape drive<br>❏ T10000B tape drive<br>❏ T9840D tape drive<br>❏ HP LTO tape drive<br>❏ IBM LTO tape drive<br>❏ Standalone |

| KMA | | | |
|---|---|---|---|
| Site Location: | KMA S/N: | KMA Name: | KMA Firmware Level: |
| KMA Number: | | Number of KMAs in Cluster: | |
| KMA IP Address: | | Service Network IP: | |
| Oracle Manager IP: | | ELOM / ILOM IP: | |
| IPv6 \| ❏ Yes ❏ No: | | DR Site \| ❏ Yes ❏ No: | |
| NTP \| ❏ Yes ❏ No: | | DHCP \| ❏ Yes ❏ No: | |
| Gateway \| ❏ Yes ❏ No: | | DNS \| ❏ Yes ❏ No: | |
| KMA Location: | | | |
| Oracle Manager Location: | | | |
| Configuration Types: | ❏ SL8500 library<br>❏ SL3000 library<br>❏ SL500 library<br>❏ 9310 library<br>❏ L-Series<br>❏ SL24/SL48 | Tape Drive Types:<br><br>How many? _____ | ❏ T10000A tape drive<br>❏ T10000B tape drive<br>❏ T9840D tape drive<br>❏ HP LTO tape drive<br>❏ IBM LTO tape drive<br>❏ Standalone |

# Obtaining Support

Technical support is available 24 hours a day, seven days a week and begins with a telephone call from you to Oracle Support. You will receive immediate attention from qualified personnel, who record problem information and respond with the appropriate level of support.

To contact Oracle about a problem:

1. Use the telephone and call:
   - 800.525.0369 (inside the United States) or
   - Contact any of Sun's worldwide offices to discuss support solutions for your organization. You can find address and telephone number information at: http://www.oracle.com/us/corporate/index.htm or http://www.oracle.com/us/support/index.html

2. Describe the problem to the call taker. The call taker will ask several questions then:
   - Route your call to the appropriate level of support
     or
   - Dispatch a service representative.

If you have the following information when you place a service call, the process will be much easier. Complete as much information as possible—if known.

| **Account name** | | | |
|---|---|---|---|
| **Site location number** | | | |
| **Contact name** | | | |
| **Telephone number** | | | |
| **Equipment model number** | ❏ **KMA** (Appliance)<br>❏ **OKM Manager** (GUI)<br>❏ SL8500 library<br>❏ SL3000 library<br>❏ SL500 library | ❏ 9310 library<br>❏ L700/1400 library<br>❏ SL24 and SL48<br>❏ Standalone<br>❏ Network/switch | ❏ T10000A tape drive<br>❏ T10000B tape drive<br>❏ T9840D tape drive<br>❏ HP LTO drive<br>❏ IBM LTO drive |
| **Device addresses** | | | |
| **IP Addresses** | | | |
| **Error Codes** | | | |
| **Urgency of problem** | | | |
| **Problem description** | | | |

# Initial Configuration Work Sheet

| Description | First KMA | | | Second KMA | | |
|---|---|---|---|---|---|---|
| | Hostname | IP Address / Netmask | DHCP?[1] | Hostname | IP Address / Netmask | DHCP?[1] |
| LAN 0 = Management | | | Yes ❑ No ❑ | | | Yes ❑ No ❑ |
| LAN 1 = ELOM/ILOM | | | Yes ❑ No ❑ | | | Yes ❑ No ❑ |
| LAN 2 = Service | | | Yes ❑ No ❑ | | | Yes ❑ No ❑ |
| LAN 3 = Aggregated | | | Yes ❑ No ❑ | | | Yes ❑ No ❑ |
| Using IPv6 addressing | Yes ❑ No ❑ | | | Yes ❑ No ❑ | | |
| KMA Name | | | | | | |
| Gateway | | | | | | |
| DNS Server | Hostname:<br>IP address: | | | Hostname:<br>IP address: | | |
| Security Officer | Login:<br>Passphrase: | | | Login:<br>Passphrase: | | |
| Root account Passphrase | Login:<br>Passphrase: | | | Login:<br>Passphrase: | | |
| ELOM Passphrase | Login:<br>Passphrase: | | | Login:<br>Passphrase: | | |
| Key Split Credentials[2] | | | | | | |
| Autonomous Unlocking [3] | | | | | | |
| Keyboard Type | | | | | | |

| Description | First KMA | | | Second KMA | | |
|---|---|---|---|---|---|---|
| | Hostname | IP Address / Netmask | DHCP?[1] | Hostname | IP Address / Netmask | DHCP?[1] |
| 1. Addresses assigned using DHCP **must be static**. The system cannot handle the DHCP server changing the IP addresses once assigned. | | | | | | |
| 2. Configuration: M of N, where M is minimum threshold and N is the size of key split configuration. List key split users (and passphrases). | | | | | | |
| 3. Autonomous Unlocking allows the KMA to enter a fully operational state after a hard or soft reset without requiring the entry of a quorum of passphrases using the OKM Manager. This information should not be written down and should be entered by the person to which they belong. These entries can be changed in the OKM Manager; so it may be desirable to enter something simple during the configuration, then change it later using the OKM GUI immediately after the KMA is configured. | | | | | | |

# User Roles Work Sheet

| User ID | Description | Passphrase ** (Confidential password) | Roles | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | Security Officer | Compliance Officer | Operator | Backup Operator | Auditor | Quorum Member |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

**Note:** The Passphrase should not be recorded here for security reasons.
This column is provided as a reminder that as User IDs are entered, the person with that ID will be required to enter a passphrase.

# Tape Drives Work Sheet

| Site Name: | | | Site Number: | |
|---|---|---|---|---|
| SDP IP Address: | | | File Pathname: | Location: |

| | Serial Number / DMOD (Last 8 digits) | Drive Type | Crypto Serial Number (6 hexadecimal characters) | Drive IP Address | Location |
|---|---|---|---|---|---|
| 1. | | | | | |
| 2. | | | | | |
| 3. | | | | | |
| 4. | | | | | |
| 5. | | | | | |
| 6. | | | | | |
| 7. | | | | | |
| 8. | | | | | |
| 9. | | | | | |
| 10. | | | | | |
| 11. | | | | | |
| 12. | | | | | |
| 13. | | | | | |
| 14. | | | | | |
| 15. | | | | | |
| 16. | | | | | |
| 17. | | | | | |
| 18. | | | | | |
| 19. | | | | | |
| 20. | | | | | |

# Agent Enrollment Work Sheet

| KMA ___ Hostname: | | | | KMA ___ Hostname: | | |
|---|---|---|---|---|---|---|
| **KMA IP Address:** | | | | **KMA IP Address:** | | |

| Drive Address | Drive Type | Drive IP Address | Agent ID | Passphrase | Tokens? | Perma |
|---|---|---|---|---|---|---|
| **1.** | | | | | Yes ❏  No ❏ | Yes ❏ |
| **2.** | | | | | Yes ❏  No ❏ | Yes ❏ |
| **3.** | | | | | Yes ❏  No ❏ | Yes ❏ |
| **4.** | | | | | Yes ❏  No ❏ | Yes ❏ |
| **5.** | | | | | Yes ❏  No ❏ | Yes ❏ |
| **6.** | | | | | Yes ❏  No ❏ | Yes ❏ |
| **7.** | | | | | Yes ❏  No ❏ | Yes ❏ |
| **8.** | | | | | Yes ❏  No ❏ | Yes ❏ |
| **9.** | | | | | Yes ❏  No ❏ | Yes ❏ |
| **10.** | | | | | Yes ❏  No ❏ | Yes ❏ |
| **11.** | | | | | Yes ❏  No ❏ | Yes ❏ |
| **12.** | | | | | Yes ❏  No ❏ | Yes ❏ |
| **13.** | | | | | Yes ❏  No ❏ | Yes ❏ |
| **14.** | | | | | Yes ❏  No ❏ | Yes ❏ |
| **15.** | | | | | Yes ❏  No ❏ | Yes ❏ |
| **16.** | | | | | Yes ❏  No ❏ | Yes ❏ |
| **17.** | | | | | Yes ❏  No ❏ | Yes ❏ |
| **18.** | | | | | Yes ❏  No ❏ | Yes ❏ |
| **19.** | | | | | Yes ❏  No ❏ | Yes ❏ |
| **20.** | | | | | Yes ❏  No ❏ | Yes ❏ |

# Glossary

This glossary defines terms and abbreviations used in this publication.

---

# A

**Advanced Encryption Standard (AES)**   A FIPS-approved NIST cryptographic standard used to protect electronic data.

**Agent**   Various types of encryption agents can be created to interact with the OKM for creating and obtaining keying material. The StorageTek T10000 models A and B, T9840D, and the HP LTO4 tape drives are types of encryption agents when enabled for encrypting.

**Agent Library**   The Agent Library is used by an Agent to retrieve key material from an Oracle Key Manager (OKM).

**Audit Log**   The OKM Cluster maintains a log of all auditable event occurring throughout the system. Agents may contribute entries to this log for auditable events.

**Auditor**   A user role that can view system audit trails (Audit List events and KMA security parameters).

**Autonomous Unlock**   When autonomous unlock is enabled a quorum of Security Officers is required to unlock a locked KMA. When disabled, the KMA can be unlocked by any Security Officer.

---

# B

**Backup File**   The file created during the backup process that contains all the information needed to restore a KMA. Encrypted with a key generated specifically for the backup. The key is contained in the corresponding backup key file.

**Backup Key File**   A file generated during the backup process containing the key used to encrypt the backup file. This file is encrypted using the system master key. The master key is extracted from the core security backup file using a quorum of the key split credentials.

**Backup Operator**   A user role that is responsible for securing and storing data and keys.

**BOT**   Beginning of Tape.

# C

**Certificate**   A Certificate is a digitally-signed document that serves to validate the holder's authorization and name.

**Certificate Authority (CA)**   A Certificate Authority registers end-users, issues their certificates, and can also create CAs below them. Within he Oracle Key Manager, the KMAs themselves act as the certificate authority to issue certificates to users, agents, and other KMAs.

**Cluster**   A Cluster is a set of Key Management Appliances that are grouped together into a single system to enhance fault tolerance, availability, and scalability.

**Compliance Officer**   A user role that manages the flow of data through your organization and can define and deploy data contexts (Key Groups) and rules that determine how data is protected and ultimately destroyed (Key Policies).

**Crypto-Accelerator**   A Crypto-Accelerator is a hardware device (a card) that can be used to increase the rate of data encryption/decryption, thereby improving system performance in high demand conditions.

**Crypto-active**   An encryption-capable tape drive that has had the encryption feature turned on.

**Crypto-ready**   A tape drive that has the ability to turn on device-encryption and become encryption-capable.

**Cryptography**   The art of protecting information by transforming it (encrypting) into an unreadable format, called cipher text. Only those who possess a special *key* can decipher (decrypt) the message into its original form.

**Cryptoperiods**   The length of time in which a key can be used for encryption. It starts when the key is first assigned to the drive.

# D

**Data Policy**   A data policy defines a set of encryption related parameters, such as the encryption and decryption "crypto-periods" for keys.

**Data Unit**   Data units are abstract entities within the OKM that represent storage objects associated with OKM policies and encryption keys. For tape drives, a data unit is a tape cartridge.

# E

**Encryption**  The translation of data into a secret code. Encryption is one of the most effective ways to achieve data security. To read an encrypted file, you must have access to a special key or password that enables you to decipher it.

# F

**FIPS**  Federal Information Processions Standards. The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration and Laboratories, which develops and promotes standards and technology, including:

- Computer Security Division and Resource Center (CSRC)
- Federal Information Processing Standards (FIPS)
- For more information visit: http://www.nist.gov/

# G

**GUI**  Graphical User Interface.

# H

**Hash Message Authentication Code (HMAC)**  In cryptography, a keyed-Hash Message Authentication Code, or HMAC, is a type of message authentication code (MAC) calculated using a cryptographic hash function in combination with a secret key.

# I

**Intelligent Platform Management Interface (IPMI)**  IPMI defines a set of common interfaces to a computer system that system administrators can use to monitor system health and manage the system.

**Internet Protocol (IP)**  A protocol used to route data from its source to its destination in an Internet environment.

**Internet Protocol address**

**IPv4** A four-byte value that identifies a device and makes it accessible through a network. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0 to 255.
For example, 129.80.145.23 could be an IP address.
Also known as TCP/IP address.

**IPv6** The next generation uses a 128-bit value written as eight groups of four hexadecimal characters separated by colons.
For example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

# K

**Key** A key in this context is a symmetric data encryption key. Agents can request new key material for encrypting data corresponding to one or more Data Units.

A key belongs to a single Key Group so that only Agents associated with the Key Group can access the key.

Keys have encryption and decryption cryptoperiods that are dictated by the Key Policy associated with the Key Group of the particular key. The type of key (that is, its length and algorithm) is specified by the Encryption Agent.

A random string of bits generated by the key management system, entered from the keyboard, or purchased.

**Key Group** Key Groups are used for organizing keys and associating them with a Key Policy. Key Groups are also used to enforce access to the key material by the Encryption Agents.

**Key Management Appliance (KMA)** A SunFire X2100-M2, X2200-M2, or X4170-M2 server preloaded with the OKM software. The appliance is a proven, dual-core processor with a Solaris 10 operating system that delivers policy-based key management and key provisioning services.

**Key Management System (KMS)** A system providing key management. The StorageTek system has a component providing key management on behalf of encryption agents. Now known as the Oracle Key Manager or OKM.

**Key Policy** A Key Policy provides settings for the cryptoperiods to be applied to keys. Each Key Group has a Key Policy, and a Key Policy may apply to zero or more Key Groups. The encryption and decryption cryptoperiods specified on the policy limit the usage of keys and trigger key life cycle events, such as the deactivation or destructions of keys.

# L

**Linear Tape-Open (LTO)**  A magnetic tape data storage technology. The standard form-factor of LTO technology goes by the name Ultrium, the "high capacity" implementation of LTO technology.

LTO Ultrium technology is an "open format" technology, which means users have multiple sources of product and media. The open nature of LTO technology also provides a means of enabling compatibility between different vendors' offerings.

# M

**Media key**  Encrypts and decrypts customer data on a tape cartridge.

# N

**network**  An arrangement of nodes and branches that connects data processing devices to one another through software and hardware links to facilitate information interchange.

**NIST**  National Institute of Standards and Technology.

# O

**Operator**  A user role responsible for managing the day-to-day operations of the system.

**OKM Cluster**  A set of one or more interconnected KMAs. All the KMAs in a Cluster should have identical information. This will not be the case only when an KMA is down, or when a newly created piece of information has not yet propagated through all KMAs in the OKM Cluster. An action taken on any KMA in the Cluster will eventually propagate to all KMAs in the OKM Cluster.

# R

**Read key**  This is a media key that is used when reading data from a tape.

**Rijndael algorithm**  An algorithm selected by the U.S. National Institute of Standards and Technology (NIST) for the Advanced Encryption Standard (AES). Pronounced "rain-dahl," the algorithm was designed by two Belgian cryptologists, Vincent Rijmen and Joan Daemen, whose surnames are reflected in the cipher's name.

**RSA**  In cryptography, **RSA** is an algorithm for public-key cryptography created by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT. The letters **RSA** are the initials of their surnames.

# S

**Secure Hash Algorithms (SHA)**  Secure Hash Algorithms are cryptographic hash functions designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard.

**Security Officer**  A user role that manages security settings, users, sites, and Transfer Partners.

**Security Policy**  A rigorous statement of the sensitivity of organizational data, various subjects that can potentially access that data, and the rules under which that access is managed and controlled.

**Site**  A site is an attribute of each OKM and Encryption Agent that indicates network proximity, or locality. When Encryption Agents connect to the OKM Cluster there is a bias towards establishing communication with KMAs in the same site as the Encryption Agent.

# T

**T10000 tape drive**  The T10000 tape drive is a small, modular, high-performance tape drive designed for high-capacity storage of data

T10000A stores up to 500 gigabytes (GB) of uncompressed data.

T10000B stores up to 1 terabyte (TB) of uncompressed data.

**T9840D tape drive**  The T9840D tape drive is a small, modular, is a small, high-performance, access-centric tape drive that has an average access time of just 8 seconds.

This drive obtains its high-performance by using a unique *dual-hub* cartridge design with midpoint load technology. This enables fast access and reduces latency by positioning the read/write head in the middle of the tape.

**Transport Layer Security (TLS)**  A cryptographic protocol that provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging and other data transfers.

# Z

**Zeroize**    To erase electronically stored data, cryptographic keys, and Critical Security Parameters by altering or deleting the contents of the data storage to prevent recovery of the data.

# Index

## Numerics

1400 installation requirements, 71, 72
3000 installation requirements, 68
3COM Switch, 39
500 installation requirements, 69
700 installation requirements, 71, 72
8500 installation requirements, 67
9310 installation requirements, 70
9741e Drive Cabinet, 70

## A

AC power factors and concerns, 35
accessory racks, SL8500, 38
adapter card
    types of, 21
Advanced Encryption Standard (AES), 2
Agents, definition, 3
aggregated
    network configuration, 39
    service port, 39
alley limitations, 34
ANSI standards, 38
assignments, customer roles, 52
auditor role, 52

## B

backup operator role, 52
batch file, LTO4, 61
behavior, LTO, 24
Belisarius card
    description, 21

## C

cabinet, specifications for installation, 38

cables, for required tools, 62
call center for support, 83
capacity
    of LTO4 tape drives, 21
    of T1000 tape drive, 20
    T9840D tape drive, 20
Capacity on Demand, 47
CBC–MAC standard, 2
CCM standard, 2
checklists
    *See Also* work sheets
    site planning, 34
    system assurance, 28
Cipher Block Chaining–Message Authentication
    Code, 2
cluster, definition of, 3
Common Criteria Consortium, 2
comparisons of tape drives and media, 23
compatibilities, media types, 23
compliance operator role, 52
concerns for site planning, 34
connectivity factors for pre-installation, 35
content management, 46
conversion bills
    9310 requirements, 70
Counter with CBC-MAC, 2
Cryptographic Accelerator, 3
cryptography, 1
customer
    contact sheet, 29
    roles, 52
    satisfaction, 27
customer-initiated maintenance, 83

## D

data path, partition planning, 49
delivery dock, 34