

Oracle Key Manager

Systems Assurance Guide



Part Number: E24530-02
October 2011

Copyright © 2008, 2011, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related software documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

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)
	April 2010	C	Refer to this revision for the list of changes. (Oracle branding, updated marketing/order numbers)
	November 2010	D	Refer to this revision for the list of changes. (Product Name Change, support for a new server [4170], a new tape drive [LTO5], and new platforms[SL24 and SL48])
	June 2011	E	■ Added information about the Auto Service Request (ASR) feature.
	July 2011	-01	■ Updated to an Oracle part number: E24530. ■ Revision -01. ■ Added information about the T10000C tape drive. ■ Included engineering comments/updates.
	October 2011	-02	■ Revision -02. ■ Updated to support Release 2.5 ■ Added information about databases in Appendix B, "Encryption for Oracle Databases" .

Note – Change bars are included in this revision.

Contents

Preface ix

Related Information ix

Documentation, Support, and Training x

1. Introduction 1

Planning for Encryption 1

Encryption Standards 2

Components 3

Encryption Hardware Kits 4

Key Manager Configurations 4

Key Management Appliance 9

SunFire 4170 Server 9

4170 Component Specifications 10

SunFire X2100 and X2200 Servers 11

SunFire X2100 Server 12

SunFire X2200 Server 13

Network Considerations 14

Management Network 14

ELOM and ILOM 14

KMA Service Port Aggregation 14

Key Management Appliance Physical Connections 17

Internet Protocol Versions 18

Automated Tape Libraries 19

Tape Drives 20

FIPS Compliant Tape Drives 20

About the StorageTek T10000 Tape Drive 21

About the StorageTek T9840D Tape Drive 21

About the LTO Tape Drives	22
Tape Drive Comparisons	23
StorageTek T-Series Tape Drives	24
LTO Tape Drives	25
LTO Encryption Behavior	25
Auto Service Request (ASR) Feature	27
2. Systems Assurance	29
Planning Meetings	30
Customer Team Member Contact Sheet	31
Oracle Team Member Contact Sheet	32
Configuration Planning	33
3. Site Preparation	37
Site Planning Checklist	38
Rack Specifications	42
SL8500 Rack Guidelines	42
Network Considerations	43
KMA Service Port Aggregation	43
Aggregated Service Network Switch Configuration	43
Network Routing Configuration	46
Cluster Discovery, Load Balancing, and Failover	46
KMA Routing Configuration and Discovery	47
Service Delivery Platform	48
Oracle Key Manager and the SDP	48
Content Management	50
Capacity on Demand	51
RealTime Growth Technology	51
Partitioning	52
Disaster Recovery	53
Planning the Data Path	53
Planning Tasks	54
Oracle Key Manager Interface	55
Role-Based Operations	56
Preparing the Tape Drives	62

T-Series Drive Data Preparation	62
Create a Drive Data File Structure	64
LTO Tape Drive Preparation	65
Required Tools	66
Supported Platforms and Web Browsers	66
Firmware Levels	67
4. Components	69
Supported Configurations	69
Supported Tape Drives	69
Supported Databases	70
Key Management Appliance	71
SL8500 Modular Library System	72
SL3000 Modular Library System	73
SL500 Modular Library System	74
9310 Automated Cartridge System	75
L-Series Libraries	76
SL24 Autoloader and SL48 Library	77
Rack Mount	78
Tape Drive Instructions	79
Library Instructions	79
Power Cables	80
ATO Bill of Materials	81
A. IBM ICSF Integration	83
System Requirements	83
IBM Mainframe	83
OKM	83
Understanding the Solution	84
Site Configurations	85
Key Stores and Master Key Mode	85
IBM Mainframe	85
Updating Information	85
B. Encryption for Oracle Databases	87

Transparent Data Encryption Overview	88
PKCS#11 Providers	88
Planning Considerations	89
Oracle Database Considerations	89
OKM Performance and Availability Considerations	89
C. Work Sheets	93
Site Log	94
Obtaining Support	95
Initial Configuration Work Sheet	96
User Roles Work Sheet	97
Drive Work Sheet	98
Agent Enrollment Work Sheet	99
Glossary	101
Index	109

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
<i>SunFire X2100 Server Installation Guide</i>	819-6589-xx
<i>SunFire X2200 Server Installation Guide</i>	819-6596-xx
<i>SunFire X4170 Server Installation Guide</i>	821-0481-xx
<i>Embedded Lights Out Manager Administration Guide</i>	819-6588-xx
<i>T10000 Tape Drive Installation Manual</i>	96173
<i>T9x40 Tape Drive Installation Manual</i>	95879
<i>SL8500 Modular Library System Installation Manual</i>	96138
<i>SL3000 Modular Library System Installation Manual</i>	316194201
<i>SL500 Modular Library System Installation Manual</i>	96114
<i>L700/1400 Library Installation Manual</i>	95843
<i>9310 PowderHorn Library Installation Manual</i>	9314
<i>Virtual Operator Panel—Service</i>	96180
<i>Virtual Operator Panel—Customer</i>	96179
<i>Oracle Key Manager Installation and Service Manual</i>	3161949xx

Publication Description	Part Number
<i>Oracle Key Manager Administration Guide</i>	3161951xx
<i>Oracle Key Manager Disaster Recovery Guide</i>	3161971xx
<i>Storage Regulatory and Safety Compliance Manual</i>	820-5506-xx
<i>Oracle Advanced Security Transparent Data Encryption Best Practices (July 2011) - Whitepaper</i>	
<i>Using Oracle Key Manager with Advanced Security Transparent Data Encryption (TDE) - Whitepaper</i>	

Documentation, Support, and Training

Function	URL	Description
Web Site	http://www.oracle.com/index.html	General information and links.
Documentation	http://www.oracle.com/technetwork/indexes/documentation/index.html http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#kmsl	Search for technical documentation. Download PDF/HTML documents. Order printed documents.
Downloads	http://www.sun.com/download/index.jsp or http://www.oracle.com/technetwork/indexes/downloads/index.html	Download firmware and graphical user interfaces, patches, and features.
E-Delivery	https://edelivery.oracle.com/	
Support	http://www.oracle.com/us/support/index.htm	Obtain and escalate support.
Online Account	https://reg.sun.com/register	Register for an Online Account.

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:

STP_FEEDBACK_US@oracle.com

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

Oracle Key Manager, Systems Assurance Guide, PN: E24530-xx

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** or Oracle **databases**.
- 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)	<p>The KMA is a SunFire™ server (such as the 2100, 2200, and 4170) for the hardware platform. This server:</p> <ul style="list-style-type: none"> ■ Runs the key manager application on a specialized, pre-loaded version of the Solaris™ 10 operating system. ■ Delivers a policy-based key manager and provisioning services. ■ Generates the raw keys for encryption
SCA6000 card	<p>An <i>optional</i> Sun Cryptographic Accelerator (SCA6000) card for cryptographic processing and administrative functions is provided for customers that require FIPS-compliance.</p> <p>Note: This is a FIPS 140-2 Level 3 hardware security module.</p>
OKM Manager or OKM Manager GUI	<p>The manager is a client-side software component with a graphical user interface (GUI).</p> <p>Note: The OKM Manager must be installed on a <i>customer-provided</i>, network-attached, PC, server, or workstation running Windows XP, Vista, 2003 Server, or running Solaris x86 or Solaris SPARC.</p>
OKM CLI	<p>A command line interface to assist with automation of management tasks such as backup and reporting.</p>
OKM Cluster	<p>A full set of KMAs in a system. All of the KMAs are aware of each other, and replicate information to each other.</p> <p>Note: <i>There must be a minimum of 2 servers in a cluster.</i></p>
Agent	<p>Agents interact with the OKM cluster for creating and obtaining keying material over a secure (TLS) session.</p>
Data Unit ID	<p>A unique ID assigned by the OKM to each individual data cartridge.</p>
Key Groups	<p>Provide organization for keys and associates them to a Key Policy. Key Groups are used by the OKM to enforce access to the key material by the Encryption Agents (tape drives) or Oracle databases.</p>
Network connections	<p>X2100/X2200 key management appliance have four network connections:</p> <p>LAN 0 = Management network</p> <p>LAN 1 = Embedded or Internal Lights Out Manager (ELOM/ILOM)</p> <p>LAN 2 = Service network, connection to the drives</p> <p>LAN 3 = Additional aggregated service port (<i>optional</i>)</p>

* **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 and Oracle databases, 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 drive-types in either a **library**, standalone **rack**, or Oracle database configuration.

The type of configuration determines how the 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 KMAs¹ (two or more) must be installed together to create a cluster². 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:

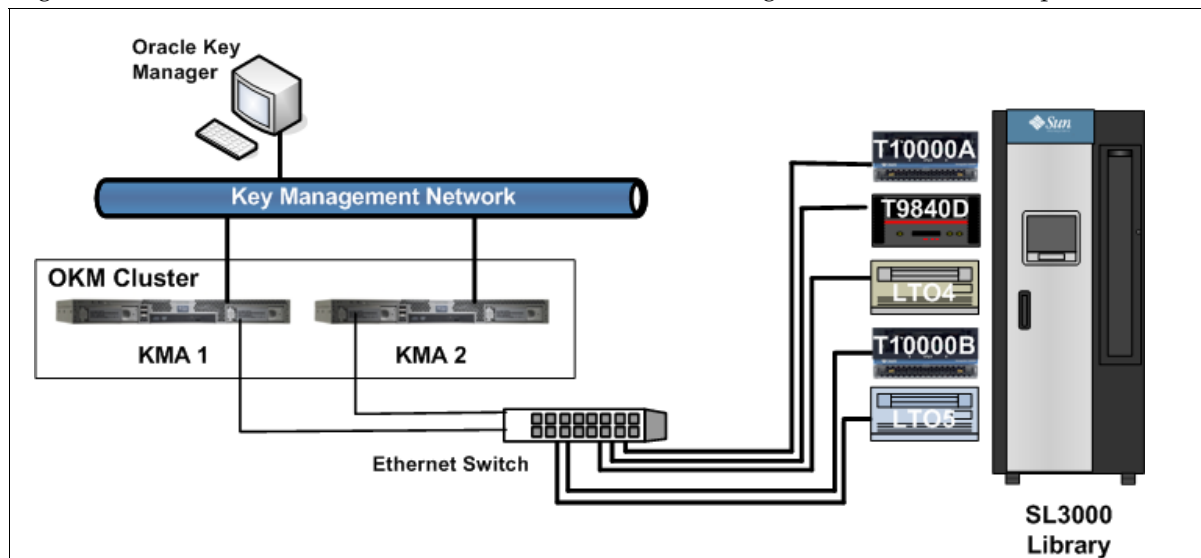
- [FIGURE 1-1](#) Single site – local area network
- [FIGURE 1-2](#) Multiple sites – wide area network
- [FIGURE 1-3](#) Multiple sites with disaster recovery – wide area network
- [FIGURE 1-4](#) Disaster Recovery Configuration
- [FIGURE 1-5](#) Database and Automated Library configuration

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

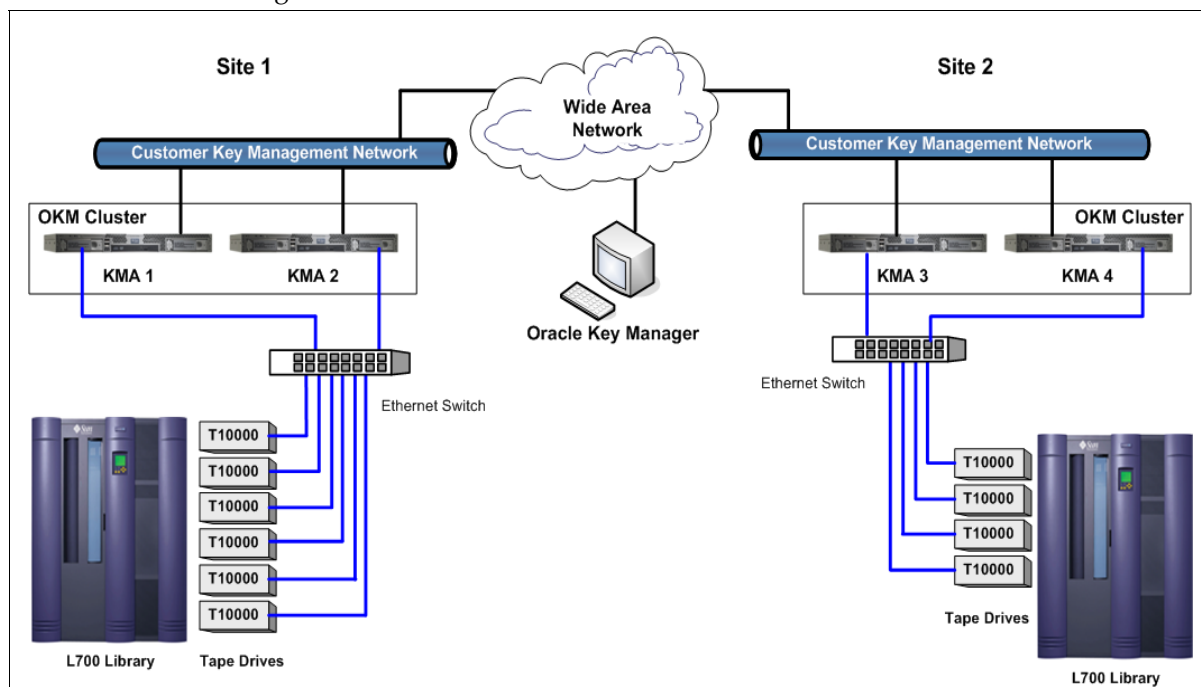
2. A **Cluster** is a group of linked appliances that work together, so that in many respects they form a single component.

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.

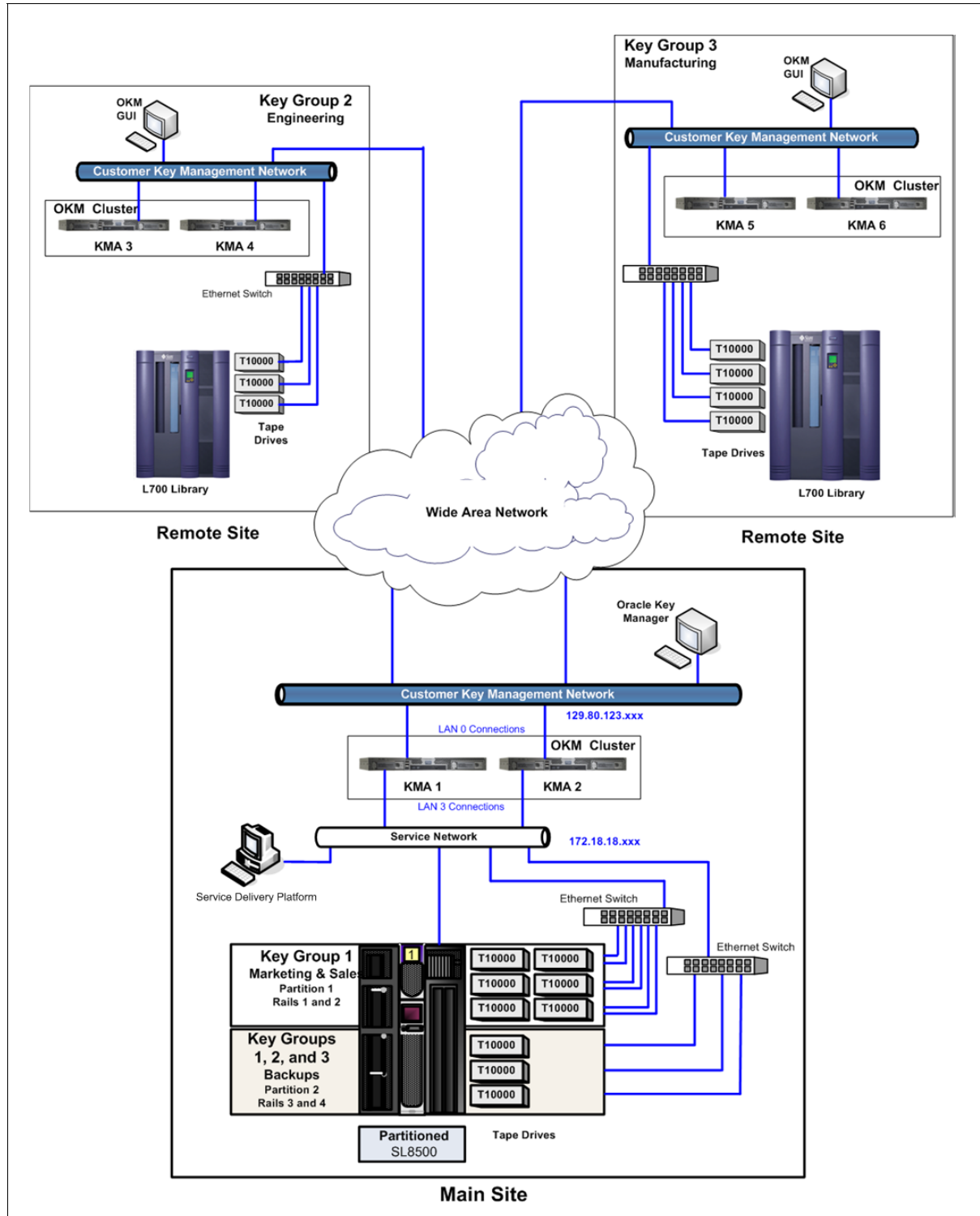


FIGURE 1-4 Disaster Recovery Configuration

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.

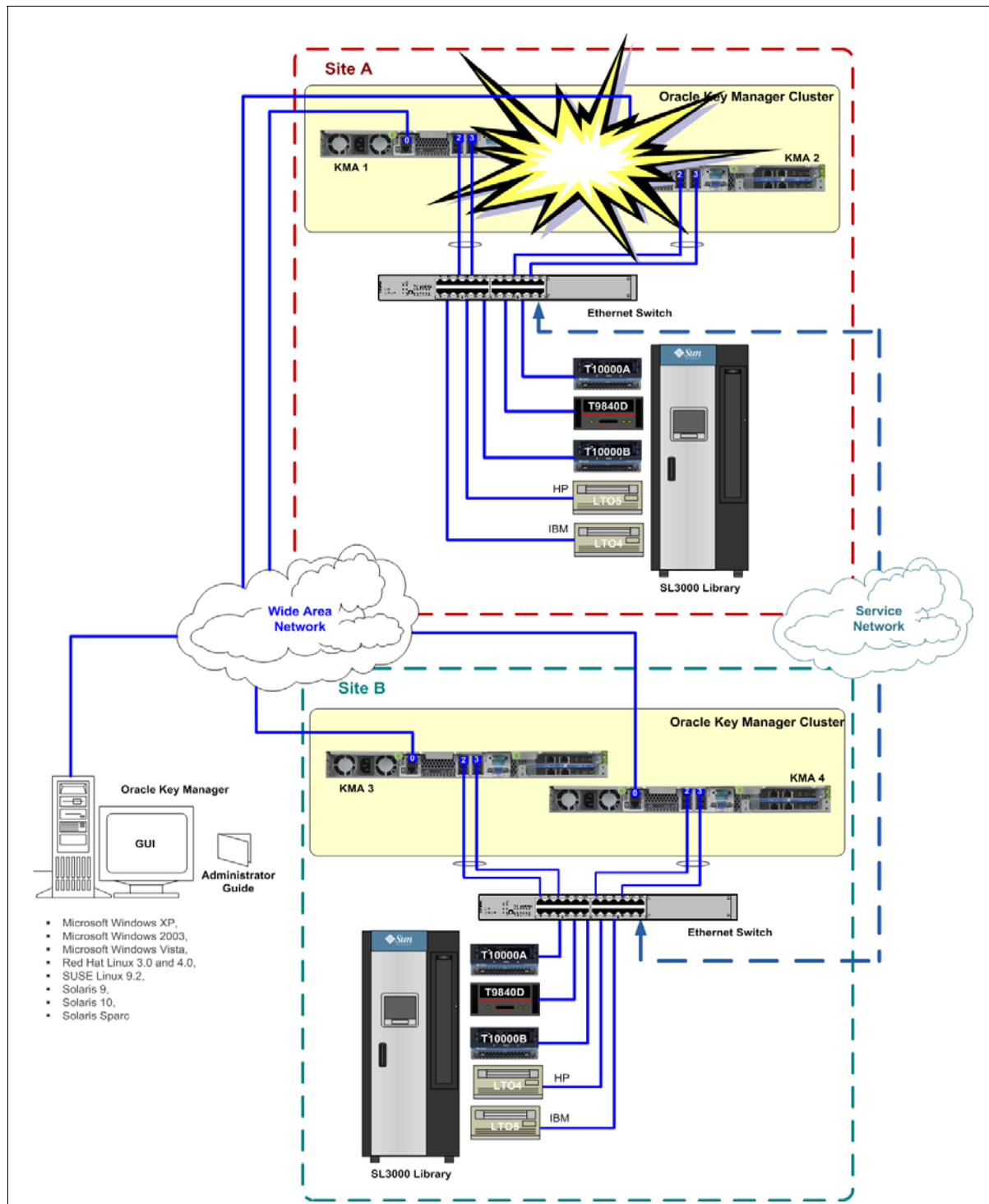
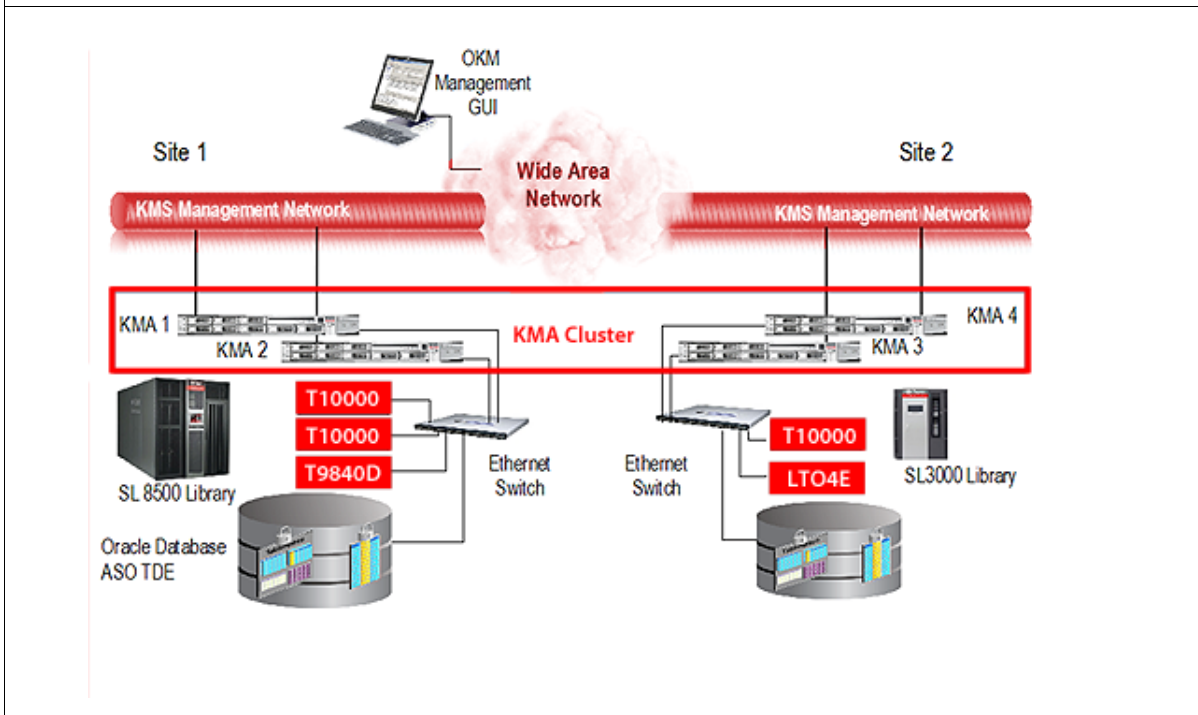


FIGURE 1-5 Database Example

In this example, four KMAs in a cluster are supporting both Automated Tape Libraries and an Oracle database with Advanced Security Transparent Data Encryption (TDE) solution.



Oracle Key Manager is now certified with Oracle Advanced Security Transparent Data Encryption. This means that the same encryption technology used in Oracle StorageTek tape drives is now available for managing encryption keys for Oracle 11g databases.

See [Appendix B, "Encryption for Oracle Databases"](#) for more information.

Key Management Appliance

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

- SunFire X2100 servers (original)
- SunFire X2200 servers (upgrade)
- SunFire X4170 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 1-6 shows a rear view of the Sun Fire X4170 M2 server.

FIGURE 1-7 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 1-6 Key Management Appliance—X4170 Rear Panel

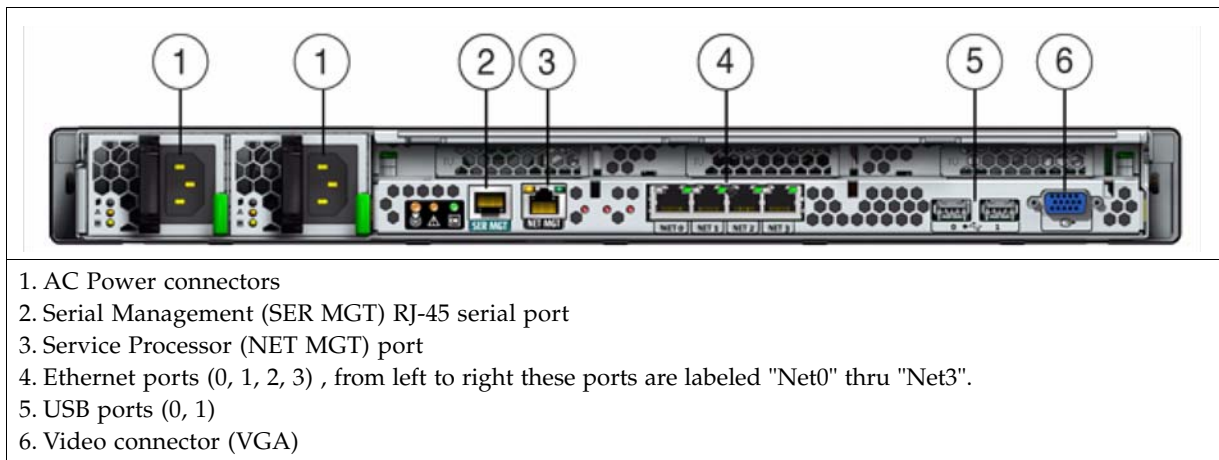
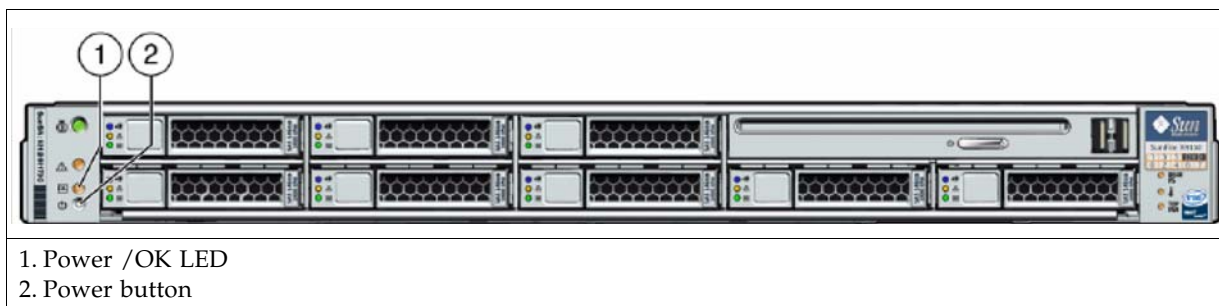


FIGURE 1-7 Key Management Appliance—X4170 Front Panel



4170 Component Specifications

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

TABLE 1-1 Specifications

Specification	
Processor	One quad-core (2.4-GHz)
Memory	1x4GB DDR3 DIMMs
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 X2100 and X2200 Servers

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

FIGURE 1-9 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 1-8 Key Management Appliance—2100/2200 Front Panel

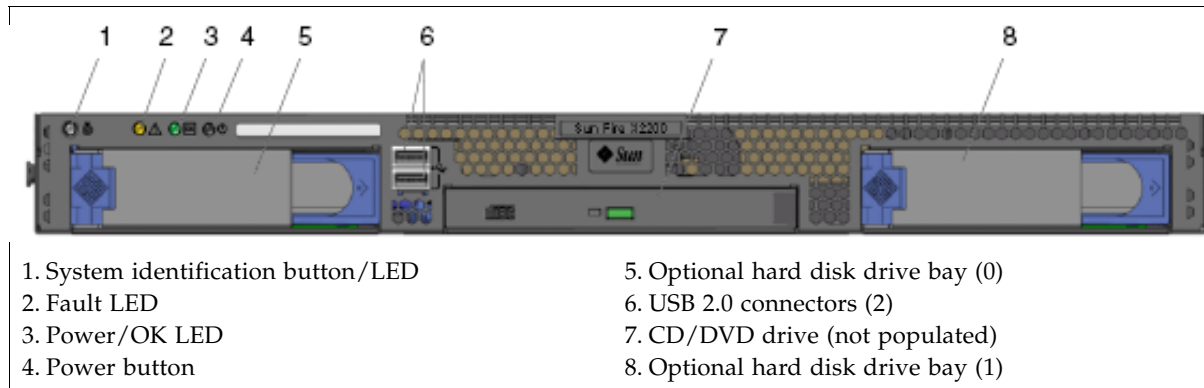
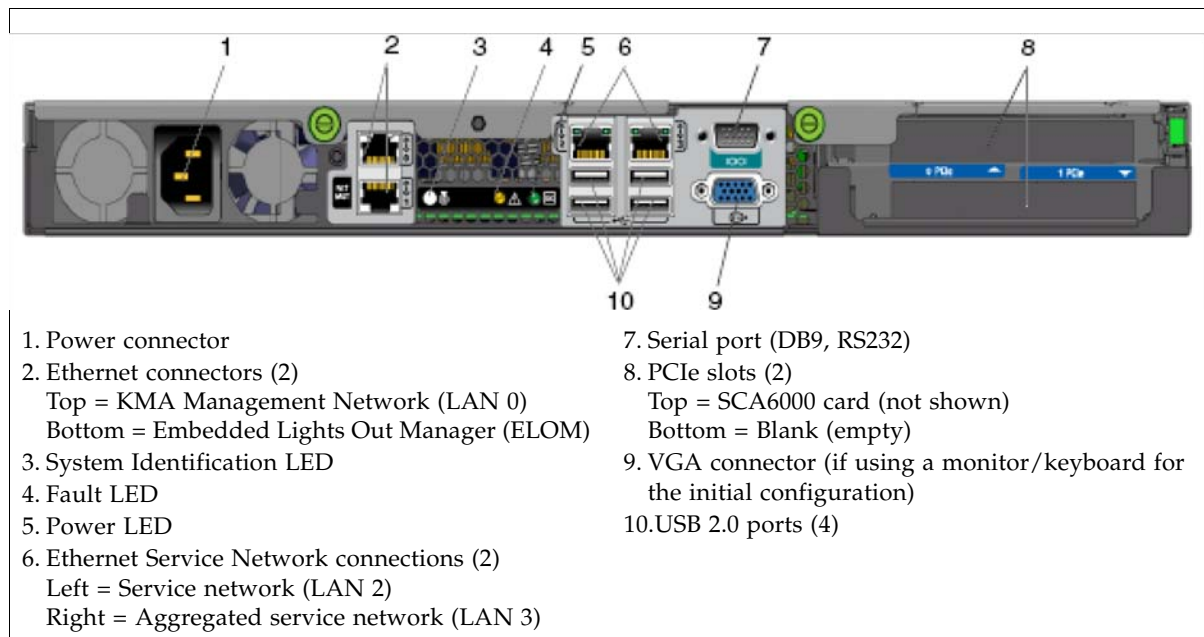


FIGURE 1-9 Key Management Appliance—2100/2200 Rear Panel



SunFire X2100 Server

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

TABLE 1-2 SunFire X2100 Specifications

Specification	
Processor	<ul style="list-style-type: none"> ■ One dual-core AMD Operton processor ■ Processor frequencies: 2.2 GHz ■ Up to 1 MB level 2 cache
Memory	<ul style="list-style-type: none"> ■ Four DIMM slots (up to 4 gigabytes) ■ Unbuffered ECC memory
IPMI 2.0	<ul style="list-style-type: none"> ■ Service processor standard ■ embedded Lights Out Manager
Mass storage	One SATA disk drive
PCI Slots	Two PCI-Express slots (PCIe) PCIe-0 contains the Sun Crypto Accelerator 6000 (SCA6000)
Networking	<ul style="list-style-type: none"> ■ Four USB 2.0 connectors on the rear panel ■ Two USB 2.0 connectors on the front panel ■ Two ports: Serial port with DB-9; VGA with DB-15 ■ 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 One 6.5 Amp non-redundant power supply at 345 Watts 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: 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	<ul style="list-style-type: none"> ■ Two Quad core AMD Opteron processors ■ Processor frequencies: 2.3Ghz
Memory	<ul style="list-style-type: none"> ■ 8 GB of RAM, installed as 4, 2 GB Dimms
IPMI 2.0	<ul style="list-style-type: none"> ■ Service processor standard ■ embedded Lights Out Manager
Mass storage	One SATA disk drive 250 GB capacity
PCI Slots	Two PCI-Express slots (PCIe) PCIe-0 contains the Sun Crypto Accelerator 6000 (SCA6000)
Networking	<ul style="list-style-type: none"> ■ Four USB 2.0 connectors on the rear panel ■ Two USB 2.0 connectors on the front panel ■ Two ports: Serial port with DB-9; VGA with DB-15 ■ 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 One 8 Amps non-redundant power supply at 500 Watts 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 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 aggregation of the KMA service network interfaces to minimize single point of failure on the KMA's service interface.

[FIGURE 1-10 on page 15](#) 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.

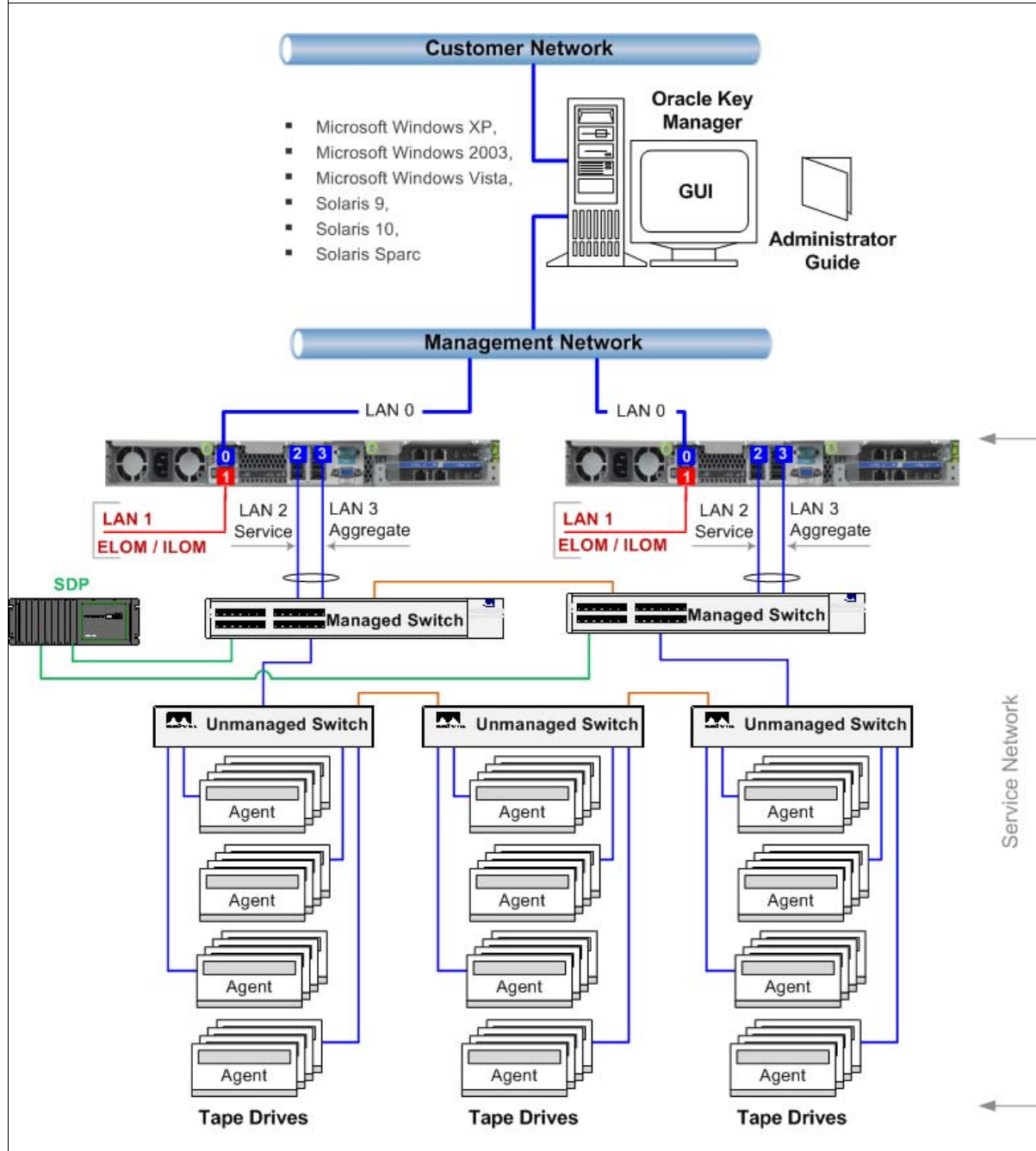
Make sure the Ethernet switch ports have the correct configuration. For example, switch ports should be:

- 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 1-10 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) for the 4170M2 appliance
- 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

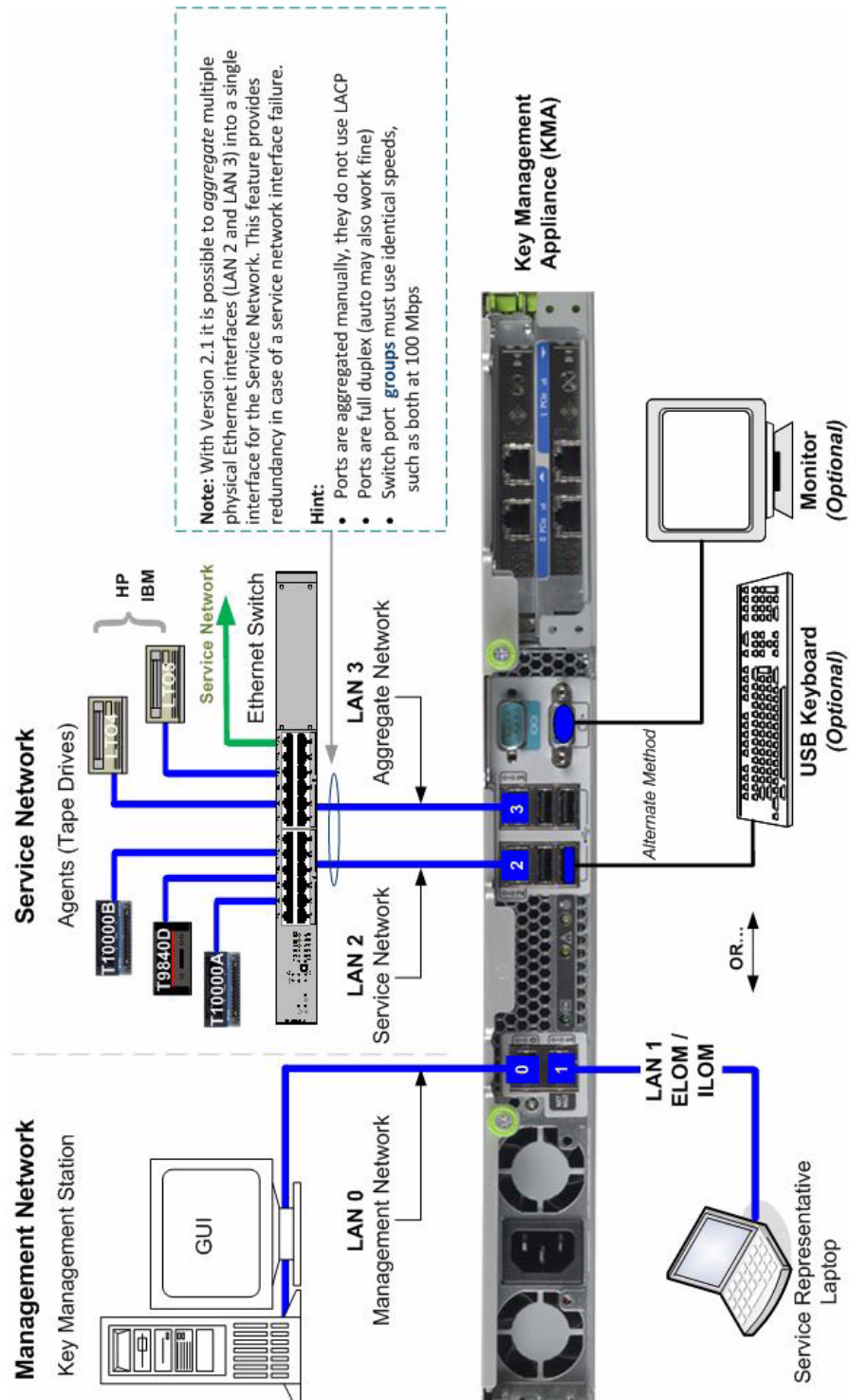
LAN 0	<p>This is a <i>required</i> connection.</p> <p>This network is called the “Management Network” and interconnects with the Key Management Appliances and management clients hosting the GUI or CLI. This network can be local, remote, or a combination of both.</p> <p>Note – Customers are expected to provide this network and connection.</p>
LAN 1*	<p>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.</p>
LAN 2	<p>This is normally a <i>required</i> connection for the tape drives.</p> <p>This network is called the “Service Network” and connects to the tape drives, either directly or through Ethernet switches to create the network.</p>
LAN 3	<p>This is an <i>optional</i> 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.</p> <p>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.</p>
<p>*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.</p>	

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. The following figure shows a Sun Fire X2100 or X2200 server.

FIGURE 1-11 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 T10000C
- 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 FIPS³ compliant.

TABLE 1-6 FIPS 140-2 Compliant Tape Drives

Tape Drive	FIPS 140-2 Level
T10000A	1
T10000B	2
T10000C	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 three models of the T10000 that support encryption:

- T10000A
- T10000B
- T10000C

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 data⁴
- T10000C = 5 terabyte (TB) of uncompressed data

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 (1,024²) megabytes = 1 terabyte

About the LTO Tape Drives

Overview	<p>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.</p> <p>Both HP and IBM offer a fourth- and fifth-generation, Ultrium series of linear tape-open products called the LTO4 and LTO5 tape drives.</p> <p><i>Note:</i> Currently, only the LTO4 and LTO5 tape drives are capable of supporting tape- or device-based encryption.</p>
Encryption Capable	<p>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.</p> <p>Key management is essential to ensure that what is written on tape can be read in the future.</p> <p>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:</p> <ul style="list-style-type: none"> ■ HP LTO4 = Dione card (external) ■ HP LTO5 = Embedded (no adapter card required) ■ IBM = Belisarius card (external) <p>With this connection, the LTO drives are capable of communicating with the OKM to transfer encryption keys over the secure network.</p> <p><i>Note:</i> Currently the LTO drives can only use <i>one encryption key at a time</i>. During a read operation, if another encryption key is found on the tape, the adapter card requests the key directly from the OKM.</p>
Media (Native capacity)	<p>LTO5 tape drives use a 1.5 TB Data Cartridge and LTO4 tape drives use an 800 GB Data Cartridge, both are compatible with other vendor cartridges and other generations of LTO tape drives.</p> <p>The drive performs the following functions:</p> <ul style="list-style-type: none"> ■ Reads/Writes LTO5 cartridges in Ultrium 5 format, including WORM ■ Reads/Writes LTO4 cartridges in Ultrium 4 format, including WORM <p>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.</p>
Interfaces	<p>LTO drives come with a Fibre Channel interface (FC), in either a single or dual port configuration.</p> <p>The HP LTO tape drives also supports:</p> <ul style="list-style-type: none"> ■ Ultra 320 Small Computer System Interface (SCSI)

Tape Drive Comparisons

TABLE 1-7 Tape Drive Comparison

	StorageTek				HP		IBM	
Specification	T10K A	T10K B	T10K C	T9840D	LTO4	LTO5	LTO4	LTO5
Capacity (native)	500 GB	1 TB	5 TB	75 GB	800 GB	1.5 TB	800 GB	1.5 TB
Transfer rates (native)	120 MB/s	120 MB/s	240 MB/	30 MB/s	120 MB/s	140 MB/s	120 MB/s	140 MB/s
Buffer size	256 MB	256 MB	2 GB	64 MB	256 MB	256 MB	256 MB	256 MB
Load Time (seconds)	16 sec	16 sec	13.1 sec	8.5 sec	19 sec	12 sec	15 sec	12 sec
Access (seconds)	46 sec	46	73.5	8 sec	72 sec	60 sec	46 sec	60 sec
Tape speed (m/s)	2–4.95	2–3.74	5.62	3.4	7.0	—	7.0	—
Rewind time (seconds)	90	90	10-13	16 / 8	106/54 sec	96/ 78 sec	106/54 sec	96/ 78 sec
Unload Time	23 sec	23 sec	23 sec	12 sec	22 sec	17 sec	22 sec	17 sec
Interfaces								
Fibre Channel	2 & 4 Gb/s	4 Gb/s	4 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	4 Gb/s	2 Gb/s	Not Supported		Not Supported	
ESCON	2 Gb/s	2 Gb/s	no	2 Gb/s				
Compatibility								
Availability (MTBF)	290,000 hrs		290,000 hrs		250,000 hrs		250,000 hrs	
Tracks	768	1152	3,584	576	896	1280	896	1280
Length—usable	855 m (2805 ft)	855 m (2805 ft)	1,107 m (3,632 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 1-8 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 1-8 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 1-9 shows a comparison between:

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

TABLE 1-9 T-Series Tape Drive and Media Support

Tape Drive Types	Media Types	
	Non-encrypted Tapes	Encrypted Tapes
Standard drive (non-encrypted)	<ul style="list-style-type: none"> ■ Fully compatible ■ Read, write, and append 	<ul style="list-style-type: none"> ■ Not capable of reading, writing to or appending to this tape ■ Can re-write from the beginning of tape (BOT)
Encryption-capable drive	<ul style="list-style-type: none"> ■ Read capability only ■ Not capable of appending to this tape ■ Can re-write from the beginning-of-tape (BOT) 	<ul style="list-style-type: none"> ■ Fully compatible ■ Read with correct keys ■ 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 1-10](#) lists the various scenarios and how HP and IBM drives behave.

TABLE 1-10 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 1-10 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.

Auto Service Request (ASR) Feature

Auto Service Request (ASR) is a Phone Home feature of Oracle Premier Support for Systems and Oracle/Sun Limited Warranty that is designed to automatically request Oracle service when specific hardware faults occur.

ASR is designed to resolve problems more quickly by eliminating the need to initiate contact with Oracle services for hardware failures, reducing both the number of phone calls needed and overall phone time required. ASR also simplifies support operations by utilizing electronic diagnostic data. ASR is easy to install and deploy is completely controlled by you to ensure security.

To enable ASR, see Auto Service Request in the Administration Guide for Release 2.4.

Note - You must have Security Officer role access to enable this feature.

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 representatives) 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. Complete the Team Member Contact sheets. Make copies as necessary.	Yes <input type="checkbox"/> No <input type="checkbox"/>
Explain the encryption solutions to the customer. See Chapter 1, “Introduction” for topics and information.	Yes <input type="checkbox"/> No <input type="checkbox"/>
Use Chapter 2, “Systems Assurance” to help define the customer requirements.	Yes <input type="checkbox"/> No <input type="checkbox"/>
Complete the Team Member Contact sheets.	Yes <input type="checkbox"/> No <input type="checkbox"/>
Review and complete Chapter 3, “Site Preparation” . <i>Comments:</i>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Review and identify “User Roles Work Sheet” . <i>Comments:</i>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Review Chapter 4, “Components” . <i>Comments:</i>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Review “Supported Configurations” . <i>Comments:</i>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Determine the installation schedule: Date: _____ Time: _____	Yes <input type="checkbox"/> No <input type="checkbox"/>
Download and provide the customer with a copy of the: <i>Administrator’s Guide</i> PN 316195101. <i>Virtual Operator Panel—Customer</i> PN: 96179 http://download.oracle.com/docs/cd/E24472_01/index.html	Yes <input type="checkbox"/> No <input type="checkbox"/>

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? Notes: <ul style="list-style-type: none"> ■ The maximum number of sites with KMAs is 20. It is possible to have sites without KMAs connected across a customer supplied wide area network. ■ Also, the 20 site limit is within a single cluster. The customer may choose to have multiple clusters; however, KMAs in one clusters are unaware of KMAs in other clusters. 	<input type="checkbox"/> Single site <input type="checkbox"/> Multiple sites <input type="checkbox"/> Disaster recovery site	How many: _____ _____ _____
How many appliances (KMAs) are needed? <ul style="list-style-type: none"> ■ The maximum number of KMAs is 20. ■ The minimum OKM size is 2*. ■ The recommendation is at least 2 (assuming sites are geographically dispersed) <p>* The exception to this standard configuration (single-node site) must be made with the approval of Encryption Engineering, Professional Services, and Support Services.</p>		How many: _____
What type of encryption hardware kits are needed? How many encryption hardware kits are needed?	<input type="checkbox"/> SL8500 <input type="checkbox"/> SL3000 <input type="checkbox"/> SL500 <input type="checkbox"/> 9310 / 9741E <input type="checkbox"/> L-Series <input type="checkbox"/> Rackmount	How many: _____ _____ _____ _____ _____ _____
How many and of what type of encryption-capable tape drives are needed?	<input type="checkbox"/> T10000A <input type="checkbox"/> T10000B <input type="checkbox"/> T10000C <input type="checkbox"/> T9840D <input type="checkbox"/> HP LTO 4 or 5 <input type="checkbox"/> IBM LTO 4 or 5	How many: _____ _____ _____ _____ _____ _____
Are external (standalone) Racks required? Type?	<input type="checkbox"/> Yes <input type="checkbox"/> No	How many: _____
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 <i>no</i> , where will the equipment be delivered? If a delivery dock <i>is</i> available, what are the hours of operation?	Yes <input type="checkbox"/> No <input type="checkbox"/> <hr/>	
Are there street or alley limitations that might hinder delivery?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
Will authorized personnel be available to handle and accept the delivery?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
Is the delivery location close to the computer room where the equipment will be installed?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
Is an elevator available to move the equipment to the appropriate floors?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
Is there a staging area where the equipment can be placed close to the installation site?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
Are there special requirements to dispose of or <i>recycle</i> packing material? Pallets, plastic, and cardboard?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
Environmental Planning		
Does the site meet the environmental requirements for temperature, humidity, and cooling?	Yes <input type="checkbox"/> No <input type="checkbox"/>	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 <input type="checkbox"/> No <input type="checkbox"/>	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 <input type="checkbox"/> No <input type="checkbox"/>	
Does the customer want redundant power options? If so, an additional APC power switch is required to create an uninterrupted power configuration.	Yes <input type="checkbox"/> No <input type="checkbox"/>	Check for updated model and part numbers. (Part number #419951602)
Are there any power cable routing requirements and concerns?	Yes <input type="checkbox"/> No <input type="checkbox"/>	See Power Cables for more information.
Personnel:		
Are there trained/qualified Oracle representatives locally to install and maintain the encryption equipment?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Names:
Connectivity: Cabling is <i>very important</i> to establish a reliable network between the OKM, KMAs, Ethernet switches, and tape drives.		
Does this customer support IPv6 implementations?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
Does the customer intend on using Managed switches for LANs 2 and 3?	Yes <input type="checkbox"/> No <input type="checkbox"/>	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 <input type="checkbox"/> No <input type="checkbox"/>	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 <input type="checkbox"/> No <input type="checkbox"/>	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 <input type="checkbox"/> No <input type="checkbox"/>	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 <input type="checkbox"/> No <input type="checkbox"/>	See SDP on page 48 for information.
Will the customer be monitoring the OKM using SNMP?	Yes <input type="checkbox"/> No <input type="checkbox"/>	SNMP v3 recommended SNMP v2 supported
Are there considerations for monitoring of ELOM/ILOM using the LAN 1 port?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Refer to the SunFire X2100/2200 ELOM Administration Guide, or X4170 ILOM Supplement Guides for information.
Have you and the customer completed a: <ul style="list-style-type: none"> ■ Cable plan? ■ Do the agents have private network? ■ Configuration drawing? A drawing can help determine the number of and length of the cables required. 	Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/>	
Have you determined the type and number of Ethernet cables required? <i>Customer supplied:</i> <ul style="list-style-type: none"> ■ OKM to the network ■ Encryption Network to the KMAs (LAN 0) ■ ELOM/ILOM monitoring (LAN 1) ■ Service network to agents (LAN 2 & 3) <i>Supplied in the encryption kits:</i> <ul style="list-style-type: none"> ■ Switch to tape drives 	Yes <input type="checkbox"/> No <input type="checkbox"/>	Note: <ul style="list-style-type: none"> ■ Ethernet cables are shipped with kits. ■ Lengths are dependant on the location of the switches and devices. 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 <input type="checkbox"/> No <input type="checkbox"/>	See “Rack Specifications” on page 42
What type of support configurations does the customer want or need? <input type="checkbox"/> Existing configuration <input type="checkbox"/> New configuration	<u>Configuration</u> <input type="checkbox"/> SL8500 <input type="checkbox"/> SL3000 <input type="checkbox"/> SL500 <input type="checkbox"/> 9310/9741e <input type="checkbox"/> L-Series <input type="checkbox"/> SL24/48 <input type="checkbox"/> Rackmount	<u>Encryption-capable Drives:</u> T-Series & LTO drives T-Series & LTO drives LTO only T-Series only T-Series only LTO only T-Series only
Does the customer have existing tape drives they want to upgrade to encryption-capable? Are these drives already installed in a library?	Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/>	See Chapter 4, “Components” for x-options (conversion bills).

TABLE 3-1 Site Planning Checklist (Continued)

Question	Completed?	Comments:
Drive types? Check current and required firmware versions.	<input type="checkbox"/> T10000A <input type="checkbox"/> T10000B <input type="checkbox"/> T9840D <input type="checkbox"/> HP LTO4 <input type="checkbox"/> IBM LTO4 <input type="checkbox"/> HP LTO5 <input type="checkbox"/> IBM LTO5	Requires drive tray and Dione card Requires drive tray and Belisarius card Requires drive tray and Belisarius card
Configurations (continued)		
Does the customer need to order more drives? ■ Tape drive type: ■ Interface types? ■ (FC) Fibre Channel (all tape drives) ■ (FI) FICON (T-Series only) ■ (ES) ESCON (T9840D) ■ SCSI (SL500 library and LTO drive only)	Yes <input type="checkbox"/> No <input type="checkbox"/> <input type="checkbox"/> T10000A <input type="checkbox"/> T10000B <input type="checkbox"/> T9840D <input type="checkbox"/> HP LTO4 <input type="checkbox"/> IBM LTO4 <input type="checkbox"/> HP LTO5 <input type="checkbox"/> IBM LTO5	How many tape drives?
Are additional cartridges required? ■ Data cartridge ■ Cleaning cartridges ■ VolSafe cartridges ■ Labels ■ Type: _____ ■ Quantity: _____	Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/>	Note: All versions of encryption tape drives use different, unique cartridges. ■ T9840 = 9840 cartridges ■ T10000 = T10000 cartridges ■ LTO4 = LTO4 cartridges. ■ LTO5 = LTO5 cartridges. All versions of each cartridge-type are supported, for example: standard, sport, VolSafe, and WORM.
Is the customer interested in the Auto Service Request (ASR) or "Phone home" feature when specific hardware faults occur?	Yes <input type="checkbox"/> No <input type="checkbox"/>	See "Auto Service Request (ASR) Feature" on page 27 and the Administration Guide for more information.
Notes:		
Configurations:		
Tape Drives and Media:		

Rack Specifications

The KMAs can be installed in standard, RETMA¹ 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 Us², 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. 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.). Recommended safe length is 66 cm (26 in.).
Equipment weight	The accessory rack itself is mounted on slides rated for 80 kg (175 lb). The recommended safe load is 64 kg (140 lb). 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. 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. Minimum cord length is component <i>plus</i> 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 aggregation 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

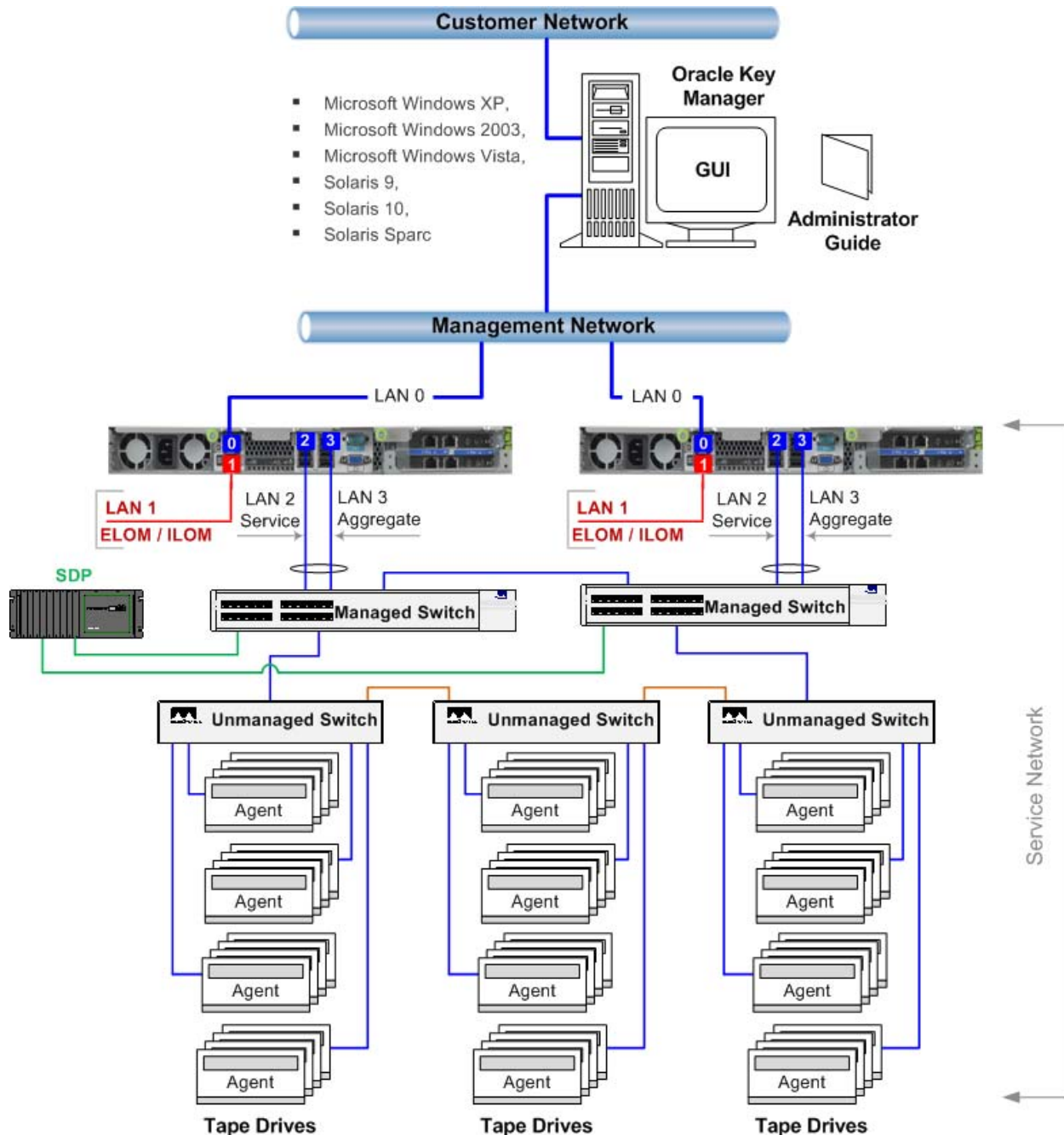
1. Use a Web browser to connect to the switch IP.
2. Select port and then link aggregation from the menu.

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 capability 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.

[FIGURE 3-1](#) 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.

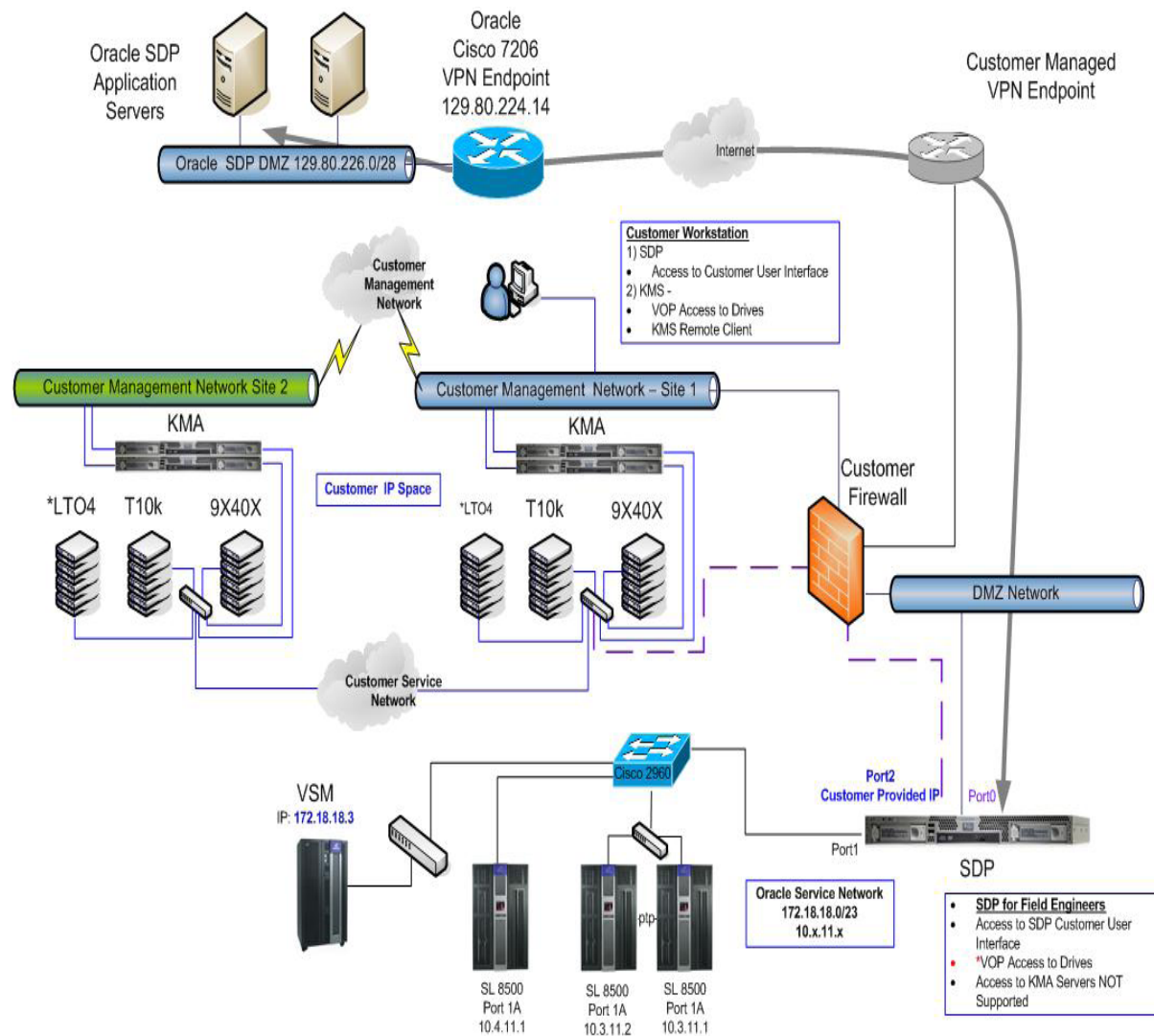
This firewall effectively partitions the service network in two: the Oracle controlled service network and the customer controlled service network. The *Service Delivery Platform Security White Paper*, May 2008 describes this network as the "Service Network interface". The Oracle Service Network interface 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 ■ 10 library complex: up to 640 drives	■ 1 to 56 tape drives	■ 1 to 18 tape drives
Encryption Drives Supported	■ T10000 A and B ■ T9840D ■ LTO 4 and 5	■ T10000 A and B ■ T9840D ■ LTO 4 and 5	■ LTO 4 and 5 only (HP, IBM)
Non-encryption Drives Supported	■ T10000 A&B ■ T9840 A, B, & C ■ LTO 3, 4, 5	■ T10000 A&B ■ T9840 C ■ LTO 3 4, 5	■ LTO 2, 3, 4, 5 (HP, IBM) ■ SDLT 600 ■ DLT-S4
Interfaces:	Note: The library interface and tape drive interfaces may be different.		
■ Libraries	■ TCP/IP only	■ TCP/IP ■ Fibre Channel	■ TCP/IP ■ Fibre Channel
■ Tape Drives	T10000 A&B FC and FICON T9840D FC, FICON, ESCON LTO 4 & 5 FC only	T10000 A&B FC and FICON T9840D FC, FICON, ESCON LTO 4 & 5 FC only	LTO4, 5Fibre Channel LTO4 SCSI (check availability)
Media*	All libraries support true-mixed media—Any Cartridge, Any Slot™		
	■ T10000 (Std, Sport, VolSafe) ■ 9840 (Std and VolSafe) ■ LTO 2, 3, 4, 5 & T-WORM ■ DLTtape III ■ Super DLTtape I & II	■ T10000 (Std, Sport, VolSafe) ■ 9840 (Std and VolSafe) ■ LTO 2, 3, 4, 5 & T-WORM	■ LTO 1, 2, 3, 4, 5 & T-WORM ■ DLTtape III ■ 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 ■ HSC	■ ACSLS ■ HSC ■ ISV	■ ACSLS ■ ISV
FC = Fibre Channel FICON = IBMs fiber connection SNMP = Simple Network Management Protocol SDP = Service Delivery Platform		ACSLs = Automated Cartridge System Library Software HSC = Host Software Component 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 planning 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

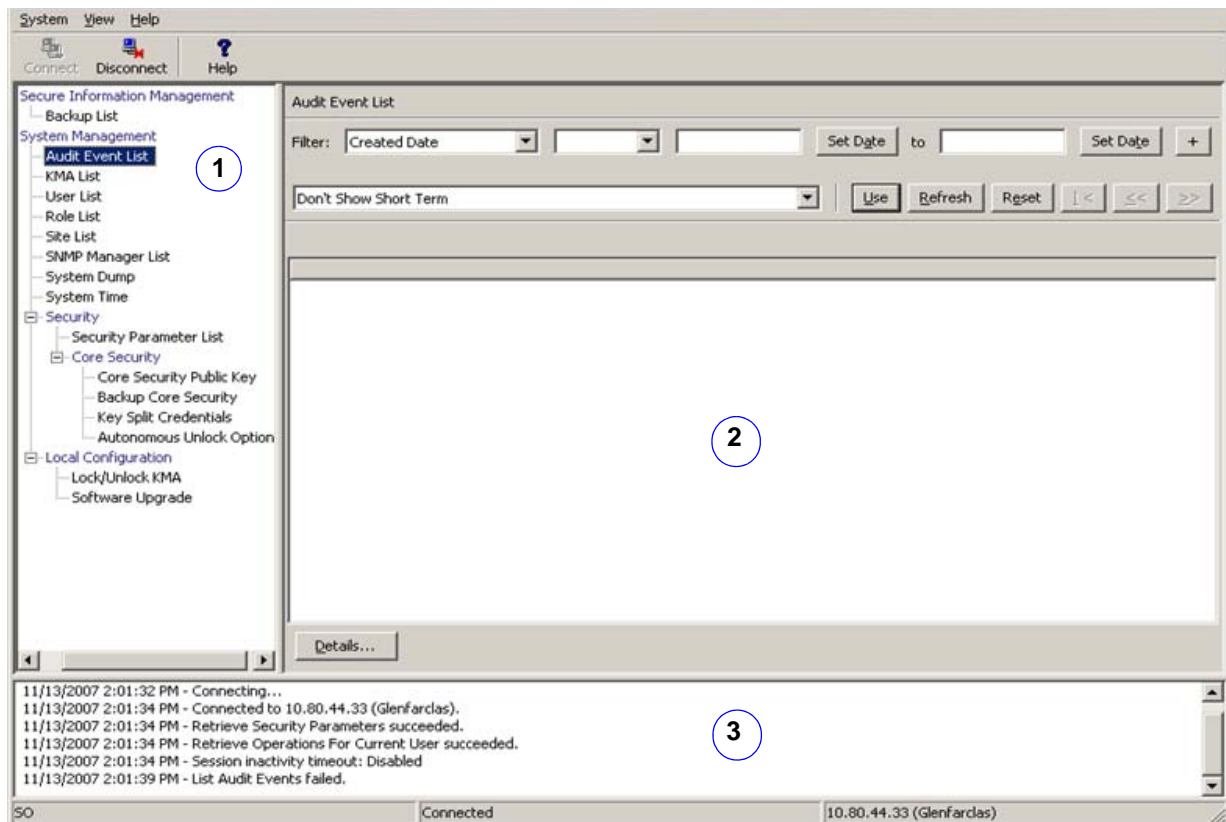
✓	Item	Task	Responsibility*
<input type="checkbox"/>	1. Team	Create a Team. When planning for content, data and partitions, use a process similar to that of the system assurance process; which is the exchange of information among team members to ensure all aspects of the implementation are planned carefully and performed efficiently. Team members should include representatives from both the customer.	<ul style="list-style-type: none"> ■ Customer ■ Administrators ■ Operators ■ SE, PS ■ Svc Rep
<input type="checkbox"/>	2. Codes	Review the software and firmware requirements. Update as required.	<ul style="list-style-type: none"> ■ Customer ■ SE, PS ■ Svc Rep
<input type="checkbox"/>	3. Planning	<ul style="list-style-type: none"> ■ Define the customer expectations ■ Complete the assessment ■ Identify the configurations ■ Complete the planning diagrams (include network planning) ■ Service Delivery Platform (SDP) 	<ul style="list-style-type: none"> ■ Customer ■ Administrators ■ SE, PS ■ Svc Rep
<input type="checkbox"/>	4. Encryption	<ul style="list-style-type: none"> ■ Complete an encryption survey (PS) ■ Select the type of tape drive, interface, and library configuration ■ Select location ■ Ensure there is adequate media 	<ul style="list-style-type: none"> ■ Customer ■ SE, PS ■ Svc Rep
<input type="checkbox"/>	5. Disaster Recovery	<ul style="list-style-type: none"> ■ Develop a business continuity and disaster recovery plan ■ Select a backup site ■ Determine network configurations (LAN, WAN, aggregation) 	<ul style="list-style-type: none"> ■ Customer ■ SE, PS ■ Svc Rep
<input type="checkbox"/>	6. Media	<ul style="list-style-type: none"> ■ Verify the distribution of cartridges and required tape drives are available and ready. 	<ul style="list-style-type: none"> ■ Customer ■ Operators
<input type="checkbox"/>	7. Library	<ul style="list-style-type: none"> ■ Install and configure a library (if necessary). 	<ul style="list-style-type: none"> ■ Svc Rep
<input type="checkbox"/>	8. Activation	<ul style="list-style-type: none"> ■ Activate the required features: <ul style="list-style-type: none"> ■ Library ■ Tape drives 	<ul style="list-style-type: none"> ■ Customer ■ Administrators ■ Svc Rep
<input type="checkbox"/>	9. Partitions	<ul style="list-style-type: none"> ■ Create partitions. 	<ul style="list-style-type: none"> ■ Customer ■ Administrators ■ Operators
<input type="checkbox"/>	10. Hosts	<ul style="list-style-type: none"> ■ Momentarily stop all host activity if currently connected. 	<ul style="list-style-type: none"> ■ Customer
<input type="checkbox"/>	11. Use	Instruct the customer how to: <ul style="list-style-type: none"> ■ Use and manage the library ■ Use the OKM GUI 	<ul style="list-style-type: none"> ■ Customer ■ SE, PS ■ Svc Rep
<input type="checkbox"/>	12. Reference	Make sure the customer has access to the appropriate documents.	<ul style="list-style-type: none"> ■ Customer ■ SE, PS ■ Svc Rep
<ul style="list-style-type: none"> ■ SE = Systems engineer ■ PS = Professional services representative ■ Service = Customer services representative (Svc Rep) ■ 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 56).

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 <i>key policies</i> and <i>key groups</i> . 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 61 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 57 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					

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

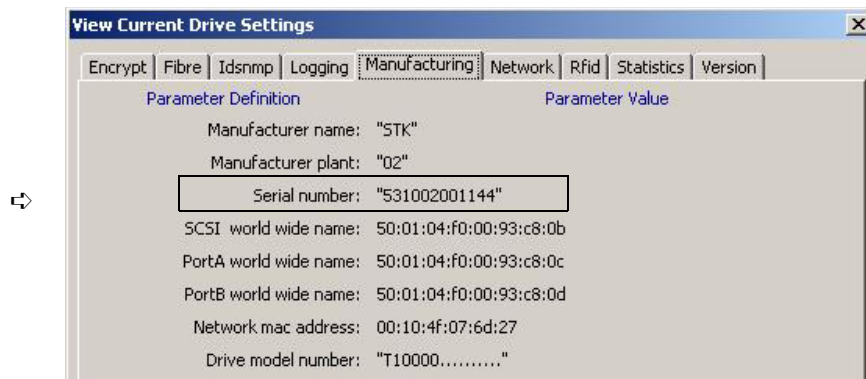
The tape drives should be installed and tested in their appropriate configuration before adding the encryption capability to them. Each drive-type has its own requirements.

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 [Work Sheets](#) 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

The screenshot shows the Sun Microsystems 'Encryption Request' form. It includes a header with the Sun logo and a navigation bar with 'Logout' and 'Home' links. The form itself is titled 'Enter the following information' and contains several input fields: First Name, Last Name, SunID, Email Address, Site Id, Case/WorkOrder #, Driver Family (a dropdown menu currently showing 'T9840D'), Serial Number, and Optional Remarks. At the bottom of the form are two buttons: 'Request Key File' and 'Reset'.

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.

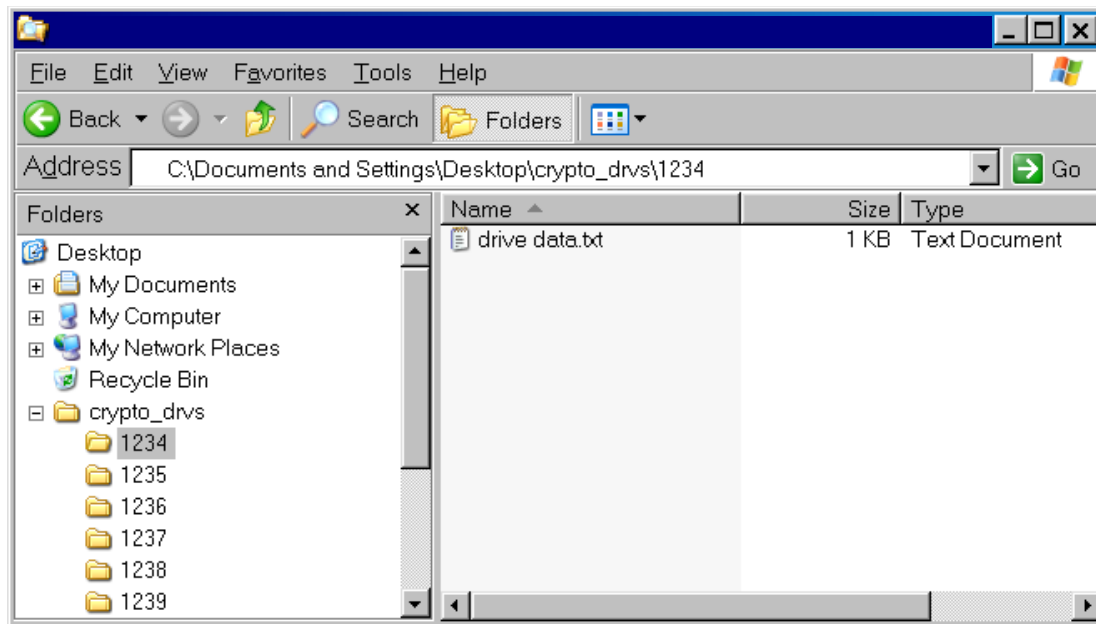
5. Continue with this process until you obtain all the drive data files for each tape drive you are going to enable.

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 [Work Sheets](#) 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:

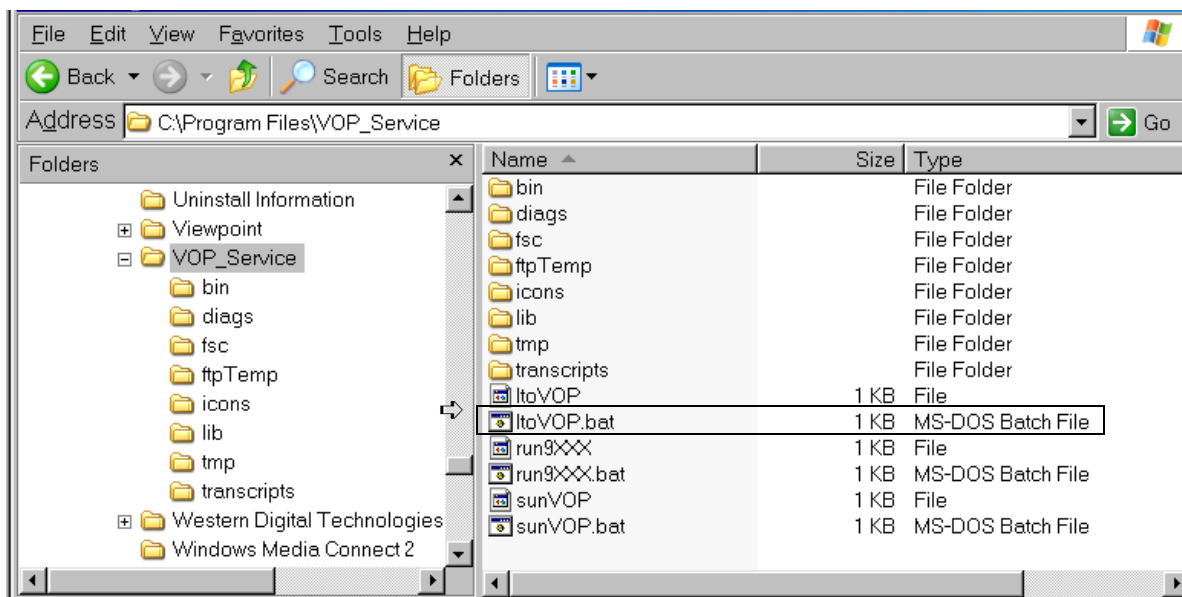
- Version 1.0.12 and higher to provide support for the HP LTO tape drives.
- Version 1.0.14 and higher to provide support for the IBM LTO tape drives.

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
<ul style="list-style-type: none"> ■ Microsoft Windows XP ■ Microsoft Windows 2003 ■ Microsoft Windows Vista ■ Windows 7 and 2008 server 	<ul style="list-style-type: none"> ■ Internet Explorer 6.0 and later ■ Mozilla 1.7.5 or later ■ Mozilla Firefox 1.0 	JRE 1.5 (Java 5.0 Update 7 or later)
<ul style="list-style-type: none"> ■ Red Hat Linux 3.0 and 4.0 	<ul style="list-style-type: none"> ■ Mozilla 1.7.5 or later ■ Mozilla Firefox 1.0 	JRE 1.5 (Java 5.0 Update 7 or later)
<ul style="list-style-type: none"> ■ Solaris 9 ■ Solaris 10 ■ Solaris Sparc ■ SUSE Linux 9.2 	<ul style="list-style-type: none"> ■ Mozilla 1.7.5 	JRE 1.5 (Java 5.0 Update 7 or later)
<p>You can download the Java 1.5 runtime environment at: http://java.com</p> <p>The current version of the ELOM guide is located at: http://dlc.sun.com/</p>		

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

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 *required* 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, T10000B and/or T10000C
- T9840D
- HP LTO4 and/or LTO5
- IBM LTO4 and/or LTO5

See [“Firmware Levels”](#) for the supported tape drive firmware versions.

Supported Databases

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

- Interfaces with Transparent Data Encryption (TDE) suite in Oracle Database 11gR2
- Oracle Database products
- Oracle Real Application Clusters (Oracle RAC)
- Oracle Data Guard
- Oracle Exadata Database Machine
- Oracle Recovery Manager (RMAN)
- Oracle Data Pump

All editions are built using the same common code base, which means your database applications can easily scale from small, single-processor servers to clusters of multi-processor servers.

Compare the following features:

TABLE 4-1 Database Selections

Key Feature Summary	Standard Edition One	Standard Edition	Enterprise Edition
Maximum (Sockets)	2	4	No Limit
RAM	OS Max.	OS Max.	OS Max.
Database size	No Limit	No Limit	No Limit
Windows	Yes	Yes	Yes
Linux	Yes	Yes	Yes
Unix	Yes	Yes	Yes
64-bit Support	Yes	Yes	Yes

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](#) or [597-1095-01](#)
- If an SCA6000 card is required; order: [375-3424-06](#)
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

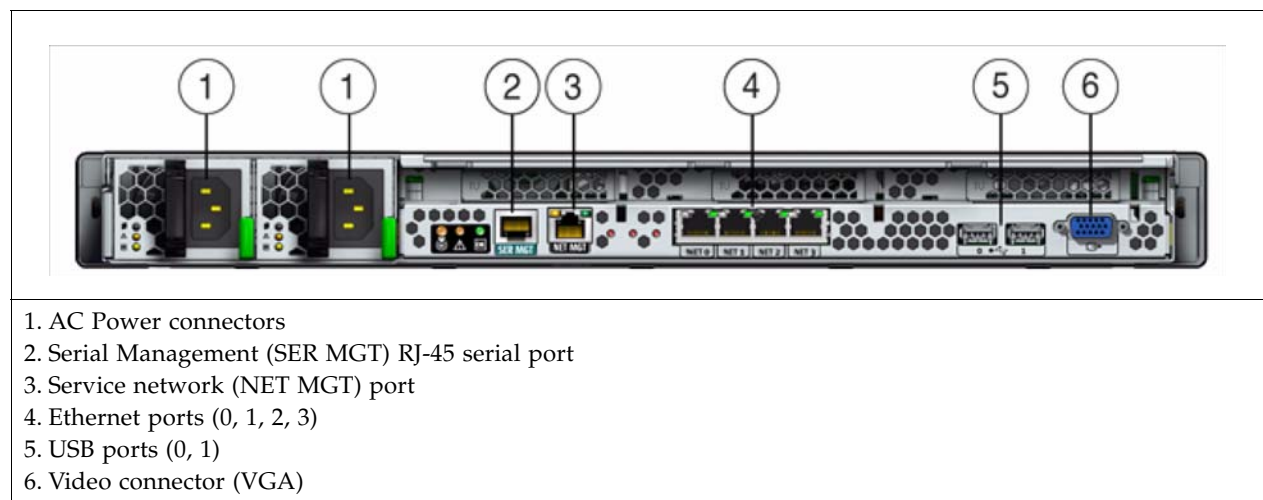
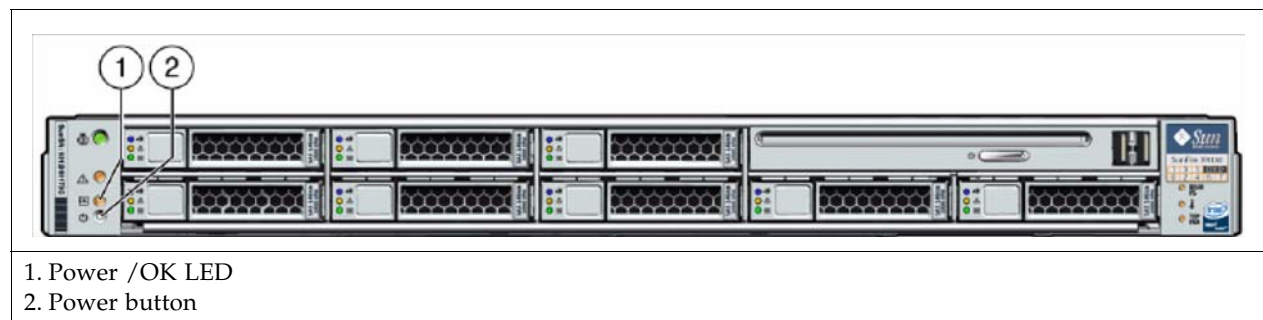


FIGURE 4-2 Key Management Appliance—4170 Front Panel



Note — [CRYPTO-1XTO23UP](#) is an upgrade kit of KMA 1.x to version 2.3.

Current version is 2.4.

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: <ul style="list-style-type: none"> ■ T10000A ■ T10000B ■ T10000C ■ T9840D ■ HP LTO4 ■ HP LTO5 ■ IBM LTO4 ■ IBM LTO5 	1.34.208 or higher 1.38.x07 or higher Check for current levels 1.42.104 or higher H58S Fibre Channel I2DS Fibre Channel 94D7 Fibre Channel 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

- SL3000 Kit 1 XSL3000-ETHRNT1-N
- SL3000 Kit 2 XSL3000-ETHRNT2-N
- SL3000 Kit 3 XSL3000-ETHRNT3-N
- SL3000 Kit 4 XSL3000-ETHRNT4-N

Description

The SL3000 uses four different part numbers for Ethernet switches and cables to 1 to 56 tape drives.

Note:

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: <ul style="list-style-type: none"> ■ T10000A ■ T10000B ■ T10000C ■ T9840D ■ HP LTO4 ■ HP LTO5 ■ IBM LTO4 ■ IBM LTO5 	1.34.208 or higher 1.38.x07 or higher Check for current levels 1.42.104 or higher H58S Fibre Channel I2DS Fibre Channel 94D7 Fibre Channel A232 Fibre Channel
Virtual Operator Panel (VOP)	Version 1.0.14 or higher 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 (<i>required</i>) 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 (<i>optional</i>) 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: ■ HP LTO4 ■ HP LTO5 ■ IBM LTO4 ■ IBM LTO5	H58S Fibre Channel (SCSI: B57S) I2DS Fibre Channel 94D7 Fibre Channel A232 Fibre Channel
Virtual Operator Panel (VOP)	Version 1.0.14 or higher for LTO4 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 ■ T10000C ■ T9840D	1.34.208 or higher 1.38.x07 or higher Check for current levels 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) ■ L700e / L1400	3.11.02 or higher
Tape Drives: ■ T10000A ■ T10000B ■ T10000C ■ T9840D	1.34.208 or higher 1.38.x07 or higher Check for current levles 1.42.104 or higher
Virtual Operator Panel (VOP)	Version 1.0.14 or higher 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) ■ SL24 autoloader ■ SL48 library	D.90/3.00e G.20/3.00e
Encryption-capable Tape Drives: ■ HP LTO5 ■ IBM LTO5	I2DS A232
Virtual Operator Panel (VOP)	Version 1.0.16 for the LTO5 tape drives 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: <ul style="list-style-type: none"> ■ T10000A ■ T10000B ■ T10000C ■ T9840D 	1.34.208 or higher 1.38.x07 or higher Check for current levels 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 4-2 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 4-3 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, CNSI0917,10A,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, CNSI0917,15A,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 4-4 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.

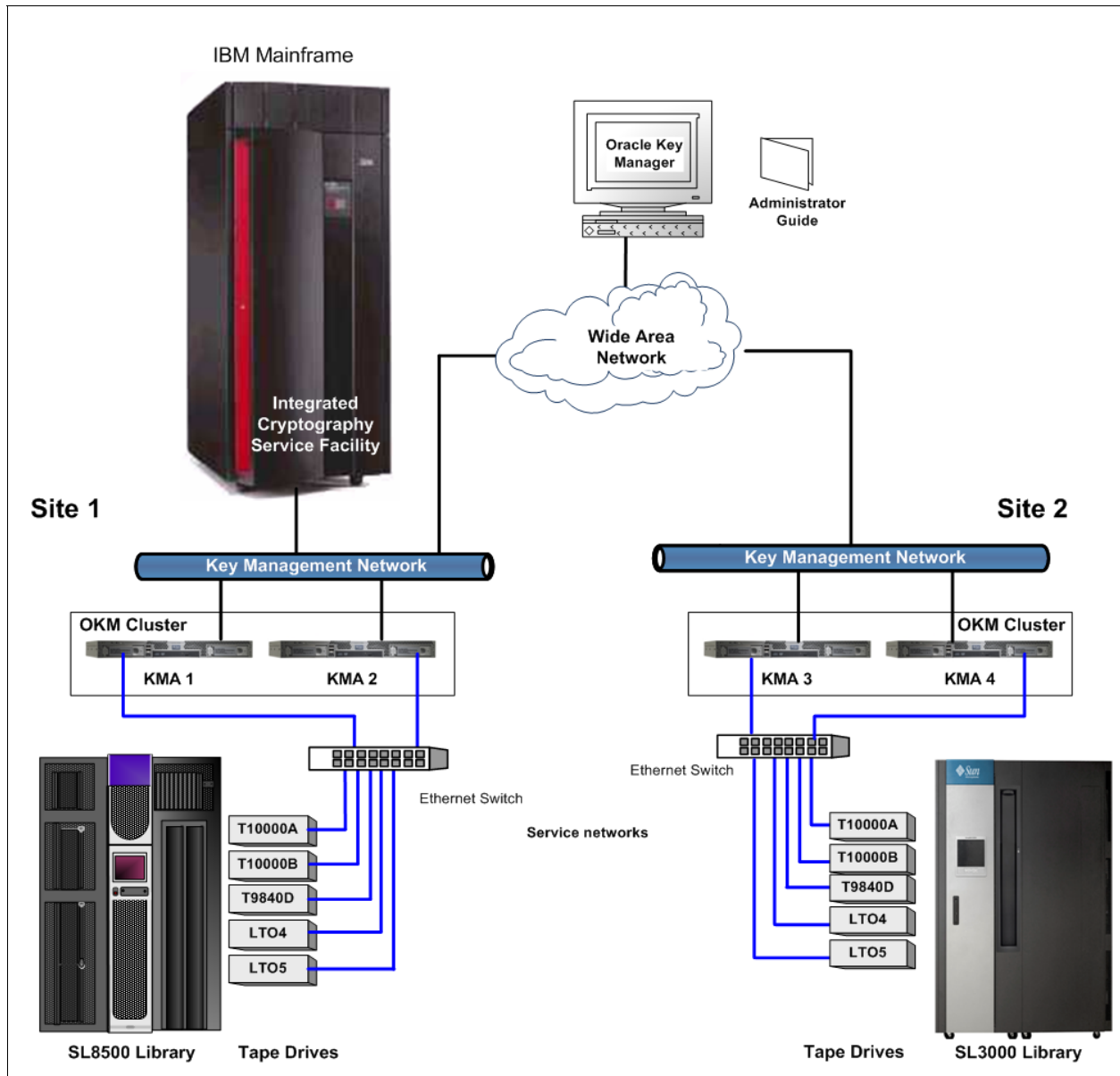
1. ICSF is a software component of z/OS providing cryptographic support either in its own software routines or through access to external cryptographic hardware, such as the Oracle Key Manager.

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.

Encryption for Oracle Databases

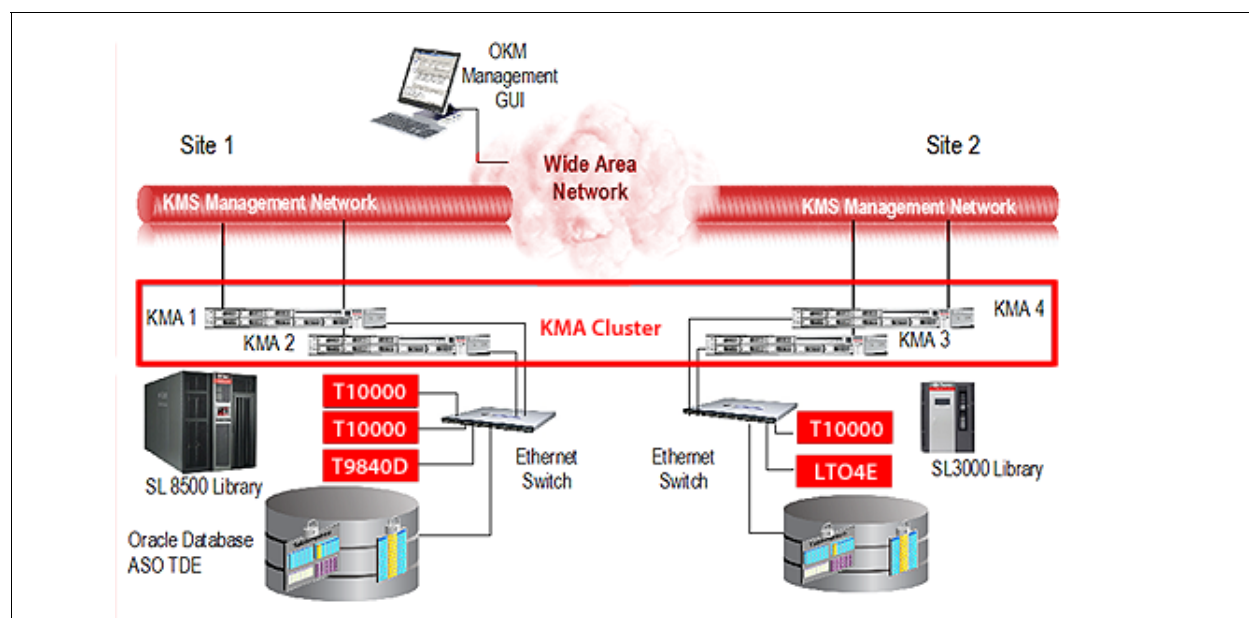
Note – For more information, refer to the two white papers: 1) “Using Oracle Key Manager with Advanced Security Transparent Data Encryption” and 2) “Oracle’s Advanced Security Transparent Data Encryption Best Practices” and the “OKM Administrator’s Guide”.

Transparent Data Encryption (TDE) with an Oracle Key Manager is an optimal, one-stop, Oracle solution for reliable management of Oracle **Database** master keys.

Oracle Key Manager (OKM) is now certified with Oracle Advanced Security Transparent Data Encryption. This means that the same encryption technology used with Oracle StorageTek tape drives is now available for managing encryption keys for an Oracle Database 11gR2, including:

- Oracle Database products
- Oracle Real Application Clusters (Oracle RAC)
- Oracle Data Guard
- Oracle Exadata Database Machine
- Oracle Recovery Manager (RMAN)
- Oracle Data Pump

FIGURE B-1 Oracle Key Manager and Oracle Database Example



Transparent Data Encryption Overview

Transparent Data Encryption (TDE) provides the services used for encrypting and decrypting sensitive database information, either at the column level or the tablespace level. The Oracle Key Manager and Transparent Data Encryption solution provides enterprise-class key management for the Transparent Data Encryption universal master keys. This solution allows the keys to be managed outside of the database.

Policy-based key management using Oracle Key Manager (OKM) provides a robust and flexible solution for managing Transparent Data Encryption master keys.

Transparent Data Encryption (TDE) provides encryption services using a two-tiered key approach for both TDE column and tablespace encryption.

- The first tier is a master encryption key is used to encrypt.
- The second tier table or tablespace data encryption keys are stored within the database.

TDE stores the master encryption key in an external security module (Oracle Wallet or HSM). Storing the master key in an HSM is a **recommended security practice** and is crucial to maintaining the highest level of security from various threats. Use of the Oracle Key Manager for the secure storage of the TDE master encryption keys is recommended. Lost keys mean lost data, so a key management system such as Oracle Key Manager (OKM), is highly recommended.

With TDE configured to use an OKM, the master encryption key is created by the OKM and safely protected. OKM protects keys through replication (multiple copies across the cluster) and through backups of the Oracle Key Manager itself.

PKCS#11 Providers

Public-Key cryptography standards (PKCS) define a platform-independent standard. A PKCS#11 provider is available for Oracle Solaris and Oracle Linux and has been certified to interface TDE with Oracle Key Manager. This provider is called "pkcs11_kms." TDE can be configured to utilize the pkcs11_kms provider through its built-in support for Hardware Security Modules (HSMs).

The Oracle Solaris pkcs11_kms provider is a configurable component of the Solaris Cryptographic Framework and conforms to the standard Oracle Solaris services for administering PKCS#11 providers. For Linux, the pkcs11_kms provider is installed separately and then configured for use with Oracle Database.

The pkcs11_kms provider interacts with Oracle Key Manager for key creation and key retrieval operations. Encryption and decryption functions are performed in the database and *not* by Oracle Key Manager. PKCS#11 consumer applications such as TDE identify key objects using a label that they define. TDE generates this label during creation of a master key. The pkcs11_kms provider passes this label along to Oracle Key Manager where it is maintained as meta-data on the data unit. In Oracle Key Manager, keys are associated with data units and for the pkcs11_kms provider this relationship is always 1:1. Each time a new master key is created a data unit with the key's label is created along with the corresponding key object.

Planning Considerations

Careful thought should be given to planning the solution. The next few sections highlight some of the primary considerations to address in the planning phase.

Oracle Database Considerations

Oracle Key Manager works with any of the following Oracle Database configurations:

- Single Instance, Oracle RAC One Node
- Oracle Database High Availability Architectures
- Oracle RAC - Oracle Database with Oracle Real Application Clusters is certified with Oracle Key Manager. Each node of the Oracle RAC system needs to have a configured pkcs11_kms provider for TDE to use.

All nodes should share the same Oracle Key Manager agent ID for authentication. With Oracle RAC, the network topology utilizes a public and private network.

The private network used for Oracle RAC node-node traffic may be shared with the Oracle Key Manager service network for better isolation of key retrieval traffic.

Depending on how this private network is configured, this likely precludes agent failover to KMAs outside the private network such as KMAs in a remote site.

- Oracle RAC Extended Cluster - In this configuration, KMAs within the Oracle Key Manager cluster should be co-located in the network with Oracle RAC nodes so that key retrieval time is minimized.
- Oracle Exadata Database Machine - See the Oracle RAC considerations.
- Oracle Data Guard - All secondary databases access the same Oracle Key Manager cluster used by the primary database.
- Multiple Database Instances - When running multiple independent database instances on a host, each instance needs to have its own PKCS#11 token configured. This amounts to creating an Oracle Key Manager agent for each database instance and having the agent authenticate to Oracle Key Manager via the token. This can all be done through use of the kmscfg(1M) tool.
- Oracle RMAN
- Oracle Data Pump

OKM Performance and Availability Considerations

Key retrievals for TDE through the pkcs11_kms token should typically take 100-200 milliseconds per KMA access. When failovers occur, the response time will be a multiple of the number of failover attempts. Backup and key transfer operations for Oracle Key Manager are database-intensive activities that can impact performance of the Oracle Key Manager database.

For this reason, thought should be given to when and where to perform Oracle Key Manager backups. Since Oracle Key Manager backups (and key transfer operations) are cluster-wide, they can be performed on KMAs that are not servicing Oracle Database

instances. Similarly key transfer operations are also cluster-wide operations and can be performed on any KMA. It is thus recommended to choose a KMA that is not servicing busy Oracle Database instances.

Disaster Recovery Planning

Disaster Recovery planning is a complex topic that is covered in the *Oracle Key Manager Disaster Recovery Reference Guide* and also in Oracle Database documents.

Disaster Recovery planning decisions influence the network planning exercise as well.

The pkcs11 provider's profile area is a new consideration for disaster recovery planning. Consider recovery scenarios for this storage area to avoid having to reconfigure a pkcs11_kms token, especially when it is shared between nodes of an Oracle RAC.

Network Planning

Oracle Key Manager cluster configuration needs to be planned in accordance with the Oracle Database servers and the enterprise's disaster recovery strategy. The networking options with Oracle Key Manager are very flexible and include multi-homed interfaces used by the Oracle Key Manager management and service network:

- **Oracle Key Manager Management Network** - Each KMA in an Oracle Key Manager cluster contains a front-end network interface referred to as the management network. This interface is primarily intended for management of the various nodes of the Oracle Key Manager cluster and for KMA peer-peer replication of cluster data. For optimal cluster replication performance, a Gigabit Ethernet network is recommended. The service network is recommended for use by agents, but the management network may also be used.
- **Oracle Key Manager Service Network** - The service network is intended for use by agents so that their key retrievals may be isolated from other network traffic. There are two Gigabit Ethernet ports on a KMA that are aggregated together for better reliability. It is recommended that TDE access be over the Oracle Key Manager service network. As briefly mentioned in the overview, the service network can be isolated to KMAs and agents within the same site by not defining a gateway to other sites. This may be desirable if other sites are too remote. For maximum availability though, configuring service network gateways to other Oracle Key Manager sites is an option to be considered.
- **Network Time Protocol** - Configuring Oracle Key Manager system time to use an external NTP server is highly recommended.

Key Management Planning

Key management planning must address the key lifecycle and security policies of the enterprise. These considerations will naturally lead to discussions on data retention.

Pre-Operational Phase

The keying material is not yet available for normal cryptographic operations. Keys may not yet be generated, or may be in the pre-activation state. System or enterprise attributes are established during this phase as well.

Operational Phase

The keying material is available and in normal use. Keys are in the active state. Keys may be designated as protect only, process only, or protect and process. Oracle Key Manager supports the protect and process (encrypt or decrypt) and process only (decrypt only) sub-states of the active state.

Post-Operational Phase

The keying material is no longer in normal use, but access to the keying material is possible and the keying material may be used for process only (decrypt only) in certain circumstances. Keys are in the deactivated or compromised states.

Destroyed Phase

Keys are no longer available. All records of their existence may have been deleted. Keys are in the destroyed or destroyed compromised states. Although the keys themselves are destroyed, the key attributes (for example: key name, type, cryptoperiod, and usage period) may be retained.

Key Policy Considerations

All TDE master keys are AES-256 bits and generated by Oracle Key Manager. KMAs may contain a Sun Crypto Accelerator 6000 PCIe Card, a FIPS 140-2 Level 3 certified HSM. When KMAs have this Hardware Security Module then their keys are created by the HSM. Otherwise, cryptographic operations utilize the Solaris Crypto Framework's software token provider. The key lifecycle is the primary configuration item with respect to key policy planning decisions. The periods chosen for the operational phase of the key's lifecycle should be chosen based upon data retention needs and the frequency with which TDE master keys will be re-keyed.

Note – The TDE's DDL supports specification of various key sizes for the master key as does the schema encryption dialogs within Oracle Enterprise Manager. Only AES-256 bit keys can be used with Oracle Key Manager.

The key policy encryption period defines the length of time for the key to be used in the protect and process (encrypt and decrypt) state of the lifecycle. This period should correspond to the time period for use of the master key before it should be re-keyed (for example, maximum one year for PCI). The key policy cryptoperiod is the remaining time allotted for use of the master key to decrypt data during the process only (decrypt only) state of the key lifecycle.

The length of this period should conform to the data retention requirements for the data protected by the TDE master key. Typically this value will be some number of years corresponding to the enterprise policy for data retention (for example a seven year retention period for US tax records).

The rate at which new keys are generated should not be a concern with TDE as re-key operations will likely be infrequent. If this becomes a concern, then consider lengthening the encryption period on the key policy and re-keying less frequently. The Oracle Key Manager key pool size configuration parameter can also be increased to have the KMAs maintain a larger pool of available keys.

Multiple key policies may be defined for use with different types of databases as needs dictate.

Key Access Control Through Key Groups

It may be necessary to control access to keys managed by the Oracle Key Manager when multiple database instances or multiple agents are accessing the Oracle Key Manager cluster for various purposes.

All Oracle Key Manager agents are assigned to at least one key group (a default key group assignment is required), which authorizes them to have access to the keys within those groups. The agent's default key group is the only key group within which a pkcs11_kms provider's agent will create keys.

Consider using multiple key groups when master keys do not need to be shared across database instances or hosts. An example might be to use a key group for production database instances and another key group for development/test databases so that isolation is assured. Agents in the test database key group would then be blocked by Oracle Key Manager if they attempt to use a master key for a production database. Such an attempt would also be flagged in the Oracle Key Manager audit log and may be an indicator of a configuration error that could disrupt a production database.

TDE also provides isolation of master keys through their key label naming convention. In the PKCS#11 specification, key labels are not required to be unique.

Oracle Key Manager enforces label uniqueness so that the scope of the label name space is global for an Oracle Key Manager cluster. Should a label conflict occur between different master keys for different database instances, the first label created will always be returned. If this is not desired behavior, then consider using key groups as a means for segregating agents. An agent attempting to access a key that shares an identical label belonging to another key group will be denied by Oracle Key Manager. This will be caught during a re-key operation and the work around will be to re-key until another, non-conflicting, label is generated.

Key and Data Destruction Considerations

Destruction of data to conform to data retention requirements can begin with the destruction of TDE's master keys. How and when these keys should be destroyed is an important planning item. Oracle Key Manager provides for this and also for tracking the Oracle Key Manager backups, which include these keys. Management of Oracle Key Manager backups is both a Disaster Recovery planning item and key destruction planning item.

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”](#)
- [“Drive Work Sheet”](#) (tape drives or database)
- [“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 <input type="checkbox"/> Yes <input type="checkbox"/> No:		DR Site <input type="checkbox"/> Yes <input type="checkbox"/> No:	
NTP <input type="checkbox"/> Yes <input type="checkbox"/> No:		DHCP <input type="checkbox"/> Yes <input type="checkbox"/> No:	
Gateway <input type="checkbox"/> Yes <input type="checkbox"/> No:		DNS <input type="checkbox"/> Yes <input type="checkbox"/> No:	
KMA Location:			
Oracle Manager Location:			
Configuration Types:	<input type="checkbox"/> SL8500 library <input type="checkbox"/> SL3000 library <input type="checkbox"/> SL500 library <input type="checkbox"/> 9310 library <input type="checkbox"/> L-Series <input type="checkbox"/> SL24/SL48 <input type="checkbox"/> <i>Oracle Database</i>	Tape Drive Types: How many? _____ Database Type: _____	<input type="checkbox"/> T10000A tape drive <input type="checkbox"/> T10000B tape drive <input type="checkbox"/> T10000C tape drive <input type="checkbox"/> T9840D tape drive <input type="checkbox"/> HP LTO tape drive <input type="checkbox"/> IBM LTO tape drive <input type="checkbox"/> 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 <input type="checkbox"/> Yes <input type="checkbox"/> No:		DR Site <input type="checkbox"/> Yes <input type="checkbox"/> No:	
NTP <input type="checkbox"/> Yes <input type="checkbox"/> No:		DHCP <input type="checkbox"/> Yes <input type="checkbox"/> No:	
Gateway <input type="checkbox"/> Yes <input type="checkbox"/> No:		DNS <input type="checkbox"/> Yes <input type="checkbox"/> No:	
KMA Location:			
Oracle Manager Location:			
Configuration Types:	<input type="checkbox"/> SL8500 library <input type="checkbox"/> SL3000 library <input type="checkbox"/> SL500 library <input type="checkbox"/> 9310 library <input type="checkbox"/> L-Series <input type="checkbox"/> SL24/SL48 <input type="checkbox"/> <i>Oracle Database</i>	Tape Drive Types: How many? _____ Database Type: _____	<input type="checkbox"/> T10000A tape drive <input type="checkbox"/> T10000B tape drive <input type="checkbox"/> T10000C tape drive <input type="checkbox"/> T9840D tape drive <input type="checkbox"/> HP LTO tape drive <input type="checkbox"/> IBM LTO tape drive <input type="checkbox"/> 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	<input type="checkbox"/> KMA (Appliance) <input type="checkbox"/> OKM Manager (GUI) <input type="checkbox"/> SL8500 library <input type="checkbox"/> SL3000 library <input type="checkbox"/> SL500 library <input type="checkbox"/> Oracle Database	<input type="checkbox"/> 9310 library <input type="checkbox"/> L700/1400 library <input type="checkbox"/> SL24 and SL48 <input type="checkbox"/> Standalone <input type="checkbox"/> Network/switch	<input type="checkbox"/> T10000A tape drive <input type="checkbox"/> T10000B tape drive <input type="checkbox"/> T10000C tape drive <input type="checkbox"/> T9840D tape drive <input type="checkbox"/> HP LTO drive <input type="checkbox"/> 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 <input type="checkbox"/> No <input type="checkbox"/>			Yes <input type="checkbox"/> No <input type="checkbox"/>						
LAN 1 = ELOM/ILOM			Yes <input type="checkbox"/> No <input type="checkbox"/>			Yes <input type="checkbox"/> No <input type="checkbox"/>						
LAN 2 = Service			Yes <input type="checkbox"/> No <input type="checkbox"/>			Yes <input type="checkbox"/> No <input type="checkbox"/>						
LAN 3 = Aggregated			Yes <input type="checkbox"/> No <input type="checkbox"/>			Yes <input type="checkbox"/> No <input type="checkbox"/>						
Using IPv6 addressing	Yes <input type="checkbox"/> No <input type="checkbox"/>			Yes <input type="checkbox"/> No <input type="checkbox"/>								
KMA Name												
Gateway												
DNS Server	Hostname: IP address:			Hostname: IP address:								
Security Officer	Login: Passphrase:			Login: Passphrase:								
Root account Passphrase	Login: Passphrase:			Login: Passphrase:								
ELOM Passphrase	Login: Passphrase:			Login: Passphrase:								
Key Split Credentials²												
Autonomous Unlocking ³												
Keyboard Type												
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.								

Drive 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 IP Address: _____					KMA ____ Hostname: _____ KMA IP Address: _____			
Drive Address	Drive Type	Drive IP Address	Agent ID	Passphrase	Tokens?	Permanent?	Set FIPS	
1.					Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	
2.					Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	
3.					Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	
4.					Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	
5.					Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	
6.					Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	
7.					Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	
8.					Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	
9.					Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	
10.					Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	
11.					Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	
12.					Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	
13.					Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	
14.					Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	
15.					Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	
16.					Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	
17.					Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	
18.					Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	
19.					Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	
20.					Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	

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 the 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.

P

PKCS Refers to a group of public-key cryptography standards devised and published by RSA Security; as in PKCS#11 which defines a platform-independent API to cryptographic tokens

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.

**Transparent Data
Encryption (TDE)**

A technology employed by Oracle to encrypt database content. TDE offers encryption at a column, table, and tablespace level.

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, 76, 77
3000 installation requirements, 73
3COM Switch, 43
500 installation requirements, 74
700 installation requirements, 76, 77
8500 installation requirements, 72
9310 installation requirements, 75
9741e Drive Cabinet, 75

A

AC power factors and concerns, 39
accessory racks, SL8500, 42
adapter card
 types of, 22
Advanced Encryption Standard (AES), 2
Agents, definition, 3
aggregated
 network configuration, 43
 service port, 43
alley limitations, 38
ANSI standards, 42
ASR, 27, 41
assignments, customer roles, 56
auditor role, 56
Auto Service Request, 27

B

backup operator role, 56
batch file, LTO4, 65
behavior, LTO, 25
Belisarius card
 description, 22

C

cabinet, specifications for installation, 42
cables, for required tools, 66
call center for support, 95
capacity
 of LTO4 tape drives, 22
 of T1000 tape drive, 21
 T9840D tape drive, 21
Capacity on Demand, 51
CBC-MAC standard, 2
CCM standard, 2
checklists
 See Also work sheets
 site planning, 38
 system assurance, 30
Cipher Block Chaining-Message Authentication Code, 2
cluster, definition of, 3
Common Criteria Consortium, 2
comparisons of tape drives and media, 24
compatibilities, media types, 24
compliance operator role, 56
concerns for site planning, 38
connectivity factors for pre-installation, 39
content management, 50
conversion bills
 9310 requirements, 75
Counter with CBC-MAC, 2
Cryptographic Accelerator, 3
cryptography, 1
customer
 contact sheet, 31
 roles, 56
 satisfaction, 29
customer-initiated maintenance, 95

D

- data path, partition planning, 53
- Database, 87
- database considerations, 89
- Database products, 87
- delivery dock, 38
- delivery of the hardware, 38
- dimensions
 - of KMA X2100 server, 12
 - of KMA X2200 server, 13
- Dione card
 - description, 22
- Disaster Recovery planning, 90
- dispatch, 95
- dock availability, 38
- drive
 - data for activating tape drives, 62
 - file structure to activate tape drives, 64
 - LTO4 preparation, 65
 - types of, 20
- dual stack Internet Protocol, 18

E

- EIA 310-D-1992 standards for racks, 42
- ELOM
 - connection, 17
 - description, 16
- embedded Lights Out Manager *See* ELOM
- encryption
 - configurations supported, 69
 - hardware kits, 4
 - introduction, 1
 - standards, 2
 - tape drives supported, 69, 70
- enrollment, work sheet, 99
- environmental parameters
 - X2100 server, 12
 - X2200 server, 13
- environmental, factors and concerns, 38
- error-free installation, 29
- Ethernet adapter cards for LTO4 drives, 22
- Extreme Network Switch configuration, 44
- Extreme Networks, 43

F

- Federal Information Processing Standards
 - encryption standard, 2

- FIPS compliant tape drives, 20
- FIPS publications list, 2
- firmware requirements, 67

G

- glossary, 101
- graphical user interface (GUI)
 - installation, 66
 - Oracle Key Manager, 3
- guides, related information, ix

H

- hardware kits, 4
- Hardware Security Modules (HSM), 88
- help center, 95
- HP LTO4
 - description, 22
- HSM, 88

I

- IBM LTO4
 - description, 22
- IEC 60927 standards for racks, 42
- initial configuration work sheet, 62
- installation, site planning checklist, 38
- Institute of Electrical and Electronics Engineers, (IEEE standards), 2
- Integrated Cryptography Service Facility (ICSF), 83
- International Standard Organization (ISO)
 - encryption standard, 2
- Internet Protocol, supported versions, 18
- ISO/IEC standards, 2

J

- Java versions, 66

K

- Key Groups, 3
- Key Management Appliance
 - definition, 3
 - order numbers, 71
 - specifications, 9
- KMA *See* Key Management Appliance

L

- LAN connections, 16
- Layer 2 broadcast switches, 14, 43
- libraries
 - 9310 PowderHorn, 75
 - L-Series, 76, 77
 - SL3000, 73
 - SL500, 74
 - SL8500, 72
- library
 - content management, 50
 - requirements for installation, 69
 - system assurance, 54
- Linear Tape-Open (LTO), 22
- local area network connections, 16
- L-Series
 - description, 76
- L-Series installation requirements, 76, 77
- L-Series libraries, 76, 77
- LTO4
 - content management, 50
 - interface types, 22
 - media, 22

M

- mainframe options (ICSF), 83
- managed switches, 14, 43
- management network connections, 16
- manuals, ix
- media
 - comparison, 24
 - introduction, 22
- Monitor Drive tab, 65

N

- National Institute of Standards and Technology (NIST) standards, 2
- National Security Agency (NSA) standards, 2
- network connections, 16

O

- OKM cluster, definition, 3
- OKM Manager
 - GUI definition, 3
 - installation, 66
- operator role, 56
- Oracle Database 11gR2, 87

- Oracle Key Manager
 - components, 3
 - configurations, 4
 - network connection, 16
- Oracle Wallet, 88

P

- partitioning, 52
- partner contact sheet, 32
- passphrases, 56
- PC Key request form, 62
- philosophy for content management, 51
- Phone Home, 27
- PKCS, 88
- planning
 - for encryption, 1
 - meetings, for system assurance, 30
 - site planning checklist, 37
- PowderHorn library, 75
- power factors, planning for installation, 39
- process, for system assurance, 29, 54
- publications, ix
- Public-Key cryptography standards (PKCS), 88

Q

- quorum members, 56

R

- rackmount installation requirements, 78
- racks, specifications, 42
- raw keys, 3
- Real Application Clusters, 87
- RealTime Growth, 51
- Recovery Manager, 87
- related publications, documents, ix
- required tools, 66
- requirements
 - 9310 library, 75
 - firmware, 67
 - for the system assurance process, 30
 - L-Series, 76, 77
 - PowderHorn, 75
 - rackmount, 78
 - SL3000 library, 73
 - SL500 library, 74
 - SL8500 library, 72
- RETMA, rack specifications, 42

roles, 56

S

- SCSI tape drive interface, 22
- security officer role, 56
- Service Delivery Platform (SDP), 48
- service network, LAN connections, 16
- service request, 95
- site planning checklist, 38
- SL24 and SL48, 77
- SL3000 requirements, 73
- SL500 requirements, 74
- SL8500 requirements, 72
- Small Computer System Interface in tape drives, 22
- Solaris 10 operating system, 3
- standards for encryption, 2
- steps for partitioning, 54
- StorageTek
 - team member contact sheet, 32
- StorageTek tape drive types, 20
- Summit switches, 43
- Sun Cryptographic Accelerator (SCA), 3
- SunFire X2100 specifications, 12
- SunFire X2200 specifications, 13
- support request, 95
- supported drive interfaces, LTO4, 22
- survey
 - site preparation, 37
 - solution planning, 33
- Symmetric encryption, 2
- system assurance
 - customer contact sheet, 31
 - planning meeting, 30
 - process, 29
 - process overview, 29, 54
 - StorageTek contact sheet, 32

T

- T10000 tape drive
 - capacity, 21
 - description, 106
 - overview, 21
- T9840 tape drive
 - description, 107
 - overview, 21
- T9840D tape drive
 - capacity, 21

- tape drive and media comparisons, 24
- tape drive comparison, 23
- tape drives
 - LTO4, 22
 - supported types, 20
 - T10000, 21
 - T9840, 21
 - work sheet, 98
- tasks for partitioning, 54
- team members, planning, 54
- technical support, 95
- tools, 66
- Transparent Data Encryption, 87
- Transparent Data Encryption (TDE), 88
- T-Series tape drives
 - T10000, 21
 - T9840, 21

U

- Ultra 320 interfaces for LTO4 drives, 22
- Ultrium, LTO tape drives, 22
- units, rack measurements, 42
- user roles, 56
- User Roles Work Sheet, 61

V

- virtual LANs (VLANs), 43
- Virtual Operator Panel
 - for tape drives, 62
 - versions, 66
- VLANs, 14

W

- Wallet, 88
- Web browsers, supported versions, 66
- work sheets
 - enrollment, 99
 - initial configuration, 62
 - KMA *See Also* checklists
 - tape drives, 98
- Write Once, Read Many (WORM), 22



Oracle Corporation
Worldwide Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A