StorageTek Crypto Key Management System

Systems Assurance Guide

Part Number: 316194805
April 2010,
Revision: C

Submit comments about this document by clicking the Feedback [+] link at: http://docs.sun.com

Crypto Key Management System, Systems Assurance Guide

316194805 Revision: C

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	This revision includes: ■ New Oracle branding ■ Updated marketing/order numbers ■ Engineering updates

Note – Change bars are included in this revision.

Contents

Preface

This guide is intended for service representatives, customers, partners, and anyone responsible for planning the installation of Oracle's StorageTek Crypto Key Management System (KMS) Version 2.x.

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

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

Related Information

These publications contain the additional information mentioned in this guide:

Publication Description	Part Number
Important Safety Information for Hardware Systems	816-7190-xx
SunFire X2100 Server Installation Guide	819-6589-xx
SunFire X2200 Server Installation Guide	819-6596-xx
Embedded Lights Out Manager Administration Guide	819-6588-xx
T10000 Tape Drive Installation Manual	96173
T9x40 Tape Drive Installation Manual	95879
SL8500 Modular Library System Installation Manual	96138
SL3000 Modular Library System Installation Manual	316194201
SL500 Modular Library System Installation Manual	96114
L700/1400 Library Installation Manual	95843
9310 PowderHorn Library Installation Manual	9314
Virtual Operator Panel—Service	96180
Virtual Operator Panel—Customer	96179

Publication Description	Part Number
Crypto Key Management Installation and Service Manual	3161949xx
Crypto Key Management System Administration Guide	3161951xx
Crypto Key Management System Disaster Recovery Guide	3161971xx
Storage Regulatory and Safety Compliance Manual	820-5506-xx

These documents are available at:

- Customer http://docs.sun.com/app/docs/prod/stortek.crypto.keymgmt20
- Employee http://docs.sfbay.sun.com/app/docs/prod/stortek.crypto.keymgmt20

Documentation, Support, and Training

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

Oracle Welcomes Your Comments

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

http://docs.sun.com

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

Crypto Key Management System, Systems Assurance Guide, PN: 31619480x

CHAPTER 1

Introduction

Encryption is based on the science of **cryptography** and 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 StorageTek encryption solutions.

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)

StorageTek offers device-based implementations, or a data-at-rest solution, for encryption. This offering provides an excellent solution for mixed environments with a variety of operating system types—both enterprise mainframe 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.

StorageTek Encryption Solutions

StorageTek offers device-based encryption solutions using the Crypto Key Management System, called the KMS.

The KMS uses a SunFire™ X2100 or X2200 server as the hardware platform for the Key Management Appliance (KMA).

The KMA runs the key management application on a minimized, pre-loaded version of the Solaris™ 10 operating system.

Each appliance contains a Sun Cryptographic Accelerator (SCA) 6000 card for all cryptographic processing and administrative functions. This is a FIPS 140-2 Level 3 hardware security module that generates the raw keys.

Components

The components for the Version 2.x encryption solution consists of:

Key Management Appliance (KMA)	The KMA is a server running the Key Management Application on Solaris 10 that delivers policy-based key management and key provisioning services.
KMS Manager or **KMS Manager GUI**	The client-side software component with a graphical user interface (GUI), that incorporates and uses the management API to communicate with the KMAs in a cluster. The KMS Manager must be installed on a *customer-provided***,** network-attached, PC, server, or workstation running Windows XP, Vista, 2003 Server, and Solaris x86 or Solaris SPARC.
KMS Cluster	A full set of KMAs in the system. All of the KMAs are aware of each other, and replicate information to each other. *Note:* The maximum number of KMAs in a cluster is 20.
Agent	A device (tape drive) is authenticated with the KMS and obtains key material over a secure (TLS) session.
Data Unit ID	A unique ID assigned by the KMS to each individual data cartridge.
Key Groups	Provide organization for keys and associates them to a Key Policy. Key Groups are used by the KMS to enforce access to the key material by the Encryption Agents.
Network connections	Each key management appliance has four network connections, these include: LAN 0 = Management network LAN 1 = Embedded Lights Out Manager (ELOM) network LAN 2 = Service network, preferred connection to the tape drives LAN 3 = Additional aggregated service port

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 in FIGURE 1-1 through FIGURE 1-3. Some key points include:

- Multiple KMAs are clustered on a dedicated, private, local, or wide area network.
- The KMAs in a KMS Cluster provide data replication so there is redundancy, which allows each KMA to serve as backups to others.
- Tape drives, called Agents, must remain connected to the network.
- Any KMA in the cluster can service any tape drive on the network provided there is an Ethernet connection.
- 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 KMA 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.
  - All administration functions can be centralized to one KMS or site.

Encryption Hardware Kits

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

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

Refer to the *Crypto Key Management System Installation and Service Manual* and the individual *product installation manuals* for specific installation instructions.

Key Management System Configurations

Multiple KMAs[1] (two or more) must be installed together to create a KMS. The KMS contains a cluster[2] of KMAs that fully replicate their data to each other. Cluster size should be strongly considered when designing the system for maximum availability.

The following configurations contain the same components; the difference is with the customer needs, requirements, and how the components are installed.

Version 2.x configurations for the key management appliance (KMA):

- FIGURE 1-1 on page 4 Single site – local area network
- FIGURE 1-2 on page 4 Multiple sites– wide area network
- FIGURE 1-3 on page 5 Multiple sites with disaster recovery – wide area network
- FIGURE 1-4 on page 6 Disaster Recovery Configuration

1. **Multiple KMAs**: Exceptions to this standard configuration *must* be made with the approval of KMS 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. Clusters are usually deployed to improve performance and/or availability.

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) T-Series (T10000 A and B, T9840D) and LTO4.

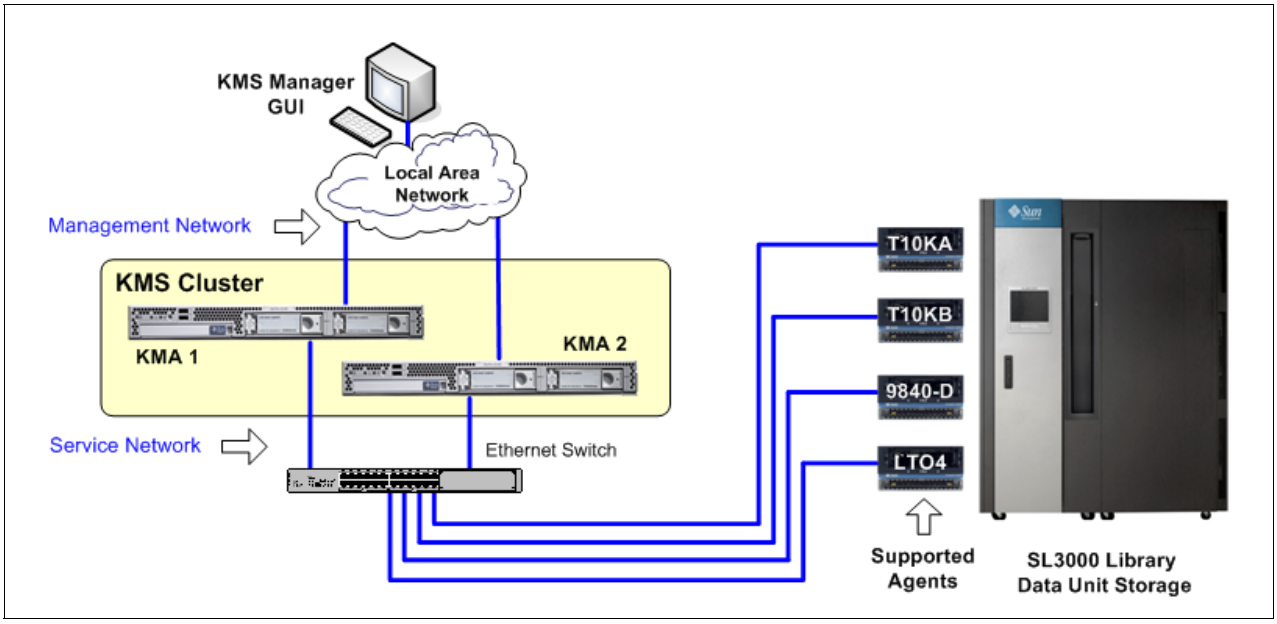
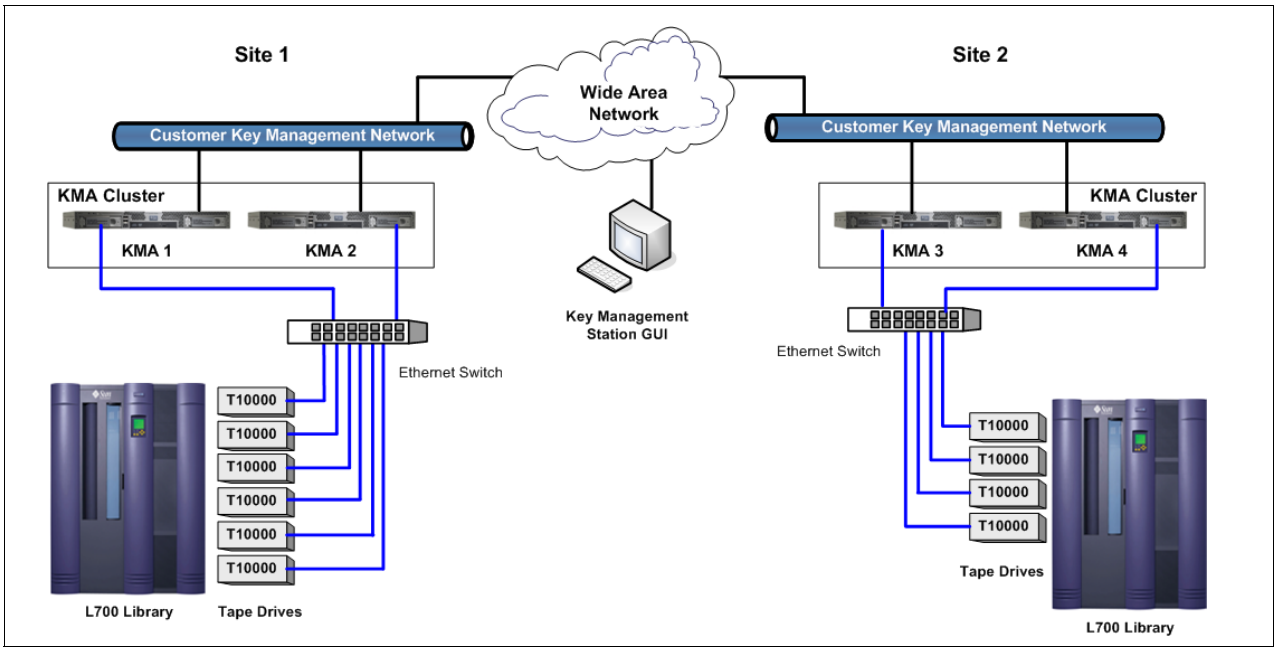


FIGURE 1-2 Dual Site Configuration

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



Note: LTO4 encryption-capable tape drives are not supported in L-Series libraries.

FIGURE 1-3 Multiple Site Configuration

This example uses both remote and local sites within one KMS cluster.
The main site contains a partitioned SL8500 library with specific key groups and provides disaster recovery facilities for all the KMAs within the cluster, local and remote sites.

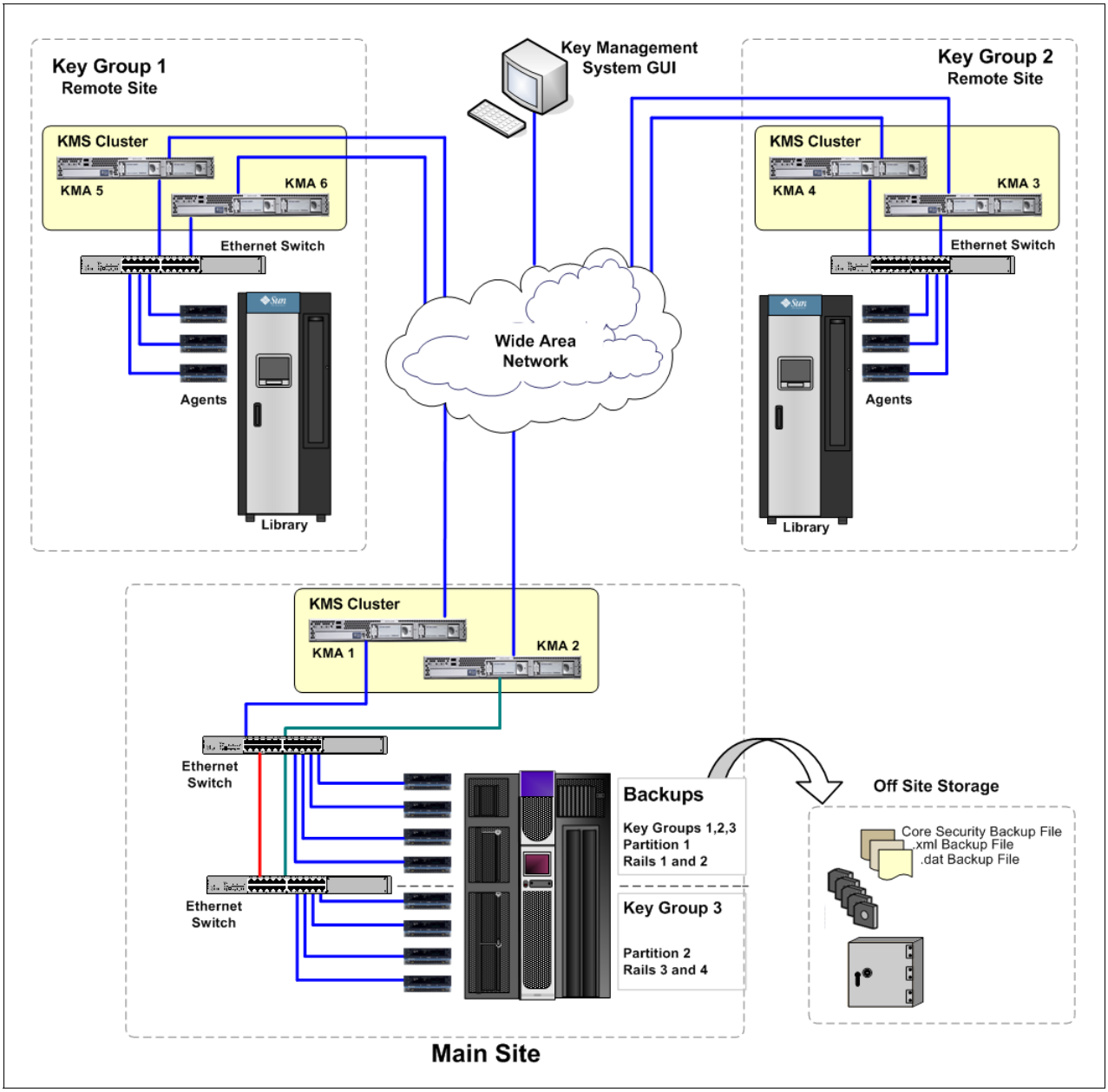
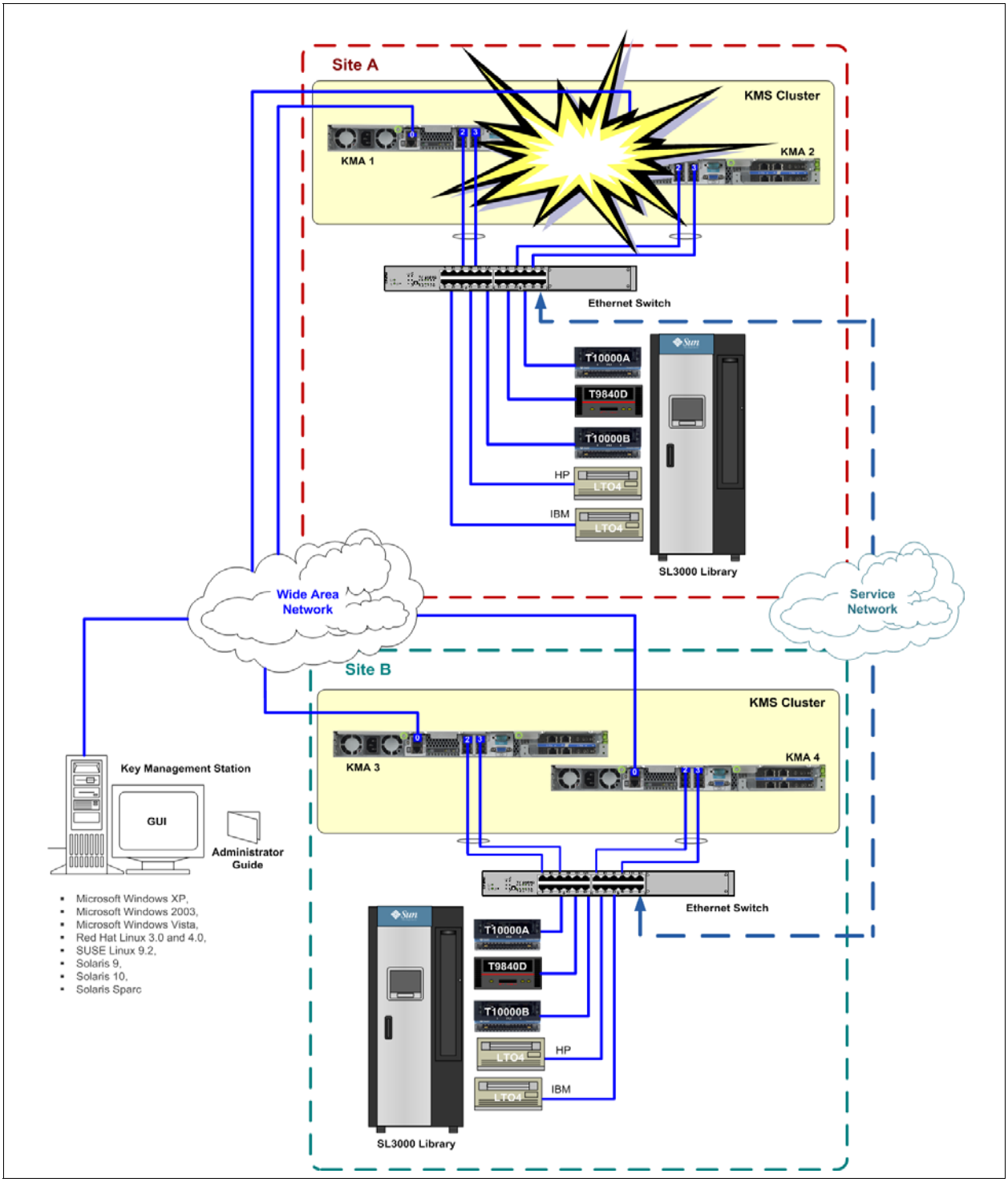


FIGURE 1-4 Disaster Recovery Configuration

In this example there are two wide area networks; one for management and one for service.

- The KMS Manager 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.



Encryption Standards

StorageTek 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, Key Life Cycle document.
- 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)

Key Management Appliance Specifications

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

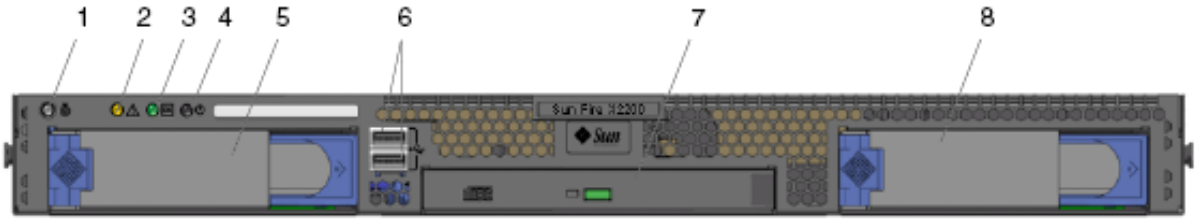
- SunFire X2100 servers
- SunFire X2200 servers

Both servers are functionally equivalent and have the same design.

Notes:

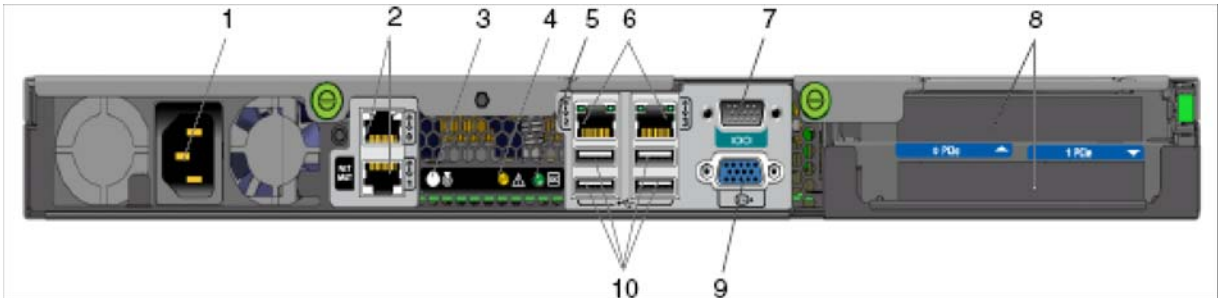
- Subsequent releases of the KMS appliance may use different server hardware but are guaranteed to be interoperable with deployed KMAs.
- A KMS may consist of a mix of SunFire X2100s or X2200s as systems are upgraded, scaled or as replacements to failed units.

FIGURE 1-5 Key Management Appliance—Front Panel



1. System identification button/LED
2. Fault LED
3. Power/OK LED
4. Power button
5. Optional hard disk drive bay (0)
6. USB 2.0 connectors (2)
7. CD/DVD drive (not populated)
8. Optional hard disk drive bay (1)
   Note: Only one bay is populated

FIGURE 1-6 Key Management Appliance—Rear Panel



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

SunFire X2100 Server

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

TABLE 1-1 SunFire X2100 Specifications

Processor	■ One dual-core AMD Operton processor ■ Processor frequencies: 2.2 GHz ■ Up to 1 MB level 2 cache
Memory	■ Four DIMM slots (up to 4 gigabytes) ■ Unbuffered ECC memory
IPMI 2.0	■ 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	■ 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 connectors ■ 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.) form factor
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 1-2 lists the specifications for the SunFire X2200 server.

TABLE 1-2 SunFire X2200 Specifications

Processor	■ Two Quad core AMD Opteron processors ■ Processor frequencies: 2.3Ghz
Memory	■ 8 GB of RAM, installed as 4, 2 GB Dimms
IPMI 2.0	■ 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	■ 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 connectors ■ 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.) form factor
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

StorageTek recommends that *customers supply* a *managed switch* for connecting KMAs to the tape drives on their service network. 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 KMS engineering:

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

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

Managed switches are recommended for the following reasons:

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

FIGURE 1-7 on page 12 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 KMS management network should use a clean gigabit Ethernet connection for optimal replication and performance.

ELOM

The ELOM network should have spanning tree turned off or disabled.

KMA Service Port Aggregation

Beginning with KMS 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.

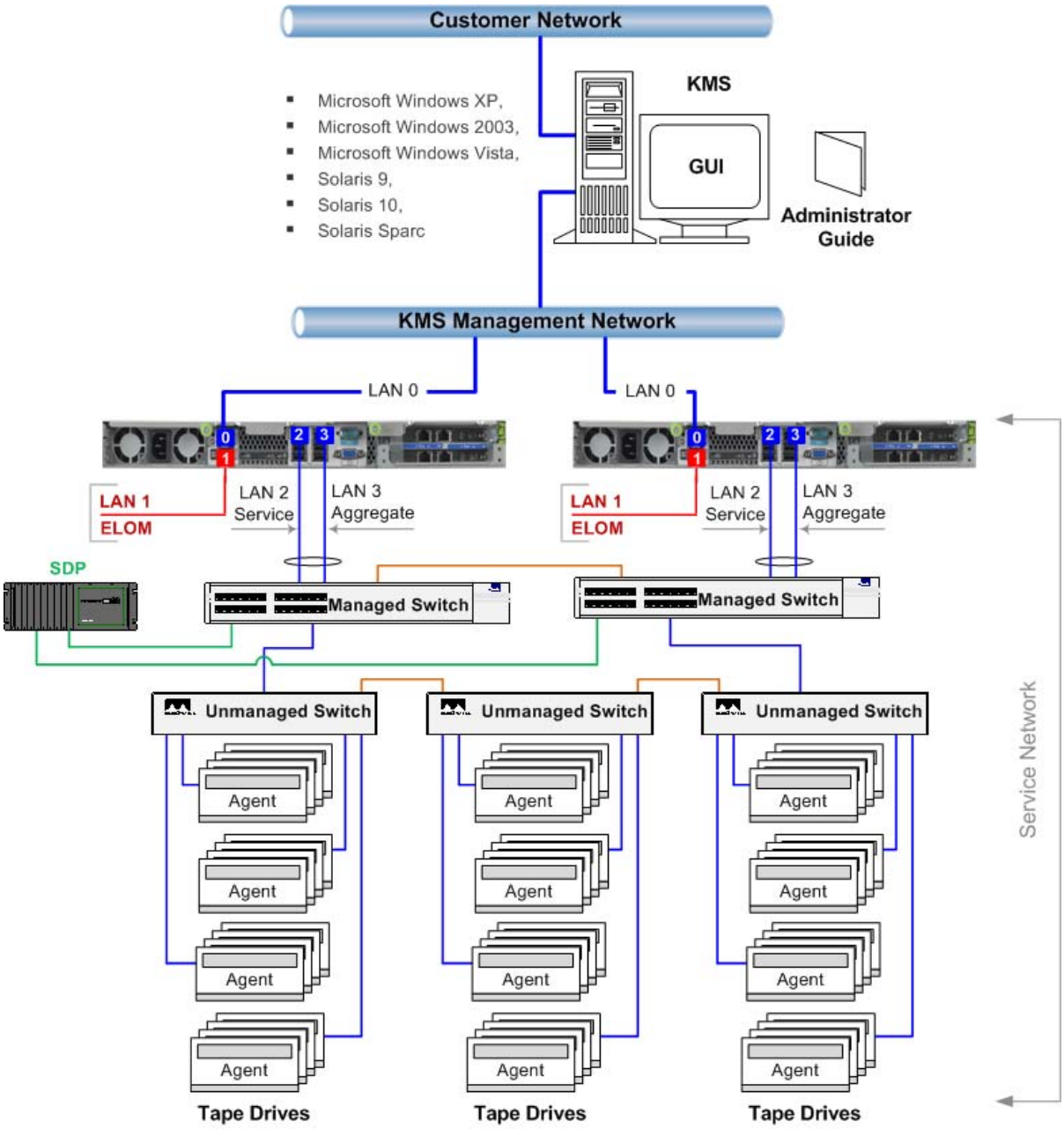
Make sure the Ethernet switch ports have the correct configuration. For example, Switch ports should be:

- 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 1-7 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
- LAN 1 = Embedded Lights Out Manager (ELOM) network
- LAN 2 = Service network
- LAN 3 = Aggregated service network

TABLE 1-3 KMA Network Connections

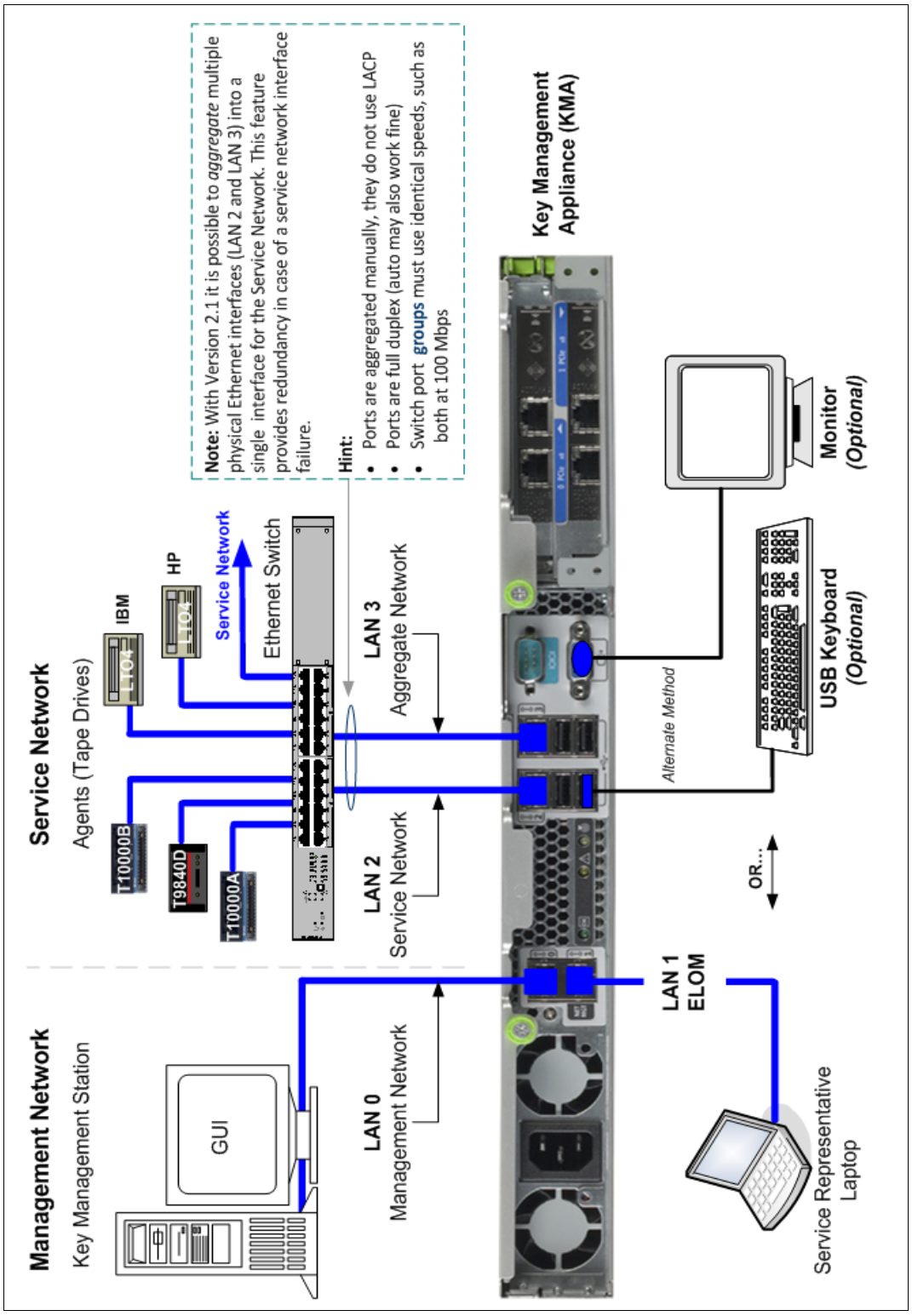
LAN 0	This is a *required* connection. This network is called the "Management Network" and interconnects with the Key Management Appliances and management clients hosting the GUI or CLI. This network can be local, remote, or a combination of both. **Note – Customers are expected to provide this network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

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

Key Management Appliance Physical Connections

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

FIGURE 1-8 Key Management Appliance—Rear Panel Connections



Note – Each Ethernet connection (blue lines) needs an IP address.

Internet Protocol Versions

Enhancements made to KMS 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 KMS 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.

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 five tape drive models to choose from:

- T10000A
- T10000B
- T9840 Model D only
- Hewlett Packard (HP) Linear Tape-Open (LTO)
- International Business Machines (IBM) Linear Tape-Open (LTO)

FIPS Compliant Tape Drives

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

TABLE 1-4 FIPS Compliant Tape Drives

Tape Drive	FIPS Level
T10000A	1
T10000B	2
T9840D	1
LTO (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 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** = 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 T10000

The T10000 tape drive is a modular, high-performance tape drive designed for high-capacity storage. There are two models of the T10000 that support encryption:

- T10000A
- T10000B

Dimensions: The tape drive is:

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

Capacity:
The T10000 uses partial response, maximum likelihood (PRML) technology to provide the high-density data format that allows the tape drive to record and store up to:

- **T10000 A** = 500 gigabytes (GB) of uncompressed data
- **T10000 B** = 1 terabyte (TB) of uncompressed data[4]

Media:
The tape cartridge for this drive uses a single-reel hub for high capacity; the supply reel is inside the cartridge and the take-up reel is inside the tape drive.

Interfaces:
The host connections to the T10000 tape drives are fiber-optic to provide a high rate of data transfer. The T10000 drives support both Fibre Channel and FICON interfaces.

Configurations:
The T10000 drives support two configurations for encryption, library and standalone.

For a variety of operating system platforms:

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

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

About the T9840D Tape Drive

The 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:
The T9840D tape drive uses a a variable rate randomizer with partial response, maximum likelihood (PRML) as the recording format. This allows the tape drive to record and store up to:

- **T9840D** = 75 gigabytes (GB) of uncompressed data

Media:
With the unique dual-hub design of the 9840 cartridge, the entire tape path is contained inside the tape cartridge. This design reduces contamination and enables the drives fast access.

Interfaces:
Host interfaces to the T9840D tape drive includes: Fibre Channel (FC), IBM's Fibre Connection (FICON), and IBM's Enterprise System Connection (ESCON).

Configurations:
The T9840 supports two configurations for encryption: library and standalone.

For a variety of operating system platforms:

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

About the LTO4 Tape Drives

Overview

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

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

Note: Currently, the LTO4 tape drive is the first generation of LTOs capable of supporting tape- or device-based encryption.

Encryption Capable

Both the HP and IBM LTO4 drives support write encryption and read decryption when integrated into a secure encryption system, such as the Crypto Key Management System Version 2.x.

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

Being able to manage the "Keys to Encryption" requires a special, custom-designed, Ethernet **adapter card** mounted inside the drive tray. This adapter card provides a means for the LTO4 drive to connect to and interface with the Key Management System. Each vendor has their own unique version of an adapter card:

- HP = Dione card
- IBM = Belisarius card

With this connection, the LTO4 is capable of communicating with the KMS to transfer encryption keys over the secure network.

Note: Currently the LTO4 drives can only use *one encryption key at a time*. During a read operation, if another encryption key is found on the tape, the adapter card requests the key directly from the KMS.

Media (Native capacity)

The LTO4 tape drive uses an 800 GB Data Cartridge and is compatible with other vendor cartridges and other generations of LTO tape drives. The drive performs the following functions:

- Reads/Writes LTO4 cartridges in Ultrium 4 format, including WORM
- Reads/Writes LTO3 cartridges in Ultrium 3 format, including WORM
- Reads but *does not* write LTO2 cartridges

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.

Important: Encryption is supported with LTO4 data cartridges only. Encryption is not supported in LTO3-, LTO2-, or LTO1-formats and, to avoid a security breach, the drive will not write in these modes once enabled for encryption.

Configurations

IBM's LTO4 tape drive can be integrated into an enclosure, or drive tray, for automated tape library applications, and used as a standalone device.

Interfaces

The LTO4 drives come with a Fibre Channel interface (FC), in either a single or dual port configuration.

The HP LTO4 tape drive support also includes:

- Ultra 320 Small Computer System Interface (SCSI)

Tape Drive and Media Comparison

TABLE 1-5 Tape Drive Comparisons

Physical Specifications	T10000A	T10000B	T9840D	HP LTO4	IBM LTO4
Height	8.25 cm (3.25 in.)	8.25 cm (3.25 in.)	8.25 cm (3.25 in.)	8.25 cm (3.25 in.)	8.25 cm (3.25 in.)
Width	14.6 cm (5.75 in.)	14.6 cm (5.75 in.)	14.6 cm (5.75 in.)	14.6 cm (5.75 in.)	14.6 cm (5.75 in.)
Length (depth)	42.5 cm (16.75 in.)	42.5 cm (16.75 in.)	38.1 cm (15 in.)	21.38 cm (8.4 in.)	20.5 cm (8.09 in.)
Weight	5 kg (11 lb)	5 kg (11 lb)	3.9 kg (8.5 lb)	2.24 kg (4.94 lb)	3 kg (6.6 lb)
Performance Specifications					
Capacity (native)	500 GB	1 TB	75 GB	800 GB	800 GB
Transfer rate (native)	2 to 4 Gb/s	4 Gb/s	30 MB/s	4 Gb/s	4 Gb/s
Throughput (native)	120 MB/s	120 MB/s	30 MB/s	120 MB/s	120 MB/s
Data Buffer size	256 MB	256 MB	64 MB	128 MB	128 MB
Number of tracks	768	1152	576	896	896
Tape Thread & Load	16 sec	16 sec	8.5 sec	19 sec	15 sec
Access Time	46 sec	46 sec	8 sec	62 sec	48 sec
Tape speed	2.0 and 4.95 m/s	2.0, 3.74, and 4.95 m/s	3.4 m/s	7.00 m/s	—
Rewind time	90 sec	90 sec	16/8 sec	124 sec	88 sec
Tape Unload	23 sec	23 sec	12 sec	22 sec	15 sec
Emulation Modes	3490E, 3590, 3592, T9940	3490E, 3592	Native, 3490E, 3590H	—	—
Interface Support	FC2, FC4, FICON	FC4, FICON	FC2, FICON. ESCON	FC4, SCSI Ultra320	FC4
MTBF (100% duty cycle)	290,000 hrs	290,000 hrs	290,000 hrs	250,000 hrs	250,000 hrs
Media/Format Compatibility					
Read/Write	Proprietary Format T10000 Cartridge		Proprietary Format	LTO2 = Read only LTO3 = Rd/Write LTO4 = Rd/Write	
VolSafe/WORM?	Yes		Yes	Yes	Yes
Power					
Auto-ranging / Amperage	88-264 VAC, 48-63 Hz			100–240 VAC 50–60 Hz 0.8A max.	
Consumption	90 W		82 W	35 W	30 W

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

T-Series Tape Drives

TABLE 1-6 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 1-6 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 1-7 shows a comparison between:

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

TABLE 1-7 T-Series Tape Drive and Media Support

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

LTO4 Tape Drives

Notes: Both HP and IBM LTO4 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

TABLE 1-8 LTO Media Compatibility

Native Capacity (Length)	**Format**	**Capability**	
		Write	**Read**
800 GB WORM	LTO4	Yes	Yes
800 GB (820m)	LTO4	Yes	Yes
400 GB WORM	LTO3	Yes	Yes
400 GB (680m)	LTO3	Yes	Yes
200 GB (580m)	LTO2	No	Yes
100 GB (580m)	LTO1	No	No
50 GB (290m)	LTO1	No	No

Note – Encryption is only supported with LTO4 Data Cartridges on LTO4 tape drives. To avoid a security breach, these drives will not write in these modes once the drive is enabled for encryption.

LTO4 Encryption Behavior

When LTO4 encryption is controlled by the Crypto Key Management System, these drives can behave differently from StorageTek T-Series drives. There can also be slight differences between the HP and IBM drives from each other. These differences arise from specific aspects of the IBM and HP drive architecture.

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

TABLE 1-9 LTO4 Encryption Behavior

LTO4 Drive Performance	**HP Implementation**	**IBM Implementation**
Not Enrolled for Encryption		
Read LTO4 non-encrypted data	OK non-encrypted	OK non-encrypted
Read LTO4 encrypted data	Error	Error
Write LTO4 from BOT	OK non-encrypted	OK non-encrypted
Read LTO3 tape	OK non-encrypted	OK non-encrypted

TABLE 1-9 LTO4 Encryption Behavior (Continued)

LTO4 Drive Performance	HP Implementation	IBM Implementation
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
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)
* Assuming 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 LTO4 drive 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 KMS when the write command is issued and this will ignore the Key Expiration Policy set by the KMS.
Note 5	HP drives will write LTO3 tapes in non-encrypted mode. The LTO3 format does not support encryption and this could be considered a security violation since an HP LTO4 drive 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.

CHAPTER **2**

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 StorageTek Crypto Key Management System are overlooked. This process promotes an error-free installation and contributes to the overall customer satisfaction.

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

Planning Meetings

The purpose of the system assurance planning meetings is to:

- Introduce the customer to the StorageTek 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 ❑ No ❑
Explain the encryption solutions to the customer. See Chapter 1, "Introduction" for topics and information.	Yes ❑ No ❑
Complete the Team Member Contact sheets.	Yes ❑ No ❑
Use "Configuration Planning" on page 29 to help define the customer requirements.	Yes ❑ No ❑
Review and complete "Site Planning Checklist" on page 32. *Comments:*	Yes ❑ No ❑
Review and identify "User Roles Work Sheet" on page 49. *Comments:*	Yes ❑ No ❑
Review "Supported Configurations" on page 57. *Comments:*	Yes ❑ No ❑
Review "Order Numbers, Descriptions, and Contents" on page 65. *Comments:*	Yes ❑ No ❑
Determine the installation schedule: **Date:** _____ **Time:** _____	Yes ❑ No ❑
Download and provide the customer with a copy of the: *Crypto Key Management System Administrator's Guide* PN 316195101. *Virtual Operator Panel—Customer* PN: 96179 http://docs.sun.com/app/docs/prod/stortek.crypto.keymgmt	Yes ❑ No ❑

Customer Team Member Contact Sheet

Complete the following information for the customer team members:

Name: _____
Title: _____
Telephone Number: _____
FAX Number: _____
Cell Phone / Pager: _____
E-mail Address: _____

Name: _____
Title: _____
Telephone Number: _____
FAX Number: _____
Cell Phone / Pager: _____
E-mail Address: _____

Name: _____
Title: _____
Telephone Number: _____
FAX Number: _____
Cell Phone / Pager: _____
E-mail Address: _____

Name: _____
Title: _____
Telephone Number: _____
FAX Number: _____
Cell Phone / Pager: _____
E-mail Address: _____

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

StorageTek Team Member Contact Sheet

Complete the following information for the StorageTek 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 – StorageTek 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 KMS the customer is considering. This checklist is geared towards planning a single Key Management System, up to 20 KMAs.

TABLE 2-2 Solution Planning Checklist

Question	Selection / Comments	Quantity
What type of configuration does the customer want? **Notes:** ■ 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.	❑ Single site ❑ Multiple sites ❑ Disaster recovery site	How many: _____ _____ _____
How many appliances (KMAs) are needed? ■ The maximum number of KMAs is 20. ■ The minimum KMS size is 2*. ■ The recommendation is at least 2 (assuming sites are geographically dispersed) * The exception to this standard configuration (single-node site) must be made with the approval of KMS Engineering, Professional Services, and Support Services.		How many: _____
What type of encryption **hardware kits** are needed? How many encryption hardware kits are needed?	❑ SL8500 ❑ SL3000 ❑ SL500 ❑ 9310 / 9741E ❑ L-Series ❑ Rackmount	How many: _____ _____ _____ _____ _____ _____
How many and of what type of encryption-capable tape drives are needed?	❑ T10000A ❑ T10000B ❑ T9840D ❑ HP LTO4 ❑ IBM LTO4	How many: _____ _____ _____ _____ _____
Are external (standalone) Racks required? Type?	❑ Yes ❑ No	How many: _____
Identify customer requirements and expectations.		

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

CHAPTER 3

Site Preparation

Use this chapter and checklists to prepare for the installation.

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

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 Key Management Systems and appliances are considered "secure" items. Follow the customers security guidelines for delivery and installation.		
Does the customer have a delivery dock? If *no*, where will the equipment be delivered? If a delivery dock *is* available, what are the hours of operation?	Yes ❑ No ❑ _____	
Are there street or alley limitations that might hinder delivery?	Yes ❑ No ❑	
Will authorized personnel be available to handle and accept the delivery?	Yes ❑ No ❑	
Is the delivery location close to the computer room where the equipment will be installed?	Yes ❑ No ❑	
Is an elevator available to move the equipment to the appropriate floors?	Yes ❑ No ❑	
Is there a staging area where the equipment can be placed close to the installation site?	Yes ❑ No ❑	
Are there special requirements to dispose of or *recycle* packing material? Pallets, plastic, and cardboard?	Yes ❑ No ❑	
Environmental Planning		
Does the site meet the environmental requirements for temperature, humidity, and cooling?	Yes ❑ No ❑	See "Key Management Appliance Specifications" on page 8

TABLE 3-1 Site Planning Checklist (Continued)

Question	Completed?	Comments:
Power Requirements		
Does the intended site meet the power requirements?	Yes ❑ No ❑	See "Key Management Appliance Specifications" on page 8 **KMA:** 90 to 132 VAC | 180 to 264 VAC 57 to 63 Hz | 47 to 53 Hz 2.3 to 4.6 Amps Maximum continuous power is 150 W
Has the customer identified the circuit breakers locations and ratings?	Yes ❑ No ❑	
Does the customer want redundant power options? If so, an additional APC power switch is required to create an uninterrupted power configuration.	Yes ❑ No ❑	Check for updated models and part numbers. (Part number #419951602)
Are there any power cable routing requirements and concerns?	Yes ❑ No ❑	See "Power Cables" on page 76 for more information.
Personnel:		
Are there trained/qualified StorageTek representatives locally to install and maintain the encryption equipment?	Yes ❑ No ❑	**Names:**
Connectivity: Cabling is *very important* to establish a reliable network between the KMS GUI, KMAs, Ethernet switches, and tape drives.		
Does this customer support **IPv6** implementations?	Yes ❑ No ❑	
Does the customer intend on using **Managed** switches?	Yes ❑ No ❑	Cable considerations are impacted by the decision to use a managed switch and the corresponding topology of the service network.
Is a Wide Area **Service** Network being considered?	Yes ❑ No ❑	Designing the service network across a WAN to remote sites adds additional failover capability to the agents and can facilitate disaster recovery scenarios.
Does the customer want to **aggregate** the service ports (LAN 2 and LAN 3)?	Yes ❑ No ❑	Requires additional cables and compatible port configuration on a customer supplied managed switch.

TABLE 3-1 Site Planning Checklist (Continued)

Question	Completed?	Comments:
Connectivity (continued)		
Will there be a Service Delivery Platform (**SDP**) installed at this site?	Yes ❑ No ❑	See SDP on page 37 for information.
Will the customer be monitoring the KMS using **SNMP**?	Yes ❑ No ❑	SNMP v3 recommended SNMP v2 supported
Are there considerations for monitoring of **ELOM** using the LAN 1 port?	Yes ❑ No ❑	Refer to the SunFire X2100/2200 ELOM Administration Guide for SNMP monitoring, IPMI, and other appliance management considerations.
Have you and the customer completed a: ■ Cable plan? ■ Configuration drawing? A drawing can help determine the number of and length of the cables required.	 Yes ❑ No ❑ Yes ❑ No ❑	
Have you determined the type and number of Ethernet cables required? *Customer supplied:* ■ KMS Manager to the network ■ Network to the KMAs (LAN 0) ■ ELOM monitoring (LAN 1) ■ Service network to agents (LAN 2 & 3) *Supplied in the encryption kits:* ■ Switch to each tape drive	Yes ❑ No ❑	**Note:** ■ Ethernet cables are shipped with kits. ■ Lengths are dependant on the location of the switches and devices.
Configurations		
Does the customer have adequate rack space to hold the KMAs and Ethernet switches?	Yes ❑ No ❑	See "Rack Specifications" on page 36
What type of support configurations does the customer want or need? ❑ Existing configuration ❑ New configuration	<u>Configuration</u> ❑ SL8500 ❑ SL3000 ❑ SL500 ❑ 9310/9741e ❑ L-Series ❑ Rackmount	<u>Encryption-capable Drives:</u> T-Series & LTO4 T-Series & LTO4 LTO4 only T-Series only T-Series 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? Drive types? Check current and required firmware versions.	Yes ❑ No ❑ Yes ❑ No ❑ ❑ T10000A ❑ T10000B ❑ T9840D ❑ HP LTO4 ❑ IBM LTO4	See "Order Numbers, Descriptions, and Contents" on page 65 for x-options (conversion bills). Requires drive tray and Dione card Requires drive tray and Belisarius card

TABLE 3-1 Site Planning Checklist (Continued)

Question	Completed?	Comments:
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 LTO4 drive only)	Yes ❑ No ❑ ❑ T10000A ❑ T10000B ❑ T9840D ❑ HP LTO4 ❑ IBM LTO4	How many tape drives?
Are additional cartridges required? ■ Data cartridge ■ Cleaning cartridges ■ VolSafe cartridges ■ Labels ■ Type: _____ ■ Quantity: _____	 Yes ❑ No ❑ Yes ❑ No ❑ Yes ❑ No ❑ Yes ❑ No ❑	**Note:** All versions of encryption tape drives use different, unique cartridges. ■ T9840 = 9840 cartridges ■ T10000 = T10000 cartridges ■ LTO4 = LTO4 cartridges only. All versions of each cartridge-type are supported, for example, standard, sport, VolSafe, and WORM.

Notes:
Configurations:
Tape Drives and Media:

Rack Specifications

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

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

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

SL8500 Rack Guidelines

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

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

TABLE 3-2 SL8500 Accessory Rack Guidelines

Guideline	Descriptions
Rack numbering	Rack numbering is top-down from 1 to 4. 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 *plus* 46 cm (18 in.) for a service loop.
Thermal requirements	Maximum power dissipation is 880 watts (3,000 Btu/hr) per rack module.
Regulatory compliance	Minimum requirements are: Safety—UL or CSA certification and Electromagnetic—Class A certification from agencies such as FCC or BSMI.

1. **RETMA** = Radio Electronics Television Manufacturers Association.
2. **U** stands for rack units. One unit is equal to 4.4 cm (1.75 in.).

Service Delivery Platform

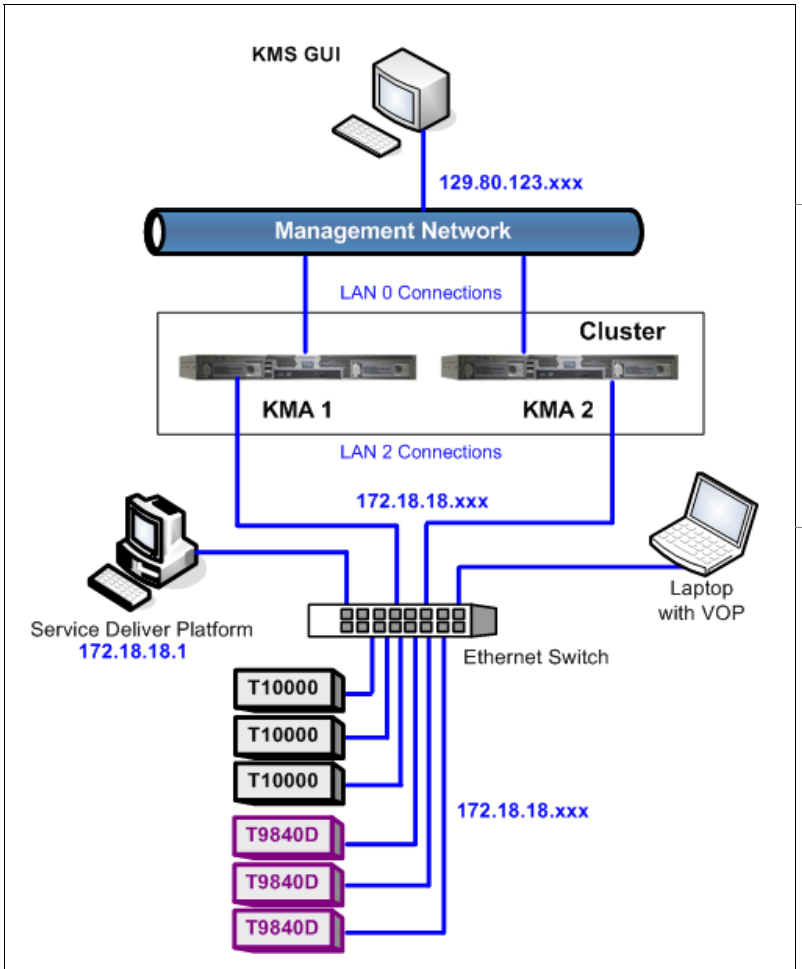
The Service Delivery Platform (SDP) is a support solution for Sun StorageTek libraries and tape drives that consists of a smart appliance and dedicated network.

The Key Management Appliance uses LAN 2 port as the service network to the tape drives; LAN 3 port as another aggregated service port.

The SDP appliance can be configured to use the Dynamic Host Configuration Protocol (DHCP) to automate the assignment of IP addresses for device connections. When incorporating the KMAs into an SDP network, it is best to use the established addresses provided by the SDP; the IP address range is 172.18.18.xxx. Optionally, the SDP can be used as the DHCP server for the KMAs service network IP address.

FIGURE 3-1 shows an example of an SDP network with connection to a KMA cluster.

FIGURE 3-1 Systems Delivery Platform



In this figure, the KMS Manager uses a customer assigned network and IP address of 129.80.123.xxx.

Each KMA that connects to this network is using its LAN 0.

The KMAs use LAN 2 (and possibly an aggregated LAN 3) to connect to the tape drives over a *private* service network.

If the SDP connects to this network it must either conform to the network IP address scheme **or** the drives and KMA need to use the SDP IP address range of 172.18.18.2 – 172.18.18.59

If using an SDP, the tape drives connect to the service network using an assigned IP address from the SDP.

The SDP will likely come with an Ethernet switch that connects to the KMA service network.

Note:
The default tape drive IP address is 10.0.0.1 and must be changed in any connection scheme.

If the customer wants this support option as part of the encryption solution, use and complete the information in the *SDP Systems Assurance Guide*. Go to:
https://csa-wiki.east.sun.com/display/SDP/Home

Important:
SDP *does not* support LTO4 drives so these drive IP addresses must be assigned statically.

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&B ■ T9840D ■ LTO4	■ T10000 A&B ■ T9840D ■ LTO4	■ HP & IBM LTO4 only
Non-encryption Drives Supported	■ T10000 A&B ■ T9840 A, B, & C ■ LTO 3, & 4	■ T10000 A&B ■ T9840 C ■ LTO 3 & 4	■ LTO 2, 3, & 4 (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 LTO4 FC only	T10000 A&B FC and FICON T9840D FC, FICON, ESCON LTO4 FC only	LTO4 Fibre 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, & T-WORM ■ DLTtape III ■ Super DLTtape I & II	■ T10000 (Std, Sport, VolSafe) ■ 9840 (Std and VolSafe) ■ LTO 2, 3, 4, & T-WORM	■ LTO 1, 2, 3, 4, & 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 ■ HSC ■ 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
- Easily 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.

Whenever building an SL3000 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 KMS 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.

A KMS 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 KMS 2.x environment from a recent database backup.

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

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

Planning the Data Path

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

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

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

Planning Tasks

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

TABLE 3-4 Steps and Tasks for Partitioning

✓	Item	Task	Responsibility*
❑	**1. Team**	Create a Team. When planning for content, data and partitions, use a process similar to that of the system assurance process; which is the exchange of information among team members to ensure all aspects of the implementation are planned carefully and performed efficiently. Team members should include representatives from both the customer.	■ Customer ■ Administrators ■ Operators ■ SE, PS ■ Svc Rep
❑	**2. Codes**	Review the software and firmware requirements. Update as required.	■ Customer ■ SE, PS ■ Svc Rep
❑	**3. Planning**	■ Define the customer expectations ■ Complete the assessment ■ Identify the configurations ■ Complete the planning diagrams ■ Service Delivery Platform (SDP)	■ Customer ■ Administrators ■ SE, PS ■ Svc Rep
❑	**4. Encryption**	■ Complete an encryption survey (PS) ■ Select the type of tape drive, interface, and library configuration ■ Select location ■ Ensure there is adequate media	■ Customer ■ SE, PS ■ Svc Rep
❑	**5. Disaster Recovery**	■ Develop a business continuity and disaster recovery plan ■ Select a backup site ■ Determine network configurations (LAN, WAN, aggregation)	■ Customer ■ SE, PS ■ Svc Rep
❑	**6. Media**	■ Verify the distribution of cartridges and required tape drives are available and ready.	■ Customer ■ Operators
❑	**7. Library**	■ Install and configure a library (if necessary).	■ Svc Rep

❑	**8. Activation**	■ Activate the required features:
		  ■ Library
		  ■ Tape drives
			■ Customer
			■ Administrators
			■ Svc Rep

❑	**9. Partitions**	■ Create partitions.	■ Customer ■ Administrators ■ Operators
❑	**10.Hosts**	■ Momentarily stop all host activity if currently connected.	■ Customer
❑	**11.Use**	Instruct the customer how to: ■ Use and manage the library ■ Use the KMS GUI	■ Customer ■ SE, PS ■ Svc Rep
❑	**12.Reference**	Make sure the customer has access to the appropriate documents.	■ Customer ■ SE, PS ■ Svc Rep

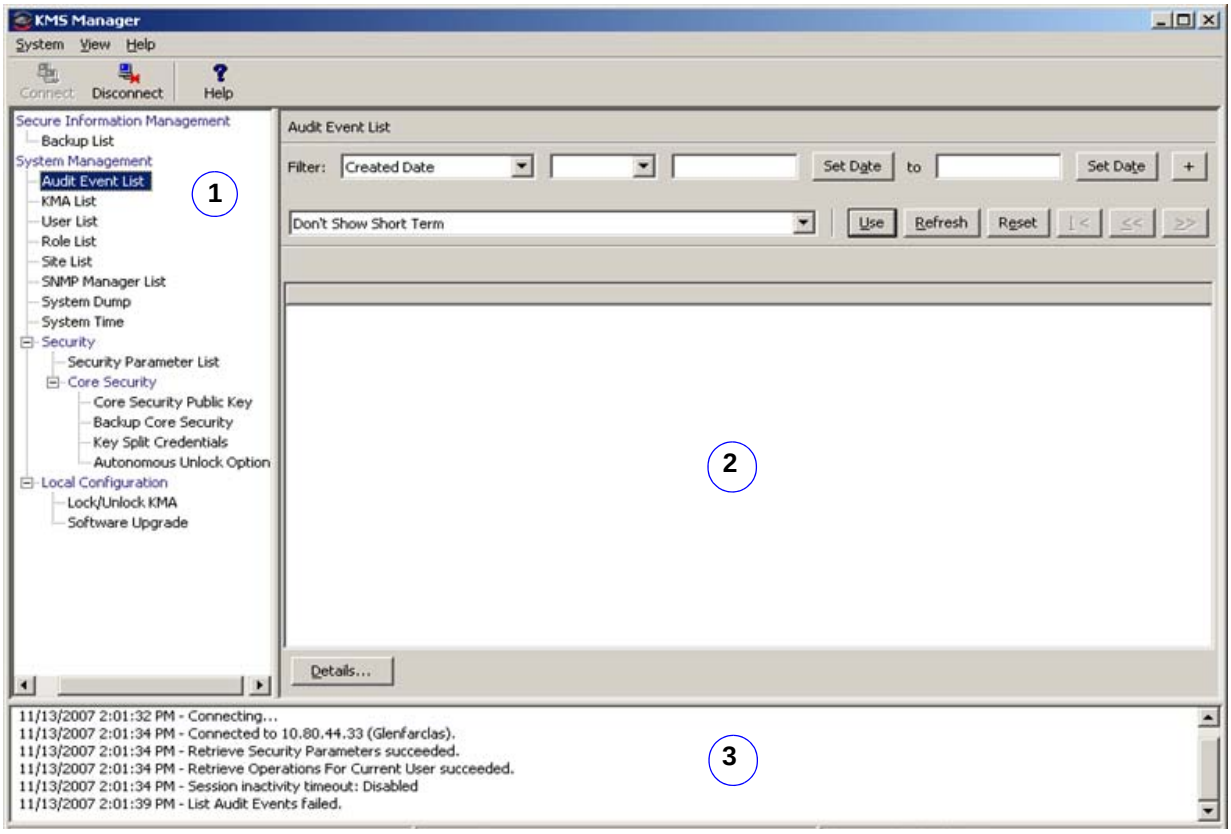
■ SE = Systems engineer
■ PS = Professional services representative
■ Service = Customer services representative (Svc Rep)
■ Customer = System administrators, network administrators, system programmers, operators

KMS Manager

The KMS 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 selection on the left.
3. On the bottom is a session events pane.

TABLE 3-5 KMS Manager Display



The KMS 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 44).

The KMS 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

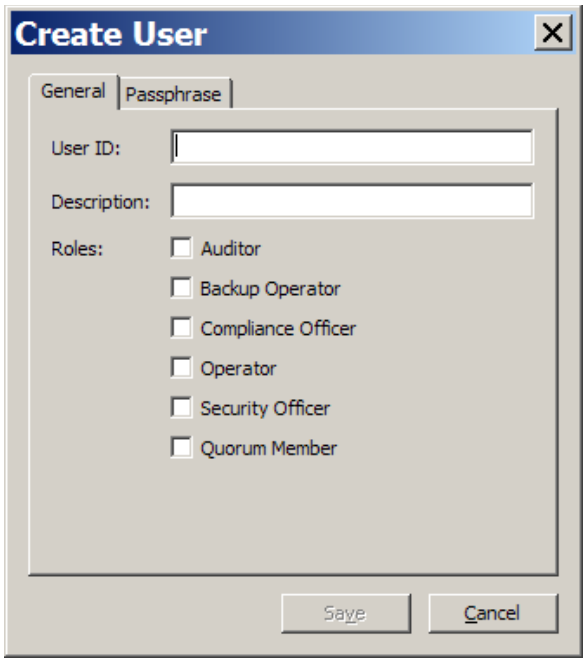
The KMS manager defines and uses the following roles. Completing and assigning roles is a customer task, service representatives should only advise.

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

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

FIGURE 3-2 shows an example of the Users Detail screen.
Use TABLE 3-7 on page 49 to help prepare for the assignments.

FIGURE 3-2 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 45 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 KMS into Cluster	Quorum					
Set User's Passphrase	Yes					
Reset KMA	Yes					
Zeroize KMA	Yes					
Logout	Yes	Yes	Yes	Yes	Yes	Yes
Connect						
Log In	Yes	Yes	Yes	Yes	Yes	Yes
Create Profile	Yes	Yes	Yes	Yes	Yes	Yes
Delete Profile	Yes	Yes	Yes	Yes	Yes	Yes
Set Config Settings	Yes	Yes	Yes	Yes	Yes	Yes
Disconnect	Yes	Yes	Yes	Yes	Yes	Yes
Key Split Credentials						
List	Yes					
Modify	Quorum					
Autonomous Unlock						
List	Yes					
Modify	Quorum					
Lock/Unlock KMA						
List Status	Yes	Yes	Yes	Yes	Yes	
Lock	Yes					
Unlock	Quorum					

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

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

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

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

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

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

TABLE 3-7 User Roles Work Sheet

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

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

Preparing the Tape Drives

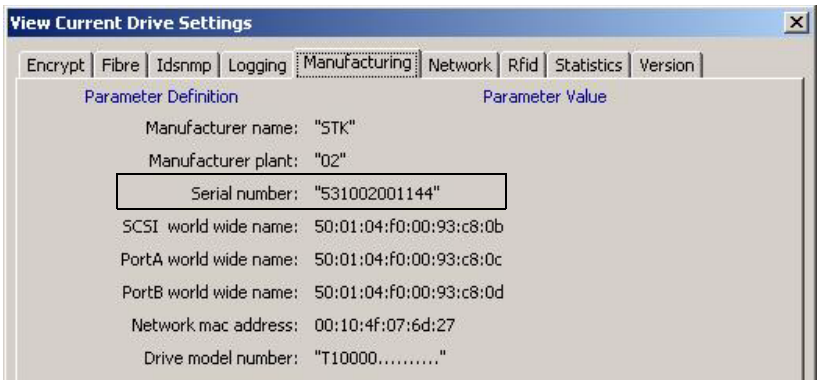
The tape drives should be installed and tested in their appropriate configuration before adding the encryption capability to them. Each drive-type has its own requirements.

T-Series Drive Data Preparation

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

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

FIGURE 3-3 Tape Drive Serial Number—VOP



2. Use "Tape Drives Work Sheet" on page 90 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 3-4 Request an Encryption Key Application

Access is Restricted: You must be an employee, complete the KMS 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 3-5 Encryption File Request for Drive Data

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

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

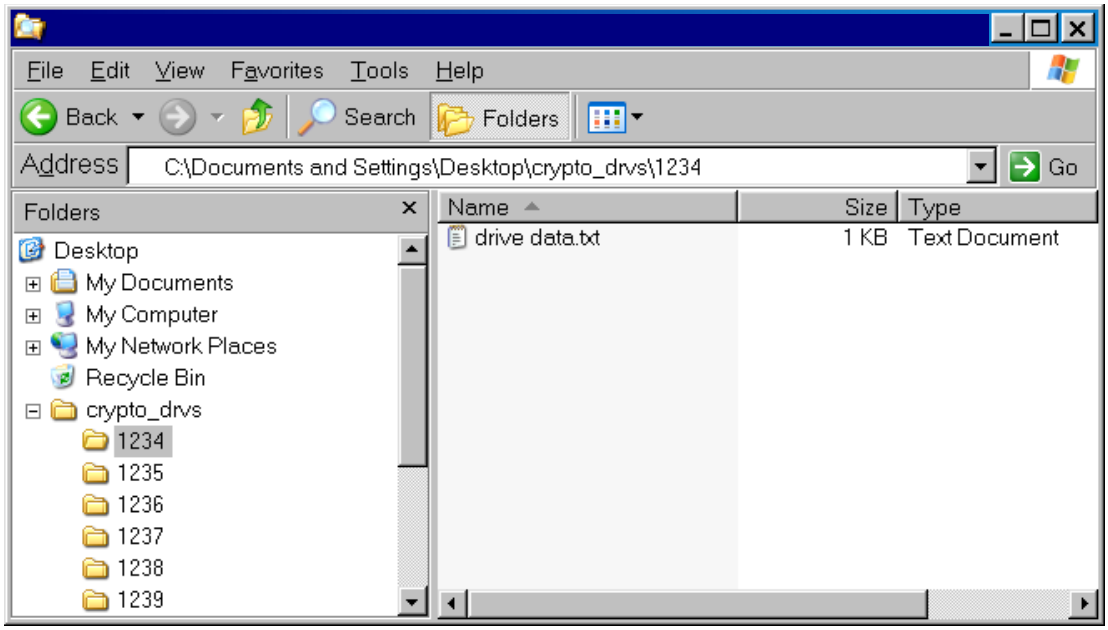
5. Continue with this process until you obtain all the drive data files for each tape drive you are going to enable.

Create a Drive Data File Structure

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

1. FIGURE 3-6 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 3-6 Drive Data File Structure



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

4. Complete "Agent Enrollment Work Sheet" on page 91 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** (KMS 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.

LTO4 Tape Drive Preparation

No enablement requirements or drive data is required for the LTO4 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 KMS manager.

Note – The Virtual Operator Panel must be at:

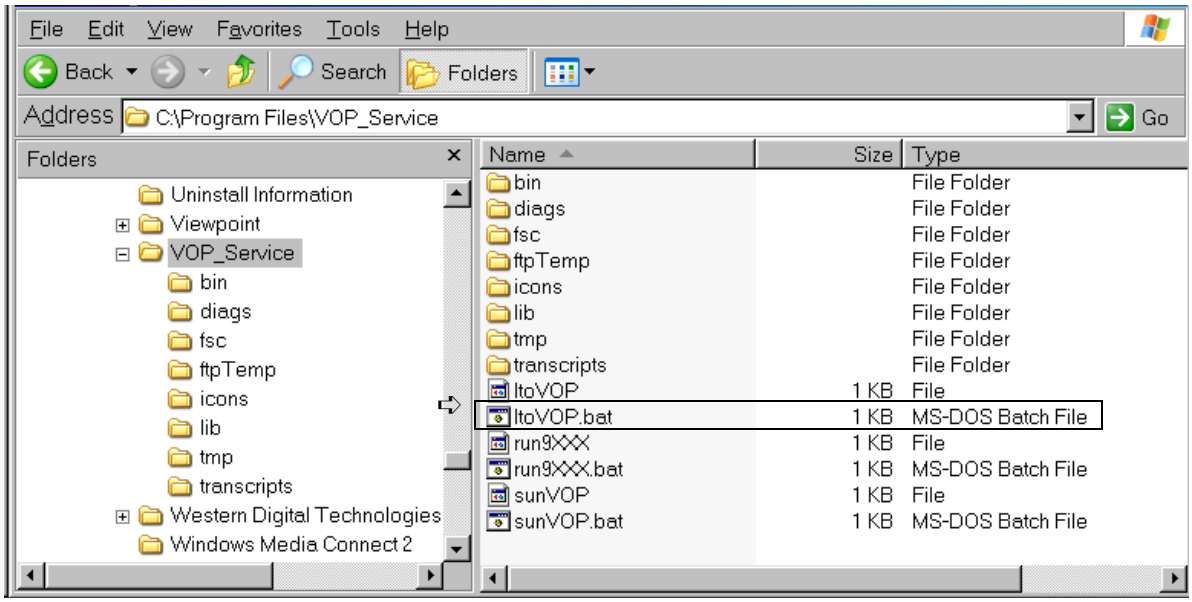
- Version 1.0.12 and higher to provide support for the HP LTO4 tape drive.
- Version 1.0.14 and higher to provide support for the IBM LTO4 tape drive.

To use the VOP for LTO4 tape drives, you need to launch a special file:

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

FIGURE 3-7 shows an example of the VOP 1.0.12 download contents.

FIGURE 3-7 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
- Virtual Operator Panel for HP LTO4 tape drives at Version 1.0.12 or higher
- Virtual Operator Panel for IBM LTO4 tape drives at Version 1.0.14 or higher

Supported Platforms and Web Browsers

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

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

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

TABLE 3-8 Operating Systems and Web Browsers

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

Required Firmware Levels

The *minimum* firmware requirements include:

TABLE 3-9 Firmware Compatibilities

Component	Version	Version	Version			
KMS Version 2.x	2.02	2.1	2.2			
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**	**9310/9311**	**SL500**	**VOP**
T10000A FC	L–3.11c D–137113	L–FRS_2.00 D–137113	L–3.17.03 D–137113	L–4.4.08 D–137113	n/a	1.0.11
T10000A FICON	L–3.11c D–137114	L–FRS_2.00 D–137114	L–3.17.03 D–137114	L–4.4.08 D–137114	n/a	1.0.11
T10000B FC	L–3.98b D–138x07	L–FRS_2.00 D–138x07	L–3.17.03 D–138x07	n/a	n/a	1.0.12
T10000B FICON	L–3.98b D–138x09	L–FRS_2.00 D–138x09	L–3.17.03 D–138x09	n/a	n/a	1.0.12
T9840D FC	L–3.98 D–142x07	L–FRS_2.00 D–142x07	L–3.17.03 D–142x07	L–4.4.08 D–142x07	n/a	1.0.12
T9840D FICON & ESCON	L–3.98 D–142x07	L–FRS_2.00 D–142x07	L–3.17.03 D–142x07	L–4.4.08 D–142x07	n/a	1.0.12
HP LTO4	L–3.98B D–H58s F (FC only)	L–2.05 D–H58s F (FC only)	n/a	n/a	L–1300 SPS D–H58s F D–B57s S	1.0.12
Dione Card	Firmware level: 1.20					
IBM LTO4	L–FRS_4.70 D–94D7 (FC only)	L–FRS_2.30 D–94D7 (FC only)	n/a	n/a	L–1373 D–94D7 (FC only)	1.0.14
Belisarius Card	Firmware level: 1.31.19					

Legend:

L–Library firmware level
D–Drive firmware level
H58s F = Fibre Channel firmware (HP LTO4)
B57s S = SCSI firmware (HP LTO4)
FC = Fibre Channel
SPS = Special firmware. Requires approval.
n/a = Not supported. Not applicable.

CHAPTER 4

Ordering

This chapter contains the order numbers and descriptions for the Sun StorageTek Crypto Key Management System (KMS) Version 2.x.

Supported Configurations

The following components can be ordered to support customer requirements and configurations for the StorageTek Version 2.0 encryption solution:

- "Key Management Appliance" on page 58
  This is a *require*d component for key creation, management, and assignments.

If you are implementing an encryption solution using a StorageTek library, review the following information and requirements:

- "SL8500 Modular Library System" on page 59
- "SL3000 Modular Library System" on page 60
- "SL500 Modular Library System" on page 61
- "9310 Automated Cartridge System" on page 62
- "L-Series Libraries" on page 63

If you are implementing an encryption solution using tape drives in a rack or standalone configuration, review the following information and requirements:

- "Rack Mount" on page 64

Supported Tape Drives

The currently supported tape drives include:

- T10000A
- T10000B
- T9840D
- HP LTO4
- IBM LTO4

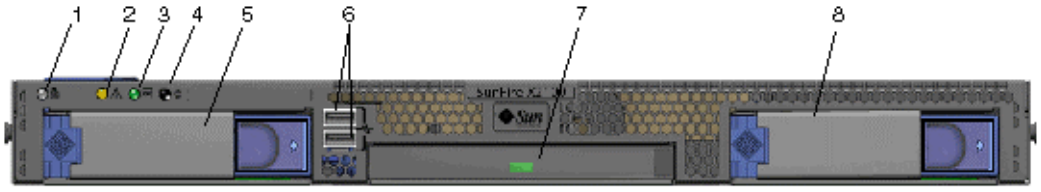
See "Tape Drive and Media Comparison" on page 20 for drive specifications and "Required Firmware Levels" on page 55 for supported firmware versions.

Key Management Appliance

The key management appliance order number is: **CRYPTO-KMA-2-Z,** which includes:

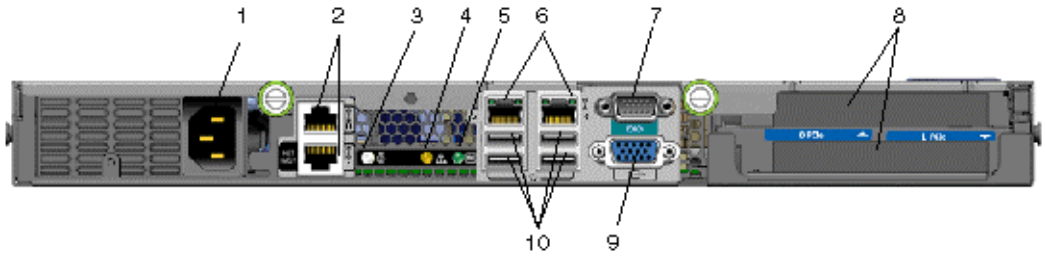
- Key Management Appliance (KMA) includes an SCA600 card
- Based on either a SunFire X2100 or X2200 Server
- Rackmount Model
- Pre-loaded Solaris 10 operating system and key management system software

FIGURE 4-1 Key Management Appliance—Front Panel



1. System identification button/LED
2. Fault LED
3. Power/OK LED
4. Power button
5. USB 2.0 connectors (2)
6. CD/DVD drive (not populated)
7. Hard drive (only one bay is populated)

FIGURE 4-2 Key Management Appliance—Rear Panel



1. Power connector
2. Ethernet connectors (2)
   Top = KMS Manager Network (LAN 0)
   Bottom = Embedded Lights Out Manager (ELOM)
3. Identify LED (blue)
4. Fault LED (red)
5. Power LED (green)
6. Ethernet connections (2)
   Left = Service Network (LAN 2)
   Right = Aggregate Service Network (LAN 3)
7. Serial port (ELOM connection)
8. PCIe slots
   Top = SCA6000 random number generator
   Bottom = Blank (empty)
9. VGA connector (if using a monitor and keyboard for the initial configuration)
10. USB 2.0 ports (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:
- 100,000 tape cartridges
- 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

* Supports Partitioning

The SL8500 provides internal rack space for the addition of the encryption hardware.

Order Number	Description
CRYPTO-2X-SL8500-Z-N	SL8500 accessory kit. **Note:** If the customer wants to install the encryption hardware—such as the KMAs and network switches—inside the SL8500 library, make sure the library has accessory racks to hold the equipment. A minimum of 2 racks with a 2N power configuration are required for redundant power features. **Rack component order numbers:** XSL8500-RACK-N = 6RU Rack XSL8500-RACK-HW-N = Rack component hardware kit XSL8500-AC-SW-N = AC Transfer Switch

Firmware Levels

Library	FRS_3.72 (FRS_3.98 or higher is recommended and to support LTO4) FRS_4.70 (current)
StreamLine Library Console	3.38
Tape Drives: ■ T10000A ■ T10000B ■ T9840D ■ HP LTO4 ■ IBM LTO4	 1.34.208 or higher 1.38.x07 or higher 1.42.104 or higher H45S Fibre Channel 94D7 Fibre Channel
Virtual Operator Panel (VOP)	Version 1.0.11 or higher Version 1.0.12 or higher for HP LTO4 Version 1.0.14 or higher for IBM LTO4

SL3000 Modular Library System

FIGURE 4-4 SL3000 Modular Library System Requirements

High-level Description: The SL3000 library offers customers the benefits of: ■ Scalability in storage capacity from 200 to 5800 slots ■ Performance from 1 to 56 tape drives ■ Heterogeneous attachments using standard interfaces (Ethernet and Fibre Channel) ■ Multiple library management software options	**Operating System Support:** The SL3000 supports all major operating systems: enterprise *and* open systems. **Host-to-Library Interface:** ■ Single Ethernet* (TCP/IP) 1x ■ Dual TCP/IP* (optional feature) 2x ■ Fibre Channel* (dual port optional feature) 2x * Supports Partitioning

Order Number	**Description**
■ SL3000 Kit 1 XSL3000-ETHRNT1-N ■ SL3000 Kit 2 XSL3000-ETHRNT2-N ■ SL3000 Kit 3 XSL3000-ETHRNT3-N ■ SL3000 Kit 4 XSL3000-ETHRNT4-N	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	Firmware Level or Higher
Library	FRS_2.0.2 FRS_2.30 (current)
StreamLine Library Console	4.0
Tape Drives: ■ T10000A ■ T10000B ■ T9840D ■ HP LTO4 ■ IBM LTO4	 1.34.208 or higher 1.38.x07 or higher 1.42.104 or higher H58S Fibre Channel or higher 94D7 Fibre Channel or higher
Virtual Operator Panel (VOP)	Version 1.0.11 or higher Version 1.0.12 or higher for HP LTO4 Version 1.0.14 or higher for IBM LTO4

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

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	SL500 base library *(required)*.
CRYPTO-2X-SL500X-N	SL500 expansion modules (*optional*) 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. ■ With 4 expansion modules, there is no room for the encryption hardware and customers may need to order an external rack.
Firmware Levels	Firmware Level or Higher
Library	i15 — 1300 i16 — 1373 i17 — 139x
Tape Drives: ■ HP LTO4 ■ IBM LTO4	 Fibre Channel: H58S or SCSI: B57S Fibre Channel: 94D7 SCSI interface: Not supported
Virtual Operator Panel (VOP)	Version 1.0.12 or higher for HP LTO4 Version 1.0.14 or higher for IBM LTO4

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-N 9310 libraries require:	9310 accessory kit. Includes Ethernet switches plus cabling. **Important:** This kit include the hardware for the first 9741e. If customer has more than one 9741E they must order additional 9741E accessory kits.
CRYPTO-2X-9741E-N	9741E Drive Cabinet accessory kit. Includes 24-port switch and cabling. **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 Feature Codes:	The 9310 requires upgrades to support the T10000 tape drive. 93T1—LSM upgrade (firmware and hardware) 93T1—LMU upgrade (firmware only) XT10—Hardware kit upgrade (9741E cabinet)
Library Firmware (minimum)	9311: 4.4.06 9330: TCP/IP - 2.1.02 code 9330: 3270 - 1.9.73 code
Tape Drives: ■ T10000A ■ T10000B ■ T9840D	 1.34.208 or higher 1.38.x07 or higher 1.42.104 or higher
Virtual Operator Panel (VOP)	Version 1.0.11 or higher

L-Series Libraries

Note – The L-Series libraries (L700 and L1400) do not support LTO4 encryption.

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** T10000 tape drives.
- *Dual frame* libraries holds
  - From 1,344 tape cartridges and
  - Up to **24** T10000 tape drives.

Operating System Support:
Supports open system platforms, such as UNIX, Windows NT, Novell, 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	L700/1400 accessory kit. Includes a 16-port switch, and cabling. **Note:** Depending on the number of tape drives installed, you may need to order an additional switch.
Firmware Levels	Firmware Level or Higher
Library (minimum) ■ L700e / L1400	 3.11.02 or higher
Tape Drives: ■ T10000A ■ T10000B ■ T9840D	 1.34.208 or higher 1.38.x07 or higher 1.42.104 or higher
Virtual Operator Panel (VOP)	Version 1.0.11 or higher Version 1.0.12 or higher

Rack Mount

FIGURE 4-8 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.

Order Number	Description
CRYPTO-2X-RACK-Z-N	StorageTek rack mount kit. Include 16-port switch and cabling.
Firmware Levels	Firmware Level or Higher
Tape Drives: ■ T10000A ■ T10000B ■ T9840D	 1.34.208 or higher 1.38.x07 or higher 1.42.104 or higher
Virtual Operator Panel (VOP)	Version 1.0.11 or higher

Order Numbers, Descriptions, and Contents

TABLE 4-1 through TABLE 4-7 on page 74 provide information about ordering components, field replaceable units (FRUs) spares, x-options (conversion bills), and service options for the StorageTek encryption solutions.

TABLE 4-1 KMS 2.x Core Parts (Sheet 1 of 2)

Numbers		Product		
Marketing	**Manufacturing**	**Description**	**Category**	**Details**
CRYPTO-KMA-2-Z-N	CRYPTO-KMA-2-Z	KMA 2.0 rack mounted server	TAPE LIB	StorageTek crypto KMA appliance rack mount model, pre-loaded Solaris, rack mounting hardware, client GUI CD. RoHS 5 compliant.
CRYPTO-X-16PT-Z	CRYPTO-X-16PT-Z	16PT ethernet switch	TAPE LIB	StorageTek 16PT ethernet switch. No mounting HW or cables. RoHS 5 compliant.
CRYPTO-X-24PT-Z-N	CRYPTO-X-24PT-Z	24PT ethernet switch	TAPE LIB	StorageTek 24PT ethernet switch. No mounting HW or cables. RoHS 5 compliant.
X-CRYPTO-1XTO2XUPZ-N	X-CRYPTO-1XTO2X	1.x to 2.0 Crypto upgrade kit	TAPE LIB	StorageTek crypto KMA appliance rack mount model, with mounting HW, pre-loaded Solaris. Client management GUI CD. RoHS 5 compliant.
CRYPTO-2X-9310-Z-N	CRYPTO-2X-9310-	Crypto kit for 9310 libraries	TAPE LIB	StorageTek crypto kit for use with 9310 libraries. 24-port ethernet switch and cables in 9310 plus 16-port ethernet switch and cables for connection to KMA externally. Rack mounting HW. RoHS 5 compliant.
CRYPTO-2X-9741E-N	CRYPTO-2X-9741E	Crypto kit for one 9741E cabinet	TAPE LIB	StorageTek crypto kit for use with 9310 libraries. 24-port ethernet switch, cables, and rack mount HW for 9741E cabinet. One required for each additional 9741E cabinet used for crypto. RoHS 5 compliant.
CRYPTO-2X-L7/14-N	CRYPTO-2X-L7/14	Crypto kit for L-series libraries	TAPE LIB	StorageTek crypto kit for use with L-Series libraries. 16-port ethernet switch, cables, and mounting HW for L-series libraries. RoHS 5 compliant.
CRYPTO-2X-SL500B-N	CRYPTO-2X-SL500	Crypto kit for SL500 library base	TAPE LIB	StorageTek crypto kit for use with SL500 library base. Ethernet switch and cables for SL500 library. RoHS compliant.

TABLE 4-1 KMS 2.x Core Parts (Sheet 2 of 2)

Numbers		Product		
Marketing	**Manufacturing**	**Description**	**Category**	**Details**
CRYPTO-2X-SL500X-N	CRYPTO-2X-SL500	Crypto kit for SL500 library expansion	TAPE LIB	StorageTek crypto kit for use with SL500 library expansion. Ethernet cables for SL500 library. RoHS compliant.
CRYPTO-2X-SL8500-N	CRYPTO-2X-SL850	Crypto kit for SL8500 library	TAPE LIB	StorageTek crypto kit for use with SL8500 libraries. 24-port ethernet switch, cables, and rackmount HW for SL8500 library. RoHS 5 compliant.
XSL3000-ETHRNT1-N	XSL3000-ETHRNT1	SL3000 Drv E-Switch harness 1	STK	StorageTek SL3000 X-Option, Ethernet Switch for Tape Drives, Includes cable harness for 8 drives, Supports 1st Drive Array in BM or DEM, BM Drives 1-8, DEM Drives 25-32, Used with T9840 and T10000 Drives, Needed for SDP and Encryption, Supports Drive Code Loads, Includes Power Cable, Includes Ethernet Switch Harness A/B, RoHS-5
XSL3000-ETHRNT2-N	XSL3000-ETHRNT2	SL3000 Drv E-Switch harness 2	STK	StorageTek SL3000 X-Option, 8 Drive Ethernet Cable Harness, Requires XSL3000-ETHRNT1-Z, Supports 2nd Drive Array in BM or DEM, BM Drives 9-16, DEM Drives 33-40, Used with T9840 and T10000 Drives, Needed for SDP and Encryption, Supports Drive Code Loads, Includes Power Cable and Switch Harness B/C, RoHS-5
XSL3000-ETHRNT3-N	XSL3000-ETHRNT3	SL3000 Drv E-Switch harness 3	STK	StorageTek SL3000 X-Option, Ethernet Switch for Tape Drives, Includes cable harness for 8 drives, Typically requires XSL3000-ETHRNT1-Z and XSL3000-ETHRNT2-Z, Supports 3rd Drive Array in BM or DEM, BM Drives 17-24, DEM Drives 41-48, Used with T9840 and T10000 Drives, Needed for SDP and Encryption, Supports Drive Code Loads, Includes Power Cable and Switch Harness A/C, RoHS-5
XSL3000-ETHRNT4-N	XSL3000-ETHRNT4	SL3000 Drv E-Switch harness 4	STK	StorageTek SL3000 X-Option, 8 Drive Ethernet Cable Harness, Requires XSL3000-ETHRNT4-Z, Supports 4th Drive Array in DEM, DEM Drives 49-56, Not needed in BM, Used with T9840 and T10000 Drives, Needed for SDP and Encryption, Supports Drive Code Loads, Includes Power Cable, Includes Ethernet Switch Harness C/C, RoHS-5
XSL3000-IFC2-Z	XSL3000-IFC2-Z	SL3000 2Gb FC Interface Card	STK	StorageTek SL3000 X-Option, 2Gb FC Interface Card (MPU2), RoHS-5

TABLE 4-2 KMS 2.x Software Activation Keys (Sheet 1 of 2)

Numbers		Product		
Marketing	**Manufacturing**	**Description**	**Category**	**Details**
9840D-EKEY-A	9840D-EKEY-A	T9840D, EKEY A Activation	STK	StorageTek Conversion Bill, T9840D drive, encryption activation A. Tape drive offers fast access to 1st byte, 30 MB/sec native transfer rate, 75 GB native capacity, FC/FI/ES interface and backward read compatibility to legacy T9840A, B, and C written media. Encryption activation for a single drive attached to an installed base KMS instance.
9840D-EKEY-B	9840D-EKEY-B	T9840D, EKEY B Activation	STK	StorageTek Conversion Bill, T9840D drive, encryption activation B. Tape drive offers fast access to 1st byte, 30 MB/sec native transfer rate, 75 GB native capacity, FC/FI/ES interface and backward read compatibility to legacy T9840A, B, and C written media. Encryption activation for a single drive when encryption is purchased at the same time as the drive order.
T10A-2FI-EKEY-A	EOL: T10A-2FI-EKEY-A Use: T10K-EKEY-A/ T10K-EKEY-B	T10KA 2GbFI CryptoKey, After market	TAPE LIB	StorageTek Crypto Key for previously installed T10000A 2Gb FICON Crypto Channel Tape Drives. Used in conjunction with StorageTek Crypto Key Management System, Crypto Library Accessory Kits and Crypto Rackmount System. Includes Software Key for enabling encryption in the tape drive.
T10A-2FI-EKEY-B	EOL: T10A-2FI-EKEY-B Use: T10K-EKEY-A/ T10K-EKEY-B	T10KA 2GbFI Crypto Key, Bundled	TAPE LIB	StorageTek Crypto Key for new (bundled) T10000A 2Gb FICON Crypto Channel Tape Drive purchases. Used in conjunction with StorageTek Crypto Key Management System, Crypto Library Accessory Kits and Crypto Rackmount System. Includes Software Key for enabling encryption in the tape drive.
T10A-4FC-EKEY-A	EOL: T10A-4FC-EKEY-A Use: T10K-EKEY-A/ T10K-EKEY-B	T10KA 4Gb Crypto Key, After market	TAPE LIB	StorageTek Crypto Key for previously installed T10000A 4Gb Fibre Channel and 2Gb FICON Tape Drives. Used in conjunction with StorageTek Crypto Key Management Station, Crypto Library Accessory Kits and Crypto Rackmount System. Includes Software Key for enabling encryption in the tape drive.

TABLE 4-2 KMS 2.x Software Activation Keys (Sheet 2 of 2)

Numbers		Product		
Marketing	**Manufacturing**	**Description**	**Category**	**Details**
T10A-4FC-EKEY-B	EOL: T10A-4FC-EKEY-B Use: T10K-EKEY-A/ T10K-EKEY-B	T10KA 4Gb Crypto Key, Bundled	TAPE LIB	StorageTek Crypto Key for new (bundled) T10000A 4Gb Fibre Channel and 2Gb FICON Tape Drive purchases. Used in conjunction with StorageTek Crypto Key Management Station, Crypto Library Accessory Kits and Crypto Rackmount System. Includes Software Key for enabling encryption in the tape drive.
T10K-EKEY-A-N	T10K-EKEY-A	C/B,ENCRYPT ACTIVATION, T10 DRV	LIBRARY	StorageTek field upgrade activation of encryption capability on T10000 tape drive after original tape drive.
T10K-EKEY-B-N	T10K-EKEY-B	C/B,ENCRYPT ACTIVATION, T10 DRV	LIBRARY	StorageTek bundled activation of encryption capability on T10000 tape drive concurrent with original tape drive.
HP-LTO4-EKEY-A-N	HP-LTO4-EKEY-A	HP LTO4 drive feature A	TAPE LIB	Drive crypto feature enablement key sold after market for HP LTO4 drive.
HP-LTO4-EKEY-B-N	HP-LTO4-EKEY-B	HP LTO4 drive feature B	TAPE LIB	Drive crypto feature enablement key bundled with HP LTO4 drive at initial sale.
IBM-LTO4E-EKEY-N	IBM-LTO4E-EKEY	IBM LTO4 drive feature	TAPE LIB	Drive crypto feature enablement key bundled with IBM LTO4 drive at initial sale.

TABLE 4-3 Tape Drive Order Numbers (Sheet 1 of 2)

Numbers		Product		
Marketing	**Manufacturing**	**Description**	**Category**	**Details**
LTO4E-HP4FC-SL30-N	LTO4E-HP4FC-SL3	LTO4 HP FC 4Gb SL3000 EncrypDr	STK	HP LTO4 FC 4Gb Encryption drive for SL3000 ■ Featuring 120 MB/Sec transfer rate, 800 GB native capacity ■ Must order cables separately ■ RoHS 5 compliant
LTO4E-HP4FC-SL500-N	LTO4E-HP4FC-SL5	LTO4 HP FC 4Gb SL500 EncrypDr	STK	HP LTO4 FC 4Gb Encryption drive for SL500 ■ Featuring 120 MB/Sec transfer rate, 800 GB native capacity ■ Must order cables separately ■ RoHS 5 compliant
LTO4E-HP4FC-SL85-N	LTO4E-HP4FC-SL8	LTO4 HP FC 4Gb SL8500 EncrypDr	STK	HP LTO4 FC 4Gb Encryption drive for SL8500 ■ Featuring 120 MB/Sec transfer rate, 800 GB native capacity ■ Must order cables separately ■ RoHS 5 compliant
LTO4E-HPSC-SL500-N	LTO4E-HPSC-SL50	LTO4 HP SCSI SL500 EncrypDr	STK	HP LTO4 SCSI Encryption drive for SL500 ■ Featuring 120 MB/Sec transfer rate, 800 GB native capacity ■ Must order cables separately ■ RoHS 5 compliant
LTO4E-IB4FC-SL500-N	LTO4E-IB4FC-SL5	LTO4 IBM FC 4Gb SL500 EncrypDr	STK	IBM LTO4 FC 4Gb Encryption drive for SL500 ■ Featuring 120 MB/Sec transfer rate, 800 GB native capacity ■ Must order cables separately ■ RoHS 5 compliant
LTO4E-IB4FC-SL30-N	LTO4E-IB4FC-SL3	LTO4 IBM FC 4Gb SL3000 EncrypDr	STK	IBM LTO4 FC 4Gb Encryption drive for SL3000 ■ Featuring 120 MB/Sec transfer rate, 800 GB native capacity ■ Must order cables separately ■ RoHS 5 compliant

TABLE 4-3 Tape Drive Order Numbers (Sheet 2 of 2)

Numbers		Product		
Marketing	**Manufacturing**	**Description**	**Category**	**Details**
LTO4E-IB4FC-SL85-N	LTO4E-IB4FC-SL8	LTO4 IBM FC 4Gb SL8500 EncrypDr	STK	IBM LTO4 FC 4Gb Encryption drive for SL8500 ■ Featuring 120 MB/Sec transfer rate, 800 GB native capacity ■ Must order cables separately ■ RoHS 5 compliant
Drive Upgrade Kits				
T10A-2GBCRYP-85UPZ	T10A-2GBCRYP-85	T10KA 2GB FICRYP8500 ONLY UPGD	STK	StorageTek T10000A 2Gb FICON to 2Gb FICON encryption upgrade kit. This kit is for SL8500 only, ROHS-5
T10A-2GBCRYP-UPGDZ	T10A-2GBCRYP-UP	T10KA 2GB FI CRYPTO ONLY UPGD	STK	StorageTek T10000A 2Gb FICON to 2Gb FICON encryption upgrade kit. This kit is for all libraries, ROHS-5
XHPLTO4E-FCUP3085-N	XHPLTO4E-FCUP30	HP LTO4 FC drive upgd SL30/85	TAPE LIB	HP LTO4 FC encryption drive upgrade for SL3000 and SL8500 ■ Serial to Ethernet interface card, cabling, back-plate. ■ RoHS compliant.
XHPLTO4E-FCUPL500-N	XHPLTO4E-FCUPL5	HP LTO4 FC drive upgd SL500	TAPE LIB	HP LTO4 FC encryption drive upgrade for SL500. ■ Serial to Ethernet interface card, cabling, back-plate. ■ RoHS compliant.
X-HPLTO4E-SCUP500-N	X-HPLTO4E-SCUP5	HP LTO4 SCSI drive upgd SL500	TAPE LIB	HP LTO4 SCSI encryption drive upgrade for SL500. ■ Serial to Ethernet interface card, cabling, back-plate. ■ RoHS compliant.
XIBLTO4E-FCUPL500-N	XIBLTO4E-FCUPL5	IBM LTO4 FC drive upgd SL500	TAPE LIB	IBM LTO4 FC encryption drive upgrade for SL500. ■ Serial to Ethernet interface card, cabling, drive tray back-plate. ■ Need serial# of existing drive tray. ■ RoHS compliant.
XIBLTO4E-FCUP3085-N	XIBLTO4E-FCUP30	IBM LTO4 FC drive upgd SL30/85	TAPE LIB	IBM LTO4 FC encryption drive upgrade for SL3000 and SL8500 ■ Serial to Ethernet interface card, cabling, drive tray back-plate. ■ Need serial# of existing drive tray. ■ RoHS compliant.

TABLE 4-4 Service Order Numbers (Sheet 1 of 2)

Numbers		Product		
Marketing	**Manufacturing**	**Description**	**Category**	**Details**
EIS-CRYPTO-E	**EIS-CRYPTO-E**	Install Crypto Kit	SERVICE	Crypto Kit into new or existing StorageTek library during local business hours
EIS-CRYPTO-E-AH	**EIS-CRYPTO-E**	Install Crypto Kit AH	SERVICE	Crypto Kit into new or existing StorageTek library after local business hours
EIS-CRYPTOSTAT-E	EIS-CRYPTOSTAT-	Install Crypto Station	SERVICE	Crypto Station into new or existing StorageTek library during local business hours
EIS-CRYPTOSTATE-AH	EIS-CRYPTOSTATE	Install Crypto Station AH	SERVICE	Crypto Station into new or existing StorageTek library after local business hours
IWU-T1AKMS-1G	IWU-T1AKMS-1G	STK CRYP-T10K MGMT UG 1YR GOLD	SERVICE	StorageTek Crypto Key Management Station upgrade to 1 year of Gold support.
IWU-T1AKMS-1P	IWU-T1AKMS-1P	STK CRYP-T10K MGMT UG 1YR PLAT	SERVICE	StorageTek Crypto Key Management Station upgrade to 1 year of Platinum support.
IWU-T1AKMS-1S	IWU-T1AKMS-1S	STK CRYP-T10K MGMT UG 1YR SLVR	SERVICE	StorageTek Crypto Key Management Station upgrade to 1 year of Silver support.
IWU-T1AKMS-24-1G	IWU-T1AKMS-24-1	STK CRYP-T10K MGMT UGOS 1Y GLD	SERVICE	StorageTek Crypto Key Management Station upgrade to 1 year of Gold 7x24 support.
NWS-3502	NWS-3502	Sun STK KMS Crypto Key Mgt Adm	SERVICE	StorageTek KMS Crypto Key Management Administration
NWS-3506	NWS-3506	Sun STK Crypto KMS 1.2 Admin	SERVICE	StorageTek Crypto Key Management Station (KMS) 1.2 Administration
NWS-3507	NWS-3507	Sun STK Crypto KMS 2.0 Admin	SERVICE	StorageTek Crypto Key Management Station (KMS) 2.0 Administration

TABLE 4-4 Service Order Numbers (Sheet 2 of 2)

Numbers		Product		
Marketing	**Manufacturing**	**Description**	**Category**	**Details**
WW-PS-ARCH-ENCRYPT	WW-PS-ARCH-ENCR	Encrypt Ready Assess	SERVICE	The Encryption Readiness Assessment provides services to bring a customer into a state of being prepared to take on a new storage encryption product. The service assists in encryption key management lifecycle, Storage policy Alignment, encryption roles and responsibilities and Best practices for storage encryption.
WW-PS-ENCR3-CUSTOM	WW-PS-ENCR3-CUS	Encryption Consulting Custom	SERVICE	The StorageTek Encryption Consulting Service helps Customer perform a security risk analysis, select an encryption vendor, and implement a encryption solution. Customized service will provide Customer with support in areas Customer does not have expertise (ie: assessing threats, identifying and engaging security vendors, conducting proof-of- concept trials or implementing and testing a solution. This custom engagement is tailored to Customer requirements to determine scope and price.
WW-PS-INTG-KMS	WW-PS-INTG-KMS	KMS Integration Service	SERVICE	The Key Management Station (KMS) Integration Service provides an integration of the KMS hardware and software into the encryption capable tape back-up and archive solution.

Professional Services

Professional Services Encryption Implementation is a requirement; one per site.

TABLE 4-5 Professional Services Ordering Instructions and Part Numbers

Order Number	Description
Important: Professional Services is required for new installations.	
❑ **WW-PS-INTG-KMS**	**KMS Integration Service**
The **Key Management System Integration Service** provides an integration of the KMS hardware and software into the encryption capable tape back-up and archive solution. **Note:** This service is required for any new tape encryption installation.	
❑ **WW-PS-ARCH-ENCRYPT**	**Encrypt Ready Assess**
The **Encryption Readiness Assessment** provides services to bring a customer into a state of being prepared to take on a new storage encryption product. The service assists in encryption key management lifecycle, Storage policy Alignment, and encryption roles.	

TABLE 4-6 Spares Order Numbers

Numbers		Product		
Marketing	**Manufacturing**	**Description**	**Category**	**Details**
#3154936-Z	#3154936-Z	Spares, KMA appliance only.	STK	StorageTek spares, KMA crypto appliance with Solaris and crypto only no slide rack, cabling or related hardware. RoHS compliant.
#371-0991	#371-0991	Spares, CRYPTO ACCEL 500 SF V240	N32	Spare Hardware Cryptographic Module (Crypto Accelerator 500) for the SunFire V125, V210, V240. RoHS-5 Compliant. X7405A-4
#375-3089	#375-3089	#FRU CRYPTO Accelerator1000	NW BOARDS	Sun Crypto Accelerator 1000 X6762A Transferred 6/19/2006
6000A	6000A	Sun Crypto Accelerator 6000	NW BOARDS	Sun Crypto Accelerator 6000 SSL/IPsec Accelerator with key store and FIPS support, PCIe card. RoHS-6 compliant. Low Profile.
6010A	6010A	Sun Crypto Accelerator 6000	NW BOARDS	Sun Crypto Accelerator 6000 SSL/IPsec Accelerator with key store and FIPS support, PCIe card. RoHS-6 compliant. Std brackets.
Ethernet Adapter Card—LTO4 Tape Drives				
		HP Ethernet Adapter Card	419954901	HP LTO4 Dione Card
#4186076		IBM Ethernet Adapter Card	418615102 418607602	IBM LTO4 Adapter card Packaged FRU FRU

TABLE 4-7 KMS 1.x Parts Order Numbers (Sheet 1 of 2)

Numbers		Product		
Marketing	**Manufacturing**	**Description**	**Category**	**Details**
CRYPTO-KMS-D-Z	CRYPTO-KMS-D-Z	Crypto KMS Desktop Appliance	TAPE LIB	StorageTek Crypto Key Management Station - Desktop Model. Includes Ultra 20 Workstation, Monitor, Token Bay, Token, Pre-loaded secure Solaris, Key Management Software and 100Gb USB external hard drive. Appropriate country kit must be ordered for keyboard/power. KMS Implementation Services required and ordered separately (part number WW-PS-INTG-KMS).
CRYPTO-L700-Z	CRYPTO-L700-Z	Crypto L180/700/1400 Kit	TAPE LIB	StorageTek Crypto L180/700/1400 Accessory Kit. For use with StorageTek Crypto Key Management System. Includes Token Bay, 2 Tokens, 16-port Switch and cabling.
CRYPTO-RACK-Z-N	CRYPTO-RACK-Z	Crypto Rackmount Kit	TAPE LIB	StorageTek Crypto Rackmount Kit. For use with StorageTek Crypto Key Management System. Includes Token Bay, 2 Tokens, 16-port Switch and cabling.
CRYPTO-TOKEN-Z	CRYPTO-TOKEN-Z	Crypto KMS Token	TAPE LIB	StorageTek Crypto Token. Secure key repository. For use with StorageTek Crypto Key Management Station and Library Accessory Kit token bays.
CRYPTO-X120-USB-Z	CRYPTO-X120-USB	USB 120GB External Hard Drive	TAPE LIB	Additional 120GB USB Disk Drive for secondary copy of key management database backup, for KMS 1.x, potentially for disaster recovery purposes. RoHS 5 Compliant.
CRYPTO-8500-HUB-Z	CRYPTO-8500-HUB	Crypto SL8500 Kit w/ Hub Only	TAPE LIB	StorageTek Crypto SL8500 Accessory Kit with Ethernet hub and cabling only. For use with StorageTek Crypto Key Management System. Includes 24-port Ethernet hub and cabling. Requires that customer already have Crypto SL8500 Accessory Kit with Rack (part being EOL-d 2/20/06) or without Rack (both include a Token Bay). Library should have separate Ethernet hub per rail.
CRYPTO-8500-RKNO-Z	CRYPTO-8500-RKN	Crypto SL8500 Kit without Rack	TAPE LIB	StorageTek Crypto SL8500 Accessory Kit without Rack. For use with StorageTek Crypto Key Management System. Includes Token Bay, 2 Tokens, 24-port Switch and cabling.

TABLE 4-7 KMS 1.x Parts Order Numbers (Sheet 2 of 2)

Numbers		Product		
Marketing	**Manufacturing**	**Description**	**Category**	**Details**
CRYPTO-9310-RK-Z	CRYPTO-9310-RK-	Crypto 9310 Kit with Rack	TAPE LIB	StorageTek Crypto 9310/L6000 Accessory Kit with Rack. For connection to 9741E cabinets in conjunction w/ StorageTek Crypto Key Management System. Includes Token Bay, 2 Tokens, 16-port Switch (for 9741e cabinet connect), 24-port Switch (for tape drive connect), 19" Rack and cabling. Supports connection to drives for a single 9741E. If customer has more than 1 9741E they must order 1 or more Crypto 9741E Accessory Kits.
CRYPTO-9741E-Z	CRYPTO-9741E-Z	Crypto 9741E Kit	TAPE LIB	StorageTek Crypto 9741E Accessory Kit. For connection to 9310/L6000 Accessory Kit in conjunction w/ StorageTek Crypto Key Management System. Includes 24-port Switch and cabling. Requires that customer has installed a Crypto 9310/L6000 Accessory Kit for the KMS to 9741E connection.
Spares				
#3144947-Z	#3144947-Z	Spares KMS Crypto key token	STK	StorageTek Spares Crypto Token. Secure key repository. Use with STK Crypto KMS and Lib Accessory Kit token bays. RoHS 6 Compliant.
#3144974-Z	#3144974-Z	Spares KMS workstation.	STK	StorageTek Spares Crypto KMS appliance desktop model with workstation, monitor, token bay, pre-loaded Solaris, token, 120GB USB external backup drive. RoHS-6 Compliant.
#3144987-Z	#3144987-Z	FRU, Token Bay, Desk Top	STK	StorageTek Spares Token Bay only, desktop for use with STK Crypto KMS. RoHS 6 Compliant.
#3144988-Z	#3144988-Z	FRU, Token Bay, Rack Mount, Front	STK	StorageTek Spares, Rack mounted (front) crypto token bay. RoHS 6 Compliant.
#3154719-Z	#3154719-Z	FRU, Token Bay, Rack Mount, Rear	STK	StorageTek Spares, Rack mounted (rear) crypto token bay. RoHS 6 Compliant.
594-4849-01	594-4849-01	1 TB Hard Disk drive		1 TB Hard Disk drive

Firmware Upgrades

TABLE 4-8 Firmware Upgrade and Instruction Part numbers

KMS Version 2.1	Description
316030302	KMS 2.1 FLAR
316059601	KMA 2.1 Installation Instructions and Release Notes
316059701	KMS 2.1 GUI for Windows
316059801	KMS 2.1 GUI for Solaris X86
316059901	KMA 2.1 code

KMS Version 2.2	Description
316030303	KMS 2.2 FLAR
316059602	KMA 2.2 Installation Instructions and Release Notes
316059702	KMS 2.2 GUI for Windows
316059802	KMS 2.2 GUI for Solaris X86
316059902	KMA 2.2 code

FLAR = Flash Archive

Power Cables

List external cables and power cords available for each model. Typically power cords are shipped with each unit, but are not structured in the CEI.

TABLE 4-9 Power Cables Order Numbers

Part Number	Description	Marketing
315495601	CORDSET, POWER, UL&CSA,15A,125V,X311L	X311L
315495701	CORDSET, POWER, EUROPE,10A,250V,X312L	X312L
315495801	CORDSET, PWR, SWITZERLAND,10A,250V,X314L	X314L
315495901	CORDSET, POWER, UK,10A,250V,X317L	X317L
315496001	CORDSET, POWER, TAIWAN,10A,5-15P,X332A	X332A
315496101	CORDSET, POWER, KOREAN,10A,250V,X321G	X312G
315496201	CORDSET, POWER, DENMARK,10A,25V,X383L	X383L
315496301	CORDSET, POWER, ITALY,10A,250V,X384L	X384L
315496401	CORDSET, POWER, AUSTRALIA,10A,250V,X386L	X386L
315496501	CORDSET, POWER, CHINESE,10A,250V,X328L	X328L

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

Tape Drive Instructions

See the specific tape drive Systems Assurance Guides for specific information.

TABLE 4-10 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 specific information.

TABLE 4-11 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

9310 Upgrades

TABLE 4-12 9310 Upgrade Ordering Instructions and Part Numbers

Order Number		Description
A T10000 software upgrade is required for each LSM (9310). The majority of customers already have the hardware needed for the T10000 tape drives; therefore, in most cases the firmware upgrade marketing part number should be ordered.		
❑	YXSL9310-T10K-FW	9310 Firmware upgrade for T10000
❑	YXSL9310-T10K-HW	9310 hardware CB for T10000
❑	YXSL9330-T10K	9330 Upgrade for T10000 One per LMU
❑	YX9741E-T10K-9310	C/B 9741E T10K Install 9310 One per cabinet

HP LTO4 Order Numbers

TABLE 4-13 HP LTO4 Order Numbers

Item	Number	Description
Marketing Numbers		
Encryption Keys	X-HP-LTO4-EKEY-B-N	One required per encryption enabled drive. Bundled with the drive at time of sale.
	X-HP-LTO4-EKEY-A-N	One required per encryption enabled drive. After market for previously purchased drives.
Warranty		1 year
X-Options		
Crypto **drive upgrade** for HP LTO4 FC SL500	XHPLTO4E-FCUPL500-N	Drive upgrade for HP LTO4 FC SL500
Crypto **drive upgrade** for HP LTO4 SCSI SL500	XHPLTO4E-SCUP500-N	Drive upgrade for HP LTO4 SCSI SL500
Crypto **drive upgrade** for HP LTO4 FC SL3000/SL8500	XHPLTO4E-FCUP3085-N	Drive upgrade for HP LTO4 FC SL3000/SL8500
LTO4 HP FC 4Gb **SL500** Encryption Drive	LTO4E-HP4FC-SL500-N	LTO4 HP FC 4Gb SL500 Encryp Dr
LTO4 HP SCSI 4Gb **SL500** Encryption Drive	LTO4E-HPSC-SL500-N	LTO4 HP SCSI SL500 Encryp Dr
LTO4 HP FC 4Gb **SL3000** Encryption Drive	LTO4E-HP4FC-SL30-N	LTO4 HP FC 4Gb SL3000 Encryp Dr
LTO4 HP FC 4Gb **SL8500** Encryption Drive	LTO4E-HP4FC-SL85-N	LTO4 HP FC 4Gb SL8500 Encryp Dr
HP Adapter Card (Dione card)		
Packaged FRU	419954901	HP LTO4 Dione Card

IBM LTO4 Order Numbers

TABLE 4-14 IBM LTO4 Order Numbers

Item	Number	Description
Marketing Numbers		
Marketing/Revenue Spare	**#4186076**	IBM LTO4 Adapter Card (Belisarius Card)
Encryption Keys	IBM-LTO4E-EKEY	One required per encryption enabled drive.
Warranty		1 year
X-Options		
Crypto **drive upgrade** for IBM LTO4 FC SL500	XIBLTO4E-FCUPL500-N CB: 003-5163-01 CB: 003-5164-01 CI: 418607401	IBM LTO4 FC encryption drive upgrade for SL500. ■ Serial to Ethernet interface card, cabling, drive tray back-plate. ■ Need serial# of existing drive tray. ■ RoHS compliant.
Crypto **drive upgrade** for IBM LTO4 FC SL3000/SL8500	XIBLTO4E-FCUP3085-N CB: 003-5165-01 CI: 4186078	IBM LTO4 FC encryption drive upgrade for SL3000 and SL8500 libraries. ■ Serial to Ethernet interface card, cabling, drive tray back-plate. ■ Need serial# of existing drive tray. ■ RoHS compliant.
LTO4 IBM FC 4Gb **SL500** Encryption Drive	LTO4E-IB4FC-SL500-N	StorageTek IBM LTO4 FC 4Gb Encryption drive for SL500 Library. ■ Featuring 120 MB/Sec transfer rate, 800 GB native capacity. ■ Must order cables separately. ■ RoHS 5.
LTO4 IBM FC 4Gb **SL3000** Encryption Drive	LTO4E-IB4FC-SL30-N	StorageTek IBM LTO4 FC 4Gb Encryption drive for SL3000 Library. ■ Featuring 120 MB/Sec transfer rate, 800 GB native capacity. ■ Must order cables separately. ■ RoHS 5.
LTO4 IBM FC 4Gb **SL8500** Encryption Drive	LTO4E-IB4FC-SL85-N	StorageTek IBM LTO4 FC 4Gb Encryption drive for SL8500 Library. ■ Featuring 120 MB/Sec transfer rate, 800 GB native capacity. ■ Must order cables separately. ■ RoHS 5.
IBM Adapter Card (Belisarius card)		
Packaged FRU FRU	418615102 418607602	IBM LTO4 Adapter card

APPENDIX **A**

IBM ICSF Integration

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

- *Crypto Key Management System: KMS-ICSF Integration Guide* PN: 31619810x
- *Crypto Key Management System: Administration Guide* PN: 31619510x

System Requirements

Both the IBM mainframe and the KMS 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.

KMS

The KMS must be running KMS Version 2.2 or higher.

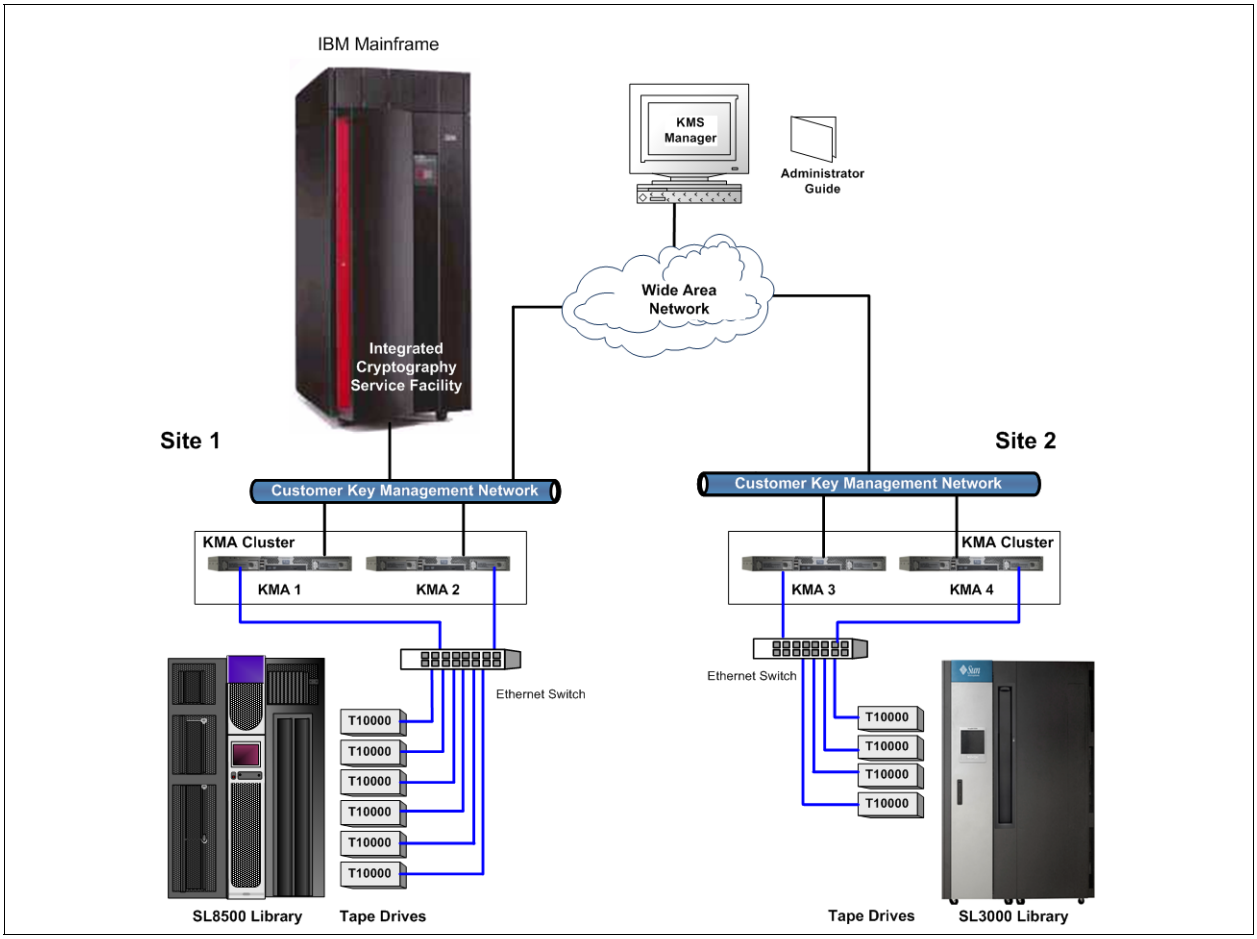
1. ICSF is a software component of z/OS providing cryptographic support either in its own software routines or through access to external cryptographic hardware, such as the StorageTek Crypto Key Management System.

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 KMS 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 KMS 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.

KMS 2.2 introduces a Master Key Mode feature. When this feature is enabled, the KMS 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 KMS equipment.

IBM Mainframe

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

Updating KMS Information

After the IBM mainframe has been configured, the z/OS systems programmer must provide the following information to the administrator of the KMS:

- 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 the KMS enters this information as the Master Key Provider settings in the Security Parameters panel of the KMS Manager GUI.

After the administrator saves these settings, the KMS 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 KMS Certificate File Name and KMS Private Key File Name fields in the Master Key Provider settings.

APPENDIX **B**

Work Sheets

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

These work sheets include:

- "Site Log" on page 86
- "Obtaining Support" on page 87
  - Make several copies and give them to the customer.
  - Explain how to use them.
- "Initial Configuration Work Sheet" on page 88
- "User Roles Work Sheet" on page 89
- "Tape Drives Work Sheet" on page 90
- "Agent Enrollment Work Sheet" on page 91

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

Obtaining Support

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

To contact StorageTek Support 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.sun.com/worldwide/
2. Describe the problem to the call taker. The call taker will ask several questions then:
   - Route your call to the appropriate level of support
     or
   - Dispatch a service representative.

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

Account name			
Site location number			
Contact name			
Telephone number			
Equipment model number	❑ **KMA** (Appliance) ❑ **KMS Manager** (GUI) ❑ SL8500 library ❑ SL3000 library ❑ SL500 library	❑ 9310 library ❑ L700/1400 library ❑ Standalone ❑ Network/switch	❑ T10000A tape drive ❑ T10000B tape drive ❑ T9840D tape drive ❑ HP LTO drive ❑ IBM LTO drive
Device addresses			
IP Addresses			
Error Codes			
Urgency of problem			
Problem description			

Initial Configuration Work Sheet

Description	First KMA			Second KMA		
	Hostname	**IP Address / Netmask**	**DHCP?[1]**	**Hostname**	**IP Address / Netmask**	**DHCP?[1]**
LAN 0 = Management			Yes ❑ No ❑			Yes ❑ No ❑
LAN 1 = ELOM			Yes ❑ No ❑			Yes ❑ No ❑
LAN 2 = Service			Yes ❑ No ❑			Yes ❑ No ❑
LAN 3 = Aggregated			Yes ❑ No ❑			Yes ❑ No ❑
Using IPv6 addressing	Yes ❑ No ❑			Yes ❑ No ❑		
KMA Name						
Gateway						
DNS Server	Hostname: 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 Credentials[2]						
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 KMS 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 KMS Manager; so it may be desirable to enter something simple during the configuration, then change it later using the KMS GUI immediately after the KMA is configured.

User Roles Work Sheet

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

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

Tape Drives Work Sheet

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

Agent Enrollment Work Sheet

KMA ___ Hostname: _____ KMA IP Address:					KMA ___ Hostname: _____ KMA IP Address:			
Drive Address		**Drive Type**	**Drive IP Address**	**Agent ID**	**Passphrase**	**Tokens?**	**Permanent?**	**Set FIPS**
1.						Yes ❑ No ❑	Yes ❑ No ❑	Yes ❑ No ❑
2.						Yes ❑ No ❑	Yes ❑ No ❑	Yes ❑ No ❑
3.						Yes ❑ No ❑	Yes ❑ No ❑	Yes ❑ No ❑
4.						Yes ❑ No ❑	Yes ❑ No ❑	Yes ❑ No ❑
5.						Yes ❑ No ❑	Yes ❑ No ❑	Yes ❑ No ❑
6.						Yes ❑ No ❑	Yes ❑ No ❑	Yes ❑ No ❑
7.						Yes ❑ No ❑	Yes ❑ No ❑	Yes ❑ No ❑
8.						Yes ❑ No ❑	Yes ❑ No ❑	Yes ❑ No ❑
9.						Yes ❑ No ❑	Yes ❑ No ❑	Yes ❑ No ❑
10.						Yes ❑ No ❑	Yes ❑ No ❑	Yes ❑ No ❑
11.						Yes ❑ No ❑	Yes ❑ No ❑	Yes ❑ No ❑
12.						Yes ❑ No ❑	Yes ❑ No ❑	Yes ❑ No ❑
13.						Yes ❑ No ❑	Yes ❑ No ❑	Yes ❑ No ❑
14.						Yes ❑ No ❑	Yes ❑ No ❑	Yes ❑ No ❑
15.						Yes ❑ No ❑	Yes ❑ No ❑	Yes ❑ No ❑
16.						Yes ❑ No ❑	Yes ❑ No ❑	Yes ❑ No ❑
17.						Yes ❑ No ❑	Yes ❑ No ❑	Yes ❑ No ❑
18.						Yes ❑ No ❑	Yes ❑ No ❑	Yes ❑ No ❑
19.						Yes ❑ No ❑	Yes ❑ No ❑	Yes ❑ No ❑
20.						Yes ❑ No ❑	Yes ❑ No ❑	Yes ❑ No ❑

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 KMS 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 a KMS.

Audit Log The KMS 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 KMS 2.x, 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 KMS that represent storage objects associated with KMS 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 or X2200-M2 server preloaded with the KMS 2.0 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 KMS component providing key management on behalf of encryption agents.

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.

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

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.

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 KMS and Encryption Agent that indicates network proximity, or locality. When Encryption Agents connect to the KMS cluster there is a bias towards establishing communication with KMAs in the same site as the Encryption Agent.

T

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

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

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

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

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

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

Z

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

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

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