



# Sun StorageTek™ Crypto Key Management System

Version 2.0

**Systems Assurance Guide**

Part Number: 316194804

Revision: BB





# Crypto Key Management System

Version 2.0

---

## Systems Assurance Guide

Sun Microsystems, Inc.  
[www.sun.com](http://www.sun.com)

Part Number: 316194804  
February 2009  
Revision: BB

Copyright © 2008, 2009 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A.  
All rights reserved.

THIS PRODUCT CONTAINS CONFIDENTIAL INFORMATION AND TRADE SECRETS OF SUN MICROSYSTEMS, INC. USE, DISCLOSURE OR REPRODUCTION IS PROHIBITED WITHOUT THE PRIOR EXPRESS WRITTEN PERMISSION OF SUN MICROSYSTEMS, INC.

Sun, Sun Microsystems, the Sun logo, Sun StorEdge, StorageTek, and STK are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

The Adobe. logo and the PostScript logo are trademarks or registered trademarks of Adobe Systems, Incorporated.

This product is covered and controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

Copyright © 2008, 2009 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, Etats-Unis.  
Tous droits réservés.

CE PRODUIT CONTIENT DES INFORMATIONS CONFIDENTIELLES ET DES SECRETS COMMERCIAUX DE SUN MICROSYSTEMS, INC. SON UTILISATION, SA DIVULGATION ET SA REPRODUCTION SONT INTERDITES SANS L'AUTORISATION EXPRESSE, ECRITE ET PREALABLE DE SUN MICROSYSTEMS, INC.

Sun, Sun Microsystems, le logo Sun, Sun StorEdge, StorageTek, et STK sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Le logo Adobe. et le logo PostScript sont des marques de fabrique ou des marques déposées de Adobe Systems, Incorporated.

Ce produit est soumis à la législation américaine sur le contrôle des exportations et peut être soumis à la réglementation en vigueur dans d'autres pays dans le domaine des exportations et importations. Les utilisations, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes biologiques et chimiques ou du nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou reexportations vers les pays sous embargo américain, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exhaustive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la législation américaine sur le contrôle des exportations et la liste de ressortissants spécifiquement désignés, sont rigoureusement interdites.

Sun is interested in improving its documentation and welcomes your comments and suggestions, you can:

- Submit them by going to: <http://www.sun.com/hwdocs/feedback>
- Use the OpinionLab [+] feedback system on the documentation Web site

Please include the publication name, part number, and edition number in your correspondence if they are available. This will expedite our response.



Please  
Recycle



Adobe PostScript

# 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	This revision includes: <ul style="list-style-type: none"><li>■ Added information about the Sun Fire X2200 server as a Key Management Appliance.</li><li>■ Added information about the FIPS-compliant tape drives (with KMS Version 2.1).</li><li>■ Added information about the Internet Protocol Version 6 (IPv6).</li><li>■ Added information about aggregate networks.</li><li>■ Added T10000B tape drive information.</li><li>■ Updated HP LTO4 information.</li><li>■ Updated tape drive and library configurations.</li><li>■ Updated <a href="#">Chapter 4, "Ordering"</a>.</li></ul>

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



# Contents

---

**Preface** xiii

**1. Introduction** 1

Planning for Encryption 1

Encryption Standards 2

Sun StorageTek Encryption Solutions 3

Key Management System Configurations 3

Version 1.x Air Gap Configuration 5

Version 1.x Network Configurations 5

Version 2.x Key Management Appliance Configurations 6

Version 2.0 Component Descriptions 8

Communications Process 9

Backups 9

Encryption Hardware Kits 10

Key Management Appliance Specifications 12

Key Management Appliance Physical Connections 15

Aggregation Network 16

Internet Protocol Versions 17

FIPS Compliant Tape Drives 17

Tape Drives 18

About the T10000 18

About the T9840D Tape Drive 19

About the HP LTO4 Tape Drive 20

Tape Drive Comparison 21

Tape Drive and Media Comparisons 22

T-Series Tape Drives 22

HP LTO4 Tape Drives	23
<b>2. Systems Assurance</b>	<b>25</b>
Planning Meetings	26
Customer Team Member Contact Sheet	27
Sun Team Member Contact Sheet	28
Configuration Planning	29
Customer Conceptual Drawing	30
<b>3. Site Preparation</b>	<b>31</b>
Site Planning Checklist	32
Rack Specifications	35
SL8500 Rack Guidelines	35
External Rack Installations	36
Redundant Power	37
Service Delivery Platform	38
FIPS Compliant Tape Drives	39
Internet Protocol Versions	39
Content Management	40
Capacity on Demand	41
RealTime Growth Technology	41
Partitioning	41
Planning the Data Path	42
Tasks	43
Preparing the Tape Drives	44
T-Series Drive Data Preparation	44
Create a Drive Data File Structure	46
HP LTO4 Tape Drive Preparation	47
Required Tools	48
Supported Platforms and Web Browsers	48
Required Firmware Levels	49
KMS Manager	50
Role-Based Operations	51



<b>4. Ordering</b>	<b>59</b>
Supported Configurations	59
Supported Tape Drives	59
Key Management Appliance	60
SL8500 Modular Library System	61
SL3000 Modular Library System	62
SL500 Modular Library System	63
9310 Automated Cartridge System	64
L-Series Libraries	65
Rack Mount	66
Order Numbers, Descriptions, and Contents	67
Power Cables	77
9310 Upgrades	78
Professional Services	78
Tape Drive Ordering Instructions	79
Library Ordering Instructions	79
HP LTO4 Order Numbers	80
<b>A. Work Sheets</b>	<b>81</b>
Initial Configuration Work Sheet	82
User Roles Work Sheet	83
Tape Drives Work Sheet	84
Drive Enrollment Work Sheet	85
<b>Glossary</b>	<b>87</b>
<b>Index</b>	<b>95</b>



# Figures

---

FIGURE 1-1	Key Management Station Configurations	4
FIGURE 1-2	Key Management Appliance Single Site Configuration	6
FIGURE 1-3	Key Management Appliance Dual Site Configuration	6
FIGURE 1-4	Key Management Appliance Configurations	7
FIGURE 1-5	Key Management Appliance—Front Panel	12
FIGURE 1-6	Key Management Appliance—Rear Panel	12
FIGURE 1-7	Key Management Appliance—Rear Panel Connections	15
FIGURE 3-1	External Rack Example	36
FIGURE 3-2	Power Redundancy	37
FIGURE 3-3	Systems Delivery Platform	38
FIGURE 3-4	Tape Drive Serial Number—VOP	44
FIGURE 3-5	Request an Encryption Key Application	44
FIGURE 3-6	Encryption File Request for Drive Data	45
FIGURE 3-7	Encryption File Request for Drive Data	45
FIGURE 3-8	Drive Data File Structure	46
FIGURE 3-9	VOP LTO Files	47
FIGURE 3-10	User Roles Detail Screen	51
FIGURE 4-1	Key Management Appliance—Front Panel	58
FIGURE 4-2	Key Management Appliance—Rear Panel	58
FIGURE 4-3	LTO4 License Keys	78



# Tables

---

TABLE 1-1	Key Management System Versions	3
TABLE 1-2	Encryption Solution Comparisons	11
TABLE 1-3	Sun Fire X2100 Specifications	13
TABLE 1-4	Sun Fire X2200 Specifications	14
TABLE 1-5	KMA Network Connections	16
TABLE 1-6	FIPS Compliant Tape Drives	17
TABLE 1-7	Tape Drive Comparisons	21
TABLE 1-8	T-Series Tape Drive Media Compatibilities	22
TABLE 1-9	Tape Drive and Media Support	22
TABLE 1-10	LTO Media Compatibility	23
TABLE 2-1	System Assurance Task Checklist	26
TABLE 2-2	Solution Planning Checklist	29
TABLE 3-1	Site Planning Checklist	32
TABLE 3-2	SL8500 Accessory Rack Guidelines	35
TABLE 3-3	FIPS Compliant Tape Drives	39
TABLE 3-4	Content Management Planning	40
TABLE 3-5	Steps and Tasks for Partitioning	43
TABLE 3-6	Operating Systems and Web Browsers	48
TABLE 3-7	Firmware Compatibilities	49
TABLE 3-8	KMS Manager Display	50
TABLE 3-9	Operator Roles and Functions	52
TABLE 3-10	User Roles Work Sheet	56
TABLE 4-1	SL8500 Modular Library System Requirements	59
TABLE 4-2	SL3000 Modular Library System Requirements	60
TABLE 4-3	SL500 Modular Library System Requirements	61
TABLE 4-4	9310 Automated Cartridge System Requirements	62

TABLE 4-5	L-Series Library Requirements	63
TABLE 4-6	Rackmount Requirements	64
TABLE 4-7	KMS 2.x Core Parts	65
TABLE 4-8	KMS 2.x Software License	67
TABLE 4-9	Tape Drives Order Numbers	69
TABLE 4-10	Service Order Numbers	70
TABLE 4-11	Spares Order Numbers	72
TABLE 4-12	KMS 1.x Parts Order Numbers	73
TABLE 4-13	Power Cables Order Numbers	75
TABLE 4-14	9310 Upgrade Ordering Instructions and Part Numbers	76
TABLE 4-15	Professional Services Ordering Instructions and Part Numbers	76
TABLE 4-16	Tape Drive Ordering Instructions	77
TABLE 4-17	Library Ordering Instructions	77
TABLE 4-18	LTO4 Configured End Items—Order Numbers	78
TABLE 4-19	LTO4 Conversion Bill Numbers	78
TABLE 4-20	Dione Card Part Number—LTO4	78
TABLE A-1	Initial Configuration Settings—Customer	80
TABLE A-2	User Roles Work Sheet—Customer	81
TABLE A-3	Tape Drive and Agents Work Sheet—Service Representative	82
TABLE A-4	Enrollment Data Work Sheet—Customer	83

# Preface

---

This guide is intended for Sun StorageTek representatives, customers, and anyone responsible for planning the installation of the Sun StorageTek encryption solution using a Crypto Key Management System (KMS) Version 2.x.



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

**Make sure these manuals and guides are available to the customer.**

Go to: <http://docs.sun.com/app/docs/prod/stortek.crypto.keymgmt20>

---

## Organization

This guide has the following organization:

Chapter	Use this chapter to:
<a href="#">Chapter 1, "Introduction"</a>	Introduce yourself and the customer to Sun StorageTek encryption solutions.
<a href="#">Chapter 2, "Systems Assurance"</a>	Describe and plan for the systems assurance process.
<a href="#">Chapter 3, "Site Preparation"</a>	Prepare for the installation.
<a href="#">Chapter 4, "Ordering"</a>	Help order the encryption solution and additional components—libraries and tape drives—for your customer's requirements.
<a href="#">Appendix A, "Work Sheets"</a>	Complete work sheets that can help prepare for the installation.
<a href="#">"Glossary"</a>	Learn the terms and abbreviations used in this publication.

## Related Information

These publications contain the additional information mentioned in this guide:

Publication Description	Part Number
Important Safety Information for Sun Hardware Systems	Sun: 816-7190-xx
<i>Sun SunFire X2100 Server Installation Guide</i>	Sun: 819-6589-xx
<i>Sun SunFire X2100 Server Service Manual</i>	Sun: 819-6591-xx
<i>Sun SunFire X2200 Server Installation Guide</i>	Sun: 819-6596-xx
<i>Sun SunFire X2200 Server Service Manual</i>	Sun: 819-6597-xx
<i>Embedded Lights Out Manager Administration Guide</i>	Sun: 819-6588-xx

Publication Description	Part Number
<i>T10000 Tape Drive Installation Manual</i>	StorageTek: 96173
<i>T10000 Service Manual</i>	StorageTek: 96175
<i>T9x40 Tape Drive Installation Manual</i>	StorageTek: 95879
<i>T9x40 Service Manual</i>	StorageTek: 95740
<i>SL8500 Modular Library System Installation Manual</i>	StorageTek: 96138
<i>SL3000 Modular Library System Installation Manual</i>	StorageTek: 316194201
<i>SL500 Modular Library System Installation Manual</i>	StorageTek: 96114
<i>L700/1400 Library Installation Manual</i>	StorageTek: 95843
<i>9310 PowderHorn Library Installation Manual</i>	StorageTek: 9314
<i>Virtual Operator Panel—Service</i>	StorageTek: 96180
<i>Virtual Operator Panel—Customer</i>	StorageTek: 96179

Publication Description	Part Number
<i>Crypto Key Management Installation and Service Manual</i>	StorageTek: 3161949xx
<i>Crypto Key Management System Administration Guide</i>	StorageTek: 3161951xx
<i>Crypto Key Management System Disaster Recovery Guide</i>	StorageTek: 3161971xx
<i>Sun Storage Regulatory and Safety Compliance Manual</i>	Sun: 820-5506-xx

When planning to support data encryption, the following documents are available to help identify and define encryption:

- Federal Information Processing Standards Publication FIPS PUB 46-3 *Data Encryption Standard*
- Federal Information Processing Standards Publication FIPS PUB 171 *Key Management*
- Federal Information Processing Standards Publication FIPS PUB 140-2 *Security Requirements for Cryptographic Modules*
- National Institute of Standards and Technology NIST Publication 800-57 *Recommendation for Key Management Parts 1 and 2*
- International Standard Organization ISO/IEC 1779 *Security Techniques—Code of Practice for Information Security Management*



# Documentation Content and Purpose

This table shows the specific documents for the Crypto Key Management System and the audience that document is intended for.

**TABLE P-1** Documentation and Audience Map

Task/Purpose	Documentation & Audience								
	AE	SE	PS	TS	T3	SR	Partner/OEM	Customer	
Site Preparation/Pre-sales	Systems Assurance Guide								
Installation & Service	Installation & Service Manual								
User / Operation	Administrator Guide								
Online Help	Online Help								
<b>Legend:</b> AE = Account executive, sales and marketing SE = Systems engineer PS = Professional services				TS = Technical specialists (NSSE) T3 = Support (Frontline and Backline) SR = Service representative (CSE)					

This table contains an overview of the documentation, intended audience, general content, and purpose.

**TABLE P-2** Documentation Content and Purpose

Document	Audience	General Content	Purpose
Systems Assurance Guide	<ul style="list-style-type: none"> <li>■ Marketing &amp; Sales</li> <li>■ Systems Engineers</li> <li>■ Installation Coordinators</li> <li>■ Professional Services</li> <li>■ Technical Specialists</li> <li>■ Service Representatives</li> <li>■ Customer</li> </ul>	<ul style="list-style-type: none"> <li>■ Product description</li> <li>■ Dimensions</li> <li>■ Weights &amp; measures</li> <li>■ Configurations</li> <li>■ Capacities</li> <li>■ Site preparation</li> <li>■ Models and features</li> <li>■ Order numbers</li> </ul>	<ul style="list-style-type: none"> <li>■ Pre-Sales</li> <li>■ Site Planning</li> <li>■ Product introduction</li> <li>■ Readiness</li> </ul>
Installation Manual	<ul style="list-style-type: none"> <li>■ Installation Coordinators</li> <li>■ Technical Specialists</li> <li>■ Service Representatives</li> </ul>	Installation: <ul style="list-style-type: none"> <li>■ Procedures</li> <li>■ Checklists</li> <li>■ Configurations</li> </ul>	<ul style="list-style-type: none"> <li>■ Installation</li> <li>■ Configuration</li> <li>■ ELOM</li> <li>■ QuickStart</li> </ul>
Service Manual	<ul style="list-style-type: none"> <li>■ Technical Specialists</li> <li>■ Service Representatives</li> </ul>	Service: <ul style="list-style-type: none"> <li>■ Fault isolation</li> <li>■ Removal/Replacement</li> </ul>	<ul style="list-style-type: none"> <li>■ Service and Maintenance</li> <li>■ Support</li> </ul>
Disaster Recovery	<ul style="list-style-type: none"> <li>■ Customer</li> <li>■ Systems Engineers</li> <li>■ Installation Coordinators</li> <li>■ Professional Services</li> <li>■ Technical Specialists</li> <li>■ Service Representatives</li> </ul>	<ul style="list-style-type: none"> <li>■ Solution architecture</li> <li>■ Policies and Practices</li> </ul>	<ul style="list-style-type: none"> <li>■ Plan and prepare for a disaster and the recovery of data</li> </ul>
Administrator Guide	<ul style="list-style-type: none"> <li>■ Customer</li> <li>■ Technical Specialists</li> <li>■ Service Representatives</li> </ul>	<ul style="list-style-type: none"> <li>■ Introduction</li> <li>■ Operator Roles</li> <li>■ How to...</li> </ul>	<ul style="list-style-type: none"> <li>■ Usage</li> <li>■ Support</li> <li>■ KMS Manager / GUI</li> </ul>

---

## Additional Information

Sun Microsystems, Inc. (Sun) offers several methods to obtain additional information.

### Sun's External Web Site

Sun's external Web site provides marketing, product, event, corporate, and service information. The external Web site is accessible to anyone with a Web browser and an Internet connection.

The URL for the external Web site is: <http://www.sun.com>

The URL for StorageTek™ brand-specific information is:  
<http://www.sun.com/storagetek/>

### Documentation and Download Web Sites

Web sites that enable customers, members, and employees to search for technical documentation, downloads, patches, features, and articles include:

- Documentation: <http://docs.sun.com/app/docs> (customers)
- Documentation: <http://docs.sfbay.sun.com/app/docs> (internal)
- Sun Partner Exchange: <https://spe.sun.com/spx/control/Login> (partners)

Firmware and graphical user interface download sites:

- Sun Download Center: <http://www.sun.com/download/index.jsp> (customers)
- Uniform Software Repository: <http://dlrequest.sfbay.sun.com:88/usr/login> (internal)

If your customer does not already have a Sun Online Account they will need to register. For a new account, go to: <https://reg.sun.com/register>

For more information about Sun StorageTek products, got to:  
[http://sunsolve.sun.com/handbook\\_pub/validateUser.do?target=STK/STK\\_index](http://sunsolve.sun.com/handbook_pub/validateUser.do?target=STK/STK_index)

### Partners Site

The Sun StorageTek Partners site is a Web site for partners with a StorageTek Partner Agreement. This site provides information about products, services, customer support, upcoming events, training programs, and sales tools to support StorageTek Partners. Access to this site, beyond the Partners Login page, is restricted. On the Partners Login page, employees and current partners who do not have access can request a login ID and password and prospective partners can apply to become StorageTek resellers.

The URL for partners with a Sun Partner Agreement is:  
<http://www.sun.com/partners/>

## 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 the Sun 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 encryption)
- Transported (appliance-based)
- Stored (device-based encryption)

Sun 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.

# Encryption Standards

Sun StorageTek encryption solutions are enhanced versions based on 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 lowest 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**,” is a block cipher encryption algorithm that uses both of these 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)

# Sun StorageTek Encryption Solutions

Sun StorageTek offers two device-based solutions; they include:

**TABLE 1-1** Key Management System Versions

<b>Version 1.x</b>	Sun Ultra 20 Workstation—called a key management station
<b>Version 2.x</b>	Sun Fire X2100 or X2200 Server—called a key management appliance

Both systems are based on the AMD Opteron processor and run a pre-loaded version of the Solaris™ 10 operating system.

Both of these systems manage all cryptographic keys and administrative functions. Each system contains a MARS card (SCA 6000), a FIPS-approved, random number generator that generates the raw keys.

## Key Management System Configurations

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

**FIGURE 1-1** shows three **Version 1.x configurations** using a key management workstation (KMS):

- Air Gap
- Network—local area network
- Network—wide area network

These configurations require the use of a token and token bay.

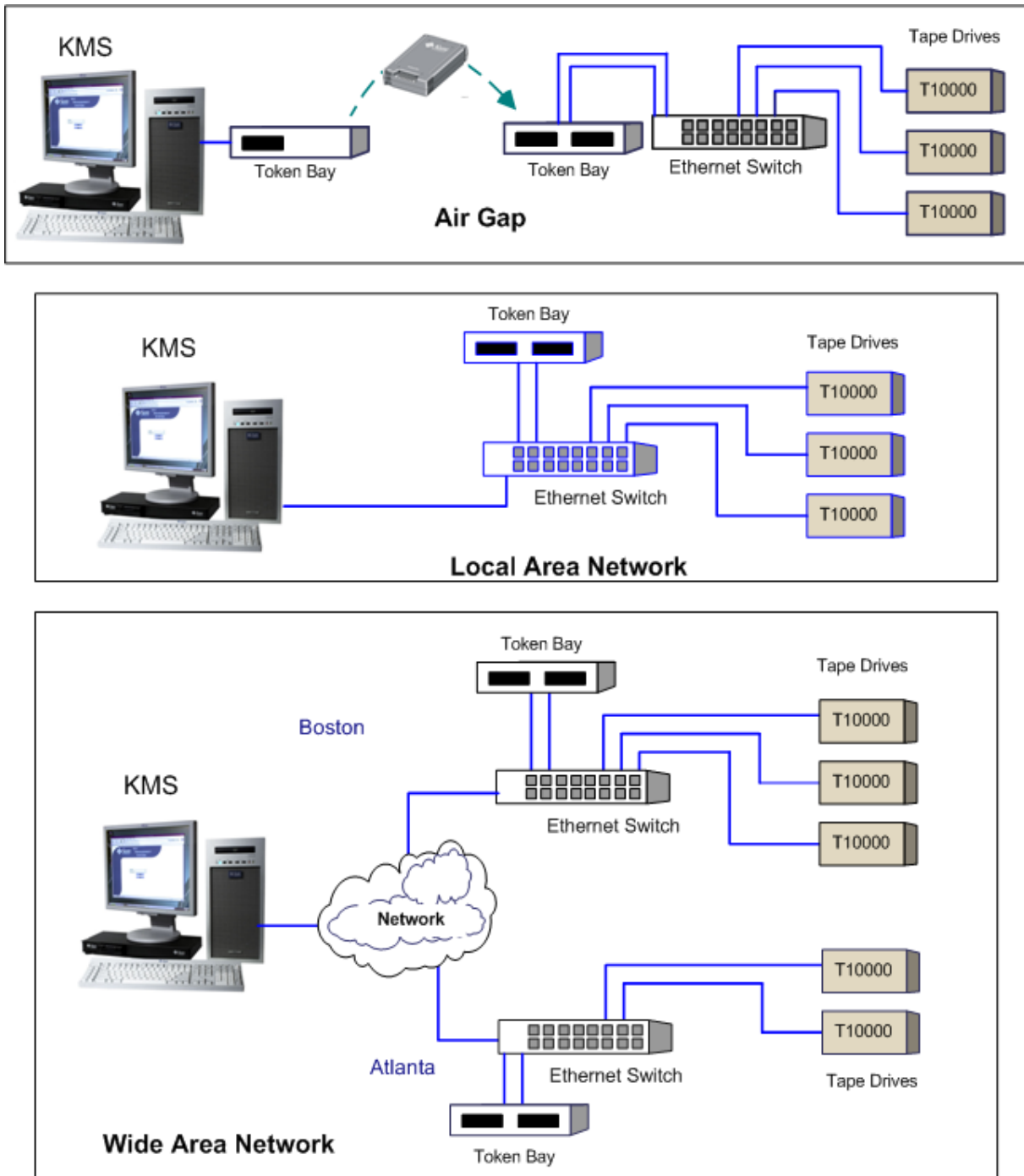
**Version 2.x configurations** for the key management appliance (KMA):

- [FIGURE 1-2 on page 6](#) Single site—local area network
- [FIGURE 1-3 on page 6](#) Multiple sites—wide area network
- [FIGURE 1-4 on page 7](#) Multiple sites—wide area network

These configurations require the use of a KMS cluster.

## Version 1.x Key Management Station Configurations

**FIGURE 1-1** Key Management Station Configurations



## Version 1.x Air Gap Configuration

The air gap configuration provides the highest levels of security. With the air gap configuration, the KMS and token bay are physically and logically isolated. Transferring keys from the key management station to the tape drives requires direct user intervention.

The hardware components are configured as:

- The KMS and token bay are separated from the library and tape drives by an “air gap,” such as in a different room.
- The token bay is connected to the KMS through an Ethernet port.
- A second token bay is attached to the encryption-capable tape drives through a separate local network.

### To write encryption keys to a token:

1. Insert a token in the KMS token bay.
2. Write to the token.
3. Physically carry the token (with the keys) to the drives.
4. Insert the token in the token bay attached to the tape drive network.

You can display the status of token only if it is inserted in the KMS token bay.

## Version 1.x Network Configurations

With the network configuration, the KMS, tape drives, and token bays all reside on a local or wide area network (LAN or WAN).

The hardware components are configured as:

- The KMS is connected to the network through an Ethernet port.
- Any number of token bays can be connected to the network.
- Tokens have static IP addresses.
- Any number of encryption-capable tape drives can be connected to the network.

### To write encryption keys to any token:

1. Inserted a token into a token bay on the network.
2. Write to the token using the static IP address.

Once the token receives the keys, it automatically transmits them across the network to the tape drives. You do not need to physically carry the tokens from one token bay to another.

You can display information about the token at the KMS.



#### **Important:**

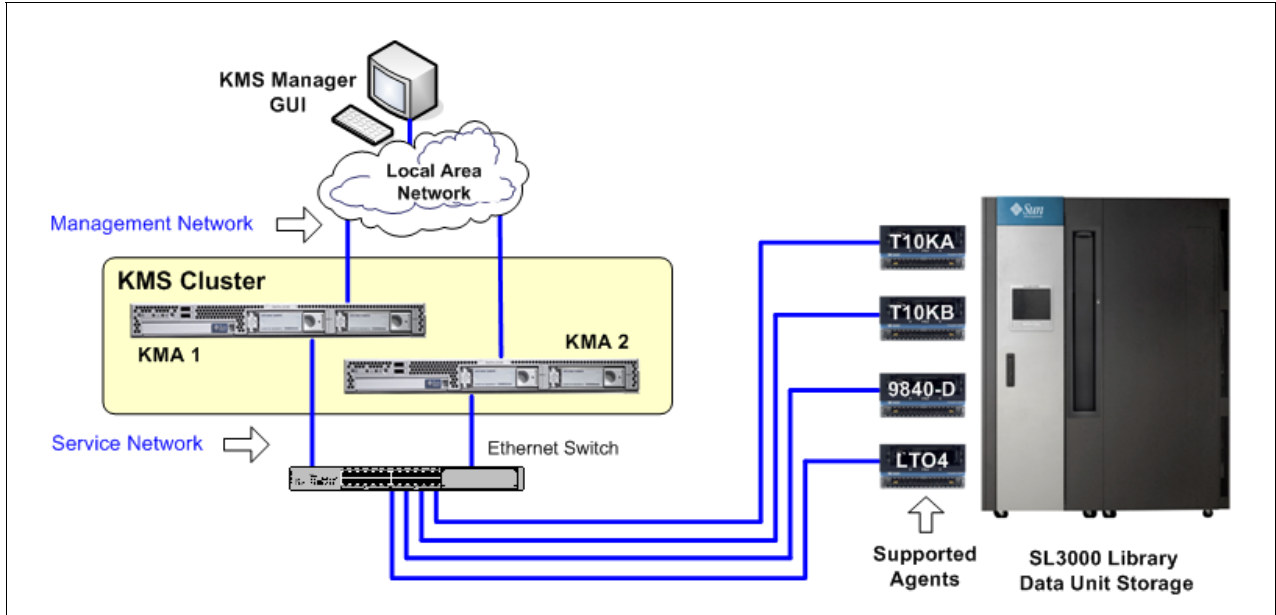
The remaining topics in this document contains specific information for the Sun StorageTek Crypto Key Management System **Version 2.0**.

Refer to the *Crypto Key Management Station Systems Assurance Guide* PN TM0018 for information about the **Version 1.x** encryption solution.

## Version 2.x Key Management Appliance Configurations

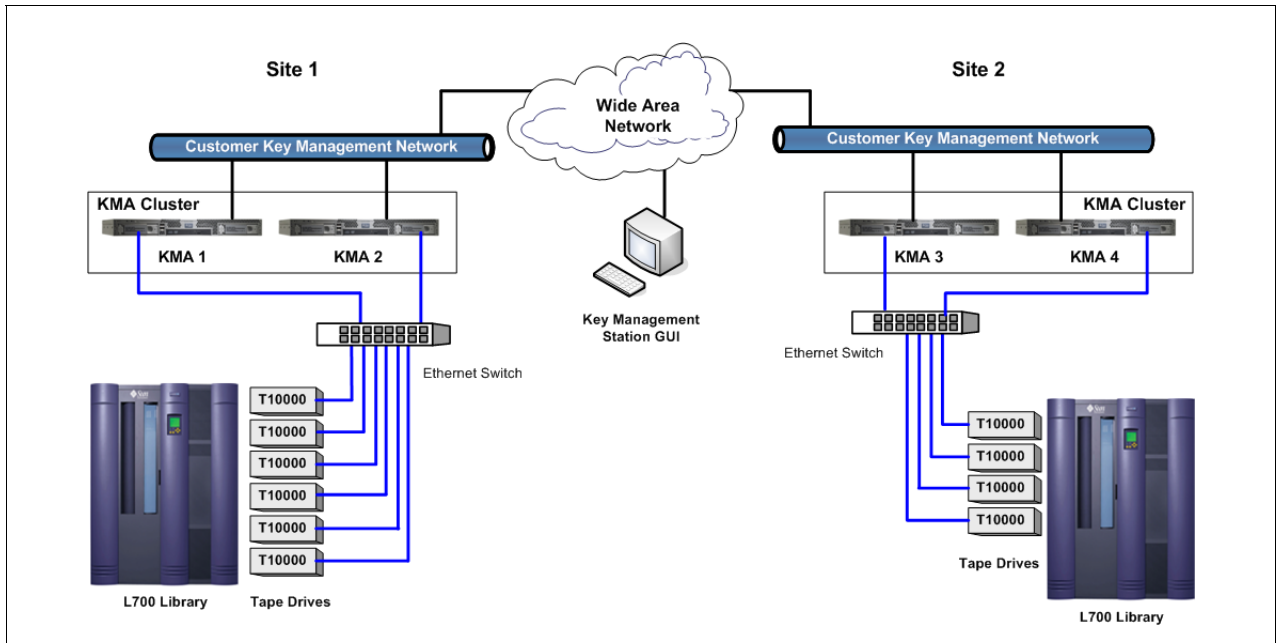
**FIGURE 1-2** Key Management Appliance Single Site Configuration

This example uses a *single site*—local area network—management network. 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 1-3** Key Management Appliance Dual Site Configuration

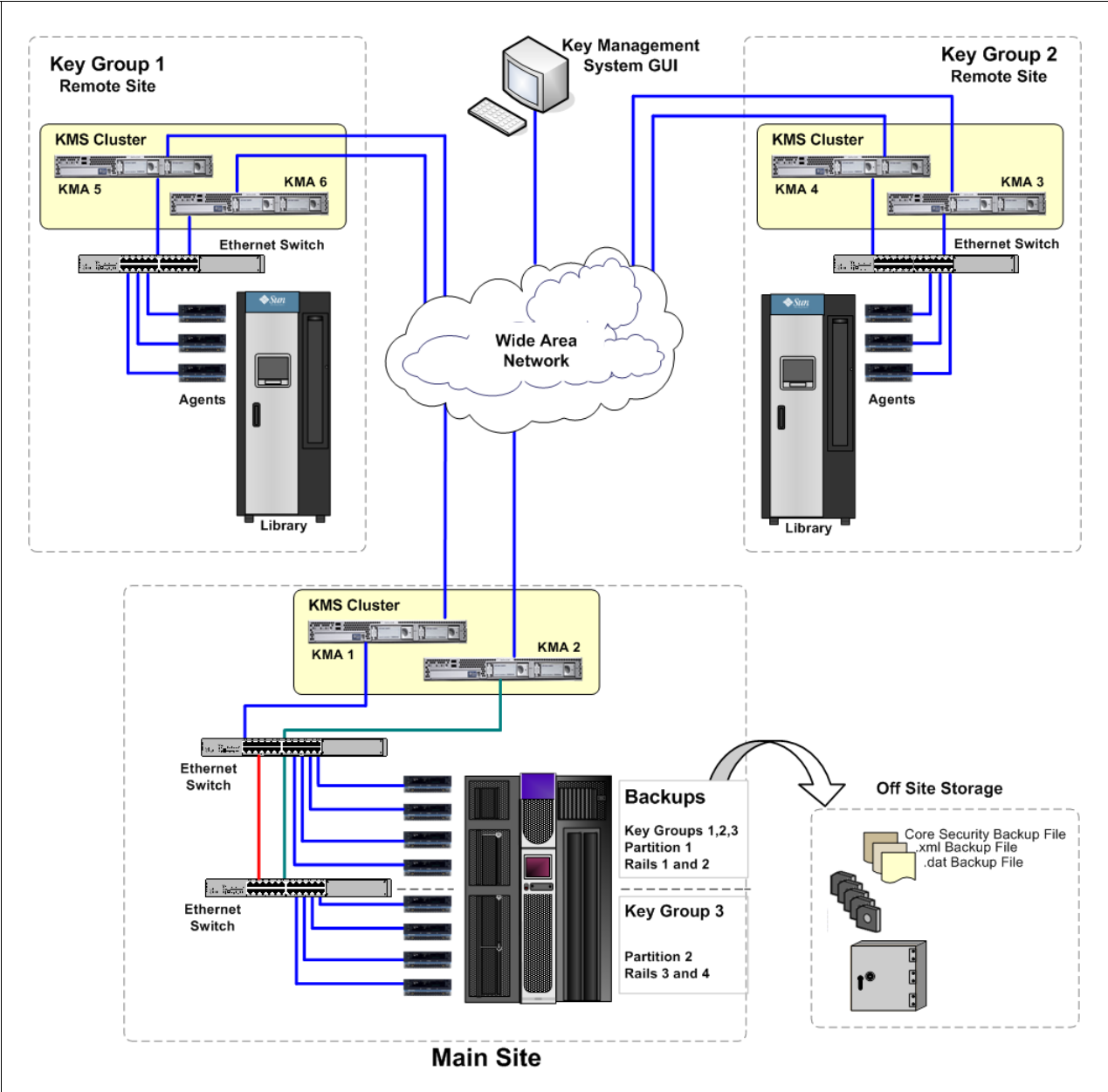
In this example, the KMAs are managed by a wide area network. Each KMA belongs in the same KMS cluster.





**FIGURE 1-4** Key Management Appliance Configurations

This example uses both remote and local sites with one KMS cluster. The main site also provides disaster recovery facilities for this company.



## Version 2.0 Component Descriptions

The architecture for the Version 2.0 encryption solution consists of:

- **Key Management Appliance (KMA)**—A proven, dual-core processor with Sun Microsystems' Solaris 10 operating system that delivers policy-based key management and key provisioning services.
- **KMS Manager** or **KMS Manager GUI**—A 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 is Web-based; and must be installed on a **customer-provided**, network-attached, PC, server, or workstation running Windows XP, or Solaris x86.

- **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.

The maximum number of KMAs in a cluster is 20.

- **Agent**—A device (tape drive) that performs encryption using keys managed by the KMA Cluster and KMS Manager.
- **Data Unit ID**—The media—a data cartridge.
- **Key Groups**—Provide organization for keys and associates them with a Key Policy. Key Groups also enforce access to the key material by the Encryption Agents.
- **Network connections**—There are two networks that provide tape drive connectivity, the management network and the service network.

The service network is the preferred connection scheme for the tape drives; however, both networks support tape drive connectivity.

For additional security and to cut down on LAN traffic, the customer may want to consider using Virtual Local Area Networks<sup>1</sup> (VLANs) when connecting tape drives to the management network. VLANs are created using special

Note: A third network is available for the embedded Lights Out Manager.

### Important:

Key management appliances *must be* installed in pairs as show in the configuration drawings in [FIGURE 1-2](#). Some key points include:

- Multiple clusters may exist on a dedicated, private, local or wide area network.
- The KMAs in a KMS Cluster provide automatic failover and backups as required.
- Tape drives—called Agents—must be, and remain, connected to the network.
- Any KMA can service any tape drive on the network.
- 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.

For example:

- 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.

---

1. 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.

## Communications Process

The communications process between a:

- Drive and KMA
- KMA to KMA
- User and KMA

are all the same. They use a passphrase to perform a Challenge & Response Protocol. If successful, the drive, KMA, or user are provided with a **certificate** and a corresponding **private key**.

- This certificate and private key establish a TLS 1.0 (secure sockets) channel<sup>2</sup>.
- Establishing this secure sockets channel uses a 2048 bit RSA<sup>3</sup>.
- Authenticating this session results in an agreed upon, 256 bit AES<sup>4</sup> key; where all subsequent communications are encrypted with an AES 256 key.

Using these certificates, both ends of any connection authenticate the other.

This process is performed during the enrollment phase.

- For a drive, this is done using a Virtual Operator Panel (VOP) session.
- For a KMA, it is part of the QuickStart program.
- For users, the process is repeated every time the user logs in.

This process is also repeated every time a tape drive comes back online (after an IPL) and after a reboot of a KMA.

All latter communications, such as a drive requesting a key, one KMA sending replication to another, or a user making a request with the KMS Manager interface, are done using the already established secure sockets session.

## Backups

Unlike Version 1.x, there is no external USB hard drive for backups. This is because of the KMA cluster—a minimum of two KMAs are required to create the cluster—and that each KMA replicates the others. This way, if one KMA goes down and is replaced, you would join into an existing KMA cluster to restore the database on the new KMA. A cluster and network established backup.

### Core Security Backup

During the initial configuration, after the QuickStart program completes, and the Key Split Credentials and Quorum are defined, the Security Officer can preform a “Core Security Backup” from the KMS Manager. This backup contains the system master key—which is split using a Shamir Shared Secret algorithm<sup>5</sup> into the number of splits define by the Key Split Credentials. A Quorum is then required to re-establish the system master key.

**Note** – Once this backup is complete, it only needs to be done when the Key Split Credentials are changed, such as a change in assignments or personnel.

---

2. Transport Layer Security = A cryptographic protocol that provide secure communications.

3. RSA = An algorithm for public-key cryptography.

4. Advanced Encryption Standard = A FIPS-approved, National Institute of Standards and Technology (NIST) cryptographic standard used to protect electronic data.

5. An algorithm in cryptograph where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret.

## Periodic Backup

Periodically a regular backup should be done by the Backup Operator using the KMS Manager. This backup creates two files, a backup file and a backup key file.

A backup file contains all the information (database and keys) and is encrypted with an AES 256 key specific to the backup. This key is placed in the backup key file, and is wrapped with the master key.

To restore a backup, you need a backup file and its corresponding backup key file, and the core security backup. A quorum of the Key Split Credentials must supply their passphrases, which are used to extract the master key from the core security backup. That allows the backup key file to be decrypted, producing the backup key. Then, the backup must be decrypted, and this is used to restore the system.

## 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.

## Encryption Version Comparisons

TABLE 1-2 shows a comparison between Version 1.x and Version 2.0 encryption solutions.

**TABLE 1-2** Encryption Solution Comparisons

Comparison	Key Management Workstation 1.x	Key Management Appliance 2.x
<b>Protocols</b>	Robust but uses manual protocols	Robust and uses automated protocols
<b>Encryption Method</b>	AES 256	AES 256
<b>KMS Platform</b>	Ultra 20 Workstation	Sun Fire X2100 appliance or Sun Fire X2200 appliance
<b>Key Update</b>	Asynchronous	On each tape mount
<b>Drive Key Strategy</b>	<ul style="list-style-type: none"> <li>■ 1 Write Key per drive</li> <li>■ 32 Cached Read Keys</li> </ul>	<ul style="list-style-type: none"> <li>■ Drive requests keys from KMA</li> <li>■ Drive still has 32-key cache</li> </ul>
<b>Key Transmission</b>	<ul style="list-style-type: none"> <li>■ Out-of-Band Ethernet TCP/IP</li> <li>■ Token as secure local key store</li> </ul>	<ul style="list-style-type: none"> <li>■ Out-of-Band Ethernet TCP/IP</li> <li>■ Direct KMS to Drive communication</li> </ul>
<b>Transmission Key Protection</b>	AES-256 CCM Mode	TLS/RSA/SHA1/AES-256 HMAC
<b>Key Assignment</b>	Manual	Automated
<b>Large Key Management</b>	Unwieldy with a large number of keys	Designed for large number of keys
<b>KMS Clustering</b>	Mirrored hot-spare	Full clustering
<b>KMS Administration</b>	Console or remote GUI	Remote GUI
<b>Key Sharing and Data Recovery</b>	Manual, with tokens	Public key based exchange
<b>Supported tape drives</b>	T10000A	T10000A T10000B T9840D HP LTO4
<b>Support other non-Tape devices</b>	No	Planned
<b>Customer Roles</b>	Three	Five
		<p><b>Additional Features:</b></p> <ul style="list-style-type: none"> <li>■ One-time setup from console</li> <li>■ Management from remote GUI</li> <li>■ Quorum for critical operations</li> <li>■ KMS/Drives use private network</li> <li>■ Multiple KMAs connected over WAN</li> <li>■ Unique write key for each tape</li> <li>■ High performance, 150ms key retrieval</li> <li>■ Data sharing with partners supported</li> <li>■ Compatible with 1.0 keys</li> </ul> <p><b>Support:</b></p> <ul style="list-style-type: none"> <li>■ 10 Sites, for a total of 20 KMAs</li> <li>■ 2 KMAs per site</li> <li>■ Up to 3,000 tape drives</li> </ul>

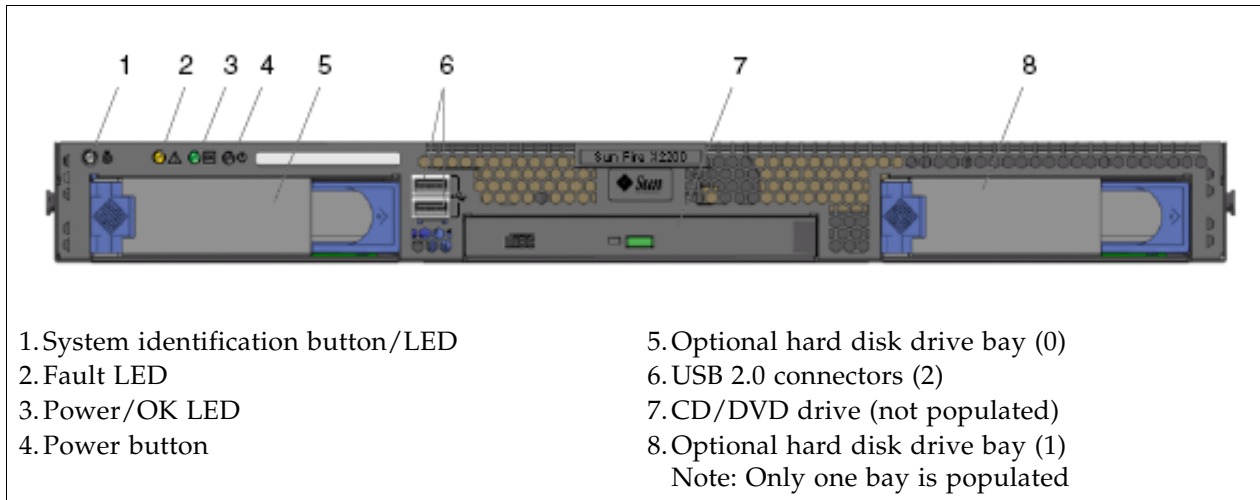
# Key Management Appliance Specifications

There are two types of servers for the Key Management Appliance (KMA) the: Sun Fire X2100 and the Sun Fire X2200. Both servers have the same layout.

- FIGURE 1-5 is an example for the front of the appliance
- FIGURE 1-6 is an example for the rear of the appliance

Note: The rear of the appliance is where all of the cable connections are made.

**FIGURE 1-5** Key Management Appliance—Front Panel



**FIGURE 1-6** Key Management Appliance—Rear Panel

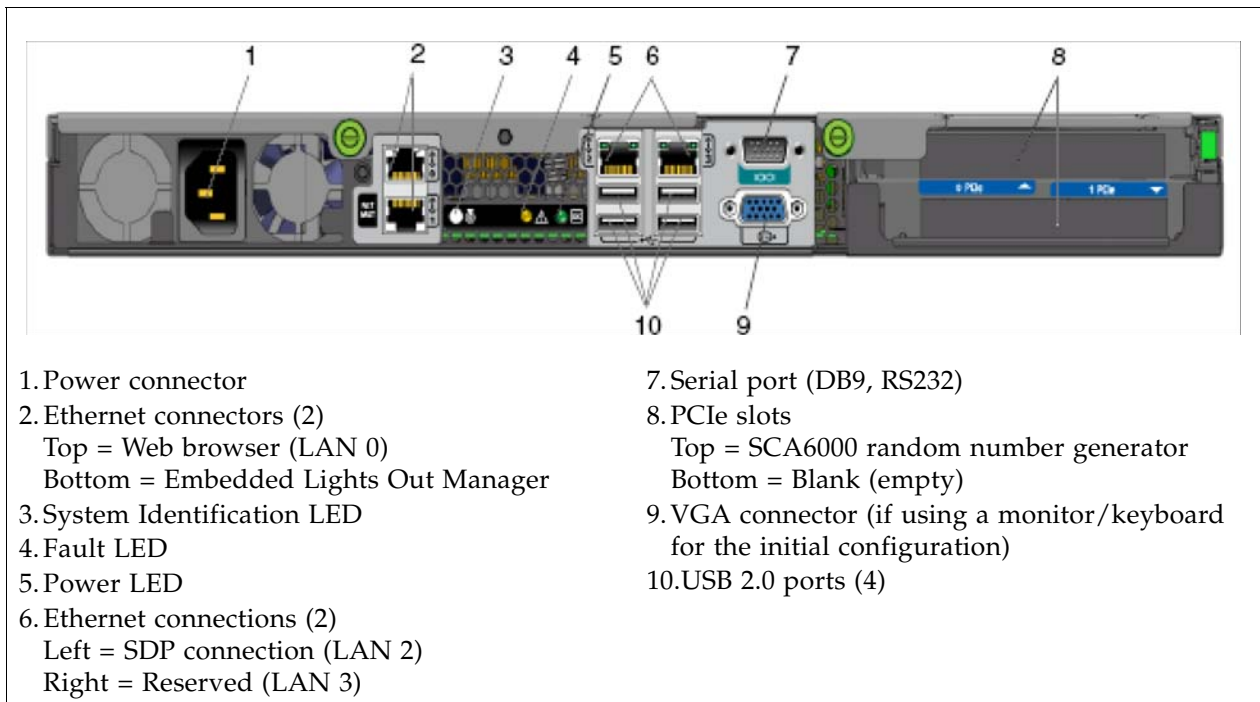


TABLE 1-3 lists the specifications for the SunFire X2100 server.

**TABLE 1-3** Sun Fire X2100 Specifications

<b>Processor</b>	<ul style="list-style-type: none"> <li>■ One dual-core AMD Operton processor</li> <li>■ Processor frequencies: 2.2 GHz</li> <li>■ Up to 1 MB level 2 cache</li> </ul>
<b>Memory</b>	<ul style="list-style-type: none"> <li>■ Four DIMM slots (up to 4 gigabytes)</li> <li>■ Unbuffered ECC memory</li> </ul>
<b>IPMI 2.0</b>	<ul style="list-style-type: none"> <li>■ Service processor standard</li> <li>■ embedded Lights Out Manager</li> </ul>
<b>Mass storage</b>	One SATA disk drive
<b>PCI Slots</b>	Two PCI-Express slots (PCIe) PCIe-0 contains the Sun Crypto Accelerator 6000 (SCA6000)
<b>Networking</b>	<ul style="list-style-type: none"> <li>■ Four USB 2.0 connectors on the rear panel</li> <li>■ Two USB 2.0 connectors on the front panel</li> <li>■ Two ports: Serial port with DB-9; VGA with DB-15 connectors</li> <li>■ Four 10/100/1000 Base-T Ethernet ports</li> </ul>
<b>Dimensions:</b>	
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
<b>Environmental parameters:</b>	
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
<b>Regulations meets or exceeds the following requirements:</b>	
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	

TABLE 1-4 lists the specifications for the SunFire X2200 server.

**TABLE 1-4** Sun Fire X2200 Specifications

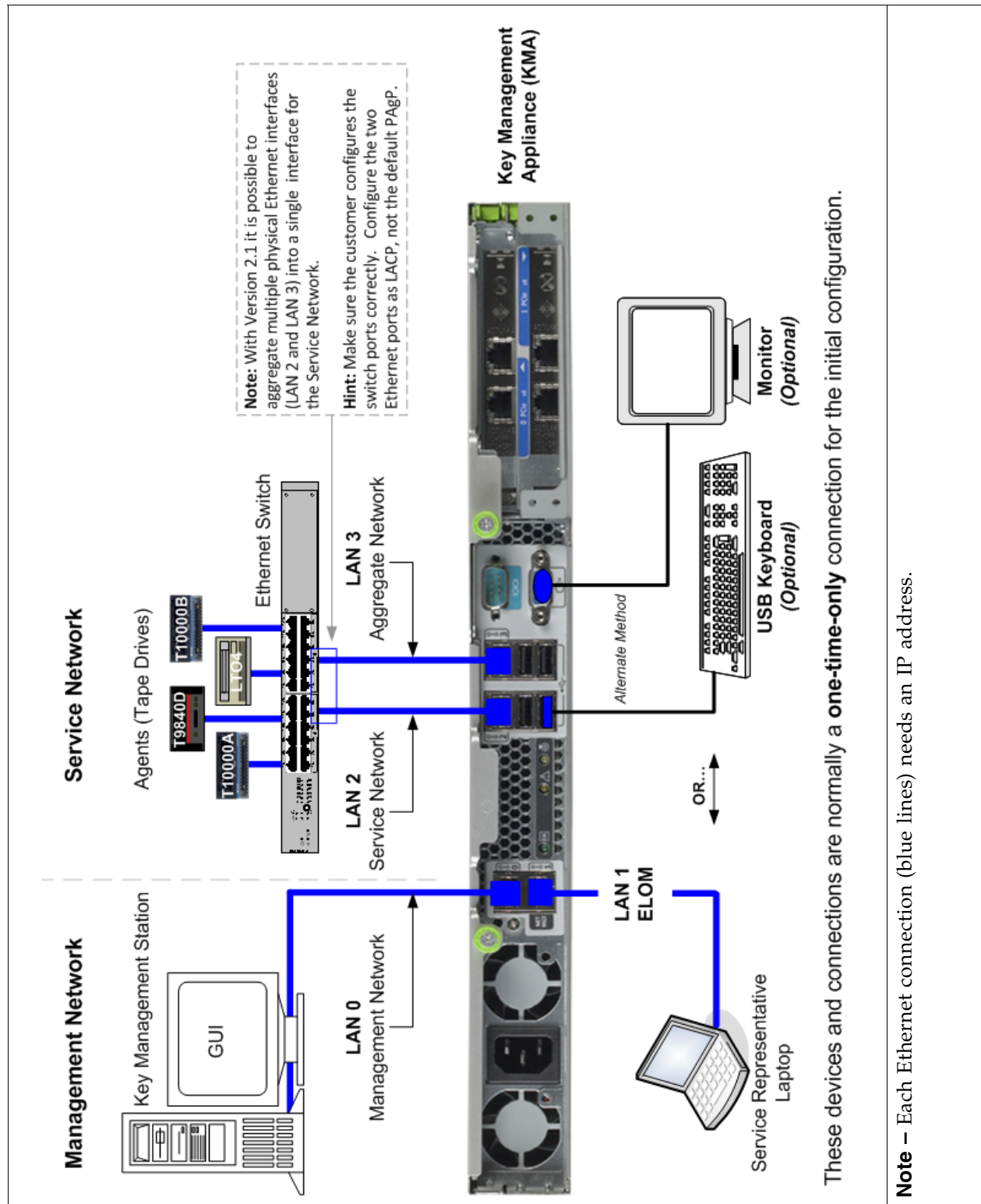
<b>Processor</b>	<ul style="list-style-type: none"> <li>■ Two Quad core AMD Opteron processors</li> <li>■ Processor frequencies: 2.3Ghz</li> </ul>
<b>Memory</b>	<ul style="list-style-type: none"> <li>■ 8 GB of RAM, installed as 4, 2 GB Dimms</li> </ul>
<b>IPMI 2.0</b>	<ul style="list-style-type: none"> <li>■ Service processor standard</li> <li>■ embedded Lights Out Manager</li> </ul>
<b>Mass storage</b>	One SATA disk drive 250 GB capacity
<b>PCI Slots</b>	Two PCI-Express slots (PCIe) PCIe-0 contains the Sun Crypto Accelerator 6000 (SCA 6000)
<b>Networking</b>	<ul style="list-style-type: none"> <li>■ Four USB 2.0 connectors on the rear panel</li> <li>■ Two USB 2.0 connectors on the front panel</li> <li>■ Two ports: Serial port with DB-9; VGA with DB-15 connectors</li> <li>■ Four 10/100/1000 Base-T Ethernet ports</li> </ul>
<b>Dimensions:</b>	
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
<b>Environmental parameters:</b>	
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
<b>Regulations meets or exceeds the following requirements:</b>	
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)	



# Key Management Appliance Physical Connections

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

**FIGURE 1-7** Key Management Appliance—Rear Panel 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
- LAN 3 = Aggregated network

**TABLE 1-5** KMA Network Connections

LAN 0	This is a <i>required</i> connection. This network is called the “Management Network” and connects to the Key Management System (KMS), graphical user interface (GUI), to the cluster. This network can be local, remote, or a combination of both. <b>Note – Customers are expected to provide this network.</b>
LAN 1*	This is a one time connection to configure the KMAs. This connection is called the “NET MGT ELOM” and provides a network connection for the Embedded Lights Out Manager. (See note below.)
LAN 2	This is normally a <i>required</i> 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 <i>optional</i> connection with KMS version 2.1. This is the “Aggregated Network” connection with LAN 2. 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.
<b>*Note –</b> The ELOM IP address is most easily configured using a serial connection. Connect a DB9-to-DB9 serial null modem cable from a laptop PC serial port to the serial port on the server. This is a <b>one time</b> connection for the <b>initial</b> configuration.	

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.

## Aggregation Network

With KMS Version 2.1 it is possible to aggregate multiple physical Ethernet interfaces into a single virtual interface.

Make sure the Ethernet switch ports have the correct c. For example, there is a difference between LACP and PAgP.

- The Link Aggregation Control Protocol (LACP) is an IEEE specification to control the bundling of several physical ports together to form a single logical channel.  
LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer.
- Port Aggregation Protocol (PAgP) is a Cisco Systems proprietary networking protocol, which is used for the automated, logical aggregation of Ethernet switch ports, known as an etherchannel. This means it can only be used between Cisco switches and/or switches from licensed vendors.

## Internet Protocol Versions

Another enhancement to KMS Version 2.1 is the support of the latest implementation of the Internet Protocol Suite, or IP. This protocol is used for switched inter-networks and the Internet.

- 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 next 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.

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



### Important:

The key management system supports a “dual stack” implementation, both protocols are used within the system. However, not all applications use IPv6, for example: Domain Name System (DNS) a hierarchical naming system.

## FIPS Compliant Tape Drives

With Version 2.1, the latest KMS software, and the latest tape drive firmware, the following drives are FIPS<sup>6</sup> compliant.

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

Tape Drive	FIPS Level
T10000A	1
T10000B	2
T9840D	1
LTO4	No plans for FIPS

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

**Level 1**—The lowest level with production-grade requirements.

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

---

6. **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.).

## Tape Drives

Well known for its *state-of-the-art* tape technology, StorageTek—a division of Sun Microsystems—has over 35 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 four tape drive models to choose from:

- T1000A
- T1000B
- T9840 Model D only
- Hewlett Packard (HP) LTO4

### About the T10000

The T10000 tape drive is a small, 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, and 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

**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 are fiber-optic to provide a high rate of data transfer. The T10000 drives support both Fibre Channel and FICON interfaces.

**Configurations:**

The T10000 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 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, and 38.1 cm (15 in.) deep.

### **Capacity:**

The T9840D uses 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 HP LTO4 Tape Drive

<b>Overview</b>	The Hewlett Packard (HP) LTO4 is the fourth-generation of Ultrium, Linear Tape-Open tape drives. This generation offers more capacity and increased performance than earlier versions of LTO tape drives.
<b>Encryption Capable</b>	<p>The Hewlett Packard LTO4 is the <i>first</i>, non-StorageTek T-Series tape drive to support the Crypto Key Management System Version 2.0.</p> <p>This encryption-capability requires a special, custom designed, Ethernet card—called the Dione card—that enables the LTO4 drive to connect to and interface with the Key Management System (KMS) network.</p> <p>With this connection, the LTO4 is capable of communicating with the KMS to transfer encryption keys over the secure network.</p> <p><i>Note:</i> The HP LTO4 can only use <i>one encryption key at a time</i>. During a read operation, if another encryption key is found, the Dione card requests the key directly from the KMS.</p>
<b>Media</b> (Native capacity)	<p>The HP LTO4 drive with LTO4 media can store up to 800 GB of data. This drive can also read and write on LTO3 media (400 GB), and provides read-only capabilities with LTO2 media (200 GB).</p> <p>The LTO4 tape drive also supports Write Once, Read Many (WORM) secure media. This non-erasable, non-rewritable media meets several compliance regulations such as HIPAA, Sarbanes-Oxley, and SEC 17A-4.</p> <p><i>Note:</i> Encryption is only possible using LTO4 media, including LTO4 WORM media, with the HP LTO4 tape drive. If you insert LTO2 or LTO3 media, encryption will be disabled.</p>
<b>Interfaces</b> (Native rates)	<p>The HP LTO4 drive supports up to 120 MB/s data transfer rates using Data Rate Matching (DRM). This feature allows the tape drive to dynamically and continuously adjust the speed of the drive, from 40 to 120 MB/s for maximum performance</p> <p>Interface support for the HP LTO4 includes:</p> <ul style="list-style-type: none"> <li>■ Ultra 320 Small Computer System Interface (SCSI)</li> <li>■ 4 Giga-bits per second (Gbps) Fibre Channel</li> </ul>

Installing this tape drive in one of Sun StorageTek's automated tape configurations offers customers with an even wider choice of tape-based storage solutions.

- Server compatibility: Fibre Channel and SCSI models on popular (qualified) platforms from vendors such as Sun, HP, IBM, and Dell.
- Software compatibility: Support for an extensive list of software applications such as ACSLS, HP, CA, VERITAS, Legato, Tivoli, and many more.
- Support for WORM media: Allows for unalterable backups using Write-Once Read-Many (WORM) media to meet compliance regulations.
- Mid-range class: Delivers confidence with a wide variety of supported backup applications.

# Tape Drive Comparison

**TABLE 1-7** Tape Drive Comparisons

<b>Physical Specifications</b>	<b>T10000A</b>	<b>T10000B</b>	<b>T9840D</b>	<b>LTO4</b>
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.)
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.)
Length (depth)	42.5 cm (16.75 in.)	42.5 cm (16.75 in.)	38.1 cm (15 in.)	20.3 cm (8 in.)
Weight	5 kg (11 lb)	5 kg (11 lb)	3.9 kg (8.5 lb)	2.24 kg (4.94 lb)
<b>Performance Specifications</b>				
Capacity (native)	500 GB	1 TB	75 GB	800 GB
Transfer rate (native)	2 Gb/s - 4 Gb/s	4 Gb/s	30 MB/s	4 Gb/s
Throughput (native)	120 MB/s	120 MB/s	30 MB/s	120 MB/s
Data Buffer size	256 MB	256 MB	64 MB	128 MB
Number of tracks	768	1152	576	896
Tape Thread & Load	16 sec	16 sec	8.5 sec	19 sec
Access Time	46 sec	46 sec	8 sec	62 sec
Tape speed	2.0 and 4.95 m/s	2.0 & 3.74 m/s 4.95 m/s legacy	3.4 m/s	7.00 m/s
Rewind time	90 sec	90 sec	16/8 sec	124 sec
Tape Unload	23 sec	23 sec	12 sec	22 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
MTBF (100% duty cycle)	290,000 hrs	290,000 hrs	290,000 hrs	250,000 hrs
<b>Media/Format Compatibility</b>				
Read/Write	Proprietary Format- T10000 Cartridge		Proprietary Format	LTO2 = Read only LTO3 = Rd/Write LTO4 = Rd/Write
VolSafe/WORM?	Yes		Yes	Yes
<b>Power</b>				
Auto-ranging / Amperage	88-264 VAC, 48-63 Hz			100–240 VAC 50–60 Hz 0.8A max.
Consumption	90 W		82 W	52 W

## Tape Drive and Media Comparisons

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

### T-Series Tape Drives

TABLE 1-8 shows the media compatibilities for the T-Series (T10000 and T9840) drives:

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

**TABLE 1-8** T-Series Tape Drive Media Compatibilities

Task	Encryption-capable	Non-encryption
Write new data encrypted	Yes	No
Write new data not encrypted	No	Yes
Read encrypted data with key available	Yes	No
Read non-encrypted data	Yes	Yes
Append non-encrypted data to encrypted tape	No	No

TABLE 1-9 shows a comparison between:

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

**TABLE 1-9** Tape Drive and Media Support

Tape Drive Types	Media Types	
	Non-encrypted Tapes	Encrypted Tapes
<b>Standard drive</b> (non-encrypted)	<ul style="list-style-type: none"> <li>■ Fully compatible</li> <li>■ Read, write, and append</li> </ul>	<ul style="list-style-type: none"> <li>■ <b>Not capable</b> of reading, writing to or appending to this tape</li> <li>■ Can re-write from the beginning of tape (BOT)</li> </ul>
<b>Encryption-capable drive</b>	<ul style="list-style-type: none"> <li>■ <b>Read</b> capability only</li> <li>■ Not capable of appending to this tape</li> <li>■ Can re-write from the beginning of tape (BOT)</li> </ul>	<ul style="list-style-type: none"> <li>■ Fully compatible</li> <li>■ Read with correct keys</li> <li>■ Write with current write key</li> </ul>



## HP LTO4 Tape Drives

HP LTO Ultrium 4 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:

Future compatibility:

In the future, HP LTO Ultrium 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

HP LTO Ultrium drives will always maintain write and read compatibility with other manufacturers' LTO Ultrium drives and tapes that meet the LTO Ultrium format specification.

**TABLE 1-10** 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** – Currently, only LTO4 media is encryption-capable on the LTO4 tape drives.

While LTO4 can read and “write” to LTO3 media, if an LTO4 drive encrypted data on LTO3 media, then LTO3 drives could not read those tapes. Therefore, when LTO3 media is inserted into an LTO4 drive, the encryption capability is disabled and the drive will write non-encrypted data without notification.



## 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 Sun 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 Sun 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 Sun representative schedules the system assurance planning meetings.

# Planning Meetings

The purpose of the system assurance planning meetings is to:

- Introduce the customer to the Sun 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 Sun team members to the customer. Complete the Team Member Contact sheets. Make copies as necessary.	Yes <input type="checkbox"/> No <input type="checkbox"/>
Explain the Sun StorageTek the encryption solutions to the customer. See <a href="#">Chapter 1, "Introduction"</a> for topics and information.	Yes <input type="checkbox"/> No <input type="checkbox"/>
Complete the Team Member Contact sheets.	Yes <input type="checkbox"/> No <input type="checkbox"/>
Use <a href="#">"Configuration Planning" on page 29</a> to help define the customer requirements.	Yes <input type="checkbox"/> No <input type="checkbox"/>
Review and complete <a href="#">"Site Planning Checklist" on page 32</a> . <i>Comments:</i>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Review and identify <a href="#">"User Roles Work Sheet" on page 56</a> . <i>Comments:</i>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Review <a href="#">"Supported Configurations" on page 57</a> . <i>Comments:</i>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Review <a href="#">"Order Numbers, Descriptions, and Contents" on page 65</a> . <i>Comments:</i>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Determine the installation schedule:  <b>Date:</b> _____  <b>Time:</b> _____	Yes <input type="checkbox"/> No <input type="checkbox"/>
Download and provide the customer with a copy of the: <i>Crypto Key Management System Administrator's Guide</i> PN 316195101. <i>Virtual Operator Panel—Customer</i> PN: 96179 <a href="http://docs.sun.com/app/docs/prod/stortek.crypto.keymgmt">http://docs.sun.com/app/docs/prod/stortek.crypto.keymgmt</a>	Yes <input type="checkbox"/> No <input type="checkbox"/>

---

# Customer Team Member Contact Sheet

Complete the following information for the customer team members:

**Name:** \_\_\_\_\_  
Title: \_\_\_\_\_  
Telephone Number: \_\_\_\_\_  
FAX Number: \_\_\_\_\_  
Cell Phone / Pager: \_\_\_\_\_  
E-mail Address: \_\_\_\_\_

**Name:** \_\_\_\_\_  
Title: \_\_\_\_\_  
Telephone Number: \_\_\_\_\_  
FAX Number: \_\_\_\_\_  
Cell Phone / Pager: \_\_\_\_\_  
E-mail Address: \_\_\_\_\_

**Name:** \_\_\_\_\_  
Title: \_\_\_\_\_  
Telephone Number: \_\_\_\_\_  
FAX Number: \_\_\_\_\_  
Cell Phone / Pager: \_\_\_\_\_  
E-mail Address: \_\_\_\_\_

**Name:** \_\_\_\_\_  
Title: \_\_\_\_\_  
Telephone Number: \_\_\_\_\_  
FAX Number: \_\_\_\_\_  
Cell Phone / Pager: \_\_\_\_\_  
E-mail Address: \_\_\_\_\_

---

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

---

---

# Sun Team Member Contact Sheet

Complete the following information for the Sun Microsystems 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** – Sun StorageTek Representatives may include: marketing, sales, and account representative, systems engineers (SEs), Professional Services (PS), installation coordinators, and trained services personnel.

---

# Configuration Planning

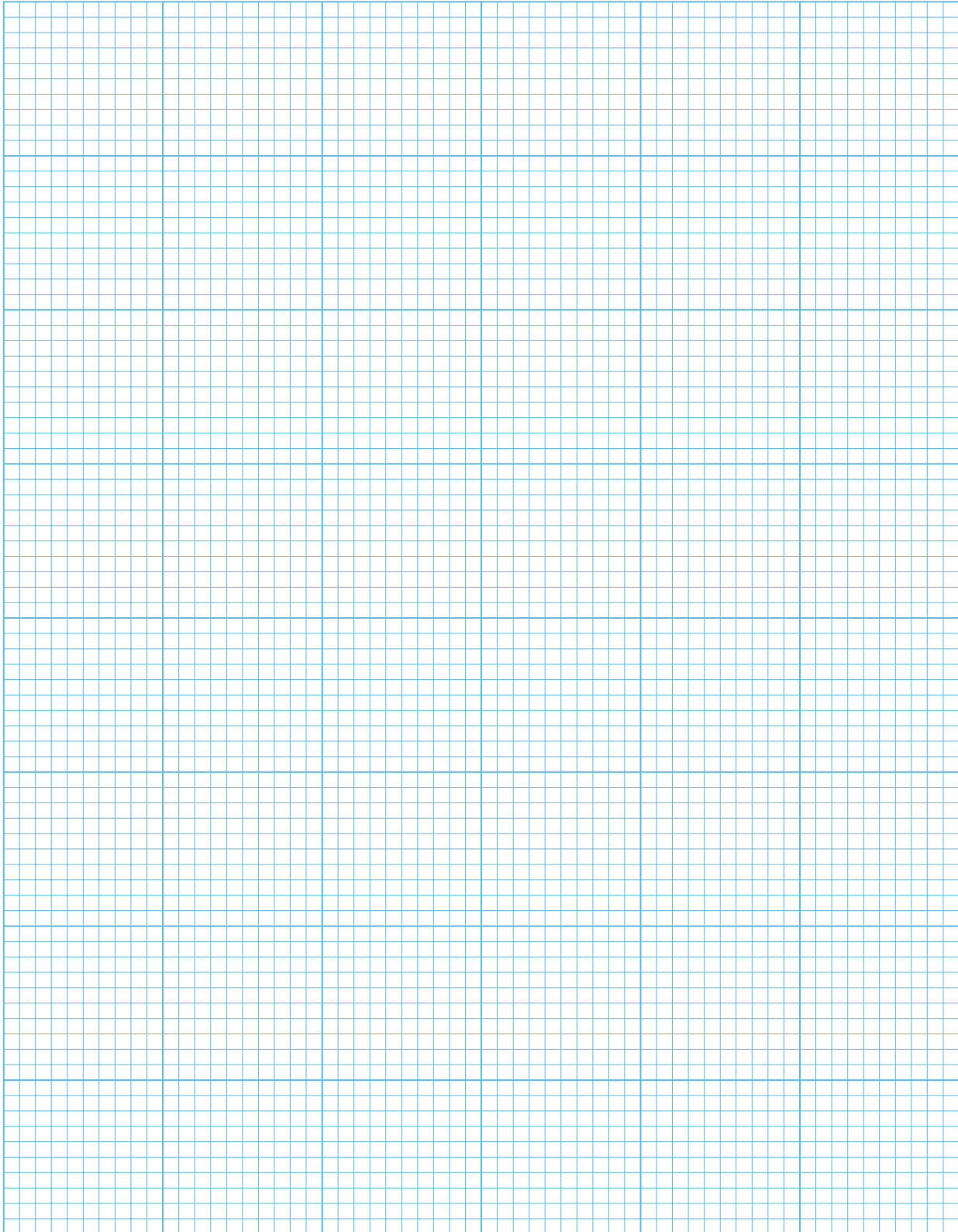
Complete the following checklist and make a conceptual drawing of to help with the installation. Provide this information and drawing to the installers.

**TABLE 2-2** Solution Planning Checklist

Question	Selection / Comments	Quantity
Which encryption solution does the customer want?	<input type="checkbox"/> <b>KMS 2.x</b> (Continue with this checklist)	
What type of configuration does the customer want? <b>Notes:</b> <ul style="list-style-type: none"> <li>■ The maximum number of sites with KMAs is 10. It is possible to have sites without KMAs connected across a customer supplied wide area network.</li> <li>■ Also, the 10 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.</li> </ul>	<input type="checkbox"/> Single site  <input type="checkbox"/> Multiple sites  <input type="checkbox"/> Disaster recovery site?	How many: _____  _____
How many appliances (KMAs) are needed?  <ul style="list-style-type: none"> <li>■ The maximum number of KMAs is 20.</li> <li>■ KMAs <i>must be</i> installed in pairs.*</li> </ul>	* <b>Installed in Pairs:</b> Exceptions to this standard configuration must be made with the approval of KMS Engineering, Professional Services, and Support Services.	
How many and of what type of encryption hardware kits are needed?	<input type="checkbox"/> SL8500 <input type="checkbox"/> SL3000 <input type="checkbox"/> SL500 <input type="checkbox"/> 9310 / 9741E <input type="checkbox"/> L-Series <input type="checkbox"/> Rackmount	How many: _____ _____ _____ _____ _____
How many and of what type of encryption tape drives are needed?	<input type="checkbox"/> T10000A <input type="checkbox"/> T10000B <input type="checkbox"/> T9840D <input type="checkbox"/> HP LTO4	How many: _____ _____ _____ _____
Are Racks required? Type?	Yes <input type="checkbox"/> No <input type="checkbox"/>	How many: _____

Identify customer requirements and expectations.

## Customer Conceptual Drawing





## Site Preparation

---

Use this chapter to prepare for the installation.

- [“Site Planning Checklist” on page 32](#)

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

- [“Rack Specifications” on page 35](#)
  - [“SL8500 Rack Guidelines” on page 35](#)
  - [“External Rack Installations” on page 36](#)
- [“Redundant Power” on page 37](#)
- [“Service Delivery Platform” on page 38](#)
- [“FIPS Compliant Tape Drives” on page 39](#)
- [“Internet Protocol Versions” on page 39](#)
- [“Content Management” on page 40](#)
  - [“Capacity on Demand” on page 41](#)
  - [“RealTime Growth Technology” on page 41](#)
  - [“Partitioning” on page 41](#)
  - [“Planning the Data Path” on page 42](#)
  - [“Tasks” on page 43](#)
- [“Required Tools” on page 48](#)
- [“Supported Platforms and Web Browsers” on page 48](#)
- [“Required Firmware Levels” on page 49](#)
- [“Role-Based Operations” on page 51](#)
  - [User Roles Work Sheet on page 56](#)

# 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:
<b>Delivery and Handling</b>		
<b>Important:</b> 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 <i>no</i> , where will the equipment be delivered?  If a delivery dock <i>is</i> available, what are the hours of operation?	Yes <input type="checkbox"/> No <input type="checkbox"/>  _____	
Are there street or alley limitations that might hinder delivery?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
Will authorized personnel be available to handle the delivery?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
Is the delivery location close to the computer room where the equipment will be installed?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
Is an elevator available to move the equipment to the appropriate floors?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
Is there a staging area where the equipment can be placed close to the installation site?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
<b>Environmental Planning</b>		
Does the site meet the environmental requirements for temperature, humidity, and cooling?	Yes <input type="checkbox"/> No <input type="checkbox"/>	KMA: 5°C to 35°C (41°F to 95°F)
Are there special requirements to dispose of or recycle the packing material, pallets, and cardboard?	Yes <input type="checkbox"/> No <input type="checkbox"/>	

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

Question	Completed?	Comments:
<b>Power Requirements</b>		
Does the intended site meet the power requirements?	Yes <input type="checkbox"/> No <input type="checkbox"/>	<b>KMA:</b> 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 300W
Have you identified the circuit breakers locations and ratings?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
Does the customer want redundant power options? If so, an additional APC power switch is required to create an uninterrupted power configuration.	Yes <input type="checkbox"/> No <input type="checkbox"/>	APC Switch = XSL8500-AC-SW-Z
Are there any power cable routing concerns?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
<b>Personnel:</b>		
Are there trained/qualified Sun StorageTek representatives locally to install and maintain the encryption equipment?	Yes <input type="checkbox"/> No <input type="checkbox"/>	<b>Names:</b>
<b>Connectivity:</b> Cabling is <i>very important</i> to establish a reliable network between the KMS GUI, KMAs, Ethernet switches, and tape drives.		
Does this customer support IPv6 implementations?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
Have you completed a: ■ Cable plan? ■ Configuration drawing?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
Have you determined the type and number of Ethernet cables required? <i>Customer supplied:</i> ■ KMS Manager to the network ■ Network to the KMAs  <i>Supplied in the encryption kits:</i> ■ Switch to each tape drive	Yes <input type="checkbox"/> No <input type="checkbox"/>	<b>Note:</b> ■ Ethernet cables come with the accessory kits. ■ Lengths are dependant on the location of the switches and devices.
<b>Configurations</b>		
Does the customer have adequate rack space to hold the KMAs and Ethernet switches?	Yes <input type="checkbox"/> No <input type="checkbox"/>	See <a href="#">"Rack Specifications"</a> on page 35 <b>Note:</b> A half-rack (20-units) can be ordered to hold the KMAs, switches, and PDUs. Kit <b>CRYPTO-20U-Z</b>

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

Question	Completed?	Comments:
What type of support configurations does the customer want?	<input type="checkbox"/> SL8500 <input type="checkbox"/> SL3000 <input type="checkbox"/> SL500 <input type="checkbox"/> 9310/9741e <input type="checkbox"/> L-Series <input type="checkbox"/> Rackmount	HP LTO4 only T-Series only T-Series only
Does the customer have existing tape drives to use?	Yes <input type="checkbox"/> No <input type="checkbox"/>	X-Options (conversion bills) may be required.
Are they already installed in a library?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
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 only)	Yes <input type="checkbox"/> No <input type="checkbox"/>  <input type="checkbox"/> T10000A <input type="checkbox"/> T10000B <input type="checkbox"/> T9840D <input type="checkbox"/> HP LTO4	How many tape drives?
<b>Media</b>		
Are additional cartridges required? ■ Data cartridge ■ Cleaning cartridges ■ VolSafe cartridges ■ Labels  ■ Type: _____  ■ Quantity: _____	Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/>	<b>Note:</b> 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.
<b>Notes:</b>		
<b>Configurations:</b>		
<b>Tape Drives:</b>		
<b>Media:</b>		

## Rack Specifications

The KMAs can be installed in standard, RETMA<sup>1</sup> 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 is required.

Each rack can hold up to 6 units—called Us<sup>2</sup>—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
<b>Rack numbering</b>	Rack numbering is top-down from 1 to 4. Rack 1 is on the top; Rack 4 is on the bottom.
<b>Rack mounting</b>	Components must be able to function in a vertical orientation.
<b>Dimensional restrictions</b>	Rack module depth is 72 cm (28 in.). Recommended safe length is 66 cm (26 in.).
<b>Equipment weight</b>	The accessory rack itself is mounted on slides rated for 80 kg (175 lb). The recommended safe load is 64 kg (140 lb). <b>The KMA is 10.7 kg (23.45 lb), the Ethernet switch is 1.5 kg (3.1 lb)</b>
<b>Power consumption</b>	Per rack module is 4 Amps (maximum). Per outlet strip is 200–240 VAC, 50 to 60 Hz. <b>The KMA is 185 W, the Ethernet Switch is 20 W.</b>
<b>Power cord</b>	Power plug to connect to the rack PDU is: IEC320 C13 shrouded male plug. Minimum cord length is component <i>plus</i> 46 cm (18 in.) for a service loop.
<b>Thermal requirements</b>	Maximum power dissipation is 880 watts (3,000 Btu/hr) per rack module.
<b>Regulatory compliance</b>	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.).

## External Rack Installations

Because some configurations might not have enough internal rack space to install the encryption hardware, an external rack is available for these configurations.

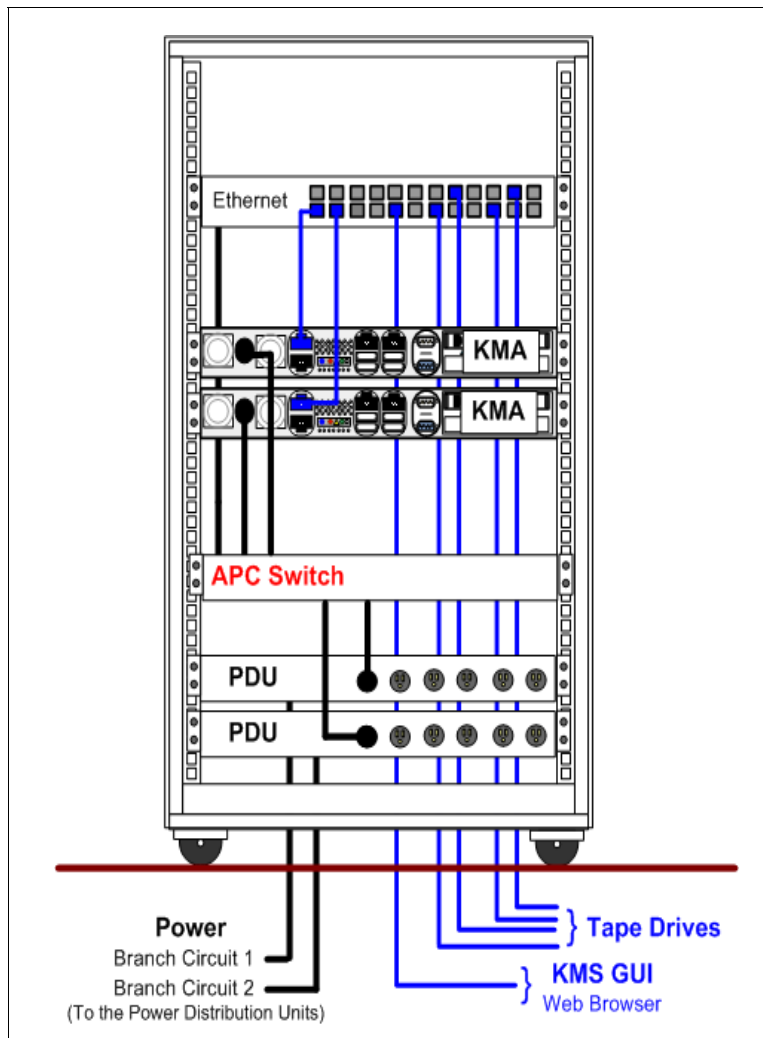
Customer's can either use existing racks or they can order this kit: **RACK-20U-Z**.

This is a half-high external rack.

- 20-units high (approximately 3 ft)
- 19-inches wide

Designed to hold the encryption hardware.

**FIGURE 3-1** External Rack Example



### Components and Part Numbers:

- Rack kit = RACK-20U-Z
- APC Switch = XSL8500-AC-SW-Z
- PDUs = PN 10124140

1. Service Network (LAN 2)
2. Management Network (LAN 0)



**Note** – Depending on the number of tape drives installed, you may need more than one Ethernet Switch. Remember, each tape drive needs an Ethernet connection.

## Redundant Power

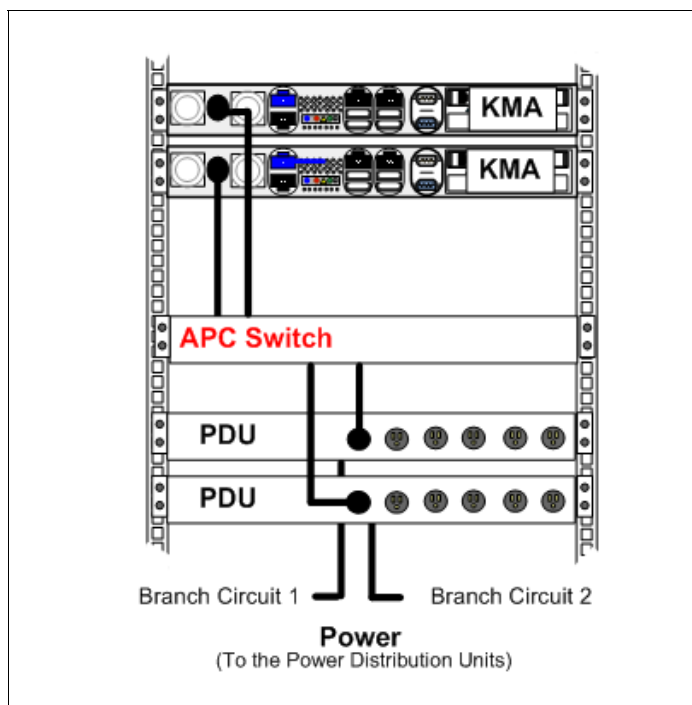
Customer may require a redundant power configuration.

When installing equipment to support *power redundancy*, make sure there are two separate branch circuits available. Should a power supply or branch circuit fail, the other equipment or circuit can maintain power to at least some of the configuration until the problem is fixed.

Because the additional hardware only has a single power supply, power distribution units are required to provide this redundancy.

FIGURE 3-2 shows an example:

**FIGURE 3-2** Power Redundancy



### Components and Part Numbers:

- APC Switch = XSL8500-AC-SW-Z
- PDUs = PN 10124140

Use the customer's existing power distribution or they can order an APC Power Switch, order number: **XSL8500-AC-SW-Z**.

## Service Delivery Platform

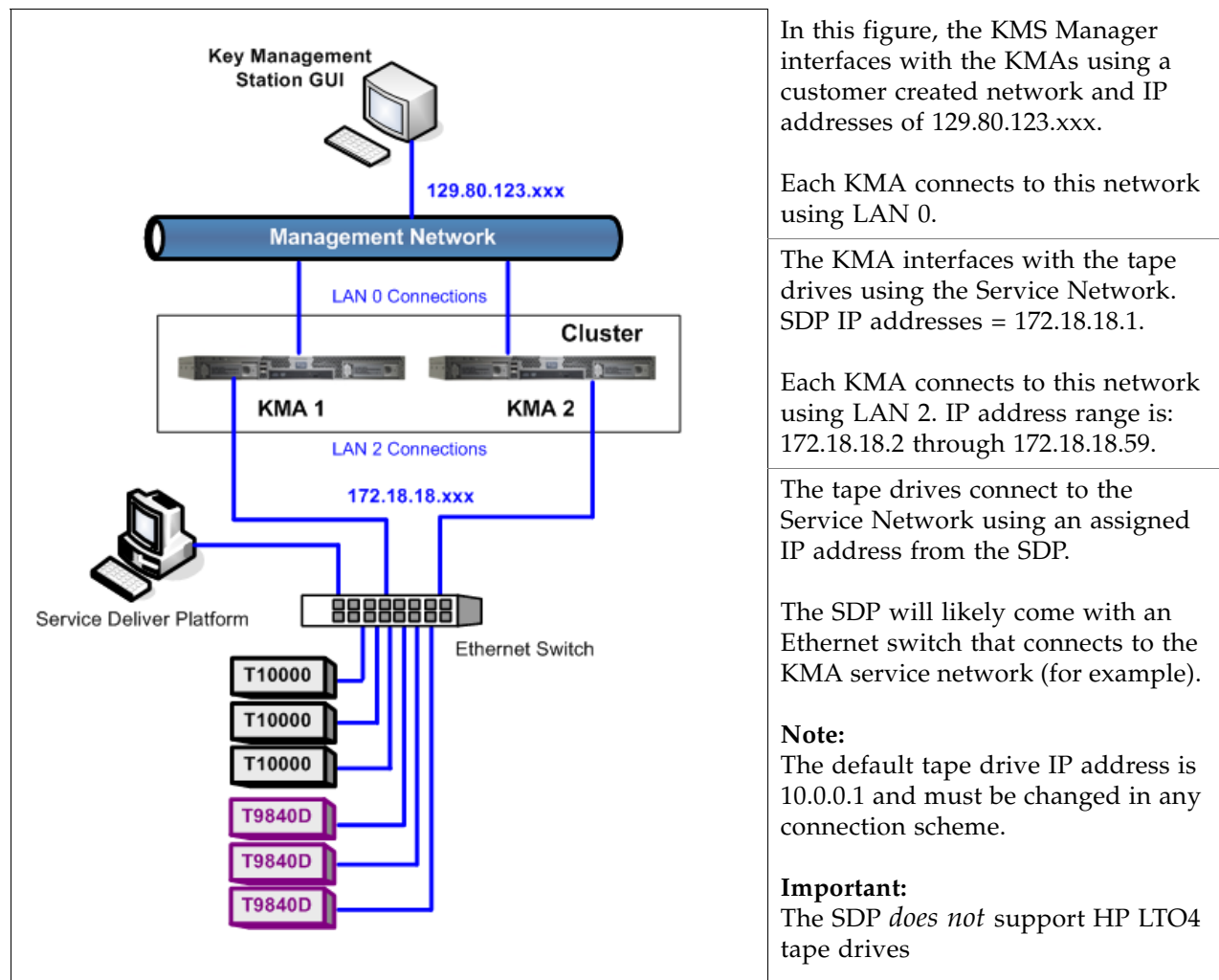
The Service Delivery Platform (SDP) is a support solution for Sun StorageTek libraries and tape drives that consists of a smart appliance and dedicated network.

The Key Management Appliance includes a specific Ethernet connection (LAN 2 port) for connection to this network.

The SDP appliance uses 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.

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

**FIGURE 3-3** Systems Delivery Platform



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: <http://csa-wiki.central.sun.com/display/SDP>



## FIPS Compliant Tape Drives

With Version 2.1, the latest KMS software, and the latest tape drive firmware, the following drives are FIPS<sup>3</sup> compliant.

**TABLE 3-3** FIPS Compliant Tape Drives

Tape Drive	FIPS Level
T10000A	1
T10000B	2
T9840D	1
LTO4	No plans for FIPS

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

**Level 1**—The lowest level with production-grade requirements.

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

## Internet Protocol Versions

Internet Protocol, or IP, is the protocol for the Internet and switched inter-networks using the Internet Protocol Suite.

- 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 next 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.

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



### Important:

The key management system supports a “dual stack” implementation, both protocols are used within the system. However, not all applications use IPv6, for example: Domain Name System (DNS) a hierarchical naming system.

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.).

# 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; however, considerations include:

**TABLE 3-4** Content Management Planning

Element	SL8500	SL3000	SL500
Drive Quantity	You may need to order multiple kits or additional Ethernet switches to support all of the encryption-capable tape drives.		
	<ul style="list-style-type: none"> <li>■ Single: 1 to 64 drives</li> <li>■ 10 library complex: up to 640 drives</li> </ul>	<ul style="list-style-type: none"> <li>■ 1 to 56 tape drives</li> </ul>	<ul style="list-style-type: none"> <li>■ 1 to 18 tape drives</li> </ul>
Encryption Drives Supported	<ul style="list-style-type: none"> <li>■ T10000 A&amp;B</li> <li>■ T9840D</li> <li>■ HP LTO4</li> </ul>	<ul style="list-style-type: none"> <li>■ T10000 A&amp;B</li> <li>■ T9840D</li> <li>■ HP LTO4</li> </ul>	<ul style="list-style-type: none"> <li>■ HP LTO4 only</li> </ul>
Non-encryption Drives Supported	<ul style="list-style-type: none"> <li>■ T10000 A&amp;B</li> <li>■ T9840 A, B, &amp; C</li> <li>■ LTO 2, 3, &amp; 4</li> </ul>	<ul style="list-style-type: none"> <li>■ T10000 A&amp;B</li> <li>■ T9840 C</li> <li>■ HP LTO 3 &amp; 4</li> </ul>	<ul style="list-style-type: none"> <li>■ LTO 2, 3, &amp; 4 (HP, IBM)</li> <li>■ SDLT 600</li> <li>■ DLT-S4</li> </ul>
Interfaces:	Note: The library interface and tape drive interfaces may be different.		
<ul style="list-style-type: none"> <li>■ Libraries</li> </ul>	<ul style="list-style-type: none"> <li>■ TCP/IP only</li> </ul>	<ul style="list-style-type: none"> <li>■ TCP/IP</li> <li>■ Fibre Channel</li> </ul>	<ul style="list-style-type: none"> <li>■ TCP/IP</li> <li>■ Fibre Channel</li> </ul>
<ul style="list-style-type: none"> <li>■ Tape Drives</li> </ul>	T10000 A&B FC and FICON T9840D FC, FICON, ESCON HP LTO4 FC only	T10000 A&B FC and FICON T9840D FC, FICON, ESCON HP LTO4 FC only	LTO4 Fibre Channel LTO4 SCSI (check availability)
Media*	All libraries support true-mixed media—Any Cartridge, Any Slot™		
	<ul style="list-style-type: none"> <li>■ T10000 (Std, Sport, VolSafe)</li> <li>■ 9840 (Std and VolSafe)</li> <li>■ LTO 2, 3, 4, &amp; T-WORM</li> <li>■ DLTtape III</li> <li>■ Super DLTtape I &amp; II</li> </ul>	<ul style="list-style-type: none"> <li>■ T10000 (Std, Sport, VolSafe)</li> <li>■ 9840 (Std and VolSafe)</li> <li>■ LTO 2, 3, 4, &amp; T-WORM</li> </ul>	<ul style="list-style-type: none"> <li>■ LTO 1, 2, 3, 4, &amp; T-WORM</li> <li>■ DLTtape III</li> <li>■ Super DLTtape I &amp; II</li> </ul>
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
Library Management	<ul style="list-style-type: none"> <li>■ ACSLS</li> <li>■ HSC</li> </ul>	<ul style="list-style-type: none"> <li>■ ACSLS</li> <li>■ HSC</li> <li>■ ISV</li> </ul>	<ul style="list-style-type: none"> <li>■ ACSLS</li> <li>■ HSC</li> <li>■ ISV</li> </ul>
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 (Veritas, Legato, TSM)	
* <b>Important:</b> 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—in front, to the left, 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

## 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 licensed 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.

Licensed capacity can be purchased in multiple increments:

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

## RealTime Growth Technology

Because the physical and the licensed slot capacities are separate, the customer has the option of installing physical capacity in advance before they are ready to activate 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 license or 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 appropriately 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 Sun 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.

## 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.

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

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

## Tasks

One essential message for content management and partitioning is planning.

**TABLE 3-5** Steps and Tasks for Partitioning

✓	Step	Task	Responsibility*
<input type="checkbox"/>	<b>1. Team</b>	Create a Team. When planning for content 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 and Sun Microsystems.	<ul style="list-style-type: none"> <li>■ Customer</li> <li>■ Administrators</li> <li>■ Operators</li> <li>■ SE, PS</li> <li>■ Svc Rep</li> </ul>
<input type="checkbox"/>	<b>2. Codes</b>	Review the software and firmware requirements. Update as required.	<ul style="list-style-type: none"> <li>■ Customer</li> <li>■ Sun SE, PS</li> <li>■ Svc Rep</li> </ul>
<input type="checkbox"/>	<b>3. Planning</b>	<ul style="list-style-type: none"> <li>■ Define the customer expectations</li> <li>■ Complete the assessment</li> <li>■ Identify the configurations</li> <li>■ Complete the planning diagrams</li> <li>■ Service Delivery Platform (SDP)</li> </ul>	<ul style="list-style-type: none"> <li>■ Customer</li> <li>■ Administrators</li> <li>■ SE, PS</li> <li>■ Svc Rep</li> </ul>
<input type="checkbox"/>	<b>4. Encryption</b>	<ul style="list-style-type: none"> <li>■ Complete an encryption survey (PS)</li> <li>■ Select the type of tape drive, interface, and configuration</li> <li>■ Select location</li> <li>■ Ensure there is adequate media</li> </ul>	<ul style="list-style-type: none"> <li>■ Customer</li> <li>■ SE, PS</li> <li>■ Sun Representatives</li> </ul>
<input type="checkbox"/>	<b>5. Media</b>	<ul style="list-style-type: none"> <li>■ Verify the distribution of cartridges and required tape drives are available and ready.</li> </ul>	<ul style="list-style-type: none"> <li>■ Customer</li> <li>■ Operators</li> </ul>
<input type="checkbox"/>	<b>6. Library</b>	<ul style="list-style-type: none"> <li>■ Install and configure a library (if necessary).</li> </ul>	<ul style="list-style-type: none"> <li>■ Svc Rep</li> </ul>
<input type="checkbox"/>	<b>7. License</b>	<ul style="list-style-type: none"> <li>■ License the required features:               <ul style="list-style-type: none"> <li>■ Library</li> <li>■ Tape drives</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>■ Customer</li> <li>■ Administrators</li> <li>■ Svc Rep</li> </ul>
<input type="checkbox"/>	<b>8. Partitions</b>	<ul style="list-style-type: none"> <li>■ Create partitions.</li> </ul>	<ul style="list-style-type: none"> <li>■ Customer</li> <li>■ Administrators</li> <li>■ Operators</li> </ul>
<input type="checkbox"/>	<b>9. Hosts</b>	<ul style="list-style-type: none"> <li>■ Momentarily stop all host activity if currently connected.</li> </ul>	<ul style="list-style-type: none"> <li>■ Customer</li> </ul>
<input type="checkbox"/>	<b>10. Use</b>	Instruct the customer how to: <ul style="list-style-type: none"> <li>■ Use and manage the library</li> <li>■ Use the KMS GUI</li> </ul>	<ul style="list-style-type: none"> <li>■ Customer</li> <li>■ SE, PS</li> <li>■ Svc Rep</li> </ul>
<input type="checkbox"/>	<b>11. Reference</b>	Make sure the customer has access to the appropriate documents.	<ul style="list-style-type: none"> <li>■ Customer</li> <li>■ Sun SE, PS</li> <li>■ Svc Rep</li> </ul>
<ul style="list-style-type: none"> <li>■ SE = Systems engineer</li> <li>■ PS = Professional services representative</li> <li>■ Service = Customer services representative (Svc Rep)</li> <li>■ Customer = System administrators, network administrators, system programmers, operators</li> </ul>			

## Preparing the Tape Drives

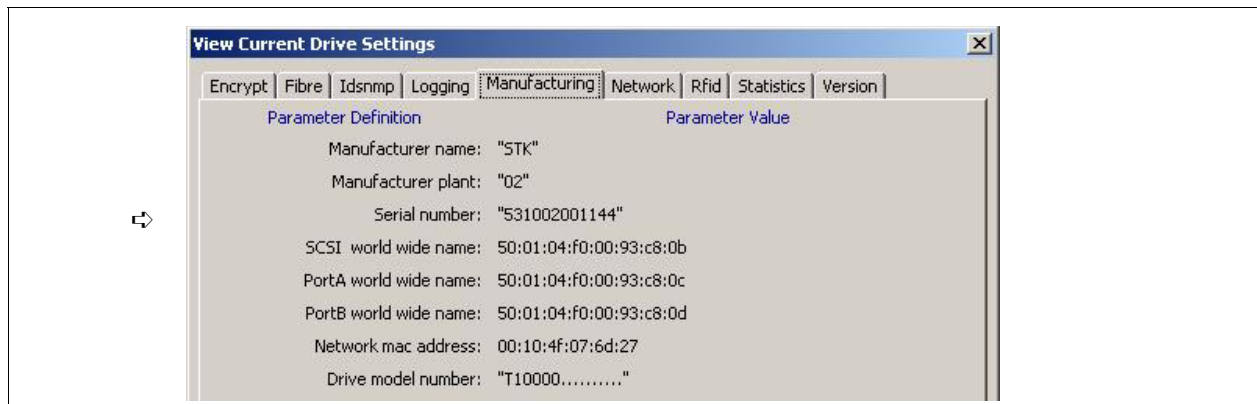
The tape drives should be installed and tested in their appropriate configuration before adding the encryption capability to them. Each drive-type has its own requirements.

### T-Series Drive Data Preparation

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

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

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



2. Use [TABLE A-3 on page 82](#) to build information about the tape drives. You will find this information helpful during the installation, licensing, and enrollment process for the tape drives (agents).
3. Request an Encryption Key File:
  - a.) Log in to the Applications Web site at: <http://crcapplications/keyswebapp/>
  - b.) Select Request an Encryption key.

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





**Access is Limited:** You must be a Sun employee, have completed the training courses, and have your name included on the list to access this link.

4. Complete the Encryption Request form.
  - a. First name, last name, and e-mail address are automatically included.
  - b. Provide a site ID and order number.
  - c. Select the tape drive type (T10000A, T10000B, or T9840D).
  - d. Complete the serial number for the selected tape drive.
  - e. Add any optional remarks and click Request Key File.  
 After submitting the Encryption File Request you will be prompted to download the file. This file contains the drive data you need to enable and enroll the drive.

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

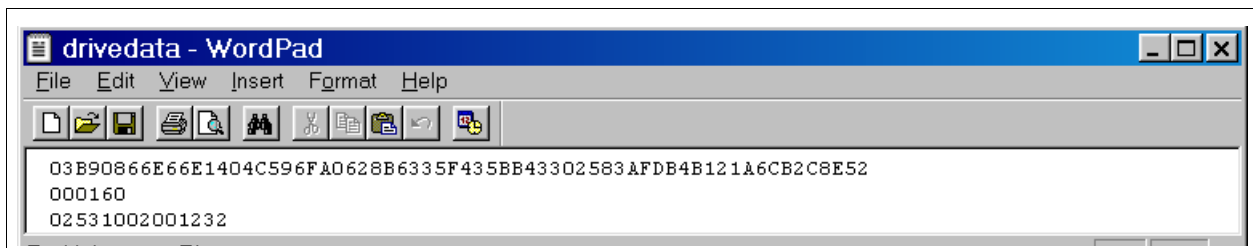
Family serial numbers start with:  
 T10000A = 5310 xxxxxxxx  
 T10000B = 5720 xxxxxxxx  
 T9840D = 5700 xxxxxxxx

When you select the drive family-type, these 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.

If you open the drive data file, using WordPad for example, you can see and verify the drive serial number, PCKey, and crypto serial number (CSN).

**FIGURE 3-7** Encryption File Request for Drive Data

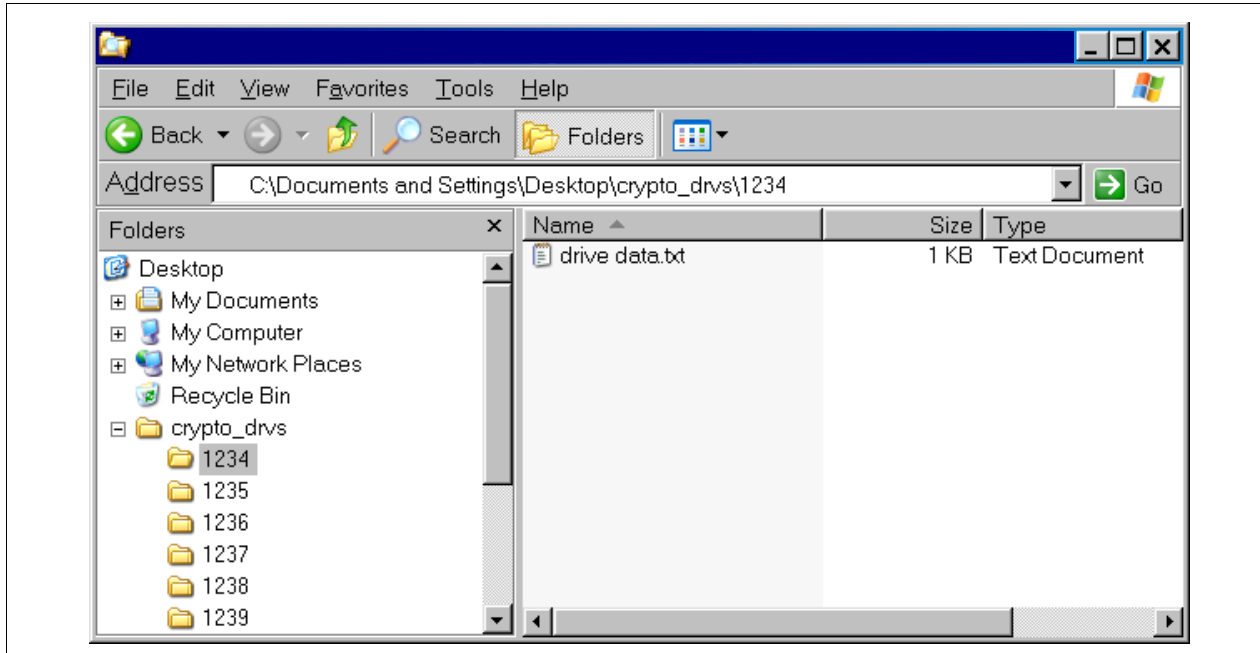


## Create a Drive Data File Structure

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

1. [FIGURE 3-8](#) 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 3-8** Drive Data File Structure



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

4. Complete [TABLE A-4 on page 83](#) to help with the licensing 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 it 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.



## HP LTO4 Tape Drive Preparation

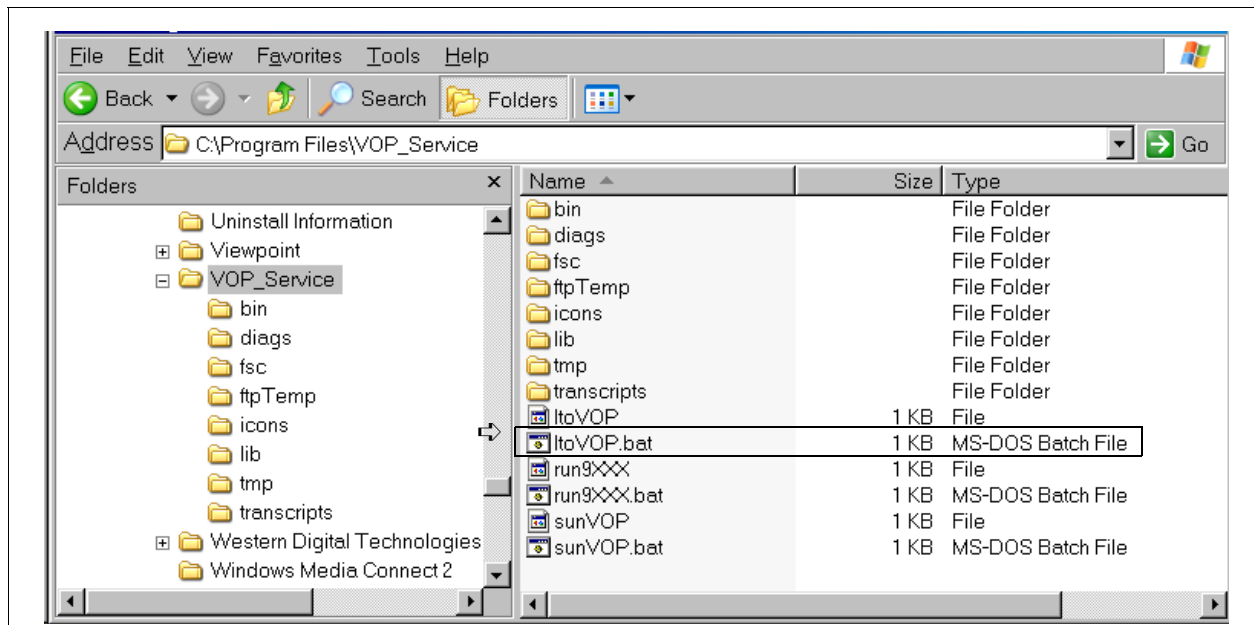
No PCKey or drive data is required for the LTO4 tape drives. The only preparation is to make sure the customer has the information to assign the IP addresses and Agent names for the tape drives for the KMS manager.

**Note** – The Virtual Operator Panel must be at Version 1.0.12 and higher to provide support for the HP LTO4 tape drive. To use the VOP for LTO4 tape drives, you need to launch a special file:

- **Windows:** Launch the batch file (**ltoVOP.bat**)
- **Solaris/Linux:** Launch the **ltoVOP** file (above the batch file)

FIGURE 3-9 shows an example of the VOP 1.0.12 download contents.

**FIGURE 3-9** 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 side cutters; 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 LTO4 tape drives at Version 1.0.12 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.

TABLE 3-6 lists the supported operating systems and Web browsers:

**TABLE 3-6** Operating Systems and Web Browsers

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

# Required Firmware Levels

The minimum—recommended— firmware requirements include:

**TABLE 3-7** Firmware Compatibilities

Component	Version	Version	
KMS Version 2.x	2.02 (recommended)	2.1	

## Library Management

ACSLs	7.1 and 7.1.1 with PUT0701, or 7.2, and 7.3
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-H45S F (FC only)	L-2.05 D-H45S F (FC only)	n/a	n/a	L-1300 SPS D-H45S F D-B44S S	1.0.12

### Legend:

L—Library firmware level

D—Drive firmware level

H45S F = Fibre Channel firmware (LTO4)

B44S S = SCSI firmware (LTO4)

FC = Fibre Channel

SPS = Special firmware. Requires approval.

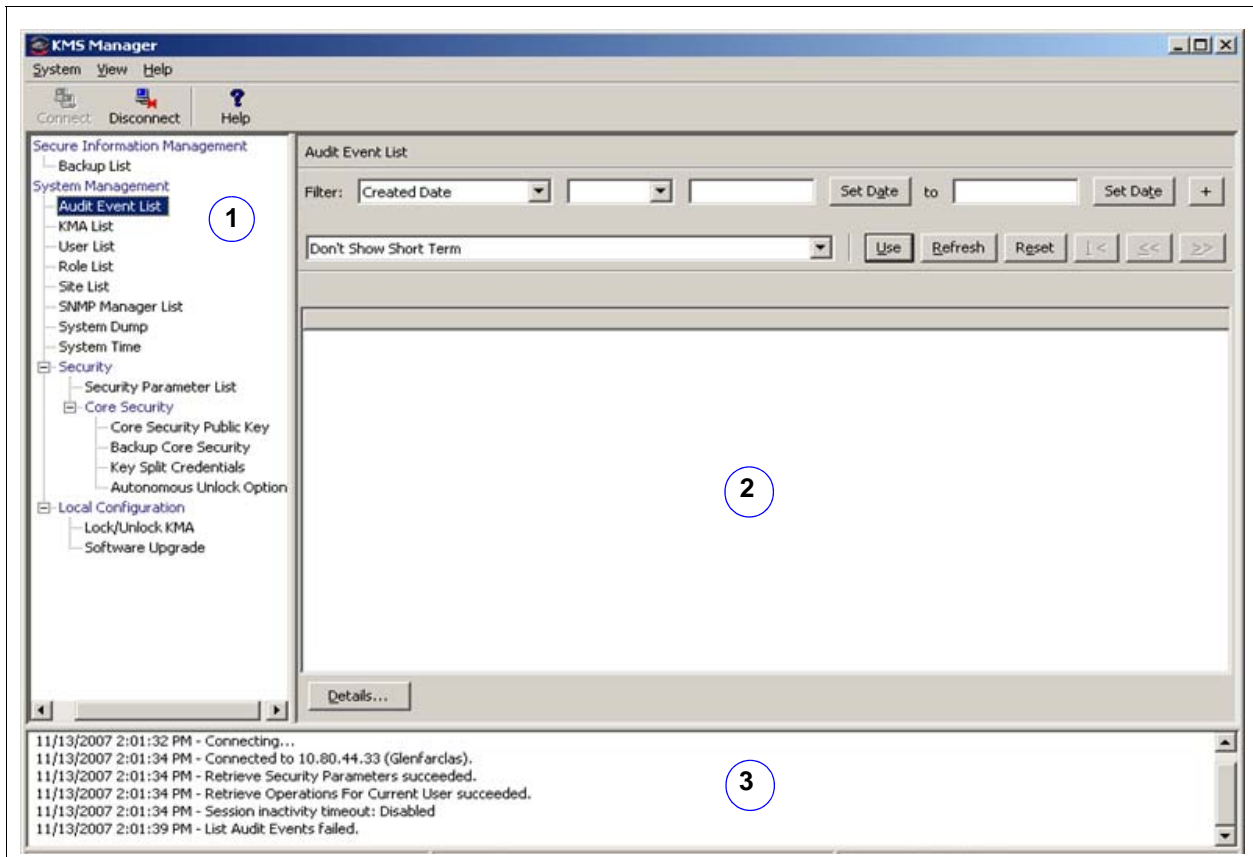
n/a = Not supported. Not applicable.

# 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 3-8** KMS Manager Display



The KMS Manager is an easy-to-use, text-based interface that allows users to configure functions of the KMAs depending on the roles that user is assigned (see [“Role-Based Operations”](#) on page 51).

The manager contains convenient 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.

■ <b>Security Officer</b>	Full authority to view, modify, create, and delete Sites, KMAs, Users, and Transfer Partners.
■ <b>Compliance Officer</b>	Management for <i>key policies</i> and <i>key groups</i> . Determines which Agents and Transfer Partners can use key groups.
■ <b>Operator</b>	Manages Agents, Data Units, and Keys.
■ <b>Backup Operator</b>	Performs backups.
■ <b>Auditor</b>	Views information about the KMS Cluster.



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

FIGURE 3-10 shows an example of the Users Detail screen.

Use TABLE 3-10 on page 56 to help prepare for the assignments.

**FIGURE 3-10** 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 and lower case, numbers, symbols)
- and 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 3-9 on page 52 shows the system entities and functions that each user role can perform. In the "Roles" columns:

- **Yes** means the role is allowed to perform the operation.
- **Quorum** the role is allowed to perform the operation but must belong to a quorum.
- **Blank** means the role is not allowed to perform the operation.

**TABLE 3-9** Operator Roles and Functions

Entity	Function	Roles				
		Security Officer	Compliance Officer	Operator	Backup Operator	Auditor
<b>Console</b>						
	Log In	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
<b>Connect</b>						
	Log In	Yes	Yes	Yes	Yes	Yes
	Create Profile	Yes	Yes	Yes	Yes	Yes
	Delete Profile	Yes	Yes	Yes	Yes	Yes
	Set Config Settings	Yes	Yes	Yes	Yes	Yes
	Disconnect	Yes	Yes	Yes	Yes	Yes
<b>Key Split Credentials</b>						
	List	Yes				
	Modify	Quorum				
<b>Autonomous Unlock</b>						
	List	Yes				
	Modify	Quorum				
<b>Lock/Unlock KMA</b>						
	List Status	Yes	Yes	Yes	Yes	Yes
	Lock	Yes				
	Unlock	Quorum				

**TABLE 3-9** Operator Roles and Functions (Continued)

Entity	Function	Roles				
		Security Officer	Compliance Officer	Operator	Backup Operator	Auditor
<b>Site</b>						
	Create	Yes				
	List	Yes		Yes		
	Modify	Yes				
	Delete	Yes				
<b>Security Parameters</b>						
	List	Yes	Yes	Yes	Yes	Yes
	Modify	Yes				
<b>KMA</b>						
	Create	Yes				
	List	Yes		Yes		
	Modify	Yes				
	Delete	Yes				
<b>User</b>						
	Create	Yes				
	List	Yes				
	Modify	Yes				
	Modify Passphrase	Yes				
	Delete	Yes				
<b>Role</b>						
	List	Yes				
<b>Key Policy</b>						
	Create		Yes			
	List		Yes			
	Modify		Yes			
	Delete		Yes			
<b>Key Group</b>						
	Create		Yes			
	List		Yes	Yes		
	List Data Units		Yes	Yes		
	List Agents		Yes	Yes		
	Modify		Yes			
	Delete		Yes			

**TABLE 3-9** Operator Roles and Functions (Continued)

Entity	Function	Roles				
		Security Officer	Compliance Officer	Operator	Backup Operator	Auditor
<b>Agent</b>						
	Create			Yes		
	List		Yes	Yes		
	Modify			Yes		
	Modify Passphrase			Yes		
	Delete			Yes		
<b>Agent/Key Group Assignment</b>						
	List		Yes	Yes		
	Modify		Yes			
<b>Data Unit</b>						
	Create					
	List		Yes	Yes		
	Modify			Yes		
	Modify Key Group		Yes			
	Delete					
<b>Keys</b>						
	List Data Unit Keys		Yes	Yes		
	Destroy			Yes		
	Compromise		Yes			
<b>Transfer Partners</b>						
	Configure	Quorum				
	List	Yes	Yes	Yes		
	Modify	Quorum				
	Delete	Yes				
<b>Backup</b>						
	Create				Yes	
	List	Yes	Yes	Yes	Yes	
	List Backups with Destroyed Keys		Yes	Yes		
	Restore	Quorum				
	Confirm Destruction				Yes	



**TABLE 3-9** Operator Roles and Functions (Continued)

Entity	Function	Roles				
		Security Officer	Compliance Officer	Operator	Backup Operator	Auditor
<b>Core Security Backup</b>						
	Create	Yes				
<b>SNMP Manager</b>						
	Create	Yes				
	List	Yes		Yes		
	Modify	Yes				
	Delete	Yes				
<b>Audit Event</b>						
	View	Yes	Yes	Yes	Yes	Yes
	View Agent History		Yes	Yes		
	View Data Unit History		Yes	Yes		
	View Data Unit Key History		Yes	Yes		
<b>System Dump</b>						
	Create	Yes		Yes		
<b>System Time</b>						
	List	Yes	Yes	Yes	Yes	Yes
	Modify	Yes				
<b>NTP Server</b>						
	List	Yes	Yes	Yes	Yes	Yes
	Modify	Yes				
<b>Software Version</b>						
	List	Yes	Yes	Yes	Yes	Yes
	Upgrade			Yes		

**TABLE 3-10** User Roles Work Sheet

User ID	Description	Passphrase ** (Confidential password)	Roles						
			Security Officer	Compliance Officer	Operator	Backup Operator	Auditor		
			<p><b>Note:</b> The Passphrase should not be recorded here for security reasons. This column is provided as a reminder that as User IDs are enter, the person with that ID will be required to enter a passphrase.</p>						

## Ordering

---

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

---

### Supported Configurations

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

- [“Key Management Appliance” on page 58](#)  
This is a required component for key creation, management, and assignments.

If you are implementing an encryption solution using a Sun 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:

- T1000A
- T1000B
- T9840D
- HP LTO4

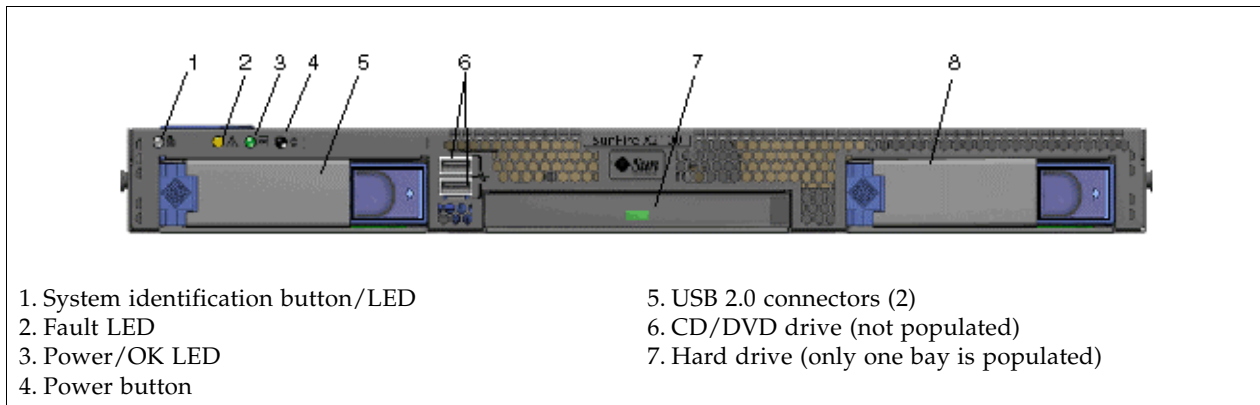
See [“Tape Drive Comparison” on page 21](#) for drive specifications and [“Required Firmware Levels” on page 49](#) for supported firmware versions.

# Key Management Appliance

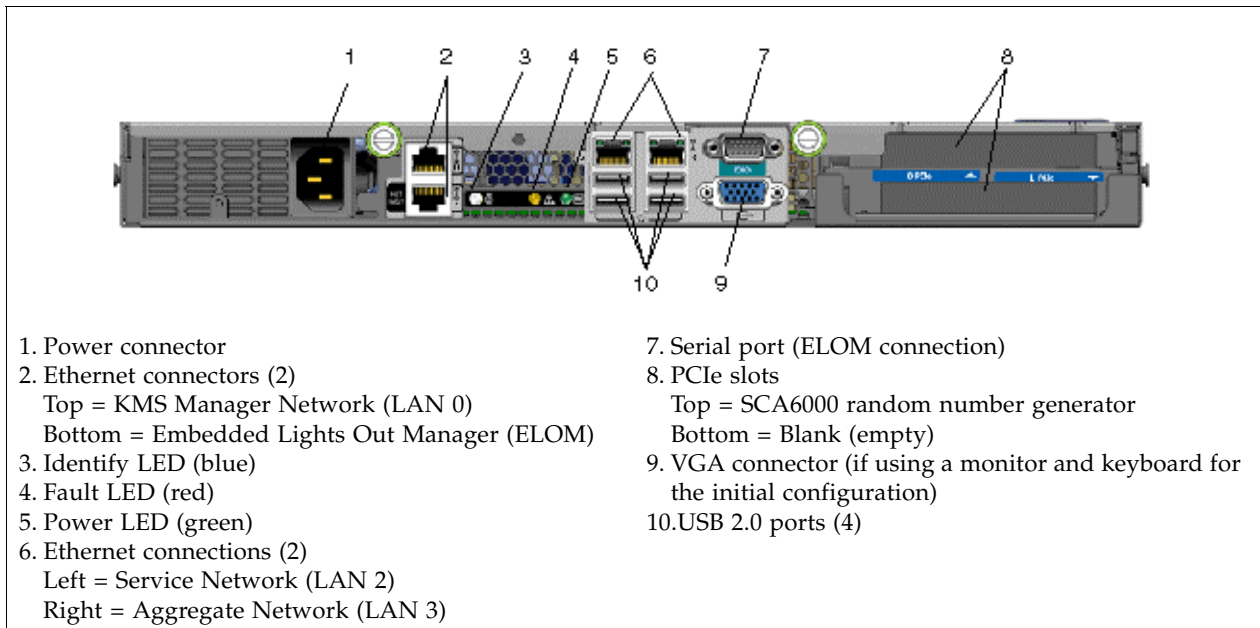
The key management appliance order number is: **CRYPTO-KMA-2-Z**, which includes:

- Key Management Appliance (KMA)
- Rackmount Model
- Includes Sun Fire X2100 Server with
- Pre-loaded Solaris 10 operating system and key management system software
- Installation included

**FIGURE 4-1** Key Management Appliance—Front Panel



**FIGURE 4-2** Key Management Appliance—Rear Panel



# SL8500 Modular Library System

**TABLE 4-1** SL8500 Modular Library System Requirements

**High-level Description:**

A single SL8500 library can store up to:

- 1,448 to 10,000 tape cartridges and
- 64 tape drives.

An SL8500 Library Complex of 10 libraries can store up to:

- 100,000 tape cartridges and
- 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

SL8500 accessory kit. Installation included.

**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-Z = 6RU Rack

XSL8500-RACK-HW-Z = Rack component hardware kit

XSL8500-AC-SW-Z = AC Transfer Switch

**Firmware Levels**

Library	3.72 (3.98 or higher is recommended and to support LTO4)
StreamLine Library Console	3.38
Tape Drives: <ul style="list-style-type: none"> <li>■ T10000A</li> <li>■ T10000B</li> <li>■ T9840D</li> <li>■ HP LTO4</li> </ul>	1.34.208 or higher 1.38.x07 or higher 1.42.104 or higher H45S Fibre Channel
Virtual Operator Panel (VOP)	Version 1.0.11 or higher Version 1.0.12 or higher for LTO4

# SL3000 Modular Library System

**TABLE 4-2** SL3000 Modular Library System Requirements




<p><b>High-level Description:</b> The SL3000 library offers customers the benefits of:</p> <ul style="list-style-type: none"> <li>■ Scalability in storage capacity from 200 to 4500 slots</li> <li>■ Performance from 1 to 56 tape drives</li> <li>■ Heterogeneous attachments using standard interfaces</li> <li>■ Multiple library management software options and programs</li> </ul>	<p><b>Operating System Support:</b> The SL3000 supports all major operating systems; enterprise <i>and</i> open systems.</p> <p><b>Host-to-Library Interface:</b></p> <ul style="list-style-type: none"> <li>■ Single Ethernet* (TCP/IP) 1x</li> <li>■ Dual TCP/IP* (optional feature) 2x</li> <li>■ Fibre Channel* 1x</li> </ul> <p>* Supports Partitioning</p>
---	--

Order Number	Description
<ul style="list-style-type: none"> <li>■ SL3000 Kit 1 XSL3000-ETHRNT1-Z</li> <li>■ SL3000 Kit 2 XSL3000-ETHRNT2-Z</li> <li>■ SL3000 Kit 3 XSL3000-ETHRNT3-Z</li> <li>■ SL3000 Kit 4 XSL3000-ETHRNT4-Z</li> </ul>	<p>The SL3000 uses four different part numbers for Ethernet switches and cables to 1 to 56 tape drives.</p> <p><b>Note:</b> The SL3000 has limited internal rack space. Depending on the number of drives, customers may need to order an external rack. See <a href="#">“External Rack Installations”</a> on page 36 if necessary.</p>

Firmware Levels	
Library	2.0.2
StreamLine Library Console	4.0
Tape Drives: <ul style="list-style-type: none"> <li>■ T10000A</li> <li>■ T10000B</li> <li>■ T9840D</li> <li>■ HP LTO4</li> </ul>	1.34.208 or higher 1.38.x07 or higher 1.42.104 or higher H45S Fibre Channel
Virtual Operator Panel (VOP)	Version 1.0.11 or higher Version 1.0.12 or higher for LTO4

# SL500 Modular Library System

**TABLE 4-3** SL500 Modular Library System Requirements

<p><b>High-level Description:</b> 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:</p> <ul style="list-style-type: none"> <li>■ From: 2 tape drives with 530 data cartridge slots</li> <li>■ To: 18 tape drives with 395 data cartridge slots</li> <li>■ A cartridge access port that holds 5 to 45 slots (depending on the number of modules)</li> </ul> <p>With a variety of tape drives and cartridges slots in-between.</p> <p><b>Operating System Support:</b> The SL500 supports all major operating systems; enterprise <i>and</i> open systems.</p> <p><b>Host-to-Library Interface:</b></p> <ul style="list-style-type: none"> <li>■ Single Ethernet* (TCP/IP) 1x</li> <li>■ Fibre Channel</li> </ul> <p>* Supports Partitioning</p>		<p>Encryption hardware can be installed in the same rack as the library; depending on the number of modules installed.</p>
---	--	--

Order Number	Description
CRYPTO-2X-SL500B-Z	SL500 base library ( <i>required</i> ). Installation included.
CRYPTO-2X-SL500X-Z	SL500 expansion modules ( <i>optional</i> ) Up to 4 additional expansion modules may be added. Installation included.
	<p><b>Note:</b> The SL500 is a rack-installed library.</p> <ul style="list-style-type: none"> <li>■ With 3 or fewer expansion modules, encryption hardware can be installed in the same rack.</li> <li>■ With 4 expansion modules, there is no room for the encryption hardware and customers may need to order an external rack.</li> </ul> <p>See <a href="#">“External Rack Installations”</a> on page 36 if necessary.</p>

## Firmware Levels

Library	i15 — 1300 (SPS)
StreamLine Library Console	
Tape Drives: <ul style="list-style-type: none"> <li>■ HP LTO4</li> </ul>	H45S Fibre Channel or B44S SCSI
Virtual Operator Panel (VOP)	Version 1.0.12 or higher

# 9310 Automated Cartridge System

**TABLE 4-4** 9310 Automated Cartridge System Requirements

<p><b>High-level Description:</b> The 9310—also called PowderHorn—can store:</p> <ul style="list-style-type: none"> <li>■ From 2,000 up to 6,000 tape cartridges</li> <li>■ Up to 4 drive cabinets with space for up to 20 drives per cabinet (80 drives total)</li> </ul> <p><b>Operating System Support:</b> The 9310 library supports all major operating systems; enterprise <i>and</i> open systems.</p> <p><b>Host-to-Library Interface:</b></p> <ul style="list-style-type: none"> <li>■ TCP/IP</li> </ul> <p>The 9310 requires additional hardware consisting of Ethernet switches and 19-inch rack.</p>	
--	--

Order Number	Description
CRYPTO-2X-9310-Z	9310 accessory kit. Includes Ethernet switches plus cabling. <b>Important:</b> This kit include the hardware for the first 9741e. If customer has more than one 9741E they must order additional 9741E accessory kits. Installation included.
9310 libraries require: CRYPTO-2X-9741E-Z	9741E Drive Cabinet accessory kit. Includes 24-port switch and cabling. Installation included.  <b>Note:</b> Each 9741E cabinet may contain up to 20 tape drives and requires the use of a 24-port Ethernet switch.

### Firmware Levels

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

**TABLE 4-5** 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-Z

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.  
Installation included.

**Firmware Levels**

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

**TABLE 4-6** Rackmount Requirements

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

This figure shows the T10000 rack module.

- The top (A) operator panel works with the drive on the left.
- The bottom (B) operator panel works with the drive on the right.

When only one drive is installed, it must be installed on the left.

**Recommendation:**

The customer should purchase a CBNT42U cabinet with this configuration.



T105\_006

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

**Firmware Levels**

Tape Drives: <ul style="list-style-type: none"> <li>■ T10000A</li> <li>■ T10000B</li> <li>■ T9840D</li> </ul>	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 4-7 through TABLE 4-20 on page 78 provide information about ordering components, field replaceable units (FRUs) spares, x-options (conversion bills), and service options for the Sun StorageTek encryption solutions.

**TABLE 4-7** KMS 2.x Core Parts

Numbers		Product		
Marketing	Manufacturing	Description	Category	Details
CRYPTO-KMA-2-Z	CRYPTO-KMA-2-Z	KMA 2.0 rack mounted server	TAPE LIB	Sun StorageTek crypto KMA appliance rack mount model, pre-loaded Solaris, rack mounting hardware, client GUI CD. Installation is included. RoHS 5 compliant.
CRYPTO-X-16PT-Z	CRYPTO-X-16PT-Z	16PT ethernet switch	TAPE LIB	Sun StorageTek 16PT ethernet switch. No mounting HW or cables. RoHS 5 compliant.
CRYPTO-X-24PT-Z	CRYPTO-X-24PT-Z	24PT ethernet switch	TAPE LIB	Sun StorageTek 24PT ethernet switch. No mounting HW or cables. RoHS 5 compliant.
X-CRYPTO-1XTO2XUPZ	X-CRYPTO-1XTO2X	1.x to 2.0 Crypto upgrade kit	TAPE LIB	Sun StorageTek crypto KMA appliance rack mount model, with mounting HW, pre-loaded Solaris. Client management GUI CD. Installation is included. RoHS 5 compliant.
CRYPTO-2X-9310-Z	CRYPTO-2X-9310-	Crypto kit for 9310 libs.	TAPE LIB	Sun StorageTek crypto kit for use with 9310 libraries. 24-port ethernet switch and cables for installation in 9310 plus 16-port ethernet switch and cables for connection to KMA externally. Rack mounting HW. RoHS 5 compliant.
CRYPTO-2X-9741E-Z	CRYPTO-2X-9741E	Crypto kit for one 9741E cab.	TAPE LIB	Sun StorageTek crypto kit for use with 9310 libraries. 24-port ethernet switch, cables, and rack mount HW for installation within 9741E cabinet. One required for each additional 9741E cabinet used for crypto. RoHS 5 compliant.
CRYPTO-2X-L7/14-Z	CRYPTO-2X-L7/14	Crypto kit for L-series libs.	TAPE LIB	Sun StorageTek crypto kit for use with L180/700/1400 libraries. 16-port ethernet switch, cables, and mounting HW for installation within L-series libraries. RoHS 5 compliant.
CRYPTO-2X-SL500B-Z	CRYPTO-2X-SL500	Crypto kit for SL500 lib, base	TAPE LIB	Sun StorageTek crypto kit for use with SL500 library base. Ethernet switch and cables for installation within SL500 library. RoHS compliant.

**TABLE 4-7** KMS 2.x Core Parts

Numbers		Product		
Marketing	Manufacturing	Description	Category	Details
CRYPTO-2X-SL500X-Z	CRYPTO-2X-SL500	Crypto kit for SL500 lib, exp	TAPE LIB	Sun StorageTek crypto kit for use with SL500 library expansion. Ethernet cables for installation within SL500 library. RoHS compliant.
CRYPTO-2X-SL8500-Z	CRYPTO-2X-SL850	Crypto kit for SL8500 library	TAPE LIB	Sun StorageTek crypto kit for use with SL8500 libraries. 24-port ethernet switch, cables, and rackmount HW for installation within SL8500 library. RoHS 5 compliant.
XSL3000-ETHRNT1-Z	XSL3000-ETHRNT1	SL3000 Drv E-Switch Harness 1	STK	Sun 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-Z	XSL3000-ETHRNT2	SL3000 Drv E-Switch Harness 2	STK	Sun 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-Z	XSL3000-ETHRNT3	SL3000 Drv E-Switch Harness 3	STK	Sun 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-Z	XSL3000-ETHRNT4	SL3000 Drv E-Switch Harness 4	STK	Sun 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	Sun StorageTek SL3000 X-Option, 2Gb FC Interface Card (MPU2), RoHS-5

**TABLE 4-8** KMS 2.x Software License

Numbers		Product		
Marketing	Manufacturing	Description	Category	Details
9840D-EKEY-A	9840D-EKEY-A	T9840D, EKEY A Activation	STK	Sun 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	Sun 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	T10A-2FI-EKEY-A	T10KA 2GbFI CryptoKey, Aftermkt	TAPE LIB	Sun StorageTek Crypto Key for previously installed T10000A 2Gb FICON Crypto Channel Tape Drives. Used in conjunction with Sun StorageTek Crypto Key Management System, Crypto Library Accessory Kits and Crypto Rackmount System. Includes Software Key for enabling encryption in the tape drive. Installation also included.
T10A-2FI-EKEY-B	T10A-2FI-EKEY-B	T10KA 2GbFI Crypto Key, Bundled	TAPE LIB	Sun StorageTek Crypto Key for new (bundled) T10000A 2Gb FICON Crypto Channel Tape Drive purchases. Used in conjunction with Sun StorageTek Crypto Key Management System, Crypto Library Accessory Kits and Crypto Rackmount System. Includes Software Key for enabling encryption in the tape drive. Installation also included.
T10A-4FC-EKEY-A	T10A-4FC-EKEY-A	T10KA 4Gb Crypto Key, Aftermkt	TAPE LIB	Sun StorageTek Crypto Key for previously installed T10000A 4Gb Fibre Channel and 2Gb FICON Tape Drives. Used in conjunction with Sun StorageTek Crypto Key Management Station, Crypto Library Accessory Kits and Crypto Rackmount System. Includes Software Key for enabling encryption in the tape drive. Installation also included.

**TABLE 4-8** KMS 2.x Software License

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

**TABLE 4-9** Tape Drives Order Numbers

Numbers		Product		
Marketing	Manufacturing	Description	Category	Details
LTO4E-HP4FC-SL30Z	LTO4E-HP4FC-SL3	LTO4 HP FC 4Gb SL3000 EncrypDr	STK	Sun StorageTek HP LTO4 FC 4Gb Encryption drive for SL3000 Library featuring 120 MB/Sec transfer rate, 800 GB native capacity. Need to order the required cables separately. RoHS 5.
LTO4E-HP4FC-SL500Z	LTO4E-HP4FC-SL5	LTO4 HP FC 4Gb SL500 EncrypDr	STK	Sun StorageTek HP LTO4 FC 4Gb Encryption drive for SL500 Library featuring 120 MB/Sec transfer rate, 800 GB native capacity. Need to order the required cables separately. RoHS 5.
LTO4E-HP4FC-SL85Z	LTO4E-HP4FC-SL8	LTO4 HP FC 4Gb SL8500 EncrypDr	STK	Sun StorageTek HP LTO4 FC 4Gb Encryption drive for SL8500 Library featuring 120 MB/Sec transfer rate, 800 GB native capacity. Need to order the required cables separately. RoHS 5.
LTO4E-HPSC-SL500Z	LTO4E-HPSC-SL50	LTO4 HP SCSI SL500 EncrypDr	STK	Sun StorageTek HP LTO4 SCSI Encryption drive for SL500 Library featuring 120 MB/Sec transfer rate, 800 GB native capacity. Need to order the required cables separately. RoHS 5.
<b>Drive Upgrade Kits</b>				
T10A-2GBCRYP-85UPZ	T10A-2GBCRYP-85	T10KA 2GB FICRYP8500 ONLY UPGD	STK	Sun 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	Sun StorageTek T10000A 2Gb FICON to 2Gb FICON encryption upgrade kit. This kit is for all libraries, ROHS-5
XHPLTO4E-FCUP3085Z	XHPLTO4E-FCUP30	HP LTO4 FC drive upgd SL30/85	TAPE LIB	HP LTO4 FC encryption drive upgrade for SL3000 and SL8500 libraries. Serial to Ethernet interface card, cabling, drive tray back-plate. RoHS compliant.
XHPLTO4E-FCUPL500Z	XHPLTO4E-FCUPL5	HP LTO4 FC drive upgd SL500	TAPE LIB	HP LTO4 FC encryption drive upgrade for SL500. Serial to Ethernet interface card, cabling, drive tray back-plate. RoHS compliant.
X-HPLTO4E-SCUP500Z	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, drive tray back-plate. RoHS compliant.

**TABLE 4-10** Service Order Numbers

Numbers		Product		
Marketing	Manufacturing	Description	Category	Details
EIS-CRYPTOKIT-E	EIS-CRYPTOKIT-E	Install Crypto Kit	SERVICE	Installation only of Crypto Kit into new or existing Sun StorageTek library during local business hours
EIS-CRYPTOKIT-E-AH	EIS-CRYPTOKIT-E	Install Crypto Kit AH	SERVICE	Installation only of Crypto Kit into new or existing Sun StorageTek library after local business hours
EIS-CRYPTOSTAT-E	EIS-CRYPTOSTAT-	Install Crypto Station	SERVICE	Installation only of Crypto Station into new or existing Sun StorageTek library during local business hours
EIS-CRYPTOSTAT-E-AH	EIS-CRYPTOSTATE	Install Crypto Station AH	SERVICE	Installation only of Crypto Station into new or existing Sun StorageTek library after local business hours
IWU-T1AKMS-1G	IWU-T1AKMS-1G	STK CRYP-T10K MGMT UG 1YR GOLD	SERVICE	Sun 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	Sun 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	Sun 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	Sun 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	Sun StorageTek KMS Crypto Key Management Administration
NWS-3506	NWS-3506	Sun STK Crypto KMS 1.2 Admin	SERVICE	Sun StorageTek Crypto Key Management Station (KMS) 1.2 Administration
NWS-3507	NWS-3507	Sun STK Crypto KMS 2.0 Admin	SERVICE	Sun StorageTek Crypto Key Management Station (KMS) 2.0 Administration



**TABLE 4-10** Service Order Numbers

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 Sun 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.

**TABLE 4-11** Spares Order Numbers

Numbers		Product		
Marketing	Manufacturing	Description	Category	Details
#3144947-Z	#3144947-Z	Spares KMS Crypto key token	STK	Sun StorageTek Spares Crypto Token. Secure key repository. Use with Sun STK Crypto KMS and Lib Accessory Kit token bays. RoHS 6 Compliant.
#3144974-Z	#3144974-Z	Spares KMS workstation.	STK	Sun 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	Sun StorageTek Spares Token Bay only, desktop for use with Sun STK Crypto KMS. RoHS 6 Compliant.
#3144988-Z	#3144988-Z	FRU, Token Bay, Rack Mount, Front	STK	Sun StorageTek Spares, Rack mounted (front) crypto token bay. RoHS 6 Compliant.
#3154719-Z	#3154719-Z	FRU, Token Bay, Rack Mount, Rear	STK	Sun StorageTek Spares, Rack mounted (rear) crypto token bay. RoHS 6 Compliant.
#3154936-Z	#3154936-Z	Spares, KMA appliance only.	STK	Sun 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 Sun Fire 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.

**TABLE 4-12** KMS 1.x Parts Order Numbers

Numbers		Product		
Marketing	Manufacturing	Description	Category	Details
CRYPTO-KMS-D-Z	CRYPTO-KMS-D-Z	Crypto KMS Desktop Appliance	TAPE LIB	Sun 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. Installation included; 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	Sun StorageTek Crypto L180/700/1400 Accessory Kit. For use with Sun StorageTek Crypto Key Management System. Includes Token Bay, 2 Tokens, 16-port Switch and cabling. Installation also included.
CRYPTO-RACK-Z	CRYPTO-RACK-Z	Crypto Rackmount Kit	TAPE LIB	Sun StorageTek Crypto Rackmount Kit. For use with Sun StorageTek Crypto Key Management System. Includes Token Bay, 2 Tokens, 16-port Switch and cabling. Installation also included.
CRYPTO-TOKEN-Z	CRYPTO-TOKEN-Z	Crypto KMS Token	TAPE LIB	Sun StorageTek Crypto Token. Secure key repository. For use with Sun 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	Sun StorageTek Crypto SL8500 Accessory Kit with Ethernet hub and cabling only. For use with Sun StorageTek Crypto Key Management System. Includes 24-port Ethernet hub and cabling. Installation also included. 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.

**TABLE 4-12** KMS 1.x Parts Order Numbers

Numbers		Product		
Marketing	Manufacturing	Description	Category	Details
CRYPTO-8500-RKNO-Z	CRYPTO-8500-RKN	Crypto SL8500 Kit without Rack	TAPE LIB	Sun StorageTek Crypto SL8500 Accessory Kit without Rack. For use with Sun StorageTek Crypto Key Management System. Includes Token Bay, 2 Tokens, 24-port Switch and cabling. Installation also included.
CRYPTO-9310-RK-Z	CRYPTO-9310-RK-	Crypto 9310 Kit with Rack	TAPE LIB	Sun StorageTek Crypto 9310/L6000 Accessory Kit with Rack. For connection to 9741E cabinets in conjunction w/ Sun 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. Installation also included.
CRYPTO-9741E-Z	CRYPTO-9741E-Z	Crypto 9741E Kit	TAPE LIB	Sun StorageTek Crypto 9741E Accessory Kit. For connection to 9310/L6000 Accessory Kit in conjunction w/ Sun 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. Installation also included.

## 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 4-13** 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

## 9310 Upgrades

**TABLE 4-14** 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, therefore in most cases the firmware upgrade marketing part number should be ordered.	
<input type="checkbox"/> YXSL9310-T10K-FW	9310 Firmware upgrade for T10000
<input type="checkbox"/> YXSL9310-T10K-HW	9310 hardware CB for T10000
<input type="checkbox"/> YXSL9330-T10K	9330 Upgrade for T10000 One per LMU
<input type="checkbox"/> YX9741E-T10K-9310	C/B 9741E T10K Install 9310 One per cabinet

## Professional Services

Professional Services Encryption Implementation Required; one per site.

**TABLE 4-15** Professional Services Ordering Instructions and Part Numbers

Order Number	Description
<b>Important: Professional Services is required for new installations.</b>	
<input type="checkbox"/> WW-PS-INTG-KMS	<b>KMS Integration Service</b> The <b>Key Management System Integration Service</b> provides an integration of the KMS hardware and software into the encryption capable tape back-up and archive solution. <b>Note:</b> This service is required for any new tape encryption installations.
<input type="checkbox"/> WW-PS-ARCH-ENCRYPT	<b>Encrypt Ready Assess</b> The <b>Encryption Readiness Assessment</b> 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.

---

## Tape Drive Ordering Instructions

See the specific tape drive Systems Assurance Guides for—order numbers, descriptions, and additional information—for the different tape drives and the availability.

**TABLE 4-16** 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 Ordering Instructions

See the specific tape drive and library Systems Assurance Guides for—order numbers, descriptions, and additional information—for the different tape drives and the availability.

**TABLE 4-17** 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

# HP LTO4 Order Numbers

## License Keys

**FIGURE 4-3** LTO4 License Keys

LTO4 Encryption Key	Marketing Number	Description
Bundled	X-HP-LTO4-EKEY-B	One required per encryption enabled drive. Bundled with the drive at time of sale.
After market	X-HP-LTO4-EKEY-A	One required per encryption enabled drive. After market for drives previously purchased.

## Configured End Items

**TABLE 4-18** LTO4 Configured End Items—Order Numbers

Part Numbers	Description
<b>SL500</b>	
LTO4E-HP4FC-SL500Z	LTO4 HP FC 4Gb SL500 Encryp Dr
LTO4E-HPSC-SL500Z	LTO4 HP SCSI SL500 Encryp Dr
<b>SL8500</b>	
LTO4E-HP4FC-SL85Z	LTO4 HP FC 4Gb SL8500 EncrypDr
<b>SL3000</b>	
LTO4E-HP4FC-SL30Z	LTO4 HP FC 4Gb SL3000 EncrypDr

## X-Options (Conversion Bills)

**TABLE 4-19** LTO4 Conversion Bill Numbers

Part Numbers	Description
<b>SL500</b>	
XHPLTO4E-FCUPL500Z	Crypto drive upgrade for HP LTO4 FC SL500
XHPLTO4E-SCUP500Z	Crypto drive upgrade for HP LTO4 SCSI SL500
<b>SL3000/8500</b>	
XHPLTO4E-FCUP3085Z	Crypto drive upgrade for HP LTO4 FC SL3000/SL8500

## Dione Card

**TABLE 4-20** Dione Card Part Number—LTO4

Part Number	Description
419954901	HP LTO4 Dione Card



## Work Sheets

---

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

These work sheets include:

- [“Initial Configuration Work Sheet” on page 80](#)
- [“User Roles Work Sheet” on page 81](#)
- [“Tape Drives Work Sheet” on page 82](#)
- [“Drive Enrollment Work Sheet” on page 83](#)

Make copies as necessary.

# Initial Configuration Work Sheet

**TABLE A-1** Initial Configuration Settings—Customer

	First KMA			Second KMA		
	Hostname	IP Address / Netmask	DHCP?¹	Hostname	IP Address / Netmask	DHCP?¹
<b>LAN 0 = Management</b>			Yes <input type="checkbox"/> No <input type="checkbox"/>			Yes <input type="checkbox"/> No <input type="checkbox"/>
<b>LAN 1 = ELOM</b>			Yes <input type="checkbox"/> No <input type="checkbox"/>			Yes <input type="checkbox"/> No <input type="checkbox"/>
<b>LAN 2 = Service</b>			Yes <input type="checkbox"/> No <input type="checkbox"/>			Yes <input type="checkbox"/> No <input type="checkbox"/>
<b>LAN 3 = Aggergate</b>			Yes <input type="checkbox"/> No <input type="checkbox"/>			Yes <input type="checkbox"/> No <input type="checkbox"/>
<b>IPv6 Support?</b>	Yes <input type="checkbox"/> No <input type="checkbox"/>			Yes <input type="checkbox"/> No <input type="checkbox"/>		
<b>KMA Name</b>						
<b>Gateway</b>						
<b>DNS Server</b>	Hostname: IP address:			Hostname: IP address:		
<b>Security Officer</b>	Login: Passphrase:			Login: Passphrase:		
<b>Root account Passphrase</b>						
<b>ELOM Passphrase</b>						
<b>Key Split Credentials</b>						
<b>Autonomous Unlocking ²</b>						
<b>Keyboard Type</b>						
<b>Note:</b>	<p>1. Addresses assigned using DHCP <b>must be static</b>. The system cannot handle the DHCP server changing the IP addresses once assigned.</p> <p>2. 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.</p>					

# User Roles Work Sheet

TABLE A-2 User Roles Work Sheet—Customer

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

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

# Tape Drives Work Sheet

**TABLE A-3** Tape Drive and Agents Work Sheet—Service Representative

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.				

# Drive Enrollment Work Sheet

**TABLE A-4** Enrollment Data Work Sheet—Customer

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



# Glossary

---

This glossary defines terms and abbreviations used in this publication.

---

## A

**Abnormal end of task**

**(abend)** A software or hardware problem that terminates a computer processing task.

**Advanced Encryption**

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

**AES** See Advanced Encryption Standard.

**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 API** See Agent Library API.

**Agent Library** The Agent Library is used by an Agent to retrieve key material from a KMS.

**Agent Library API** The API provided by the Agent Library. Agents call this API.

**Audit** See Audit Log.

**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 Lock** 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

- CA** See Certificate Authority (CA).
- Certificate** A Certificate is a digitally-signed document that serves to validate the holder's authorization and name. The document consists of a specially formatted block of data that contains the name of the certificate holder (Subject DN), a serial number, validity dates, holder's public key, Issuer's DN, and the digital signature of the Issuer for authentication. The Issuer attests that the holder's name is the one associated with the public key in the document.
- Certificate Authority (CA)** A Certificate Authority registers end-users, issues their certificates, and can also create CAs below them. Within KMS 2.0, 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.
- Communications key** Adds another layer of encryption and authentication during transmission over a LAN from the token to the drive.
- 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).
- Critical Security Parameter** Security-related information (for example, secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module.
- Crypto Key Management Station** See Key Management Station.
- 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** And encryption-capable tape drive that has had the encryption feature turned on in the drive.



- 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. This value corresponds to the “Originator Usage Period” in NIST 800-57.

---

## 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. The concrete definition of a data unit is defined by the Encryption Agent that creates it. For tape drives, a data unit is a tape cartridge.
- Device key** Enables the tape drive for encryption. KMS Version 1.x term.

---

## E

- EKT** Enabling key token (device keys). KMS Version 1.x term.
- Enable key** Unique 64 character key used to enable the tape drive. See also PC Key.
- 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

**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.

- Keys**
  - A random string of bits generated by the key management system, entered from the keyboard, or purchased. Types of keys include:
    - Device keys enable the tape drive encryption feature.
    - Media keys encrypt and decrypt customer data on a tape cartridge.
    - PC Keys enable the tape drive for encryption.
    - [Transmission keys](#):
    - Communication key adds another layer of encryption (authentication) to the media key during transmission over the LAN from the token to the drive.
    - Split keys are unique to each drive and work with the wrap key for protection.
    - Wrap keys encrypt the media key on the LAN and the token.

**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 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 Sun 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.

Key Policies also control where keys governed by the Key Policy can be exported to other Key Transfer Partners or imported from other Key Transfer Partners.

**Key Transfer File**

A file containing keys and associated data units (if defined) used to move key material from one KMS Cluster to another. Both parties to the transfer must configure a key transfer partner of the other party to the exchange. The key transfer file is signed and encrypted to ensure both privacy of the transferred information as well its integrity.

**Key Transfer Partner**

The Key Transfer Partner is the recipient of keys being exported from one KMS to another.

**KMA**

See Key Management Appliance.

**KMS**

See Key Management System.

**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.

---

## 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

**OKT** Operational key token (media keys). KMS Version 1.x term.

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

---

## P

**PC Key** Enables the tape drive to read and write in encrypted mode.

---

## 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.

**Shamir's Secret Sharing** An algorithm in cryptography where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret. Counting on all participants to combine together the secret might be impractical, and therefore a quorum or threshold scheme is used.

**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.

**System Dump** A user-invoked operation that results in all the relevant data being collected into a single file and then that file being downloaded to the machine from which the user invoked this operation. Once the download is complete, this file is deleted from the KMA.

---

## T

**T10000 tape drive** The T10000 tape drive is a small, modular, high-performance tape drive designed for high-capacity storage of data—up to 500 gigabytes (GB) 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.

**Token** KMS Version 1.x term.  
Tokens are handheld, intelligent devices that connect to a token bay with an Ethernet connection. The two roles of the tokens are:

- Enabling key token
- Operational key token

**Token bay** KMS Version 1.x term.  
A chassis that houses the physical tokens and provides power and connectivity for one or two tokens through the rear blind-mating connector. The token bay is compatible with a standard 19-inch rack—a 1U form factor. The token bay comes in two styles: desktop and rack-mount.

**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.

---

## U

**UID** A string that serves as a unique identifier for a KMS entity, e.g. an encryption agent or user.

**Ultra Tape Drive Encryption Agent** Ultra 2.0 compliant encrypting tape drives utilize Ultra Tape Drive Encryption Agent software for key management. These drives acquire key material from the KMS to be used with tape volumes. Each write from BOT results in the use of fresh key material being used for encryption of data on the volume. Consequently, the definition of a data unit maps to a tape volume where the external ID of the data unit is the volume serial number.

**UTC** Coordinated Universal Time.

---

## V

**Volume Serial Number** A six-, seven-, or eight-character alpha-numeric label that identifies a tape volume.

---

## W

**Wrap key** Encrypts the media keys on the LAN and on the token.

**Write key** This is a media key that is used when writing data to a tape.

---

## 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

---

## A

- AC power factors and concerns, 33
- accessory racks, SL8500, 35
- Advanced Encryption Standard (AES), 2
- Agents, definition, 8
- air gap configuration, 5
- alley limitations, 32
- altitude, 13, 14
- AMD Opteron processor, 3
- ANSI standards, 35
- APC Switch, part numbers, 36
- assignments, 51
- auditor role, 51
- Authenticating, 9

## B

- backup operator role, 51
- backups, types of, 9
- batch file, LTO4, 47

## C

- cabinet, specifications for installation, 35
- capacity
  - tape drive, 18, 19
- Capacity on Demand, 41
- CBC-MAC standard, 2
- CCM standard, 2
- certificate, 9
- Challenge & Response Protocol, 9
- checklists
  - site planning, 32
  - system assurance, 26
- Cipher Block Chaining-Message Authentication Code, 2
- cluster, 8

- Common Criteria Consortium, 2
- communications process, 9
- comparison, tape drive and media, 22
- compatibilities, media types, 22
- compliance operator role, 51
- compliance regulations, 20
- concerns for site planning, 29, 32, 52
- configurations, supported, 59
- connectivity
  - factors for pre-installation, 33
- content management, 40
  - philosophy, 41
- conversion bills
  - 9310 requirements, 64
  - x-option numbers, 71
- Core Security Backup, 9
- Counter with CBC-MAC, 2
- cryptography, 1
- customer
  - contact sheet, 27
  - satisfaction, 25

## D

- data path, partition planning, 42
- definition, 8
- delivery dock, 32
- delivery of the hardware, 32
- depth, 13, 14
- device-based solutions, 3
- DHCP, 38
- dimensions
  - KMA X2100, 13
  - KMA X2200, 14
- Dione card part number, 80
- dock availability, 32
- drive data, 44
- drive file structure, 46

dual stack protocol, 17, 39  
Dynamic Host Configuration Protocol, 38

## E

EIA 310-D-1992 standards for racks, 35  
ELOM  
    connection location, 15  
    network connections, 16  
embedded Lights Out Manager *See* ELOM  
encryption, 1  
    comparisons, 11  
    hardware kits, 10  
    standards, 2  
enrollment data work sheet, 85  
environmental parameters, 13, 14  
environmental, factors and concerns, 32  
error-free installation, 25  
external rack installations, 36

## F

Federal Information Processing Standard, 2  
Federal Information Processing Standards  
    Publications, xiv  
FIPS compliant, 17, 39  
FIPS publications, 2  
firmware requirements, 49

## G

glossary, 87  
graphical user interface, 8, 16  
GUI, 8  
    definition, 8  
    installation, 48  
    LAN connection, 16  
guides, xiv

## H

hardware kits, 10  
heat output  
    X2100, 13  
    X2200, 14  
height, 13  
    X2200, 14  
Hewlett Packard, 20  
HP LTO4 Order Numbers, 80

## I

IEC 60927 standards for racks, 35  
initial configuration work sheet, 44, 82  
installation, site planning checklist, 32  
Institute of Electrical and Electronics Engineers,  
    (IEEE standards), 2  
interfaces, types of, 20  
International Standard Organization, 2  
Internet Protocol, 17, 39  
IPv4 overview, 17, 39  
IPv6, 39  
IPv6 overview, 17  
ISO/IEC standards, 2

## J

Java versions, 48

## K

Key Groups, 8  
Key Management Appliance  
    definition, 8  
    installation, 3  
    order numbers, 60  
Key Management Station configurations, 3  
Key Split Credentials, 10  
KMA  
    dimensions, 13, 14  
KMA *See* Key Management Appliance  
KMA, specifications, 12  
KMS Cluster, definition, 8  
KMS Manager  
    GUI definition, 8  
    installation, 48  
    network connection, 16

## L

LAN connections, 16  
libraries  
    SL3000, 62  
    SL500, 63  
library  
    requirements for installation, 59  
    system assurance, 25, 43  
library content management, 40  
Linear Tape-Open, 20  
local area network connections, 16



- L-Series, order numbers, 65
- LTO Media Compatibility, 23
- LTO4
  - and the SDP, 38
  - interface types, 20
  - media, 20, 40
  - order numbers, 80

## M

- management network
  - LAN connections, 16
- manual organization, xiii
- manuals, xiv
- MARs card, 3
- mass storage, 13, 14
- media
  - comparison, 22
  - introduction, 20
- memory, 13, 14
- Mid-range class, 20
- Monitor Drive tab, 47
- mounting options, 13, 14

## N

- National Institute of Standards and Technology, 2
- National Security Agency, 2
- network configuration, 5
- NIST standards, 2
- NSA, 2

## O

- operator role, 51
- order numbers, 59
- organization of this manual, xiii

## P

- partitioning, 41
- Partner Agreement, xvi
- partner contact sheet, 28
- Partners Web site, xvi
- passphrases, 51
- PC Key request form, 44
- PCI-Express slots, 13, 14
- PDU part numbers, 36
- periodic backups, 10

- philosophy for content management, 41
- planning
  - for encryption, 1
  - meetings, for system assurance, 26
  - site, 31
- PowderHorn library, 64
- power
  - factors for pre-installation planning, 33
  - supply, 13, 14
- private key, 9
- process, for system assurance, 25, 43
- processor, 13, 14
- Professional Services, 78
- publications, xiv

## Q

- quorum, 51

## R

- rackmount requirements, 66
- racks, specifications for installation, 35
- random number generator, 3
- raw keys, 3
- RealTime Growth, 41
- redundant power, 37
- related publications, documents, xiv
- relative humidity, 13, 14
- required tools, 48
- requirements
  - 9310 library, 64
  - for the system assurance process, 26
  - L-Series, 65
  - PowderHorn, 64
  - rackmount, 66
  - SL500 library, 63
  - SL8500 library, 61
- requirements, firmware, 49
- resellers, xvi
- RETMA, 35
- roles, 51

## S

- SATA disk drive, 13, 14
- SCA6000 card, 3
- SCSI interfaces, 20
- SDP, 38
- secure sockets, 9

- security officer role, 51
- Service Delivery Platform, 38
- service network, LAN connections, 16
- site planning checklist, 32
- size of tape drive, 18
- SL3000 requirements, 62
- SL500 requirements, 63
- SL8500
  - installation requirements, 62, 63
- SL8500 requirements, 61
- Solaris 10 operating system, 3
- specifications
  - KMA, 12
- standalone rack installations, 36
- standards for encryption, 2
- standards, compliance, 2
- steps for partitioning, 43, 50, 51, 56, 83
- StorageTek
  - Partners site, xvi
  - team member contact sheet, 28
  - Web site, xvi
- Sun
  - Fire X2100 Server, 3
  - Partners Web site, xvi
  - Ultra 20 Workstation, 3
  - Web site, xvi
- Sun Crypto Accelerator 6000, 13, 14
- Sun Fire X2100 specifications, 13
- Sun Fire X2200 specifications, 14
- supported configurations, 59
- survey
  - site preparation, 31
  - solution planning, 29
- Symmetric encryption, 2
- system assurance
  - customer contact sheet, 27
  - planning meeting, 26
  - process overview, 25, 43
  - StorageTek contact sheet, 28
- system assurance process, 25

## T

- T10000 Tape Drive
  - capacity of the tape drive, 18, 19
  - description of, 18
  - size, 18
- T9840 Tape Drive
  - description, 19
  - description of, 93

- size, 93
- tape drive and media comparison, 22
- tape drive comparisons, 21
- tape drive work sheet, 84
- tape drives
  - supported types, 18, 59
  - T9840, 19
- tasks for partitioning, 43, 50, 51, 56, 83
- team members, 43
- temperature, 13, 14
- T-Series
  - T10000, 18
  - T9840, 19

## U

- Ultrium, 20
- units, rack measurements, 35
- user roles, 51
- User Roles Work Sheet, 56
- user roles work sheet, 83

## V

- Virtual Operator Panel (VOP), 48

## W

- Web browsers, supported versions, 48
- Web sites, xvi
- weight, 13, 14
- width, 13, 14
- work sheets, 81
  - agents, 84
  - copies of, 81
  - initial configuration, 44, 82
  - tape drive enrollment, 85
  - user roles, 83
- WORM media, 20
- Write-Once Read-Many, 20



Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN Web [sun.com](http://sun.com)



ARGENTINA: 5411-4317-5636 • AUSTRALIA: 1-800-550-786 • AUSTRIA: 43-1-601-26-0 • BALKANS: 301-6188-111 • BELGIUM: 32-2-704 89 83 • BRAZIL: 55-11-51872100 • BRUNEI: 65-216-8333 • CANADA: 1-800-422-8020 (GENERAL); 416-964-2001 (LEARNING MANAGEMENT SYSTEM SALES, TORONTO) • CHILE: 562-372-4500 • COLOMBIA: 571-629-2323  
CZECH REPUBLIC: 420 2 33009311 • DENMARK: 45 4556 5040 • EGYPT: 00 202 570 9442 • FINLAND: 358-9-525-551 • FRANCE: 33-1-41-33-17-17 • GERMANY: 49-89-460-08-2788 • GREECE: 30-01-6188101 • HONG KONG: 852-2877-7077 • HUNGARY: 361-202-4415 • INDIA: 91-80-229-8989 • INDONESIA: 65-216-8333 • IRELAND: 353-1-668-4377  
ISRAEL: 972-9-9710500 • ITALY: 39-02-9259511 • JAPAN: 81-3-5779-1820 • KOREA: 82-2-3453-6602 • MALAYSIA: 603-2116-1887 • MIDDLE EAST: 00 9714 3366333 • MEXICO: 525-261-0344 • NETHERLANDS: 31-33-4515200 • NEW ZEALAND: 0800-786-338 • NORTH WEST AFRICA: 00 9714 3366333 • NORWAY: FROM NORWAY: 47-22023950, TO NORWAY: 47-23369650 • PAKISTAN: 00-9714-3366333 • PEOPLE'S REPUBLIC OF CHINA: 8610-6803-5588 • PHILIPPINES: 632-885-7867 • POLAND: 48-22-8747848 • PORTUGAL: 351-21-413-4000 • RUSSIA: 7-095-935-8411 • SAUDI ARABIA: 00 9714 3366333 • SINGAPORE: 65-216-8300 • SOUTH AFRICA: 27-11-256-6300 • SPAIN: 34-902-210-412 • SRI LANKA: 65-2168333 • SWEDEN: 46-8-631 22 00 • SWITZERLAND: 41-1-908-90-50 (GERMAN) 41-22-999-0444 (FRENCH) • TAIWAN: 886-2-25185735 • THAILAND: 662-344-6855 • TURKEY: 90 212 335 22 00 • UNITED KINGDOM: 44-1276-416-520 • UNITED STATES: 1-800-422-8020 • VENEZUELA: 582-905-3800 • VIETNAM: 65-216-8333 • WORLDWIDE HEADQUARTERS: 1-650-960-1300

**SUN™** THE NETWORK IS THE COMPUTER ©2006 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, and the Sun logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.