



Sun StorageTek™ Crypto Key Management System

Version 2.0

Systems Assurance Guide

Part Number: 316194802

Revision: B



Crypto Key Management System

Version 2.0

Systems Assurance Guide

Sun Microsystems, Inc.
www.sun.com

Part Number: 316194802
May 2008
Revision: B

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

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

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.

Use is subject to license terms. This distribution may include materials developed by third parties. This distribution may include materials developed by third parties. Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California.

UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd. Sun, Sun Microsystems, the Sun logo, Solaris, Sun StorageTek Crypto Key Management System, StorageTek and the StorageTek logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Products covered by and information contained in this service manual are 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. Use of any spare or replacement CPUs is limited to repair or one-for-one replacement of CPUs in products exported in compliance with U.S. export laws. Use of CPUs as product upgrades unless authorized by the U.S. Government is strictly prohibited.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

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

Sun Microsystems, Inc. détient les droits de propriété intellectuels relatifs à la technologie incorporée dans le produit qui est décrit dans ce document.

En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains listés à l'adresse <http://www.sun.com/patents> et un ou les brevets supplémentaires ou les applications de brevet en attente aux Etats - Unis et dans les autres pays.

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.

L'utilisation est soumise aux termes de la Licence. Cette distribution peut comprendre des composants développés par des tierces parties. Cette distribution peut comprendre des composants développés par des tierces parties. Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie.

UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd. Sun, Sun Microsystems, le logo Sun, Solaris, Sun StorageTek Crypto Key Management System, StorageTek et le logo StorageTek sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Ce produit est soumis à la législation américaine en matière de 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 en matière de contrôle des exportations et la liste de ressortissants spécifiquement désignés, sont rigoureusement interdites. L'utilisation de pièces détachées ou d'unités centrales de remplacement est limitée aux réparations ou à l'échange standard d'unités centrales pour les produits exportés, conformément à la législation américaine en matière d'exportation. Sauf autorisation par les autorités des Etats-Unis, l'utilisation d'unités centrales pour procéder à des mises à jour de produits est rigoureusement interdite.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON.

We welcome your feedback. Use the OpinionLab [+] feedback system on the documentation Web site or Send your comments to:

Sun Learning Services
Sun Microsystems, Inc.
500 Eldorado Blvd.
Mailstop: UBRM06-307
Broomfield, CO 80021-6307
USA

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	This revision includes: <ul style="list-style-type: none">■ New documentation feedback system■ Additional Information on page xvi■ New “Configuration Planning” on page 23■ Obtain the Drive Data on page 34■ Support for the T9840D tape drive (throughout)■ Deleted conceptual drawings from Chapter 1■ Reader’s comments

Note – Change bars are included in this revision.

Contents

Preface xiii

Organization xiii

Related Information xiv

 Reference Documentation xiv

 Documentation Content and Purpose xv

Additional Information xvi

 Sun's External Web Site xvi

 Documentation and Download Web Sites xvi

 Partners Site xvi

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 2.0 Key Management Appliance Configurations 6

 Version 2.0 Configuration Descriptions 8

 Networks 9

 Communications Process 9

 Backups 10

 Encryption Hardware Kits 10

 Encryption Version Comparisons 11

 Tape Drives 12

 About the T10000 12

	About the T9840D Tape Drive	13
	About the HP LTO4 Tape Drive	13
	Tape Drive Comparison	14
	Tape Drive and Media Comparisons	15
	Key Management Appliance Specifications	16
2.	Systems Assurance	19
	Planning Meetings	20
	Customer Team Member Contact Sheet	21
	Sun Team Member Contact Sheet	22
	Configuration Planning	23
	Customer Conceptual Drawing	24
3.	Site Preparation	25
	Site Planning Checklist	26
	Rack Specifications	29
	SL8500 Rack Guidelines	29
	External Rack Installations	30
	Redundant Power	31
	Service Delivery Platform	32
	Content Management	33
	Capacity on Demand	34
	RealTime Growth Technology	34
	Partitioning	34
	Planning the Data Path	35
	Tasks	36
	Required Tools	37
	Supported Platforms and Web Browsers	37
	Required Tape Drive Firmware Versions	38
	Required Library Firmware Versions	38
	KMS Manager	39
	Role-Based Operations	40

4. Ordering	47
Supported Configurations	47
Supported Tape Drives	47
Key Management Appliance	48
SL8500 Modular Library System	49
SL3000 Modular Library System	50
SL500 Modular Library System	51
9310 Automated Cartridge System	52
L-Series—L180, L700e, and L1400 Libraries	53
Rack Mount	54
Order Numbers, Descriptions, and Contents	55
9310 Upgrades	61
Professional Services	61
Tape Drive Ordering Instructions	62
Library Ordering Instructions	62
A. Work Sheets	63
Initial Configuration Work Sheet	64
User Roles Work Sheet	65
Tape Drives Work Sheet	66
Drive Enrollment Work Sheet	67
Obtain the Drive Data	68
Create a Drive Data File Structure	70

Figures

FIGURE 1-1	Key Management Station Configurations	4
FIGURE 1-2	Key Management Appliance Configurations	6
FIGURE 1-3	Key Management Appliance—Front Panel	17
FIGURE 1-4	Key Management Appliance—Rear Panel	17
FIGURE 3-1	External Rack	30
FIGURE 3-2	Power Redundancy	31
FIGURE 3-3	Systems Delivery Platform	32
FIGURE 3-4	User Roles Detail Screen	40
FIGURE 4-1	Key Management Appliance—Front Panel	48
FIGURE 4-2	Key Management Appliance—Rear Panel	48
FIGURE A-1	Tape Drive Serial Number—VOP	68
FIGURE A-2	Request an Encryption Key Application	68
FIGURE A-3	Encryption File Request for Drive Data	69
FIGURE A-4	Encryption File Request for Drive Data	69
FIGURE A-5	Drive Data File Structure	70

Tables

TABLE P-1	Documentation and Audience Map	xv
TABLE P-2	Documentation Content and Purpose	xv
TABLE 1-1	Key Management System Versions	3
TABLE 1-2	Encryption Solution Comparisons	11
TABLE 1-3	Tape Drive Comparisons	14
TABLE 1-4	Media Compatibilities	15
TABLE 1-5	Tape Drive and Media Support	15
TABLE 1-6	Sun Fire X2100 Specifications	16
TABLE 2-1	System Assurance Task Checklist	20
TABLE 2-2	Solution Planning Checklist	23
TABLE 3-1	Site Planning Checklist	26
TABLE 3-2	SL8500 Accessory Rack Guidelines	29
TABLE 3-3	Content Management Planning	33
TABLE 3-4	Steps and Tasks for Partitioning	36
TABLE 3-5	Operating Systems and Web Browsers	37
TABLE 3-6	Tape Drive Firmware Versions	38
TABLE 3-7	Library Firmware Versions	38
TABLE 3-8	KMS Manager Display	39
TABLE 3-9	Operator Roles and Functions	41
TABLE 3-10	User Roles Work Sheet	45
TABLE 4-1	SL8500 Modular Library System Requirements	49
TABLE 4-2	SL3000 Modular Library System Requirements	50
TABLE 4-3	SL500 Modular Library System Requirements	51
TABLE 4-4	9310 Automated Cartridge System Requirements	52
TABLE 4-5	L-Series Library Requirements	53
TABLE 4-6	Rackmount Requirements	54

TABLE 4-7	Order Numbers	55
TABLE 4-8	9310 Upgrade Ordering Instructions and Part Numbers	61
TABLE 4-9	Professional Services Ordering Instructions and Part Numbers	61
TABLE 4-10	Tape Drive Ordering Instructions	62
TABLE 4-11	Library Ordering Instructions	62
TABLE A-1	Initial Configuration Settings—Customer	64
TABLE A-2	User Roles Work Sheet—Customer	65
TABLE A-3	Tape Drive Work Sheet—Service Representative	66
TABLE A-4	Enrollment Data Work Sheet—Customer	67

Preface

This guide is intended for Sun StorageTek representatives, customers, and anyone responsible for planning the installation of the Sun StorageTek encryption solution.

Organization

This guide has the following organization:

Chapter	Use this chapter to:
Chapter 1, "Introduction"	Introduce you and the customer to the Sun StorageTek encryption solutions.
Chapter 2, "Systems Assurance"	Describe and plan for the systems assurance process.
Chapter 3, "Site Preparation"	Prepare for the installation.
Chapter 4, "Ordering"	Help order the encryption solution and additional components—libraries and tape drives—for your customers requirements.
Appendix A, "Work Sheets"	Complete work sheets that can help prepare for the installation.
"Glossary"	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: 816-7190-10
Sun SunFire X2100 Server Installation Guide	Sun: 819-6589-10

These publications are for Sun StorageTek personnel or authorized third parties who install StorageTek brand tape and library products.

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

These publications are related to the Key Management System:

Publication Description	Part Number
Crypto Key Management System Installation and Service Manual	StorageTek: 316194901
Crypto Key Management System Administrator Guide	StorageTek: 316195101

Reference Documentation

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 140-2
Security Requirements for Cryptographic Modules
- Federal Information Processing Standards Publication FIPS PUB 171
Key Management
- 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					
Legend: 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"> ■ Marketing & Sales ■ Systems Engineers ■ Installation Coordinators ■ Professional Services ■ Technical Specialists ■ Service Representatives ■ Customer 	<ul style="list-style-type: none"> ■ Product description ■ Dimensions ■ Weights & measures ■ Configurations ■ Capacities ■ Site preparation ■ Models and features ■ Order numbers 	<ul style="list-style-type: none"> ■ Pre-Sales ■ Site Planning ■ Product introduction ■ Readiness
Installation and Service Manual	<ul style="list-style-type: none"> ■ Installation Coordinators ■ Technical Specialists ■ Service Representatives 	Installation: <ul style="list-style-type: none"> ■ Procedures ■ Checklists ■ Configurations Service: <ul style="list-style-type: none"> ■ Fault isolation ■ Removal/Replacement 	<ul style="list-style-type: none"> ■ Installation ■ Configuration ■ Embedded Lights Out Manager (ELOM) ■ QuickStart
Administrator Guide	<ul style="list-style-type: none"> ■ Customer ■ Technical Specialists ■ Service Representatives 	<ul style="list-style-type: none"> ■ Introduction ■ Operator Roles ■ How to... 	<ul style="list-style-type: none"> ■ Usage ■ Support ■ Graphical user interface (KMS GUI)
Online Help	<ul style="list-style-type: none"> ■ Customer ■ Technical Specialists ■ Service Representatives 	<ul style="list-style-type: none"> ■ Online help 	<ul style="list-style-type: none"> ■ Usage ■ Support ■ Graphical user interface (KMS GUI)

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)
- Internal access: <http://docs.sfbay.sun.com/app/docs> (internal)
- Sun Download Center: <http://www.sun.com/download/index.jsp> (customers)
- Sun Partner Exchange: <https://spe.sun.com/spx/control/Login> (partners)
- 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

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 also 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.

The Sun StorageTek solution will be certified at Level 2.

- **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.
This is a computationally efficient, high-strength cipher type sometimes called the “secret key algorithm” because the key is never made available to the public and must be kept secure. *Synonymous with Asymmetric keys*, which use two different keys, one to encrypt and one to decrypt. This cipher type is computationally difficult, lower-strength and used for public key implementations.
- **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)
 - Mutual authentication using x509 v3 certificates

Sun StorageTek Encryption Solutions

Sun StorageTek offers two device-based solutions using:

- Federal Information Processing Standard (FIPS) approved appliances called the Crypto Key Management System.
- Sun StorageTek T10000—state-of-the-art—tape drives with either Fibre Channel or IBMs FICON interfaces.
- Supporting infrastructure and network.

There are two types of Crypto Key Management Systems (KMS); they include:

TABLE 1-1 Key Management System Versions

Version 1.x	A Sun Ultra 20 Workstation—called a key management station
Version 2.0	A Sun Fire X2100 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 (SCA6000), 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.

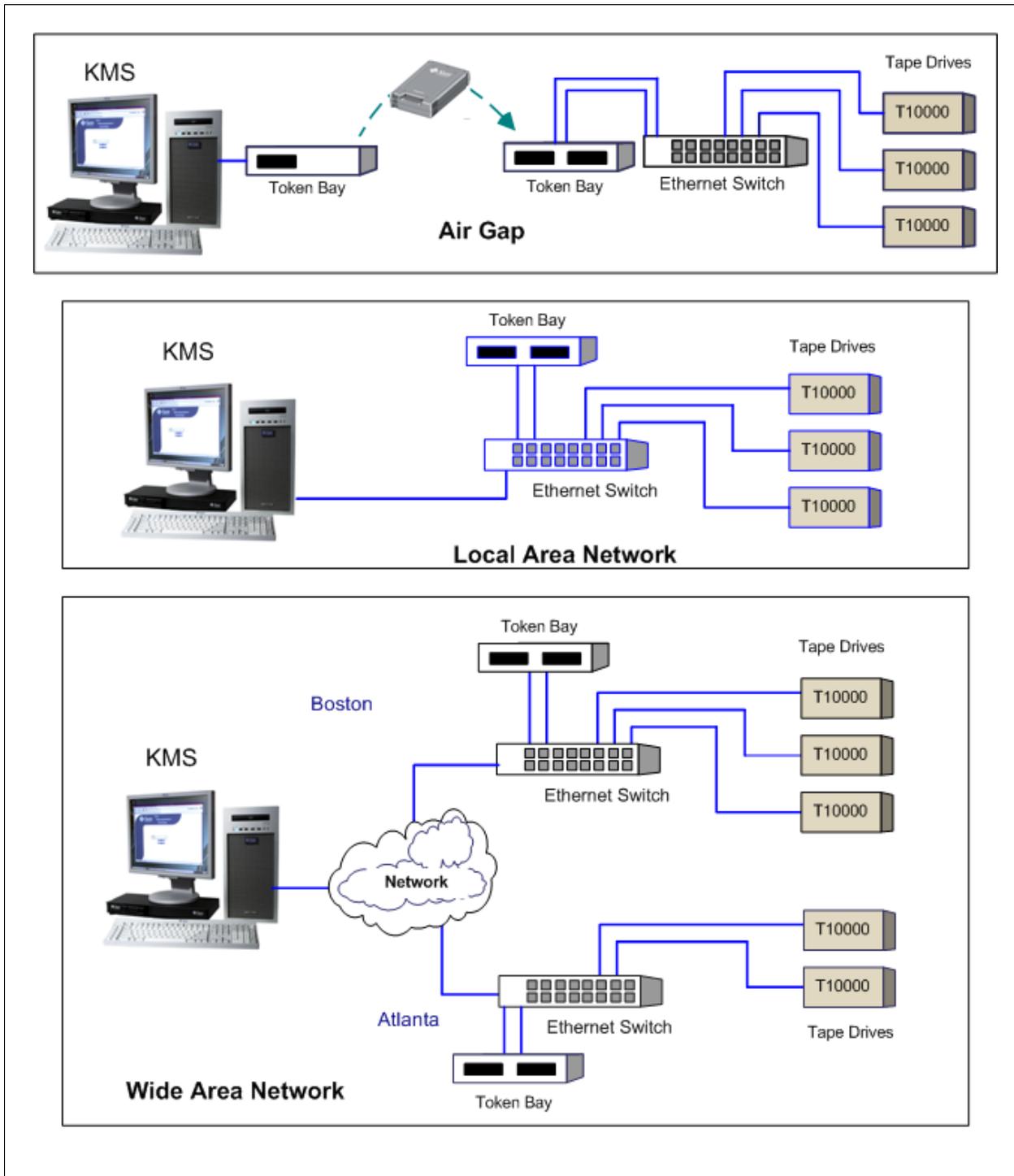
FIGURE 1-2 shows three **Version 2.0 configurations** for the key management appliance (KMA):

- Single site—local area network
- Multiple sites—wide area network
- Multiple sites—wide area network—grouped by specific key groups

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:

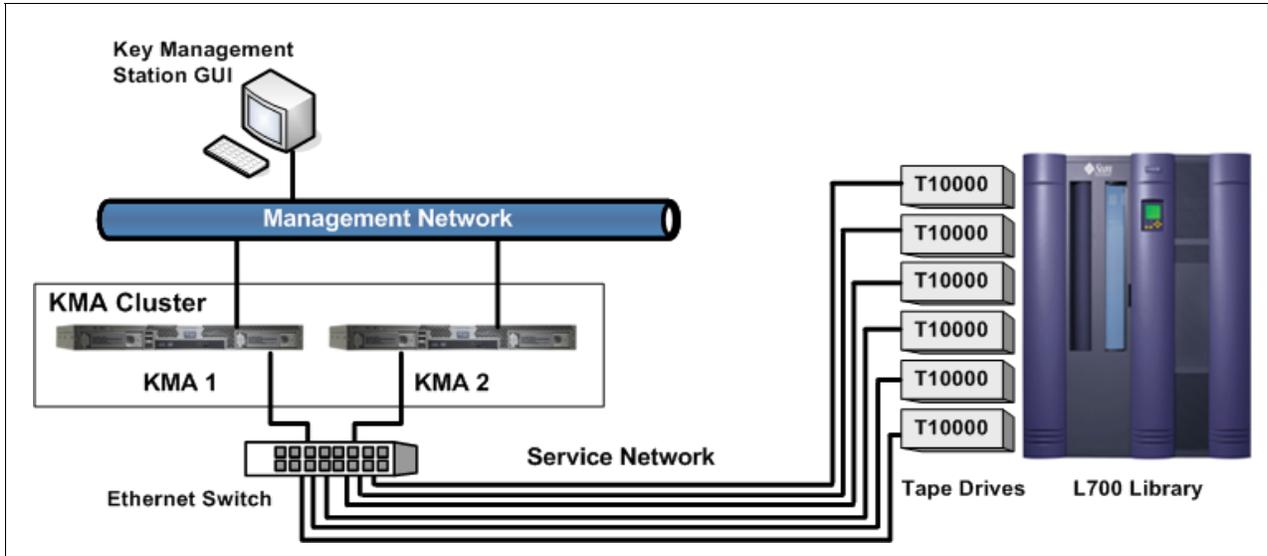
The remaining chapters in this document contains specific information for Version 2.0 of the Crypto Key Management System.

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

Version 2.0 Key Management Appliance Configurations

FIGURE 1-2 Key Management Appliance Configurations

A) Single site—local area network—using the service network for the tape drive connections



B) Multiple sites—wide area network—using the management network for the tape drive connections

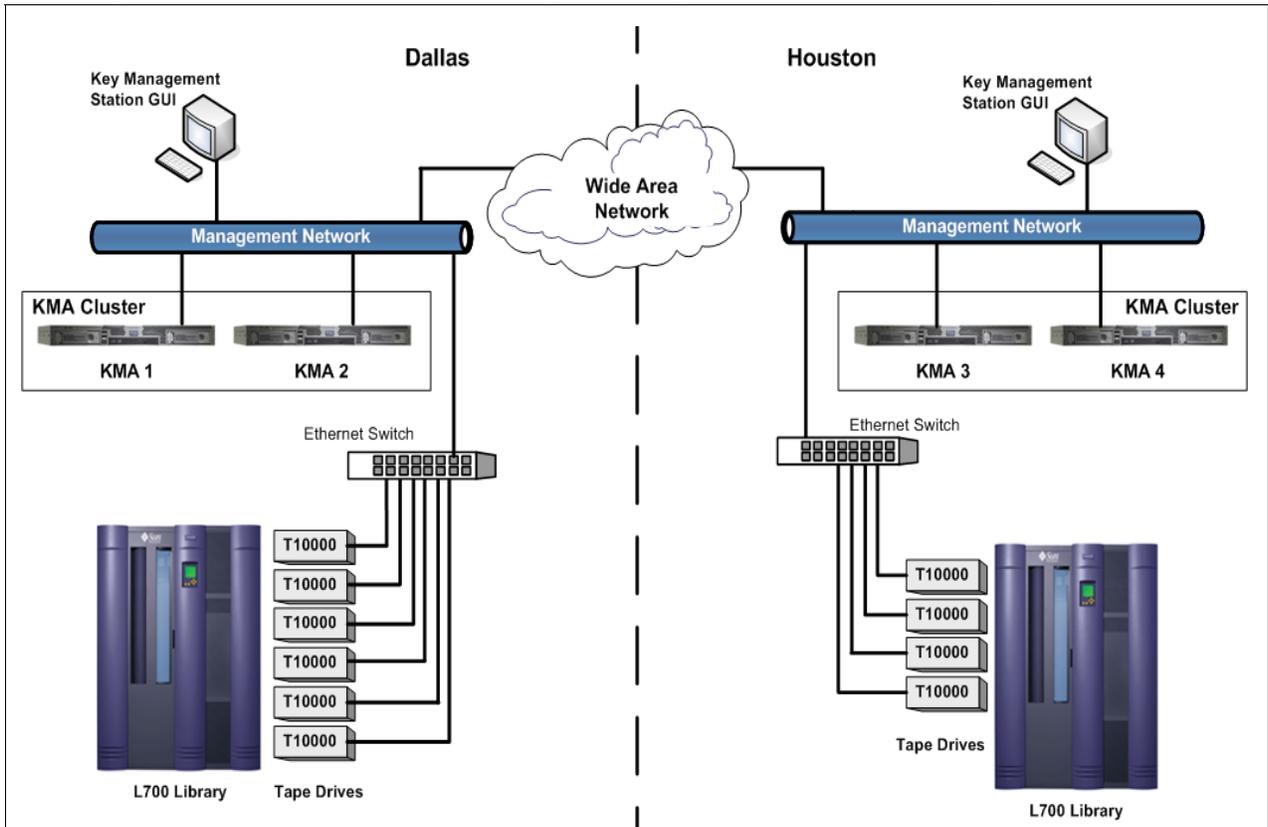
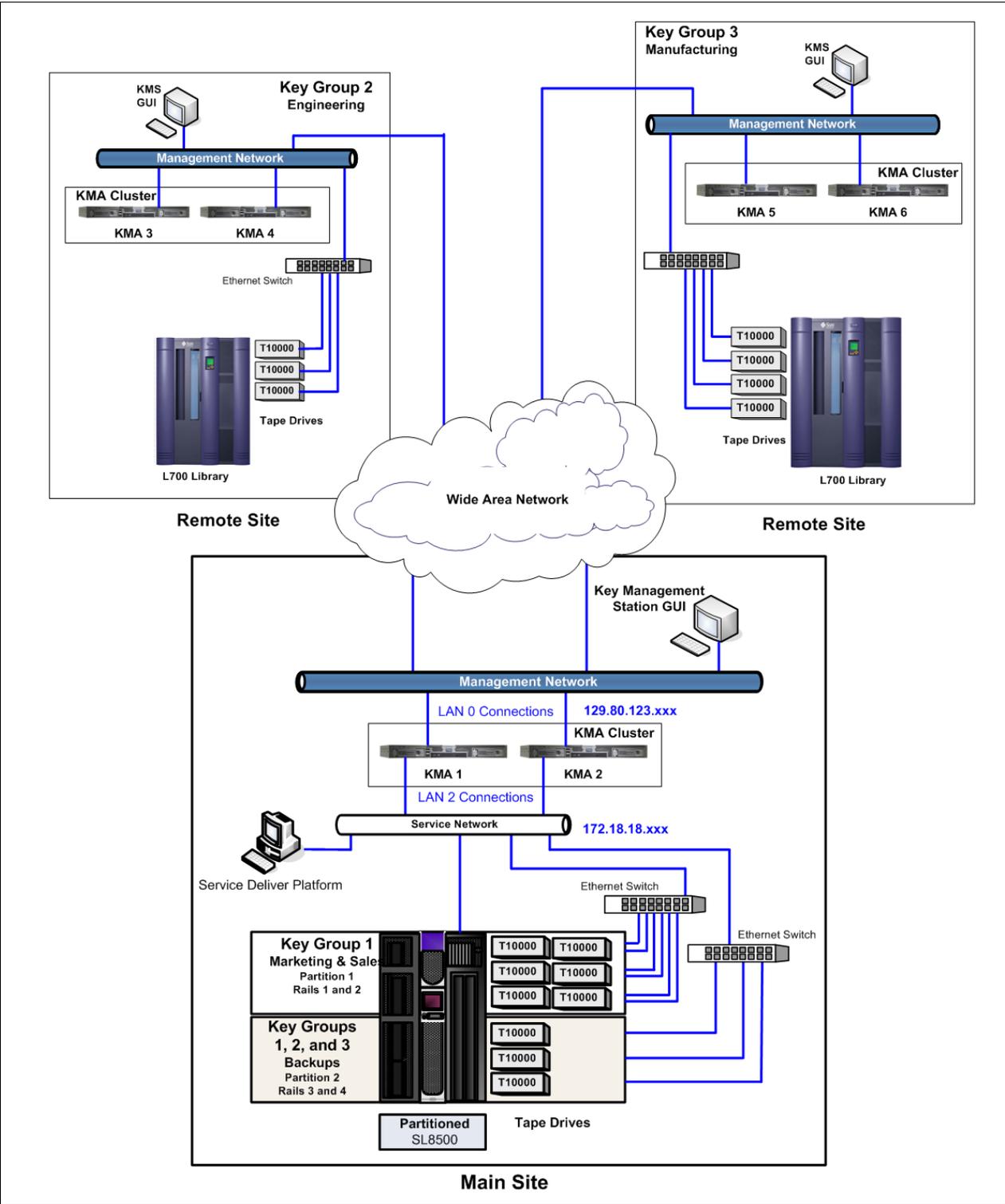


FIGURE 1-2 Key Management Appliance Configurations (Continued)

C) Multiple sites—wide area network—specific key groups—local disaster recovery in a partition. Uses the both the management (remote) and service (local) networks for the tape drive connections.



Version 2.0 Configuration 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 Networks¹ (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.

Networks

There are two networks where communications normally occur, the:

Management network	Note – Customers are expected to provide this network. The management network services the KMAs and the tape drives when installed in that configuration.
Service network	The service network is provided by Ethernet switches that come in the library accessory kits. The service network is intended to connect between the KMAs and drives, and could also include a Service Delivery Platform (SDP), an optional appliance if available.
Both of these networks and connections are shown in FIGURE 1-2 on page 7 .	

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) channel².
- Establishing this secure sockets channel uses a 2048 bit RSA³.
- Authenticating this session results in an agreed upon, 256 bit AES⁴ 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.

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.

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 algorithm⁵ 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.

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.

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.

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

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:

- T10000A
- T10000B (*check on availability*)
- T9840D only
- HP LTO4 (*check on availability*)

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:

- T10000 A
- T10000 B

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 a technology called partial response, maximum likelihood (PRML) 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

There are plans to include the Hewlett Packard, linear-tape-open (LTO) generation 4 technology in to the Sun StorageTek encryption offerings.

This is a future plan. Check on availability.

When this is supported, this document will be updated.

Tape Drive Comparison

TABLE 1-3 Tape Drive Comparisons

Physical Specifications	T10000A	Check on Availability for these Drives		
		T10000B	T9840D	LTO4
Height	8.25 cm (3.25 in.)	8.25 cm (3.25 in.)	8.25 cm (3.25 in.)	8.25 cm (3.25 in.)
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)
Performance Specifications				
Capacity (native)	500 GB	1TB	75GB	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, SAS 3 GB
MTBF (100% duty cycle)	290,000 hrs	290,000 hrs	290,000 hrs	250,000 hrs
Media/Format Compatibility				
Read/Write	Proprietary Format- T10000 Cartridge		Proprietary Format	LTO2 = Read only LTO3 = Rd/Write LTO4 = Rd/Write
VolSafe/WORM?	Yes		Yes	Yes
Power				
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.

TABLE 1-4 shows the media compatibilities for:

- Encryption-capable tape drives
- Non-encryption tape drives

TABLE 1-4 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 1-5 shows a comparison between:

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

TABLE 1-5 Tape Drive and Media Support

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

Key Management Appliance Specifications

TABLE 1-6 lists the specifications for the SunFire X2100 server.

TABLE 1-6 Sun Fire X2100 Specifications

Processor	<ul style="list-style-type: none"> ■ One dual-core AMD Operton processor ■ Processor frequencies: 2.2 GHz ■ Up to 1 MB level 2 cache
Memory	<ul style="list-style-type: none"> ■ Four DIMM slots (up to 4 gigabytes) ■ Unbuffered ECC memory
IPMI 2.0	<ul style="list-style-type: none"> ■ Service processor standard ■ embedded Lights Out Manager
Mass storage	One SATA disk drive
PCI Slots	Two PCI-Express slots (PCIe) PCIe-0 contains the Sun Crypto Accelerator 6000 (SCA6000)
Networking	<ul style="list-style-type: none"> ■ Four USB 2.0 connectors on the rear panel ■ Two USB 2.0 connectors on the front panel ■ Two ports: Serial port with DB-9; VGA with DB-15 connectors ■ Four 10/100/1000 Base-T Ethernet ports
Dimensions:	
Height	43 mm (1.7 in.)
Width	425.5mm (16.8 in.)
Depth	633.7 mm (25 in.)
Weight (maximum)	10.7 kg (23.45 lb)
Mounting options	19-inch rackmount kit; Compact 1 rack-unit (1.75 in.) form factor
Environmental parameters:	
Temperature	5°C to 35°C (41°F to 95°F)
Relative humidity	27°C (80°F) max wet bulb
Altitude	Up to 3,000 m (9,000 ft)
Power supply	One 6.5 Amps at 345 Watts Heat output is about 850 BTU/hour
Regulations meets or exceeds the following requirements:	
Acoustic Noise Emissions declared in accordance with ISO 9296	
Safety IEC 60950, UL/CSA60950, EN60950, CB scheme	
RFI/EMI FCC Class A, Part 15 47 CFR, EN55022, CISPR 22, EN300-386:v1.31, ICES-003	
Immunity: EN55024, EN300-386:v1.3.2	
Certifications: Safety CE Mark, GOST, GS Mark, cULus Mark, CB scheme, CCC, S Mark	
EMC CE Mark, Emissions and Immunity Class A Emissions Levels: FCC, C-Tick, MIC, CCC, GOST, BSMI, ESTI, DOC, S Mark	

- FIGURE 1-3 is an example for the front of the appliance
 - FIGURE 1-4 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 1-3 Key Management Appliance—Front Panel

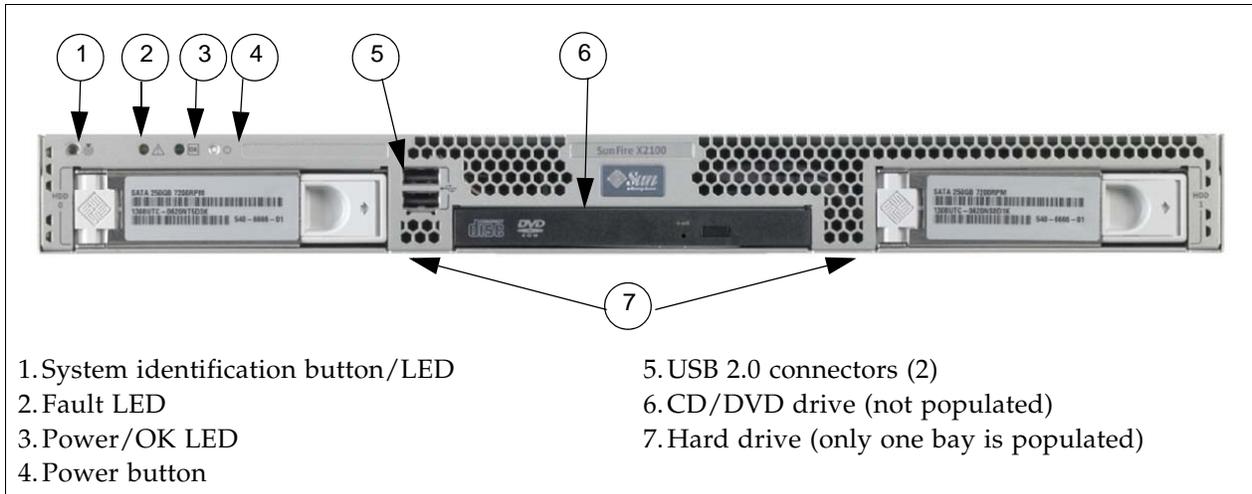
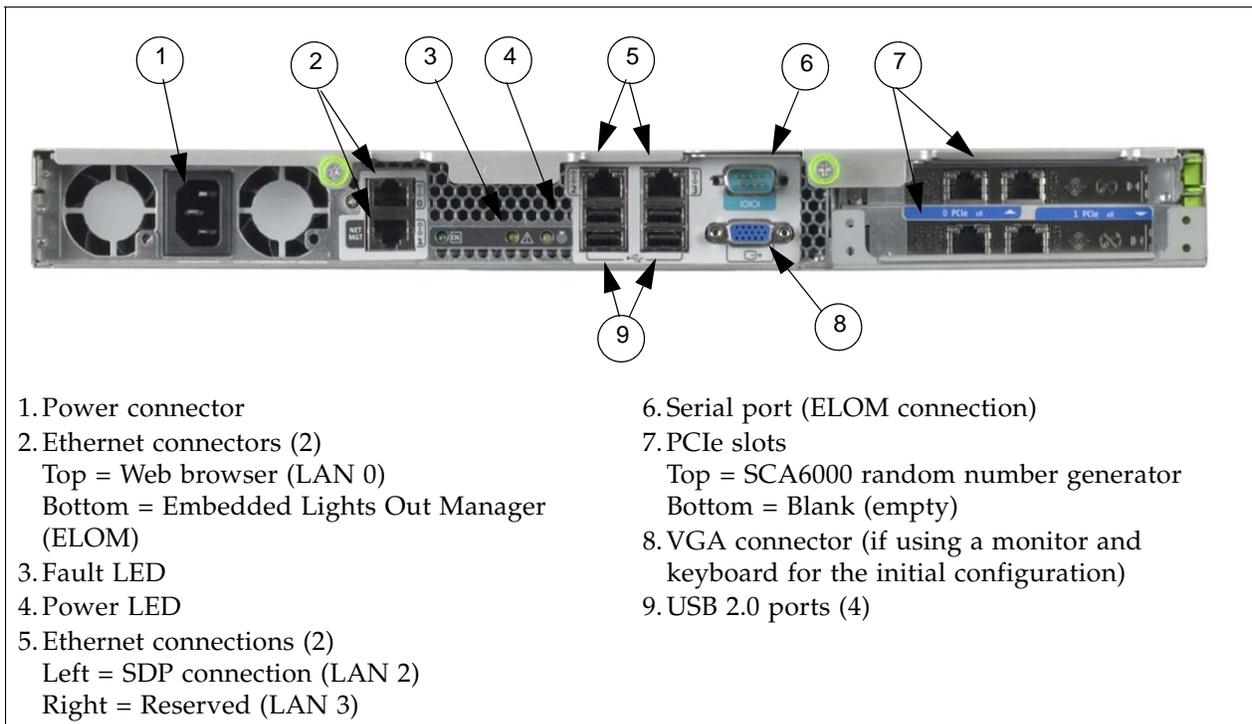


FIGURE 1-4 Key Management Appliance—Rear Panel



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 Chapter 1, "Introduction" 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 "Configuration Planning" on page 23 to help define the customer requirements.	Yes <input type="checkbox"/> No <input type="checkbox"/>
Review and complete "Site Planning Checklist" on page 26. <i>Comments:</i>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Review and identify "User Roles Work Sheet" on page 45. <i>Comments:</i>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Review "Supported Configurations" on page 47. <i>Comments:</i>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Review "Order Numbers, Descriptions, and Contents" on page 55. <i>Comments:</i>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Determine the installation schedule: Date: _____ Time: _____	Yes <input type="checkbox"/> No <input type="checkbox"/>
Download and provide the customer with a copy of the <i>Crypto Key Management System Administrator's Guide</i> PN 316195101. http://docs.sun.com/app/docs	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.

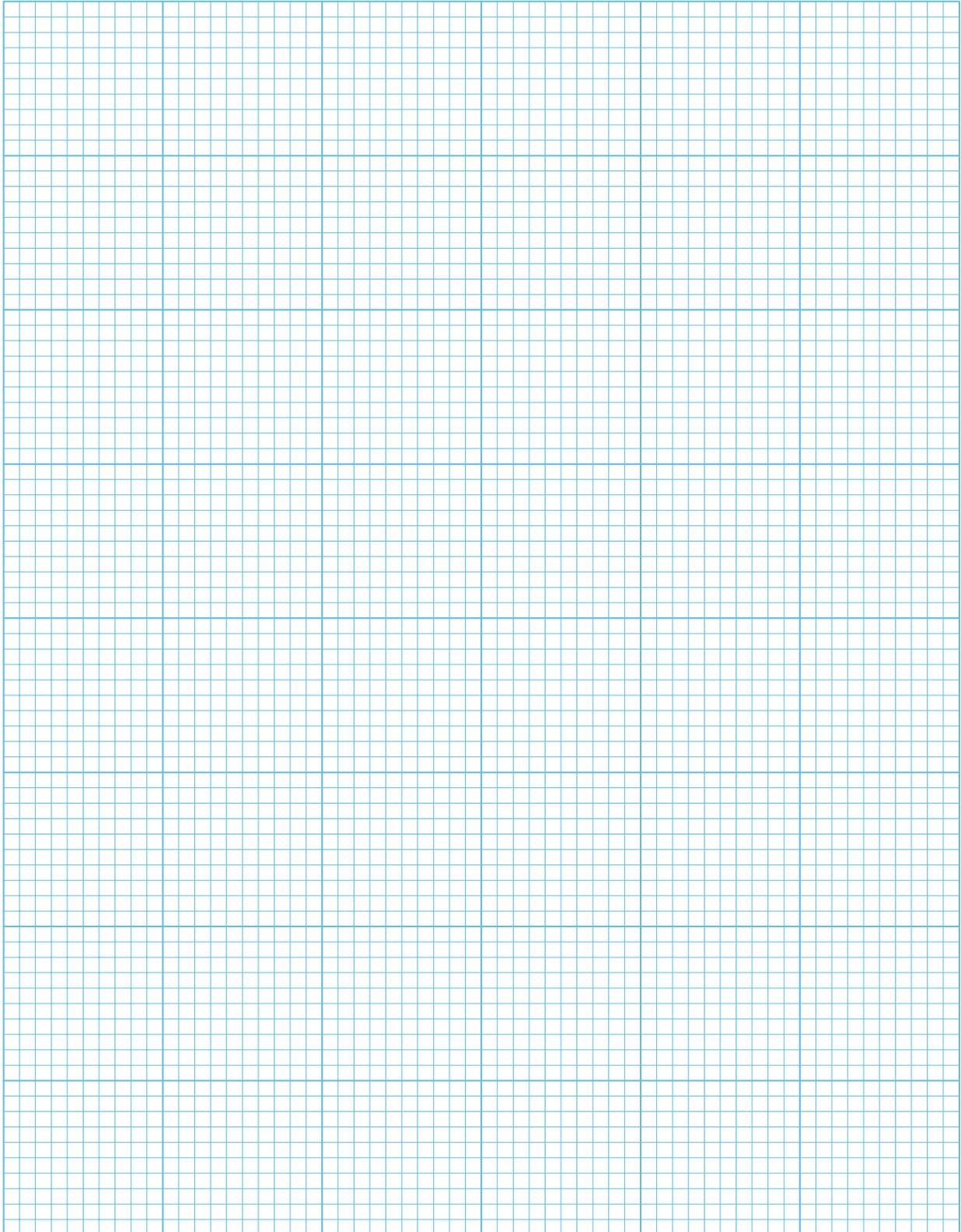
Configuration Planning

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
Which encryption solution does the customer want?	<input type="checkbox"/> KMS 2.x (Continue with this checklist) <input type="checkbox"/> KMS 1.x
What type of configuration does the customer want? Notes: <ul style="list-style-type: none"> ■ 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 (WAN). ■ 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. 	<input type="checkbox"/> Single site <input type="checkbox"/> Multiple sites How many: _____ <input type="checkbox"/> Disaster recovery ?
How many KMA appliances are needed? Notes: <ul style="list-style-type: none"> ■ The maximum number of KMAs is 20. ■ KMAs <i>must be</i> installed in pairs. 	
How many and of what type of encryption hardware kits are needed?	<input type="checkbox"/> SL8500 How many: _____ <input type="checkbox"/> SL3000 (<i>Future—check on availability</i>) <input type="checkbox"/> SL500 (<i>LTO4 only—check on availability</i>) <input type="checkbox"/> 9310 9741E How many: _____ <input type="checkbox"/> L-Series How many: _____ Type: <input type="checkbox"/> L180, <input type="checkbox"/> L700, <input type="checkbox"/> L1400 <input type="checkbox"/> Rackmount How many: _____
How many and of what type of encryption tape drives are needed?	<input type="checkbox"/> T10000A How many: _____ <input type="checkbox"/> T10000B (<i>Future—check on availability</i>) <input type="checkbox"/> T9840D How many: _____ <input type="checkbox"/> HP LTO4 (<i>Future—check on availability</i>)
Identify customer requirements and expectations.	

Customer Conceptual Drawing



Site Preparation

Use this chapter to prepare for the installation.

- [“Site Planning Checklist” on page 26](#)

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

- [“Rack Specifications” on page 29](#)
 - [“SL8500 Rack Guidelines” on page 29](#)
 - [“External Rack Installations” on page 30](#)

- [“Redundant Power” on page 31](#)
- [“Service Delivery Platform” on page 32](#)
- [“Content Management” on page 33](#)
 - [“Capacity on Demand” on page 34](#)
 - [“RealTime Growth Technology” on page 34](#)
 - [“Partitioning” on page 34](#)
 - [“Planning the Data Path” on page 35](#)
 - [“Tasks” on page 36](#)

- [“Required Tools” on page 37](#)
- [“Supported Platforms and Web Browsers” on page 37](#)
- [“Required Tape Drive Firmware Versions” on page 38](#)
- [“Role-Based Operations” on page 40](#)
 - [User Roles Work Sheet on page 45](#)

Site Planning Checklist

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

TABLE 3-1 Site Planning Checklist

Question	Completed?	Comments:
Delivery and Handling		
Important: The Key Management Systems and appliances are considered “secure” items. Follow the customers security guidelines for delivery and installation.		
Does the customer have a delivery dock? If <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"/>	
Environmental Planning		
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:
Power Requirements		
Does the intended site meet the power requirements?	Yes <input type="checkbox"/> No <input type="checkbox"/>	KMA: 90 to 132 VAC 180 to 264 VAC 57 to 63 Hz 47 to 53 Hz 2.3 to 4.6 Amps Maximum continuous power is 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"/>	
Personnel:		
Are there trained/qualified Sun StorageTek representatives locally to install and maintain the encryption equipment?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Names:
Are there trained/qualified Sun StorageTek representatives locally to install and maintain the supported configurations?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
Connectivity: Cabling is <i>very important</i> to establish a reliable network between the KMS GUI, KMAs, Ethernet switches, and tape drives.		
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"/>	Note: ■ Ethernet cables come with the accessory kits. ■ Lengths are dependant on the location of the switches and devices.

TABLE 3-1 Site Planning Checklist (Continued)

Question	Completed?	Comments:
Configurations		
Does the customer have adequate rack space to hold the KMAs and Ethernet switches?	Yes <input type="checkbox"/> No <input type="checkbox"/>	See "Rack Specifications" on page 29 for information. Note: A half-rack (20-units) can be ordered to hold the KMAs, switches, and PDUs. Kit CRYPTO-20U-Z
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	(Check on availability) HP LTO4 only (Check on availability)
Does the customer have existing tape drives to use?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
Are they already installed in a library?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
Does the customer need to order more drives? ■ How many tape drives? ■ T10000 A ■ T10000 B (<i>Check on availability</i>) ■ T9840D ■ HP LTO4 (<i>Check on availability</i>) ■ Interface types? ■ Fibre Channel ■ FICON (T-Series only) ■ ESCON (T9840D)	Yes <input type="checkbox"/> No <input type="checkbox"/>	Check on availability Not all versions of tape drives and interfaces will be available with this initial release of Version 2.0. Currently supported tape drives: ■ T10000A ■ T9840D
Media		
Are additional cartridges required? ■ Data cartridge ■ Cleaning cartridges ■ VolSafe cartridges ■ Labels	Yes <input type="checkbox"/> No <input type="checkbox"/>	Note: All 3 versions of encryption tape drives use different, unique cartridges. ■ T9840 = 9840 cartridges ■ T10000 = T10000 cartridges ■ LTO4 = LTO-compatible cartridges All versions of each cartridge-type are supported, for example: standard, sport, VolSafe, and WORM.
Notes:		
Configurations:		
Tape Drives:		
Media:		

Rack Specifications

The KMAs can be installed in standard, RETMA¹ 19-inch, four post racks or cabinets. Note: Two-post racks are *not* supported.

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

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

SL8500 Rack Guidelines

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

Each rack can hold up to 6 units—called Us²—of equipment, such as the key management appliances and the Ethernet switches. Each rack has a six-connector power distribution unit (PDU) that provides power, and two cooling fans that provides additional air flow. [Table 3-2](#) lists the rack guidelines.

TABLE 3-2 SL8500 Accessory Rack Guidelines

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

1. RETMA = Radio Electronics Television Manufacturers Association.

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

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.

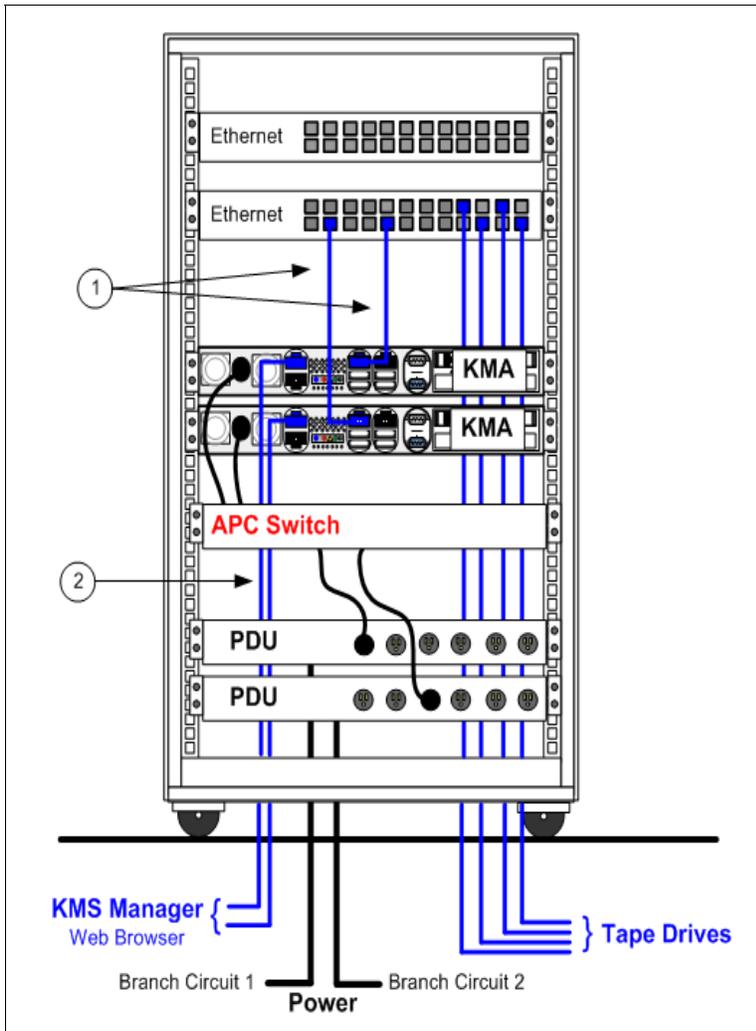
Customer's can either use existing racks or they can order this kit: **CRYPTO-20U-Z**.

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



Components and Part Numbers:

- Rack kit = CRYPTO-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

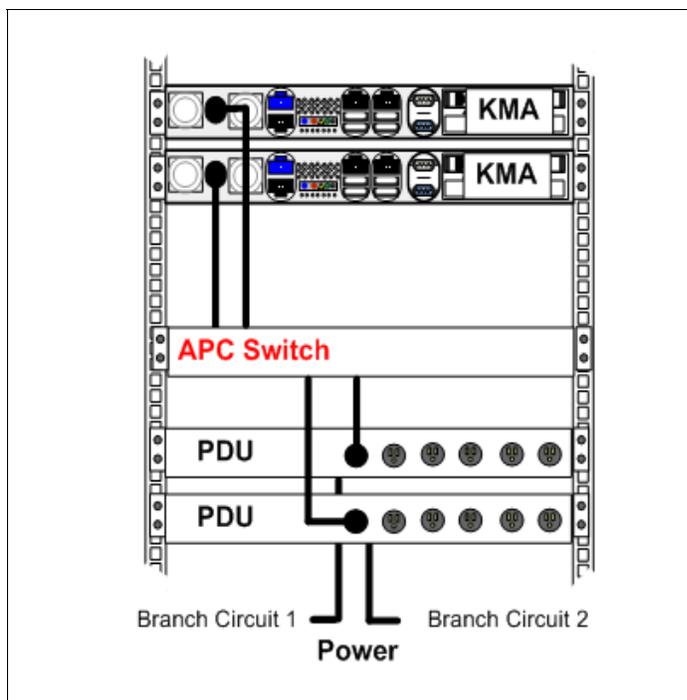
Customer may require a redundant power configuration.

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

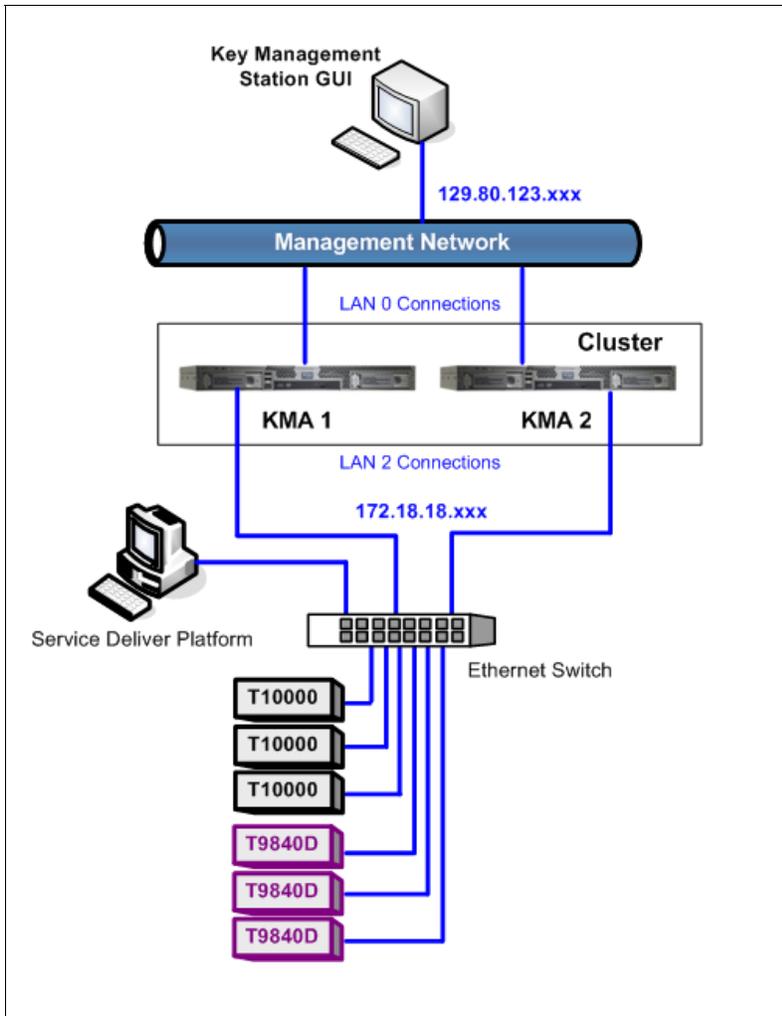
The Service Delivery Platform (SDP) is a support solution for Sun StorageTek libraries and tape drives that consists of a smart appliance and dedicated network.

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



In this figure, the KMS Manager interfaces with the KMAs using a customer created network and IP addresses of 129.80.123.xxx.

Each KMA connects to this network using LAN 0.

The KMA interfaces with the tape drives using the Service Network. SDP IP addresses = 172.18.18.1.

Each KMA connects to this network using LAN 2. IP address range is: 172.18.18.2 through 172.18.18.59.

The tape drives connect to the Service Network using an assigned IP address from the SDP.

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

Note:

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



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

Content Management

Encryption-capable tape drives adds another element to the design for content management in an SL8500, SL3000, and SL500 library installation.

All three libraries have a different design, all three libraries share similar elements; however, some considerations include:

TABLE 3-3 Content Management Planning

Element	SL8500	SL3000	SL500
Drive Quantity	You may need to order multiple kits or additional Ethernet switches to support all of the encryption-capable tape drives.		
	<ul style="list-style-type: none"> ■ Single: 1 to 64 drives ■ 10 library complex: up to 640 drives 	<ul style="list-style-type: none"> ■ 1 to 56 tape drives 	<ul style="list-style-type: none"> ■ 1 to 18 tape drives
Encryption Drives Supported	<ul style="list-style-type: none"> ■ T10000 A&B ■ T9840D ■ HP LTO4 	<ul style="list-style-type: none"> ■ T10000 A&B ■ T9840D ■ HP LTO4 	<ul style="list-style-type: none"> ■ HP LTO4 only
Non-encryption Drives Supported	<ul style="list-style-type: none"> ■ T10000 A & B ■ T9840 A, B, & C ■ LTO 2, 3, & 4 	<ul style="list-style-type: none"> ■ T10000 A&B ■ T9840 C ■ HP LTO 3 & 4 	<ul style="list-style-type: none"> ■ LTO 2, 3, & 4 (HP, IBM) ■ SDLT 600 ■ DLT-S4
Interfaces:	Note: The library interface and tape drive interfaces may be different.		
<ul style="list-style-type: none"> ■ Libraries 	<ul style="list-style-type: none"> ■ TCP/IP only 	<ul style="list-style-type: none"> ■ TCP/IP only ■ Fibre Channel 	<ul style="list-style-type: none"> ■ TCP/IP only ■ Fibre Channel
<ul style="list-style-type: none"> ■ Tape Drives 	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	Fibre Channel SCSI
Media	All libraries support true-mixed media—Any Cartridge, Any Slot™		
	<ul style="list-style-type: none"> ■ T10000 (Std, Sport, VolSafe) ■ 9840 (Std and VolSafe) ■ LTO 2, 3, 4, & T-WORM ■ DLTtape III ■ Super DLTtape I & II 	<ul style="list-style-type: none"> ■ T10000 (Std, Sport, VolSafe) ■ 9840 (Std and VolSafe) ■ LTO 2, 3, 4, & T-WORM 	<ul style="list-style-type: none"> ■ LTO 1, 2, 3, 4, & T-WORM ■ DLTtape III ■ Super DLTtape I & II
Partitioning	Yes	Yes	Yes
SNMP	Yes	Yes	Yes
SDP	Yes	Yes	Yes
Power Redundancy	Yes	Yes	No
Operating Systems	Enterprise and Open Systems	Enterprise and Open Systems	Open systems platforms
Library Management	<ul style="list-style-type: none"> ■ ACSLS ■ HSC 	<ul style="list-style-type: none"> ■ ACSLS ■ HSC ■ ISV 	<ul style="list-style-type: none"> ■ ACSLS ■ HSC ■ ISV
FC = Fibre Channel FICON = IBMs fiber connection SNMP = Simple Network Management Protocol SDP = Service Delivery Platform		ACSLs = Automated Cartridge System Library Software HSC = Host Software Component ISV = Independent Software Vendor (Veritas, Legato, TSM)	

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 appropriate sized library resources.

**Tip:**

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

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

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

Essential guidelines for understanding partitions are:

- Clear communication between the system programmers, network administrators, library software representatives and administrators, and 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 3-4 Steps and Tasks for Partitioning

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

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
 - Service version (PN: 96180)
 - Customer version (PN: 96179)

Supported Platforms and Web Browsers

KMS Manager Platforms:

The KMS Manager (graphical user interface—GUI) must be installed on either a Windows XP or Solaris 10 updates 3x86 or 4x86 platform.

Note – Windows Vista and Solaris 9 are *not* supported.

Web Browsers:

Embedded Lights Out Manager is sensitive to Web browser and Java versions.

TABLE 3-5 lists the supported operating systems and Web browsers:

TABLE 3-5 Operating Systems and Web Browsers

Client OS	Java Runtime Environment Including Java Web Start	Web Browsers
<ul style="list-style-type: none"> ■ Microsoft Windows XP ■ Microsoft Windows 2003 ■ Microsoft Windows Vista 	JRE 1.5 (Java 5.0 Update 7 or later)	<ul style="list-style-type: none"> ■ Internet Explorer 6.0 and later ■ Mozilla 1.7.5 or later ■ Mozilla Firefox 1.0
<ul style="list-style-type: none"> ■ Red Hat Linux 3.0 and 4.0 		<ul style="list-style-type: none"> ■ Mozilla 1.7.5 or later ■ Mozilla Firefox 1.0
<ul style="list-style-type: none"> ■ Solaris 9 ■ Solaris 10 ■ Solaris Sparc ■ SUSE Linux 9.2 		<ul style="list-style-type: none"> ■ Mozilla 1.7.5

You can download the Java 1.5 runtime environment at: <http://java.com>

The current version of the ELOM guide is located at: <http://dlc.sun.com/>

Required Tape Drive Firmware Versions

The required firmware (microcode) versions for the tape drives are:

TABLE 3-6 Tape Drive Firmware Versions

Tape Drive	Interface Type	Firmware Version (or higher)
T10000 A	Fibre Channel	1.37.108
	FICON	1.37.114
T10000 B	Fibre Channel	To be supplied Check on availability
	FICON	
T9840 D	Fibre Channel	1.42.104
	FICON	1.42.104
	ESCON	1.42.104
HP LTO4	Fibre Channel	To be supplied Check on availability
	SCSI	

Required Library Firmware Versions

The required firmware (microcode) versions for the tape drives are:

TABLE 3-7 Library Firmware Versions

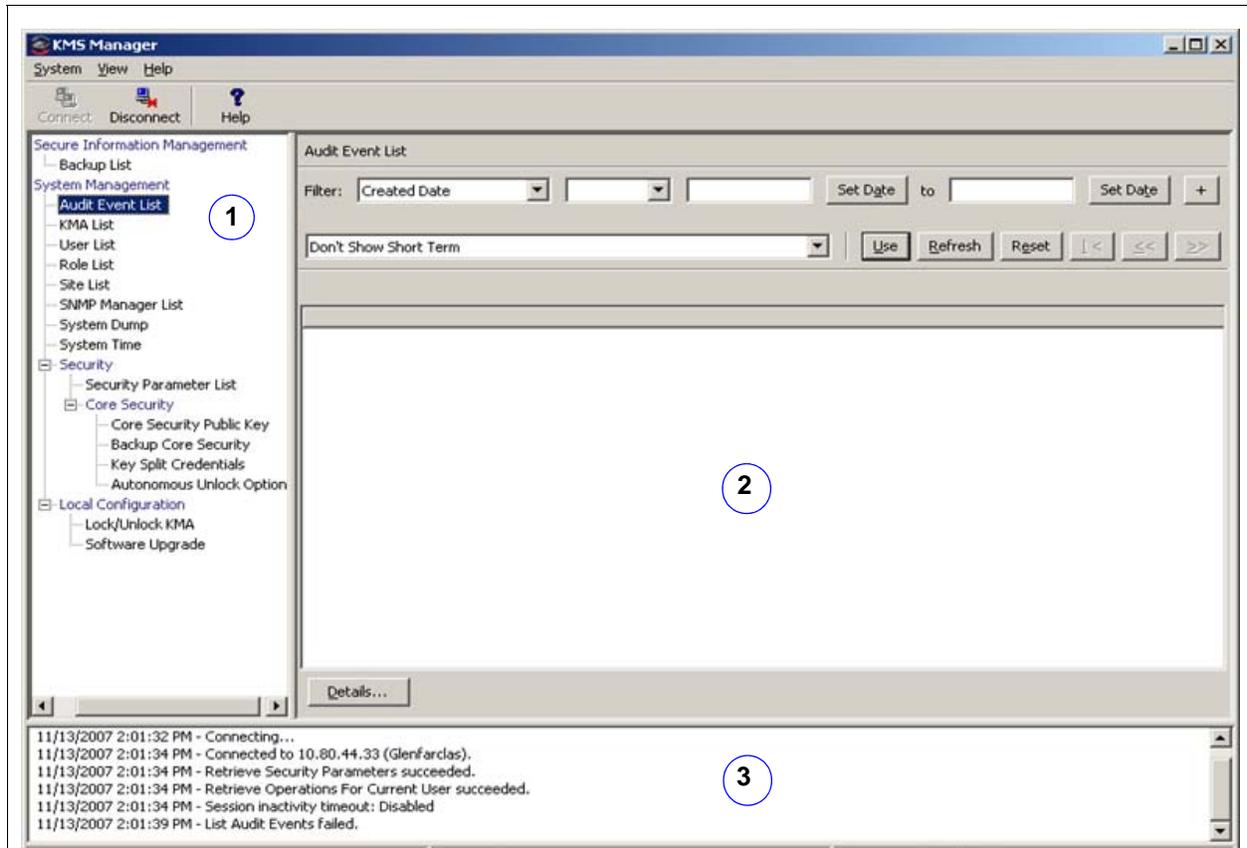
Library	Firmware Version (or higher)
SL8500	FRS_3.72
SL3000	To be supplied
SL500	1201
9310	9311: 4.4.06 9330: TCP/IP - 2.1.02 code 9330: 3270 - 1.9.73 code
L-Series	3.15.02

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 40).

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.

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

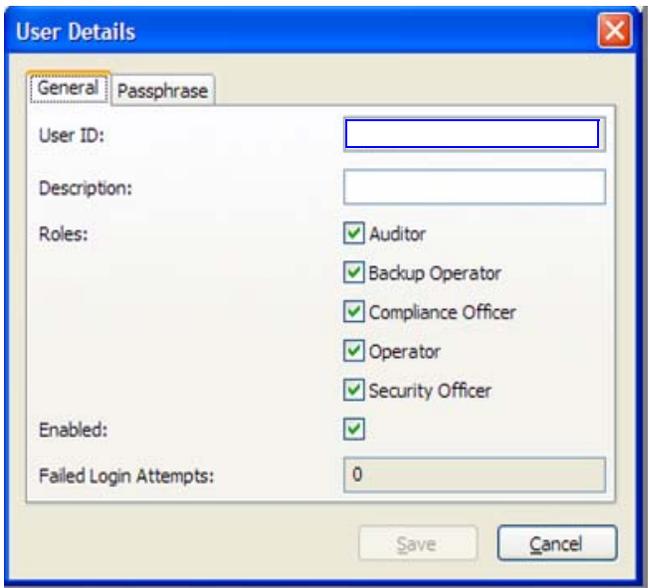


Note: Each person or user may fulfill one or more of these roles.

[FIGURE 3-4](#) shows an example of the Users Detail screen.

Use [TABLE 3-10 on page 45](#) to help prepare for the assignments.

FIGURE 3-4 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 41](#) 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
Console						
	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
Connect						
	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
Key Split Credentials						
	List	Yes				
	Modify	Quorum				
Autonomous Unlock						
	List	Yes				
	Modify	Quorum				
Lock/Unlock KMA						
	List Status	Yes	Yes	Yes	Yes	Yes
	Lock	Yes				
	Unlock	Quorum				

TABLE 3-9 Operator Roles and Functions (Continued)

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

TABLE 3-9 Operator Roles and Functions (Continued)

Entity	Function	Roles				
		Security Officer	Compliance Officer	Operator	Backup Operator	Auditor
Agent						
	Create			Yes		
	List		Yes	Yes		
	Modify			Yes		
	Modify Passphrase			Yes		
	Delete			Yes		
Agent/Key Group Assignment						
	List		Yes	Yes		
	Modify		Yes			
Data Unit						
	Create					
	List		Yes	Yes		
	Modify			Yes		
	Modify Key Group		Yes			
	Delete					
Keys						
	List Data Unit Keys		Yes	Yes		
	Destroy			Yes		
	Compromise		Yes			
Transfer Partners						
	Configure	Quorum				
	List	Yes	Yes	Yes		
	Modify	Quorum				
	Delete	Yes				
Backup						
	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
Core Security Backup						
	Create	Yes				
SNMP Manager						
	Create	Yes				
	List	Yes		Yes		
	Modify	Yes				
	Delete	Yes				
Audit Event						
	View	Yes	Yes	Yes	Yes	Yes
	View Agent History		Yes	Yes		
	View Data Unit History		Yes	Yes		
	View Data Unit Key History		Yes	Yes		
System Dump						
	Create	Yes		Yes		
System Time						
	List	Yes	Yes	Yes	Yes	Yes
	Modify	Yes				
NTP Server						
	List	Yes	Yes	Yes	Yes	Yes
	Modify	Yes				
Software Version						
	List	Yes	Yes	Yes	Yes	Yes
	Upgrade			Yes		

Ordering

This chapter contains the order numbers and descriptions for the Sun StorageTek key management appliance and encryption solution.

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 48](#)
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 49](#)
- [“SL3000 Modular Library System” on page 50](#)
- [“SL500 Modular Library System” on page 51](#) (*check on availability*)
- [“9310 Automated Cartridge System” on page 52](#)
- [“L-Series–L180, L700e, and L1400 Libraries” on page 53](#)

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 54](#)

Supported Tape Drives

The currently supported tape drives include:

- T1000A
- T9840D

Check on Availability for these Drives

- T1000B
- HP LTO4

See [“Tape Drive Comparison” on page 14](#) for drive specifications and [TABLE 3-6 on page 38](#) 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

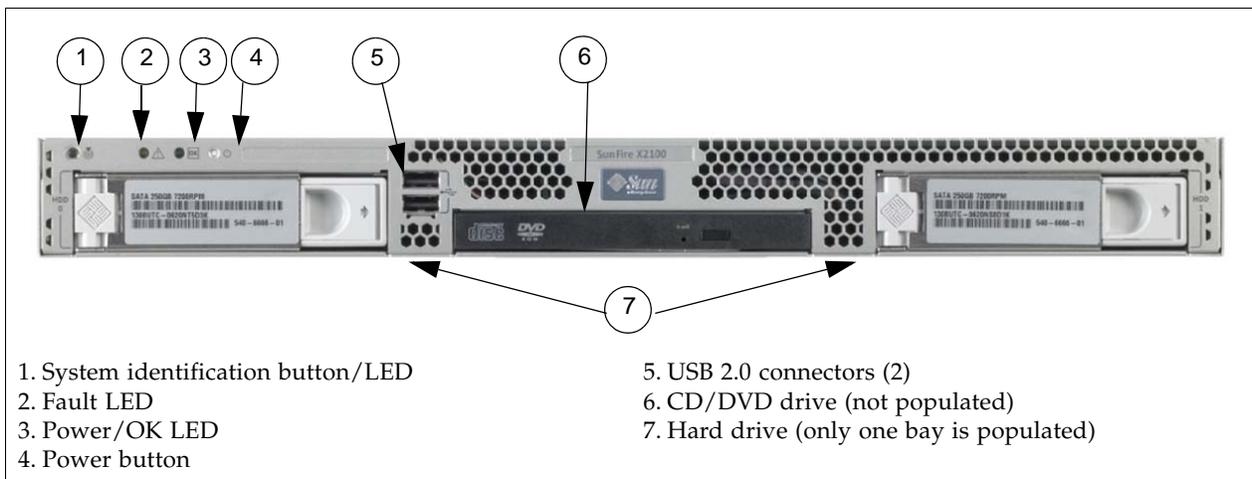
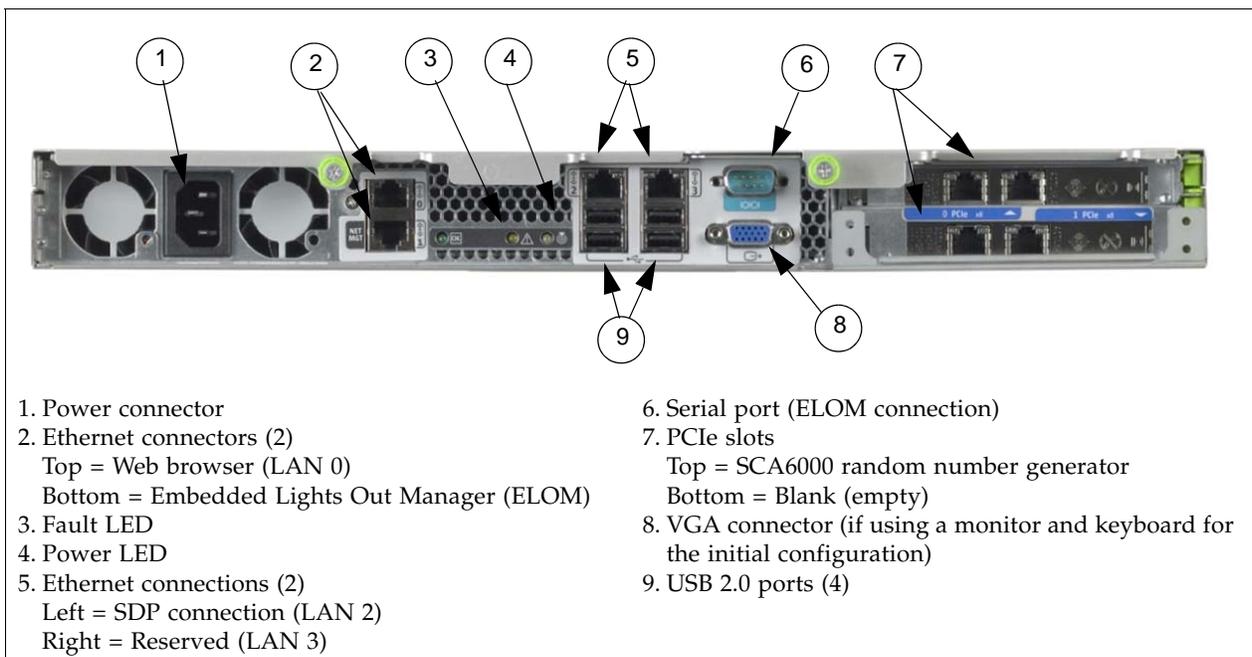


FIGURE 4-2 Key Management Appliance—Rear Panel



SL8500 Modular Library System

TABLE 4-1 SL8500 Modular Library System Requirements

<p>High-level Description: A single SL8500 library can store up to:</p> <ul style="list-style-type: none"> ■ 1,448 to 10,000 tape cartridges and ■ 64 tape drives. <p>An SL8500 Library Complex of 10 libraries can store up to:</p> <ul style="list-style-type: none"> ■ 100,000 tape cartridges and ■ 640 tape drives <p>Operating System Support: The SL8500 supports all major operating systems; enterprise <i>and</i> open systems.</p> <p>Host-to-Library Interface:</p> <ul style="list-style-type: none"> ■ Single Ethernet* (TCP/IP) 1x ■ Dual TCP/IP* (optional feature) 2x ■ Multi-host (optional feature) 4x <p>* Supports Partitioning</p> <p>The SL8500 provides internal rack space for the addition of the encryption hardware.</p>	
--	--

Order Number	Description
CRYPTO-2X-SL8500-Z	<p>SL8500 accessory kit. Installation included.</p> <p>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.</p> <p>Rack component order numbers: XSL8500-RACK-Z = 6RU Rack XSL8500-RACK-HW-Z = Rack component hardware kit XSL8500-AC-SW-Z = AC Transfer Switch</p>

Firmware Levels

Library	3.72 or higher (recommended)
StreamLine Library Console	3.38
Tape Drives: <ul style="list-style-type: none"> ■ T10000A ■ T10000B ■ T9840D ■ HP LTO4 	1.34.208 or higher <i>(Check on availability)</i> 1.42.104 or higher <i>(Check on availability)</i>
Virtual Operator Panel (VOP)	Version 1.0.11 or higher

SL3000 Modular Library System

TABLE 4-2 SL3000 Modular Library System Requirements



High-level Description:

- The SL3000 library offers customers the benefits of:
- Scalability in storage capacity from 200 to 4500 slots
 - Performance from 1 to 56 tape drives
 - Heterogeneous attachments using standard interfaces
 - Multiple library management software options and programs

Operating System Support:

The SL3000 supports all major operating systems; enterprise *and* open systems.

Host-to-Library Interface:

- Single Ethernet* (TCP/IP) 1x
 - Dual TCP/IP* (optional feature) 2x
 - Fibre Channel* 1x
- * Supports Partitioning

Order Number

Description

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

The SL3000 uses four different part numbers for Ethernet switches and cables to 1 to 56 tape drives.
Note:
 The SL3000 has limited internal rack space. Depending on the number of drives, customers may need to order an external rack.
 See [“External Rack Installations”](#) on page 30 if necessary.

Firmware Levels

Library	FRS_4.0
StreamLine Library Console	2.0
Tape Drives: <ul style="list-style-type: none"> ■ T10000A ■ T10000B ■ T9840D ■ HP LTO4 	1.34.208 or higher <i>(Check on availability)</i> 1.42.104 or higher <i>(Check on availability)</i>
Virtual Operator Panel (VOP)	Version 1.0.11 or higher

SL500 Modular Library System

TABLE 4-3 SL500 Modular Library System Requirements

<p>High-level Description: The SL500 library, is a self contained, fully automated, cartridge tape storage system that is scalable and mounts into a standard 483 mm (19 in.) rack or cabinet. The library can consist of 1 to 5 modules (one base and up to four expansion modules). Because of the scalability, the capacity of an SL500 library can store:</p> <ul style="list-style-type: none"> ■ From: 2 tape drives with 530 data cartridge slots ■ To: 18 tape drives with 395 data cartridge slots ■ A cartridge access port that holds 5 to 45 slots (depending on the number of modules) <p>With a variety of tape drives and cartridges slots in-between.</p> <p>Operating System Support: The SL500 supports all major operating systems; enterprise <i>and</i> open systems.</p> <p>Host-to-Library Interface:</p> <ul style="list-style-type: none"> ■ Single Ethernet* (TCP/IP) 1x ■ Fibre Channel <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>Note: The SL500 is a rack-installed library.</p> <ul style="list-style-type: none"> ■ With 3 or fewer expansion modules, encryption hardware can be installed in the same rack. ■ With 4 expansion modules, there is no room for the encryption hardware and customers may need to order an external rack. <p>See “External Rack Installations” on page 30 if necessary.</p>

Firmware Levels	
Library	Check on Availability
StreamLine Library Console	
Tape Drives: ■ HP LTO4	
Virtual Operator Panel (VOP)	Version 1.0.11 or higher

9310 Automated Cartridge System

TABLE 4-4 9310 Automated Cartridge System Requirements

<p>High-level Description: The 9310—also called PowderHorn—can store:</p> <ul style="list-style-type: none"> ■ From 2,000 up to 6,000 tape cartridges ■ Up to 4 drive cabinets with space for up to 20 drives per cabinet (80 drives total) <p>Operating System Support: The 9310 library supports all major operating systems; enterprise <i>and</i> open systems.</p> <p>Host-to-Library Interface:</p> <ul style="list-style-type: none"> ■ TCP/IP <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. Important: 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. Note: 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: targeted for 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 (Check on availability) 1.42.104 or higher
Virtual Operator Panel (VOP)	Version 1.0.11 or higher

L-Series–L180, L700e, and L1400 Libraries

TABLE 4-5 L-Series Library Requirements

<p>High-level Description: L700 and L1400 libraries support two models:</p> <ul style="list-style-type: none"> ■ <i>Single frame</i> libraries can hold: <ul style="list-style-type: none"> ■ From 678 tape cartridges and ■ Up to 12 T10000 tape drives. ■ <i>Dual frame</i> libraries holds <ul style="list-style-type: none"> ■ From 1,344 tape cartridges and ■ Up to 24 T10000 tape drives. <p>Operating System Support: Supports open system platforms, such as UNIX, Windows NT, Novell, and Linux.</p> <p>Host-to-Library Interface:</p> <ul style="list-style-type: none"> ■ LVD or HVD SCSI ■ Fibre Channel option <p>The L700e/L1400M libraries have internal rack space for the encryption hardware.</p>	
---	--

Order Number	Description
CRYPTO-2X-L7/14-Z	L180/700/1400 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) <ul style="list-style-type: none"> ■ L700e / L1400 ■ L180 	3.11.02 or higher
Tape Drives: <ul style="list-style-type: none"> ■ T10000A ■ T10000B ■ T9840D ■ HP LTO4 	1.34.208 or higher <i>(Check on availability)</i> 1.42.104 or higher <i>(Check on availability)</i>
Virtual Operator Panel (VOP)	Version 1.0.11 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.



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"> ■ T10000A ■ T10000B ■ T9840D 	1.34.208 or higher <i>(Check on availability)</i> 1.42.104 or higher
Virtual Operator Panel (VOP)	Version 1.0.11 or higher

Order Numbers, Descriptions, and Contents

TABLE 4-7 Order Numbers

Part Name	Part Number	Order Information	Kit Includes
Key Management Appliance:			
Crypto Key Management Appliance 2.0	CRYPTO-KMA-2-Z	Minimum Order two (2) per site. Provides clustering config, High-availability (HA), and auto-mirroring of key database.	<ul style="list-style-type: none"> ■ KMA ■ Pre-loaded Solaris ■ Rack mounting hardware ■ Client GUI CD
Encryption Library Kits			
Crypto SL8500 Library Kit	CRYPTO-2X-SL8500-Z	Minimum of one kit needed per SL8500 library Maximum of 4 per fully populated library. One required for each rail.	<ul style="list-style-type: none"> ■ 24 port ethernet switch ■ cables ■ rack mounting hardware SL8500 rack part numbers: <ul style="list-style-type: none"> ■ XSL8500-RACK-Z ■ XSL8500-RACK-HW-Z
Crypto SL500 Base Kit	CRYPTO-2X-SL500B-Z	NOT AVAILABLE UNTIL 2Q08 with HP LTO4 encryption capable drives. For use with KMS 2.x.	<ul style="list-style-type: none"> ■ 16 port ethernet switch ■ cables ■ rack mounting hardware
Crypto SL500 Expansion Kit	CRYPTO-2X-SL500X-Z	NOT AVAILABLE UNTIL 2Q08 with HP LTO4 encryption capable drives. For use with KMS 2.x. Purchase up to 4 kits per library rack. Cannot install 4 kits and encryption in same rack.	<ul style="list-style-type: none"> ■ Additional cables to extend from switch in base kit to each expansion kit. ■ May require extra rack
Crypto 9310 Library Kit	CRYPTO-2X-9310-Z	One kit needed per 9310. Includes first connection hardware to a 9741e Drive Cabinet	<ul style="list-style-type: none"> ■ 24 port ethernet switch for use in first 9741E cabinet ■ 16 port ethernet switch external to cabinet ■ cables ■ rack mounting hardware.
Crypto 9741e Drive Cabinet Kit	CRYPTO-2X-9741E-Z	One kit needed per 9741E cabinet Maximum of 3 per single 9310 silo. (Total of 4 9741e Drive Cabinets)	<ul style="list-style-type: none"> ■ 24 port ethernet switch ■ cables ■ rack mounting hardware.

TABLE 4-7 Order Numbers

Part Name	Part Number	Order Information	Kit Includes
Crypto L180/700/1400 Library Kit	CRYPTO-2X-L7/14-Z	One kit needed per Lxxx library.	<ul style="list-style-type: none"> ■ 16 port ethernet switch, cables, and rack mounting hardware.
SL3000 uses multiple part numbers depending on the library configuration:			
Crypto SL3000 Library Kits	Multiple Part Numbers	Minimum of one kit needed per SL3000, max (4) per fully populated SL3000.	See SL3000 configurator for PNs and pricing which vary based on library module. These numbers also used with the Service Delivery Platform SDP.
SL3000 Kit 1	XSL3000-ETHRNT1-Z	Switch: supports drives 1-8 in the Base/DEM	If library encryption upgrade, check installation to verify if already installed. Kit (PNs) also used for SDP.
SL3000 Kit 2	XSL3000-ETHRNT2-Z	Cables: supports drives 8-16 in the Base/DEM	If library encryption upgrade, check installation to verify if already installed. Kit (PNs) also used for SDP.
SL3000 Kit 3	XSL3000-ETHRNT3-Z	Switch: supports drives 17-24 in the Base/DEM	If library encryption upgrade, check installation to verify if already installed. Kit (PNs) also used for SDP.
SL3000 Kit 4	XSL3000-ETHRNT4-Z	Cables: supports drives 25-32 in the DEM	If library encryption upgrade, check installation to verify if already installed. Kit (PNs) also used for SDP.

TABLE 4-7 Order Numbers

Part Name	Part Number	Order Information	Kit Includes
Crypto Accessories			
Rack kit for SL8500	XSL8500-RACK-Z	Sun StorageTek SL8500 Tape Library, Conversion Bill, Rack Component HW Kit. See upgrade planner for additional detail: http://sunwebcms.central.sun.com:8001/sunweb/cda/mainAssembly/0,2685,369146_47679,00.html	<ul style="list-style-type: none"> ■ Rack mounting hardware to place switches in SL8500.
APC for SL8500	XSL8500-AC-SW-Z	Power supply for SL8500	<ul style="list-style-type: none"> ■ Optional power supply which may be used with encryption configuration within SL8500 library.
External, 20U Rack	RACK-20U-Z	One (optional) with 9310, unless customer has external rack already available. May be required for other libraries.	<ul style="list-style-type: none"> ■ External, half-high rack for use as needed, primarily with 9310 ■ Includes no mounting hardware
Crypto Rack	CRYPTO-2X-RACK-Z	One (optional) for use with rackmount drives.	<ul style="list-style-type: none"> ■ Extra 16 port switch ■ mounting hardware as needed
Crypto 16PT ethernet switch	CRYPTO-X-16PT-Z	One or more (optional) for redundancy or replacement.	<ul style="list-style-type: none"> ■ Extra 16 port switch ■ no mounting hardware ■ no cables
Crypto 24PT ethernet switch	CRYPTO-X-24PT-Z	One or more (optional) for redundancy or replacement.	<ul style="list-style-type: none"> ■ Extra 24 port switch ■ no mounting hardware ■ no cables
Monitor/Keyboard and rack mount accessory kit, US only PN 315496601.	XCRYPTO-KEYBD-MONZ	One (optional) for use in lieu of customer provided client or workstation.	<ul style="list-style-type: none"> ■ Optional monitor and keyboard.
Drive Enablement Keys			
T10000A drive encryption key, bundled	T10A-4FC-EKEY-B	One required per encryption enabled tape drive. Bundled with T10000A drive at time of sale.	Software license key from Web Site for drive license and encryption enablement.
T10000A drive encryption key, after market	T10A-4FC-EKEY-A	One required per encryption enabled tape drive. After market for T10000A drives previously purchased.	Software license key from Web Site for drive license and encryption enablement.

TABLE 4-7 Order Numbers

Part Name	Part Number	Order Information	Kit Includes
T10000A drive encryption key, bundled	T10A-2FI-EKEY-B	One required per encryption enabled tape drive. Bundled with T10000A drive at time of sale.	Software license key from Web Site for drive license and encryption enablement.
T10000A drive encryption key, after market	T10A-2FI-EKEY-A	One required per encryption enabled tape drive. After market for T10000A drives previously purchased.	Software license key from Web Site for drive license and encryption enablement.
T10000B drive encryption key, bundled	X-T10B-EKEY-B	T10KB drive feature B	Software license key from Web Site for drive license and encryption enablement.
T10000B drive encryption key, after market	X-T10B-EKEY-A	T10KB drive feature A	Software license key from Web Site for drive license and encryption enablement.
T9840D drive encryption key, bundled	9840D-EKEY-B	One required per encryption enabled tape drive. Bundled with 9840D drive at time of sale.	Software license key from Web Site for drive license and encryption enablement.
T9840D drive encryption key, after market	9840D-EKEY-A	One required per encryption enabled tape drive. After market for T9840D drives previously purchased.	Software license key from Web Site for drive license and encryption enablement.
HP LTO4 drive encryption key, bundled	X-HP-LTO4-EKEY-B	NOT AVAILABLE UNTIL 2Q08 with HP LTO4 encryption capable drives For use with KMS 2.x.	One required per encryption enabled tape drive. Bundled with HP LTO4 drive at time of sale.
HP LTO4 drive encryption key, after market	X-HP-LTO4-EKEY-A	NOT AVAILABLE UNTIL 2Q08 with HP LTO4 encryption capable drives For use with KMS 2.x.	One required per encryption enabled tape drive. After market for HP LTO4 drives previously purchased.

TABLE 4-7 Order Numbers

Part Name	Part Number	Order Information	Kit Includes
HP LTO4 Drive Upgrade Kits			
Crypto Drive Upgrade for HP LTO4 FC SL500	XHPLTO4E-FCUPL500Z	HP LTO4 FC drive upgrade SL500	<ul style="list-style-type: none"> ■ HP LTO4 FC encryption drive upgrade for SL500
Crypto Drive Upgrade for HP LTO4 FC SL3000 / SL8500	XHPLTO4E-FCUP3085Z	HP LTO4 FC drive upgrade SL3000 / SL8500	<ul style="list-style-type: none"> ■ Serial to Ethernet interface card, cabling, drive tray back-plate
Crypto Drive Upgrade for HP LTO4 SCSI SL500	X-HPLTO4E-SCUP500Z	HP LTO4 SCSI drive upgrade SL500	
Service Delivery Platform (SDP): These numbers also used with the Service Delivery Platform			
Crypto SL3000 Library Kits	Multiple Part Numbers	Minimum of one kit needed per SL3000, max (4) per fully populated SL3000.	See SL3000 configurator for PN's and pricing which vary based on library module. These numbers also used with the Service Delivery Platform (SDP)
SL3000 Kit 1	XSL3000-ETHRNT1-Z	Switch: supports drives 1-8	Kit also used for SDP.
SL3000 Kit 2	XSL3000-ETHRNT2-Z	Cables: supports drives 8-16	If library encryption upgrade, check installation to verify if already installed.
SL3000 Kit 3	XSL3000-ETHRNT3-Z	Switch: supports drives 17-24	
SL3000 Kit 4	XSL3000-ETHRNT4-Z	Cables: supports drives 25-32	
KMS 1.x to KMS 2.0 Upgrade—Check on Availability			
Upgrade From: Version 1.x Key Management Workstation (KMS) To: Version 2.0 Key Management Appliance (KMA)	X-CRYPTO-1XTO2XUPZ	<p>Minimum (2) per each KMS Version 1.x being replaced.</p> <p>Note: The KMS must be at Version 1.2 and above to transfer keys.</p>	<ul style="list-style-type: none"> ■ KMA ■ pre-loaded Solaris ■ rack mounting hardware ■ client GUI CD ■ PLUS conversion bill and documentation for migration

TABLE 4-7 Order Numbers

Part Name	Part Number	Order Information	Kit Includes
Version 1.x Field Replaceable Units (FRUs)			
Spares, Workstation, KMS, Value Add	#3144974-Z	Spares KMS workstation.	<ul style="list-style-type: none"> ■ Spares Crypto KMS ■ Workstation only
FRU, Crypto KMS token key	#3144947-Z	Spares KMS Crypto key token	<ul style="list-style-type: none"> ■ Spares Crypto Token ■ Secure key repository ■ Use with Crypto KMS
FRU, Token Bay, Desktop	#3144987-Z	FRU, Token Bay, Desktop	<ul style="list-style-type: none"> ■ Spares Token Bay only ■ Desktop for Crypto KMS
FRU, Token Bay, Rack Mount, Ethernet (front)	#3144988-Z	FRU, Token Bay, Rack Mount, Front	<ul style="list-style-type: none"> ■ rack mounted (front Ethernet access) token bay
FRU Token Bay, Rack Mount, Ethernet (rear)	#3154719-Z	FRU, Token Bay, Rack Mount, Rear	<ul style="list-style-type: none"> ■ rack mounted (rear Ethernet access) token bay
Spares, External Hard Drive	#3144973-Z	100 GB USB hard drive	<ul style="list-style-type: none"> ■ Spares, KMS hard drive
	#3133781-Z	120 GB USB hard drive (Must be at KMS V 1.2)	
Version 2.0 Field Replaceable Units (FRUs)			
FRU Crypto KMA appliance	#3154936-Z	Spares, KMA appliance only	<ul style="list-style-type: none"> ■ KMA appliance with pre-loaded Solaris, no hardware
FRU HP LTO4 Encryption Dione Card	#4199549-Z	FRU, Dione Encryption Card <i>HP LTO4 only</i>	<ul style="list-style-type: none"> ■ FRU, Dione encryption card and cable replacement for HP LTO4 encrypting drives

9310 Upgrades

TABLE 4-8 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 4-9 Professional Services Ordering Instructions and Part Numbers

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

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 4-10 Tape Drive Ordering Instructions

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

Library 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 4-11 Library Ordering Instructions

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

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 64](#)
- [“User Roles Work Sheet” on page 65](#)
- [“Tape Drives Work Sheet” on page 66](#)
- [“Drive Enrollment Work Sheet” on page 67](#)
- [“Obtain the Drive Data” on page 68](#)

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
LAN 0 = Management			Yes <input type="checkbox"/> No <input type="checkbox"/>			Yes <input type="checkbox"/> No <input type="checkbox"/>
LAN 1 = ELOM			Yes <input type="checkbox"/> No <input type="checkbox"/>			Yes <input type="checkbox"/> No <input type="checkbox"/>
LAN 2 = Service			Yes <input type="checkbox"/> No <input type="checkbox"/>			Yes <input type="checkbox"/> No <input type="checkbox"/>
LAN 3 = Reserved						
KMA Name						
Gateway						
DNS Server	Hostname: IP address:			Hostname: IP address:		
Security Officer	Login: Passphrase:			Login: Passphrase:		
Root account Passphrase						
ELOM Passphrase						
Key Split Credentials						
Autonomous Unlocking ²						
Keyboard Type						
Note:	<p>1. Addresses assigned using DHCP must be static. 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>					

Tape Drives Work Sheet

TABLE A-3 Tape Drive 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

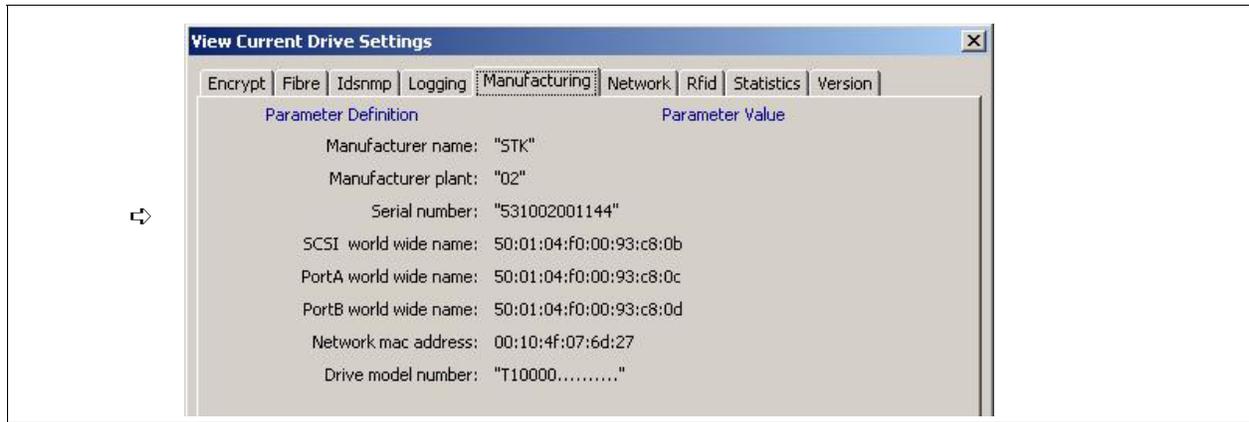
KMA Hostname:		KMA Hostname:			
KMA IP Address:		KMA IP Address:			
Drive Address	Drive Type	Drive IP Address	Agent ID	Passphrase	Permanent?
1.					Yes <input type="checkbox"/> No <input type="checkbox"/>
2.					Yes <input type="checkbox"/> No <input type="checkbox"/>
3.					Yes <input type="checkbox"/> 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"/>

Obtain the Drive Data

To obtain the drive data for *each* 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 A-1 Tape Drive Serial Number—VOP



2. Use [TABLE A-3 on page 66](#) 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://craapplications/keyswebapp/>
 - b. Select Request an Encryption key.

FIGURE A-2 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.

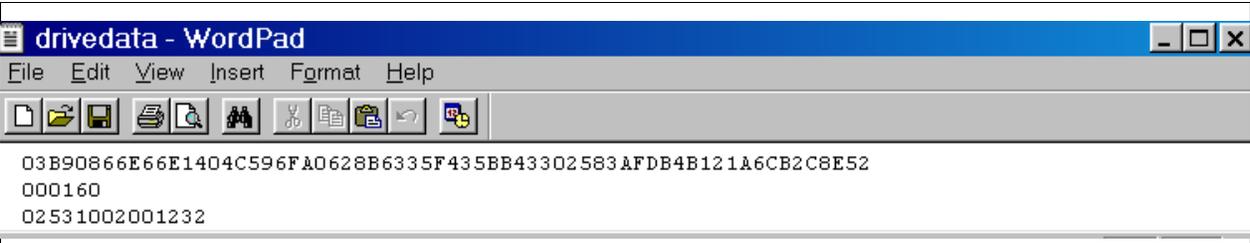
FIGURE A-3 Encryption File Request for Drive Data

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 A-4 Encryption File Request for Drive Data

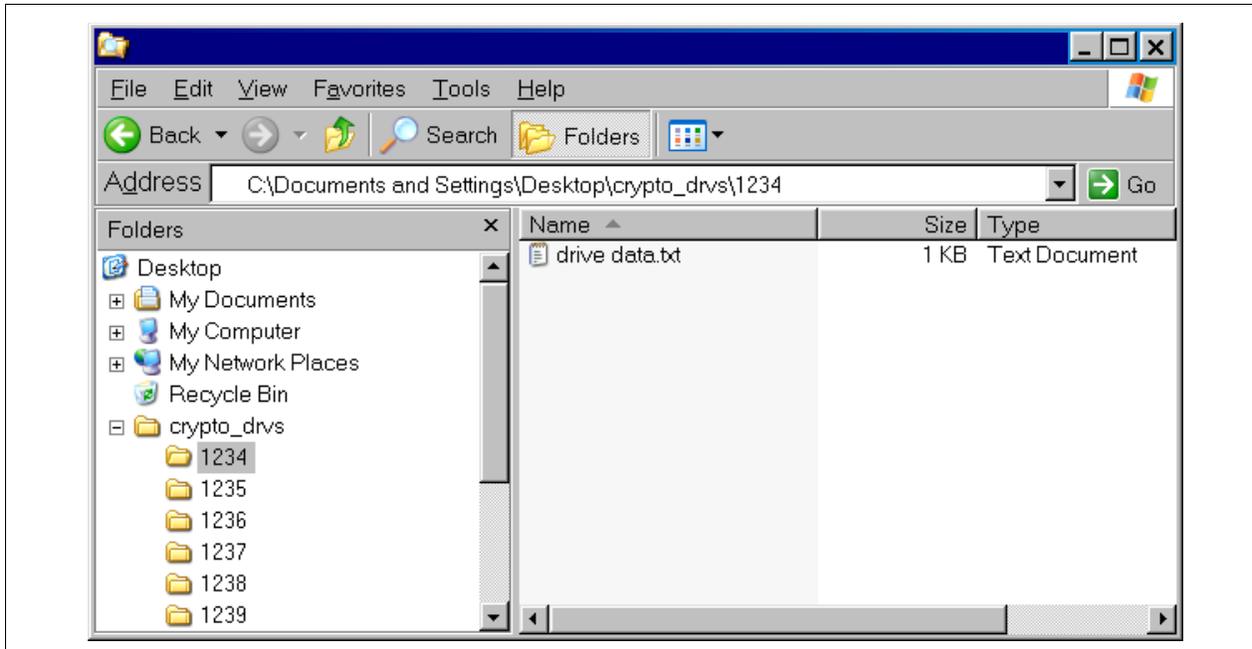


Create a Drive Data File Structure

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

1. [FIGURE A-5](#) 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 A-5 Drive Data File Structure



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

4. Complete [TABLE A-4 on page 67](#) 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.

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 (IP)
address** 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.

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

Numerics

1000 order numbers, rack, 54
1400, order numbers, 53
180, order numbers, 53
3000, order numbers, 50
500, order numbers, 51
700, order numbers, 53
8500, order numbers, 49
9310 installation requirements, 52, 53
9310 library, 52
9310 upgrades, 61
9310, order numbers, 52
9741e Drive Cabinet, 52
9741e, order numbers, 52

A

AC power factors and concerns, 27
accessory racks, SL8500, 29
Advanced Encryption Standard, 2
AES, 2
Agents, definition, 8
air gap configuration, 5
alley limitations, 26
altitude, 16
AMD Opteron processor., 3
ANSI standards, 29
APC Switch, part numbers, 30
assignments, 40
auditor, 40
Authenticating, 9

B

backup operator, 40
backups, types of, 10

C

cabinet, drive, 52
cabinet, specifications for installation, 29
capacity
 tape drive, 12, 13
Capacity on Demand, 34
CBC-MAC standard, 2
CCM standard, 2
certificate, 9
Challenge & Response Protocol, 9
checklists
 site planning, 26
 system assurance, 20
Cipher Block Chaining-Message Authentication Code, 2
cipher-suite, 2
cluster, 8
Common Criteria Consortium, 2
communications process, 9
comparison, tape drive and media, 15
compatibilities, media types, 15
compliance operator, 40
concerns for site planning, 23, 26, 41
configurations, supported, 47
connectivity
 factors for pre-installation, 27
content management, 33
 philosophy, 34
conversion bills
 9310 requirements, 52
Core Security Backup, 10
Counter with CBC-MAC, 2
Crypto Key Management Station
 configurations, 3
Crypto Key Management System, 3
cryptography, 1
customer

- contact sheet, 21
- satisfaction and the
 - system assurance process, 19

Customer Resource Center (CRC), xvi

D

- data path, partition planning, 35
- definition, 8
- delivery dock, 26
- delivery of the hardware, 26
- depth, 16
- description, order numbers, 55
- device-based solutions, 3
- DHCP, 32
- dimensions
 - tape drive, 12, 77
- dimensions, KMA, 16
- dock availability, 26
- drive cabinet, 52
- drive data, 68
- drive file structure, 70
- Dynamic Host Configuration Protocol, 32

E

- EIA 310-D-1992 standards for racks, 29
- encryption, 1
 - comparisons, 11
 - hardware kits, 10
- encryption hardware kits, 10
- encryption standards, 2
- enrollment data work sheet, 67
- environmental
 - factors and concerns, 26
- environmental parameters, 16
- error-free installation, 19
- Establishing, 9
- external rack installations, 30

F

- Federal Information Processing Standard, 3
- Federal Information Processing Standards, 2
- Federal Information Processing Standards Publications, xiv
- FIPS, 3
- FIPS publications, 2

G

- glossary, 71
- graphical user interface, 8
- GUI, 8
 - definition, 8
 - installation, 37
- guides, xiv

H

- hardware kits, 10
- heat output, 16
- height, 16
- Hewlett Packard, linear-tape-open, 13

I

- IEC 60927 standards for racks, 29
- IEEE standards, 2
- initial configuration work sheet, 64, 68
- installation
 - site planning checklist, 26
- Institute of Electrical and Electronics Engineers, 2
- International Standard Organization, 2
- ISO/IEC standards, 2

J

- Java versions, 37

K

- Key Groups, 8
- Key Management Appliance
 - definition, 8
 - order numbers, 48
- Key Management Station
 - installation, 3
- Key Split Credentials, 10
- kit contents, 55
- KMA
 - dimensions, 16
 - network types, 9
 - specifications, 16
- KMA *See* Key Management Appliance
- KMS Cluster, definition, 8
- KMS Manager
 - GUI definition, 8
 - installation, 37

L

- L1400, 53
- L180, 53
- L700, 53
- libraries
 - SL500, 51
- library
 - requirements for installation, 47
 - system assurance, 19, 36
- library content management, 33
- linear-tape-open, 13
- L-Series
 - order numbers, 53
- LTO, 13

M

- manual organization, xiii
- manuals, xiv
- MARs card, 3
- mass storage, 16
- media comparison, 15
- memory, 16
- mounting options, 16
- mutual authentication, 2

N

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

O

- operators, 40
- order numbers, 47
- order numbers, list of, 55
- organization of this manual, xiii

P

- partial response, maximum likelihood, 12, 13
- partitioning, 34
- partitioning is planning, 36
- Partner Agreement, xvi
- partner contact sheet, 22

- Partners Web site, xvi
- passphrases, 40
- PC Key request form, 68
- PCIe, 16
- PCI-Express slots, 16
- PDU part numbers, 30
- periodic backups, 10
- philosophy for content management, 34
- planning
 - for encryption, 1
 - site, 25
- planning meetings, for system assurance, 20
- PowderHorn library, 52
- power
 - factors for pre-installation planning, 27
 - supply, 16
- private key, 9
- PRML technology, 12, 13
- process, for system assurance, 19, 36
- processor, 16
- Professional Services, 61
- publications, xiv

Q

- quorum, 40

R

- rackmount order numbers, 54
- rackmount requirements, 54
- racks, specifications for installation, 29
- random number generator, 3
- raw keys, 3
- RealTime Growth, 34
- redundant power, 31
- related publications, documents, xiv
- relative humidity, 16
- required firmware levels, tape and library, 38
- required tools, 37
- requirements
 - 9310 library, 52
 - for the system assurance process, 20
 - L-Series, 53
 - PowderHorn, 52
 - rackmount, 54
 - SL500 library, 51
 - SL8500 library, 49
- resellers, xvi
- RETMA, 29

roles, 40

S

SATA disk drive, 16
SCA6000, 16
SCA6000 card, 3
SDP, 32
secure sockets, 9
security officer, 40
Service Delivery Platform, 32
site planning, 25
site planning checklist, 26
size of tape drive, 12, 77
SL3000 order numbers, 50
SL500 library, 51
SL500 order numbers, 51
SL8500
 installation requirements, 49, 50, 51
 order numbers, 49
 overview, 49
Solaris 10 operating system, 3
specifications
 KMA, 16
standalone order numbers, 54
standalone rack installations, 30
standards for encryption, 2
steps for partitioning, 36, 39, 40, 45, 65
StorageTek
 Customer Resource Center (CRC), xvi
 Partners site, xvi
 team member contact sheet, 22
 Web site, xvi
Sun
 Customer Resource Center (CRC), xvi
 Fire X2100 Server, 3
 Partners Web site, xvi
 Ultra 20 Workstation, 3
 Web site, xvi
Sun Crypto Accelerator 6000, 16
Sun Fire X2100 Specifications, 16
supported configurations, 47
survey
 site preparation, 25
 solution planning, 23
Symmetric encryption, 2
system assurance
 customer contact sheet, 21
 planning meeting, 20
 process overview, 19, 36

StorageTek contact sheet, 22

T

T10000 Tape Drive
 capacity of the tape drive, 12, 13
 description of, 12, 77
 size, 12, 77
T9840
 description, 13
T9840 Tape Drive
 description of, 77
 size, 77
tape drive
 comparisons, 14
tape drive and media comparison, 15
tape drive work sheet, 66
tape drives
 supported types, 12, 47
 T9840, 13
tasks for partitioning, 36, 39, 40, 45, 65
team members, 36
temperature, 16
T-Series
 T10000, 12
 T9840, 13
types of KMA networks, 9

U

units, rack measurements, 29
User Roles Work Sheet, 45
user roles work sheet, 65
users, 40

V

Virtual Operator Panel, 37
VOP, 37

W

Web browsers, supported versions, 37
Web sites, xvi
weight, 16
width, 16
work sheets, xiii, 63
 initial configuration, 64, 68
 tape drive enrollment, 67
 tape drives, 66
 user roles, 65

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN Web 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.