

Crypto Key Management Station and Data-at-Rest Encryption

Technical Brief
November 2006

Revision: 2.2

Copyright © 2006 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, Ladson, Sun Microsystems, the Sun logo; Solaris, Sun StorageTek Crypto Key Management Station, StorageTek and StorageTek 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 re-export 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 © 2006 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, Etats-Unis. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle 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 Station, StorageTek et 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. Please contact the Sun Learning Services Feedback System at:

SLSFS@Sun.com

or

Sun Learning Services
Sun Microsystems, Inc.
One StorageTek Drive
Louisville, CO 80028-3256
USA

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

Contents

Introduction	5
Data-at-rest Encryption.....	5
The Encryption Method.....	6
Components	7
Configurations	8
Kits	8
Key Management Station	9
Tokens.....	10
Token Bay.....	11
Keys.....	12
Raw Keys.....	12
Device Keys	12
Media Keys	12
Key Protection.....	13
Tape Drive	14
PC Key.....	14
Crypto Serial Number.....	14
Tape Drive Block Diagram	15
Media	16
What Is Written on Tape?	16
Nonce.....	16
Decryption.....	17
Roles in an Encryption Environment.....	18
Operational Flow to Encryption.....	18
Enabling a Drive	19
Creating Media Keys	19
Mapping Key Sets with Tape Drives.....	20
Examples.....	21
Standards and Compliance.....	22
Environmental.....	22
Safety	22
EMC Compliance.....	22
Media.....	22
Specifications	22
Frequently Asked Questions.....	23
Glossary.....	27

Introduction

This technical brief is intended for anyone interested in Sun's Data-at-Rest encryption solution. This brief provides a high-level overview and describes the methods and strategy used for encryption, which includes Sun StorageTek tape and tape automation products.

Encryption 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 it.

Sun's Storage Group has been involved in several projects concerning data protection for many years. These projects have yielded significant developments in the technology for encrypting data.

Encryption can occur at any one of three points in the life of data, when it is:

- Created – host-based encryption or at the operating system level
- Transported across the LAN – appliance-based, such as Decru and NeoScale products
- Stored on a device (data-at-rest encryption)

Key Management:

For all three methods, data access is controlled with an encryption key.

Therein lies the risk: *Lose the key and you lose your data.*

That fact alone makes key management one of the most important aspects of data security in an encrypted world.

The Challenge:

A successful data encryption strategy must address proper key management and to make sure that the keys to unlock the data are never lost.

Data-at-rest Encryption

Data-at-rest encryption—or device-based encryption (the implementation)—is a good solution for mixed environments; those with a variety of operating systems. This is because the *storage devices* handle the task of encryption: There is no process overhead or delays in transmission that might occur with other methods.

Note: Choosing a data-at-rest encryption solution is *least disruptive* to existing system infrastructure.

Encryption functionality is built directly into the tape drive or other device, so there is no need to maintain special software exclusively for encrypted data.

In addition, device-based encryption is:

- An optimal encryption method for archive data
- Easy to implement
- More efficient, the host no longer requires process time to encrypt or decrypt data
- Supports compression before encryption
- Cost-effective for scaling solutions for data center environments
- Supports heterogeneous environments
- Is least disruptive to the existing infrastructure

The Encryption Method

The SUN StorageTek implementation for data-at-rest encryption uses the CCM–AES-256 encryption process.

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

AES is a National Institute of Standards and Technology (NIST) standard defining a cryptographic cipher that uses a block length and the Rijndael symmetric block cipher algorithm.

AES by itself is a very strong cipher; but adding counter mode makes it much more difficult to break or spot patterns. Then when it is bundled with the CBC-MAC message integrity method, it ensures that messages have not been tampered with. This combination provides for a very efficient and reliable method of encryption.






While the intention of this technical brief is *not* to describe the encryption process, the basic concept is:

- A key management system must be set up in advance.
This system and the keys—which are random binary numbers—must be kept secure.
 - When writing data to a tape, the originator uses a key for encryption of the data.
 - When reading data from a tape, the recipient uses the same key for decryption (Symmetric Key encryption).
- Encryption uses a write key, plain text, and a nonce to create cipher text, which is recorded on a tape.
- Decryption takes a read key, cipher text, and a nonce to return the encoded data to plain text.

Components

The following shows the components of the SUN StorageTek device-based, data-at-rest solution.

Figure 1: Components

Host Operating Systems (no changes required)		Heterogeneous platform support	
Applications (no changes required)		Customer selectable	
Data-at-rest Encryption Solution	Key Management Station (KMS) 	<ul style="list-style-type: none"> Ultra 20 workstation <p>The KMS is shipped with a secure version of Solaris 10 and key management software (the application)</p>	
	Encryption-capable Storage Device 	<ul style="list-style-type: none"> SUN StorageTek T10000 tape drive Capacity: 500 GB (native) Transfer rate: 120 MB/s (native) Data compression Media 	
	Tokens 	<p>Small, portable, microprocessor-based, intelligent device used for securely sharing and storing keys</p>	
	Token bay 	<p>A token bay can hold either one or two tokens in a 1-U rack mount or desktop enclosure.</p> <p>Each token bay provides:</p> <ul style="list-style-type: none"> Power for the tokens Ethernet connectivity to the KMS or tape drives 	
	Ethernet	<p>Connectivity between KMS and token bay, or token bay and tape drives</p>	<p>A <i>private network</i></p>
	Ethernet Hub or Switch 	<p>Connectivity between the tokens and the tape drives</p>	

Configurations

The data-at-rest encryption configurations from SUN StorageTek include library and rack mount configurations that use Key Management Stations and kits for the encryption hardware.



Key Management Station

- Sold as a complete appliance only
 - Ultra20 desktop workstation with monitor, keyboard, and mouse
 - SCA 6000 crypto-card (random number generator for keys)
 - Token bay, typically a desktop unit with one open slot and one tokens
 - External USB hard drive
-

Kits



SL8500 Encryption Accessory Kit

This kit includes a dual-slot rack mount token bay, and everything to install it in an SL8500 accessory rack module including a 24-port Ethernet switch and cables.

You can also order this kit with or without the accessory rack module.



L-Series—L180/L700e/L1400M Encryption Accessory Kit

This kit includes a dual-slot rack mount Token bay, and everything to install it in an L-Series internal rack including a 16-port Ethernet switch, cables, and power distribution unit.



9310 Encryption Accessory Kit

This kit includes a dual-slot rack mount Token bay, and everything to install it in an *external* rack (provided), including 16-port and 24-port Ethernet switches, cables, and two power distribution switches for power redundancy.

If the customer is using more than one 9741E cabinet, additional 9741E Encryption Accessory Kits a required.



Stand-alone Rack Mount Drive Encryption Accessory Kit

This kit includes a dual-slot rack mount Token bay, and everything to install it in an accessory rack with the tape drives.



T10000 Tape Drives

These are encryption-ready, 4Gb-capable tape drives that connect to a Fibre Channel interface. In the future, these drives will also support IBM's FICON interface.

Key Management Station

Important:

The key management station (KMS) is a *dedicated appliance*. Customers *will not* be able to use existing hardware, install other applications, make modifications to, or apply patches to this appliance.

Each KMS configuration includes:

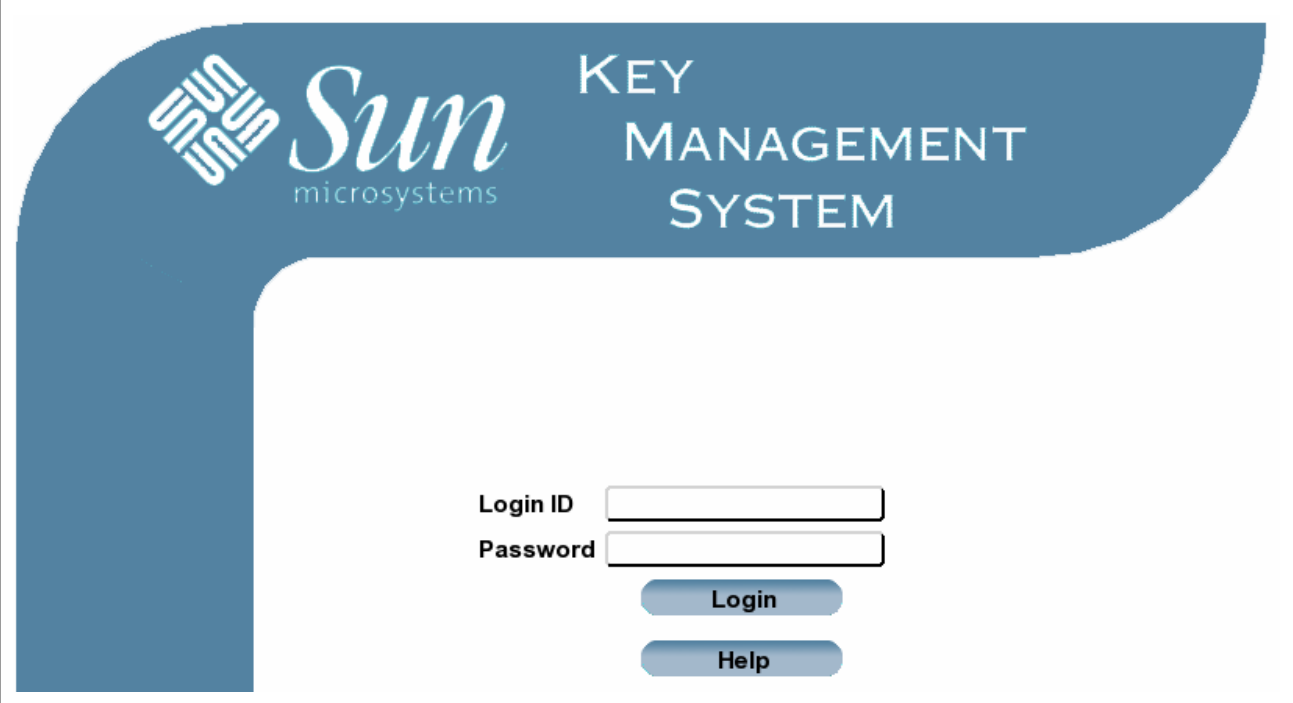
- Ultra 20 workstation running a version of the Solaris 10 operating system
- SCA6000 crypto-module card, that includes a random number generator to provide raw keys.
Note: Raw keys may also be imported from CD-ROM or entered manually.
- Easy to use Key Management System (application) with a graphical user interface
- External USB-attached hard drive for database backups

In addition, each key management station:

- Provides an assured backup of every key and its associated key ID
- Provides comprehensive logging capability
- Facilitates the customer's security policy and procedures
- Allows the customer to create, assign and revoke encryption keys
- Supports the device keys used to protect media keys
- Supports key assignment across all encryption agents

This figure shows an example of the user interface login screen.

Figure 2: Key Management System User Interface



The screenshot shows the login interface for the Sun Key Management System. The top header is a dark blue banner with the Sun Microsystems logo on the left and the text "KEY MANAGEMENT SYSTEM" on the right. Below the banner, the "Login ID" and "Password" fields are displayed as text labels next to empty input boxes. Below these fields are two blue buttons: "Login" and "Help".

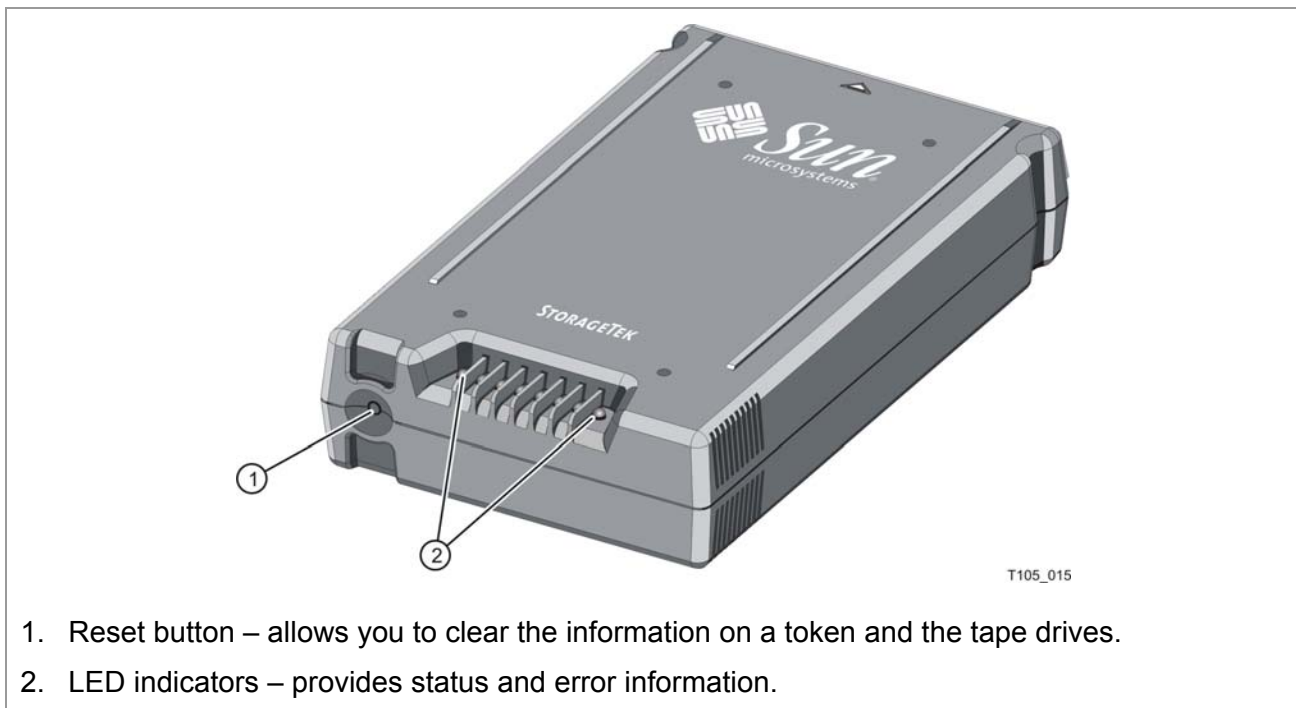
Tokens

Tokens are small, portable, microprocessor-based, intelligent devices that plug into a Token bay that connects to an Ethernet port.

There is one physical token that performs different functions based on the operation being completed. It can be used as an enabling key token or an operational key token.

- Enabling key tokens (EKT) convey device keys (in encrypted form) from the KMS to a tape drive. Once device keys have been successfully transmitted to a drive, they are erased from the EKT memory. The drive and KMS permanently maintains these keys.
- Operational key tokens (OKT) transport, in encrypted form, one write/read media key and up to 31 read media keys that are being conveyed from the KMS to the drive (32 keys total).

Figure 3: Token



Up to two tokens can plug into the token bay, which provides both the Ethernet and power connection for the tokens to function.

The benefits of having two tokens are:

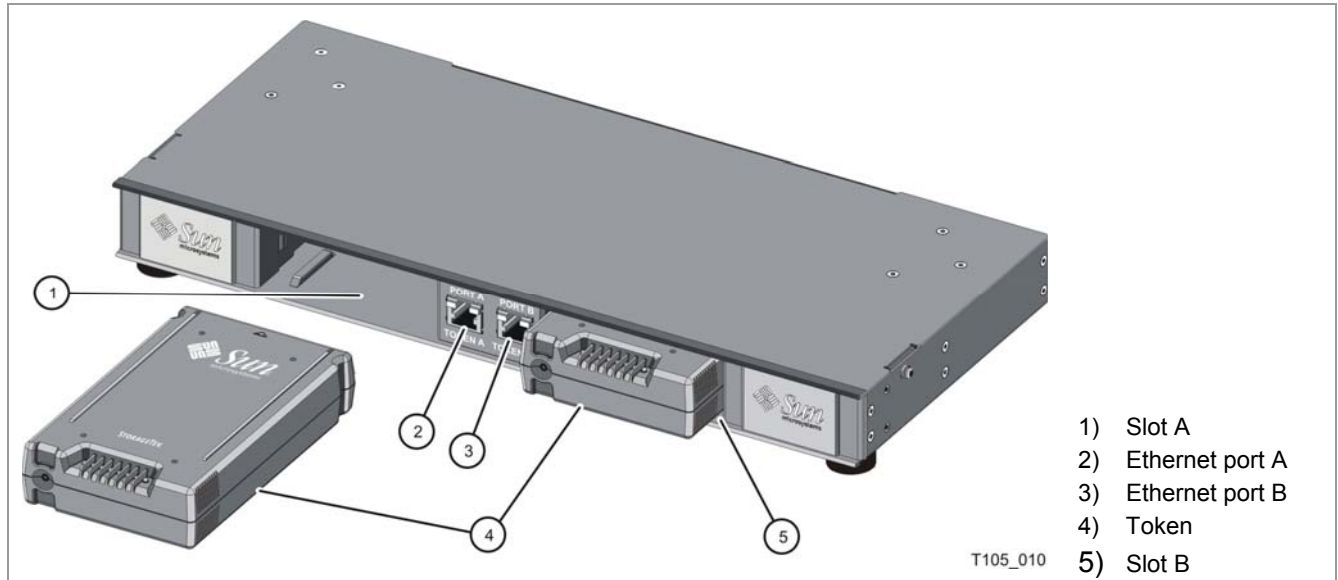
- Allow for redundancy depending on the power configuration
- Upgrade functions where you can remove a token to upgrade keys
- Support for multiple drive pools and key sets

Note: A token holds the *keys* for encryption; up to 1,850 drives.

Token Bay

The token bay is compatible with standard 19-inch rack measurements—a 1U form factor. It provides power and connectivity for one or two tokens through the rear blind-mating connector.

Figure 4: Rack Mount Token Bay



The token bay can be used in both rack mount (shown above) and desktop (one slot) configurations.

- **Rack mount configuration**

The rack mount token bay (not shown) has two slots and is supplied with mounting flanges. The rack mount configuration can be mounted either horizontally or vertically to support both standard and library rack mount configurations.

- **Desktop configuration**

The desktop token bay has only one port and is supplied with standoffs (foot pads). This configuration is normally supplied with the KMS.

Dimensions of the token bay:

Height	5 cm (2.0 in)
Width	44 cm (17.32 in.)
Depth	20 to 25.5 cm (8 to 10 in.)
Weight	TBD

Power requirements:

The token bay has two independent DC adaptors—each provides power to one token slot.

- AC input: 100 to 240 VAC, 50/60Hz, at 0.2 to 0.5 Amps
- DC output: 12V, 1.5A, 18W maximum

AC input power is supplied to the token bay using two IEC Power Inlet Connectors mounted at the rear of the unit.

Keys

A key is a string of 256 bits, in a random bit pattern generated by the Key Management Station, or manually entered from the keyboard, or purchased and downloaded to the application.

There are three classes of keys:

- Raw keys
- Device key
- Media keys

Raw Keys

A raw key is a string of 32 bytes (256 bits), in a random bit pattern. Raw keys are the building blocks for device and media keys—they have not yet been assigned to drives or key sets.

Raw keys are typically generated by random number generator card included in the Key Management Station. They can also be purchased from an external source (such as on a CD-ROM).

Device Keys

Device keys are used to enable drives for encryption and protect media keys while they reside on the operating key token (OKT). A device key is unique to each tape drive and assigned by the KMS.

Note: To ensure that device keys are kept secure, their values are never displayed.

There are three types of device keys that are automatically generated to provide three layers of protection during transmission:

- Wrap keys encrypt packages of media keys and key IDs during transmission.
- Split keys obscure media keys using an exclusive-or function.
- Communication keys provide another layer of encryption and authentication for every drive.

All of this is taken care of transparently—requiring no intervention—as part of the KMS/token/drive communications protocol. The device key values never appear to the user, keeping them secure.

Media Keys

Media keys encrypt and decrypt customer data on a tape cartridge.

Media keys are generated by a random number generator in the KMS, imported from a CD, or manually entered. Then these keys are assigned to key sets and sent to the drive through an Ethernet connection using the tokens.

Each drive can store up to 32 keys—one write key used to both encrypt and decrypt data and 31 read keys to decrypt data. The customer, through the KMS, can decide which write key and which read keys are assigned to each drive.

Recommendations are that *initial* configurations—all T10000 tape drives in a library—use the same write key and share the same set of read keys.

As future encryption phases occur, customers can take advantage of the flexibility and added features of the KMS, key assignments, and partitioning.

The media key values must be kept secure.

Each media key has a unique Key ID that is written to a tape in plain text so the tape drive knows which key value to use to decrypt the data

Key Protection

Media keys can reside in any of the following locations:

KMS database	To ensure the security of media keys, the Key Management Station should be kept in a secure location.
OKT	To ensure their security, media keys are encrypted on the OKT.
Drive	To ensure their security, media keys on a drive are stored in volatile memory.

Note: The media keys are erased from the drive’s memory whenever the drive is powered-off or removed from the library. When the drive re-initializes, it must recover the media keys in order to be able to read and write to tape. For this reason, it is important that the OKT be kept in the token bay connected to the encryption drives.

The layers of key protection are shown in the following figure.

Figure 5: Key Protection

Location				
Levels of Protection				
	Key Management Station	Token	Ethernet	Tape Drive
	<ul style="list-style-type: none"> –Kept in a secure location –Keys stored in non-volatile memory –Keys protected by permission-level access – Keys never appear in clear text form unless the KMS operator is manually entering in key values 	<ul style="list-style-type: none"> –Device keys encrypted by the KMS –Media keys transported in split and encrypted form 	<ul style="list-style-type: none"> –All transmissions are encrypted 	<ul style="list-style-type: none"> –Device and media keys stored in locations that cannot be read out over any drive interface –Device keys stored in non-volatile memory –Split Media keys and corresponding key numbers stored in volatile memory. Plain text media keys are not present in any readable memory location
Key types	Media key Split key Wrap key Communications key	Wrap key {Media key ⊕ Split key} Communications key	Communications key [Wrap key {Media key ⊕ Split key}]	Media key Split key Wrap key Communications key

Blue = Volatile Memory

Black = Non-volatile Memory

Tape Drive

The T10000 4Gb Fibre Channel tape drive is the first Sun StorageTek drive to support data-at-rest encryption. This tape drive is built encryption-capable. All you need to do is enable it with an optional software-keyed feature.

The T10000 includes the circuitry required to encrypt and decrypt data as it is written to and read from tape. In addition, the T10000 provides the firmware required to control the encryption hardware and to receive, decrypt, and store the keys provided from the KMS.

Important:

For security reasons, once you enable the T10000 to write in encrypted mode, it is not possible to reset it to non-encryption in the field. An encryption-enabled drive will be able to read non-encrypted tapes but will not be able to write to a tape in non-encrypted mode.

In addition, it will not be possible to mix encrypted and non-encrypted data on the same tape. An encryption drive will not be able to append to a tape that contains non-encrypted data.

Figure 6: Tape Drive and Media Capabilities

Tape Drive Capabilities	Media Capabilities	
	Non-encrypted Tape	Encrypted Tape
Standard tape drive (non-encrypting)	<ul style="list-style-type: none"> Fully compatible Business as usual 	Not capable of reading or appending to this tape.
Encryption-enabled drive	Read but will not be able to append to this tape	<ul style="list-style-type: none"> Read with correct key Write with current write key

During the manufacturing process, each drive is programmed with a unique value of PC key and assigned a specific crypto serial number (CSN) which is burned into flash memory.

Enable or PC Key 32 bytes (64hexadecimal characters)

Crypto serial number 3 bytes (6 hexadecimal characters)

As part of the enabling process, when the customer receives the encryption-capable tape drives, they need to enter the PC Key and crypto serial numbers into the Key Management Station.

PC Key

The enable key or PC Key (preset communication key), is a manufacturing preset code that enables the T10000 tape drive for encryption.

This key must be kept secure.

Crypto Serial Number

The crypto serial number (CSN) does not need to be kept secure. This number helps the token communicate with the correct drive.

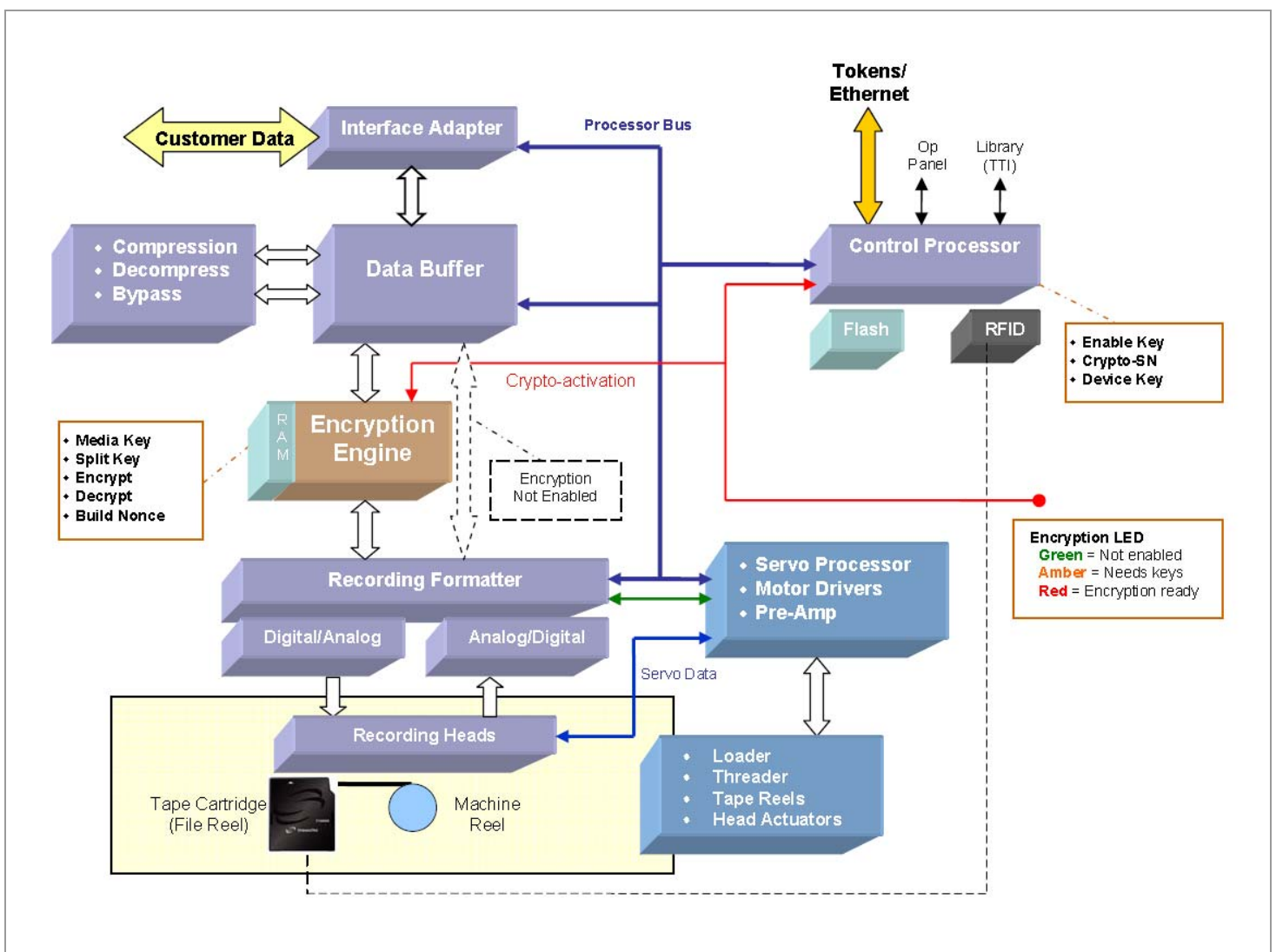
Note: For convenience, the PC Key and CSN can be provided on a CD and imported to help with the process of key entry.

Tape Drive Block Diagram

This figure shows a block diagram for the T10000 with encryption. Things to note about this block diagram are:

- Encryption occurs after the data buffer
- Encryption occurs after data compression
- The same drive is capable of either encryption or non-encryption, not both (once encryption is enabled, it is always enabled)
- The drive has a physical indicator that shows when encryption is enabled (an LED)
- Ethernet port is used to communicate with the token
- Enable PC Key and crypto serial number (CSN)


Figure 7: Tape Drive Block Diagram



Media

Encryption is supported on all T10000 media types including the standard cartridge, sport cartridge, and VolSafe or WORM cartridge.

Figure 8: Tape Cartridge

	<p>The encrypted package written on a tape comprises of:</p> <ul style="list-style-type: none">• Encryption header• Key ID• Non-repeating nonce• Encrypted data• Encryption tag used with the encryption header to authenticate data <p>Important: No key is present on a tape.</p> <p>If the drive does not have the correct key to read the encrypted data, it reports the required key ID to the key management station using the token, data path, application, and virtual operator panel (VOP).</p>
---	--

What Is Written on Tape?

Once the encryption hardware has been activated, encrypted data will be written to a tape.

During write operations, the tape drive receives the logical record, processes it for compression, then produces a nonce and transforms the data into an encrypted logical record.

Nonce

What is a nonce?

- A nonce is a number that is structured such that the values can never repeat.
- A nonce is automatically and randomly created by the KMS.
- A nonce is a value that is used as the initialization vector for the encryption process.
- A nonce ensures that each cipher text is different even if the plain text to be encrypted is not.
- A nonce is recorded on tape because it does not need to be random or kept secret

This method of using a nonce achieves the strong concept of privacy for the encryption scheme.

Each encrypted block on tape contains the nonce and media key ID that is used during encryption.

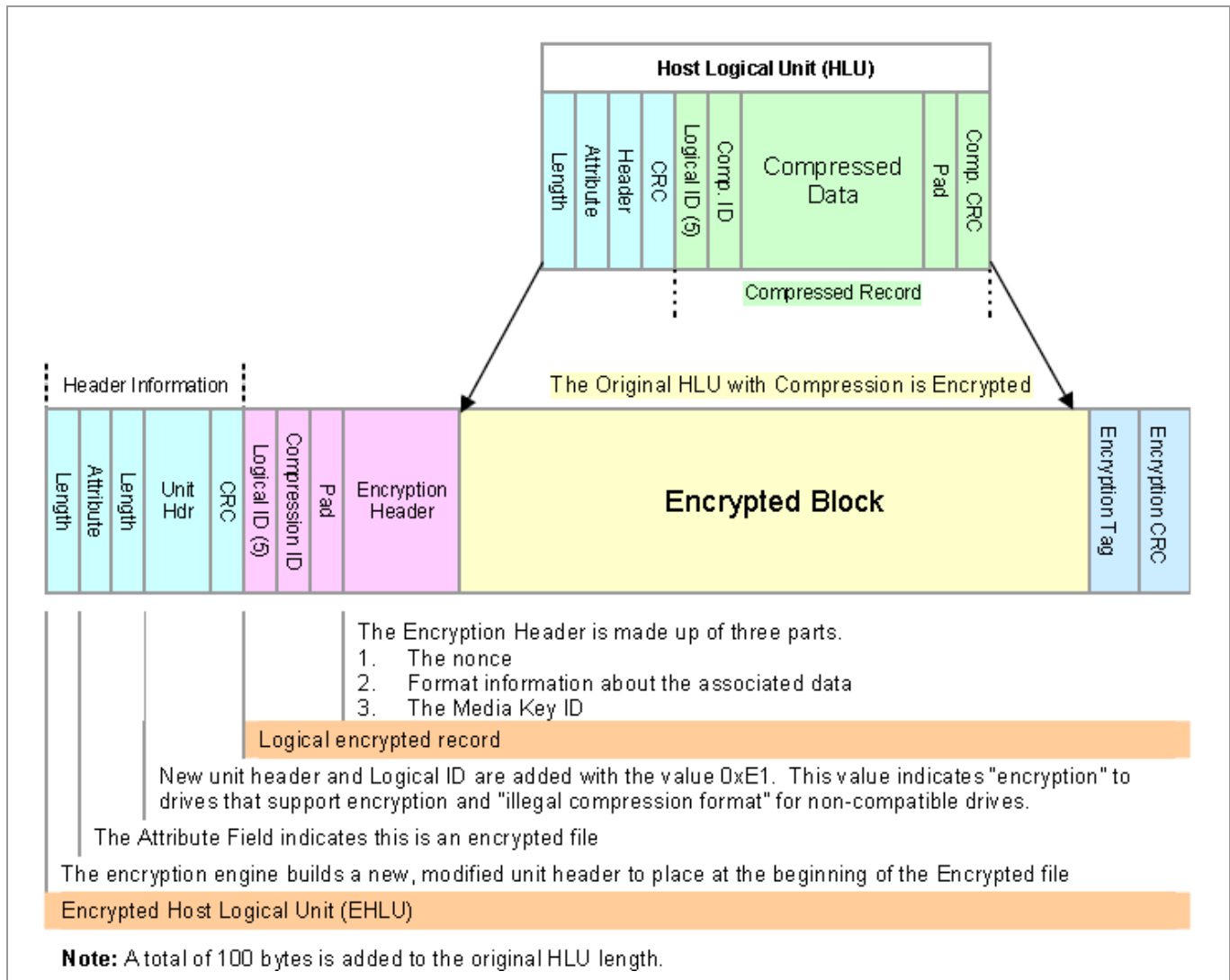
Important: The Media Key does not appear anywhere on a tape.

The contents of a nonce may include:

- Operation Code identifies what is being performed (varies)
- CCM is the mode of encryption
- Serial number is the crypto serial number (CSN)
- Key management station content
- Data and time stamp from the KMS
- Block count
- Block length

The following figure shows an example of a logical record and the data transformation.

Figure 9: Recorded Format



Decryption

The basic process during a read operation is:

- If the encryption bit *is not set* in the attribute field of the header, then pass the data through the encryption engine without any transformation.
- If the encryption bit *is set*, then process the unit header and use the keys for that encryption to decrypt the data.
 - If the key cannot be found, then:
 - Report a read error and illegal format.
 - Send an error message to the token, data path, and application with the missing key ID.
 - If the key ID is found, then:
 - Provide the decryption engine with the nonce and the key value.
 - Decrypt the data.
 - Check the encryption tag to ensure it decrypted correctly.

Roles in an Encryption Environment

The Key Management System supports three types of operators—each with specific roles. These roles conform to the Federal Information Processing Standard (FIPS) Level 2 Security requirements.

Roles	Tasks	Functional Area
Administrator	<ul style="list-style-type: none"> • Create the security officer login and password • Create key sets and keys • Import keys • Export keys 	Role assignment Key creation
Security Officer	<ul style="list-style-type: none"> • Create the user login and password • Create the enabling key token (EKT) • Create tokens • Write device keys • Enable the encryption-capable tape drives 	Tape drive enablement
User	<ul style="list-style-type: none"> • Creates drive pools and drives • Map key sets to drive pools • Create tokens • Write media keys (OKT) 	Usage

Note: An employee or staff member can function in one or more of these roles but cannot be logged in at the same time.

Operational Flow to Encryption

The operational flow has three steps that the operator roles need to perform.

Step	Task	Admin	Security Officer	User
1	Import and create keys	<input type="checkbox"/>		
	Create additional operator roles	<input type="checkbox"/>		
2	Write Device Keys (EKT)		<input type="checkbox"/>	
	Create additional operator roles		<input type="checkbox"/>	
3	Enter the tape drive information			<input type="checkbox"/>
	Create drive pools			<input type="checkbox"/>
	Map key sets to drive pools			<input type="checkbox"/>
	Write Media Keys (OKT)			<input type="checkbox"/>

Note: Creating tokens and writing tokens are independent operations. However, you must first create the token before you can write to it. Once the token is created, it can be used as an EKT, an OKT, or both, but not at the same time.

Enabling a Drive

The process to enable a tape drive to support encryption involves entering a:

- Unique drive name for *each* tape drive—up to 20 characters
- Description for *each* tape drive—up to 256 characters

Then supply values for the:

- PC Key, a unique and secret 64-character number
- Crypto serial number, a unique number *per drive*

Figure 10: Enabling a Tape Drive

The form for enabling a tape drive includes the following fields and controls:

- Drive Name***: A single text input field.
- Description**: A single text input field.
- PC Key***: Eight individual text input boxes for a 64-character key.
- Confirm PC Key***: Eight individual text input boxes for confirming the PC key.
- Crypto Serial Number***: A single text input field.
- Buttons**: Three buttons labeled "Apply", "Cancel", and "Help" are positioned at the bottom of the form.

The KMS then assigns the unique set of device keys to that drive.

After all drives have been entered into the KMS database, the enabling key token can be written. This token, when installed in the token bay, transfers the device keys to the specific drives, which enables them for encryption.

Once you have enabled the tape drives, the EKT is no longer necessary.

Creating Media Keys

Each media key has a unique, customer created, key ID that is written to a tape in plain text so the tape drive knows which key value to use to decrypt the data.

To create a media key,

- Click the New Key button (the fields on the screen are populated with data)
- Complete a description for that new key
- Select the key set from the list

Figure 11: Creating a Media Key

The form for creating a media key includes the following fields and controls:

- Key ID***: A text input field containing "001E0001", followed by a yellow highlight, an empty box, another yellow highlight, another empty box, and a text input field containing "00000000000000000000". A "New Key" button is located to the right of this field.
- Description**: A single text input field.
- Crypto Key***: Eight individual text input boxes for a 64-character key.
- Confirm Key***: Eight individual text input boxes for confirming the crypto key.
- Key Set***: A dropdown menu currently showing "MyKeySetName".
- Buttons**: Three buttons labeled "Apply", "Cancel", and "Help" are positioned at the bottom of the form.

After the keys have been entered into the KMS database, the operational key token (OKT) can be written. This token must remain with the token bay incase the tape drives loose power or a re-IPL of the drive. When the tape drives initialize, they automatically recover and look for the media keys.

Note: A best practice for the operational token is to keep it in the Token bay—always available for the tape drives.

Mapping Key Sets with Tape Drives

- Key sets simplify key assignments and key rotation operations. They provide a group of media keys (the write key and necessary read keys) for the tape drives to use for encryption.
- Drive pools simplify operations by grouping tape drives that share keys and key sets.

With drives enabled and keys created, users can *map* which key sets and keys to use with which tape drives, plus select which write key to use from the list of keys in that key set.

Figure 12: Mapping Drives with Keys

The screenshot shows the Sun Key Management System interface. At the top, the Sun Microsystems logo is on the left, and the text "KEY MANAGEMENT SYSTEM" is on the right. A vertical navigation menu on the left includes "Drives", "Drive Pools", "Mapping", "Modify" (highlighted), "Tokens", and "Logoff". The main content area is titled "Drive Pool Name" with the value "Pool_1". Below this is a section for "Available Keysets" containing a list box with "KeySet3: Third" and "Key_Set_1: Initial Key Set". There are "Add Keysets" and "Remove Keyset" buttons. Below that is a "Keysets in Pool" section with a list box containing "KeySet2: Second key set". At the bottom, there is a "Write Key*" field with a long hexadecimal string: "001e0003f1000005000000000000000020000000000000000000000000000000000000". "Apply", "Cancel", and "Help" buttons are at the bottom, followed by the text "2 keys in drive pool" in green.

Note: When a new write key is selected, the previous write key remains in the drive pool mapping as a read key without any action by the user. It will cease to be available as a read key only if it is explicitly removed from the drive pool mapping (for example, by removing the key set).

Examples

The design of a key management station and encryption solution is very flexible and under strict control of the customer. This design allows assignment of keys to tape drives to be changed as often as the customer desires.

Here are some examples:

- If the customer wanted to assign a new write key to the drive pool each month:

In January 2006 the drives would have only one key (Key_1) to both write and read data.

In February 2006 the customer could issue a new key (Key_2) to write—*append*—and read data, and the January key is now a read-only key.

This scheme would continue until December 2006, the drives would then have 12 keys.

- Key_12 would be the write and read data key.
- Key_1 through Key_11 would be read-only keys.

This design allows all the drives in the pool to read all of the data written during the year.

In January 2007, the customer could do several different things with their data, such as:

- Archive the media and the data with the keys (1 through 12) as a complete package. Then start fresh with a new January key.
- Continue with this scheme and make January 2007 Key_13—appending and reading to the existing data with the previous keys. The customer could use this scheme up to August 2008.

Note: A best practice for key management is to only define as many keys that can be held in a drive, which is 32 total.

- Keep only one year's worth of active data, in which case the customer could make the January 2006 data unreadable by removing Key_1 from the key set.

Add a January 2007 key (such as Key_13) to both write and read data. Key_2 through Key_12 would now be the read keys.

In this way the data written January 2006 can not be read. If an attempt was made to read this data, the tape drive would report a read error with an illegal format. Send an error message to the token, data path, and application with the missing key ID (Key_1).

- Another example might be a separation between different departments.

Accounting data is using one key set (key_set_1acc) with its own group of encryption keys.

Engineering data is using a different key set (key_set_2eng) and group of encryption keys.

This scheme ensures a total segregation of drives, keys, and data between organizations.

Standards and Compliance

The SUN StorageTek Encryption solution will comply with the following regulatory standards.

Environmental

- RoHS and WEEE
- EDS 6-2 Temperature and Humidity
- EDS 6-2 Shipping and Handling, Dynamics

Safety

- UL Listed to UL 60950-1, 1st Edition
- CSA Certified to CAN/CSA C22.2 No. 60950-1-03
- TUV T-Mark to EN/IEC 60950-1

EMC Compliance (Emissions/Immunity)

- FCC Title 47, Part 15 Subpart B, Unintentional Radiators Class A
- VCCI Class A
- European CE Emissions Standards
- EMC Framework Australia AS/NZS 3548:1995
- BCIQ EMC Law Taiwan: CNS13438
- Canadian EMC Law: ICES-003

Media

- IEEE P1619.1

Specifications

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 17799
Security Techniques—Code of Practice for Information Security Management*

Plus others.

Frequently Asked Questions

Question: How do you enable encryption on a T10000 drive?

Answer: The customer orders a T10000 tape drive with the Crypto Active Drive feature.
 Note: All 4-Gb Fibre Channel T10000 tape drive come with the capability to encrypt data.
 Next, the customer receives the PC Key and drive crypto serial number, such as on a CD.

- This information is entered into the KMS.
- The customer generates raw keys to create device keys.
- The Security Officer—with these keys—writes the Enabling Key Token (EKT).
- The EKT is placed into the token bay connected to the drives, which enables the encryption feature.

Question: How do you work with a third-party Disaster Recovery (DR) facility or trusted third party vendor?

Answer: There are three different ways:

1. Set up the KMS at the DR site and mirror it to the primary KMS at the home site.
2. Set up a direct connection from the home site KMS to the token hub at the DR site.
3. Ship a token to the DR site.

For options 2 and 3, drives must be pre-assigned to the home KMS. Assignment is based on the crypto serial number built into the drive and PC Key delivered with the encryption feature.

Question: How do you replace an encrypted tape drive?

Answer: The replacement tape drive includes the Crypto Active Drive feature.
 To enable it, the Security Officer creates a new Enabling Key Token (EKT) with the new drive PC Key and crypto serial number. The new token is placed in the token bay for that drive, and the new drive is enabled.
 Then use the standard procedures to assign the drive to the same drive pool and key set.

Option 1: Enable new drives as needed using the KMS. This requires operator involvement.

Option 2: Pre-assign replacement drives to existing drive pools. At that point you can simply replace the drive and it will be immediately identified by the token as part of existing drive pool and the correct keys will be automatically loaded.

Question: What are the different KMS roles and what are their functions?

Answer: The key management system supports three types of operator roles:

- Administrator: Creates keys and assigns security officer roles
- Security Officer: Enables drives and assigns user roles
- User: Performs day-to-day media key assignments

These roles conform to the Federal Information Processing Standard (FIPS) Level 2 Security requirements.

Note: An employee or staff member can function in one or more of these roles—but a different login is required for each role.

Question: How do you backup the KMS?

Answer: Any time changes are made to KMS database, the KMS automatically:

- Backs up to an encrypted database in the KMS internal hard drive
 - Mirrors the KMS to any active, attached KMS
 - Backs up the entire system to an external USB attached hard drive (which is also encrypted)
-

Question: How many keys does the T10000 tape drive hold?
How many keys does a token hold?

Answer: The T10000 can hold up to 32 keys. One write/read key and 31 read keys.
The token can hold about 60,000 keys (32 keys for 1,850 different tape drives).

Question: How are keys generated in the Key Management Station?

Answer: Keys are created in one of three ways:

- Randomly using the Crypto 6000 random number generator (a card in the KMS)
 - Customer imports keys from a CD containing customer-procured raw key data
 - Customer can manually input the keys
-

Question: What is the T10000 encryption scheme?

Answer: CCM–AES-256. Counter with CBC-MAC, Advanced Encryption Standard. A block cipher encryption algorithm that is a National Institute of Standards and Technology (NIST) standard

Question: How does the encryption impact the performance of the T10000 tape drive?

Answer: Encryption has no measurable impact to tape drive performance (transfer rate).
There is very little overhead for encryption.

In lab testing, the T10000 drive was able to exceed the 120 MB/s specification for uncompressed transfer rates with the encryption feature turned on.

Question: What happens when or if someone deciphers (breaks) AES 256?

Answer: In theory, security would be compromised and cartridges will have to be rewritten with a new algorithm.

Note: An NIST evaluation predicts that the AES-256 bit encryption will not be compromised until the year 2030.

Question: Can you mix encrypted and unencrypted drives in the same library?

Answer: Yes, when you meet certain conditions.

Library control software allocates cartridge resources based on the Drive ID. Initially, within a single library, all T10000 drives should be encryption capable or not.

This will prevent media and illegal format errors if you maintain the tape drives and cartridges at the same level of compatibility.

Question: What is the security risk with losing the token (with the proper keys), an encryption-capable drive, data cartridge, or any combination of these?

Answer: Any two components can be compromised or stolen without exposure to secured data. You would need to recreate the entire process from the KMS and key assignments to recording the data.

However, the chances of this happening are practically impossible because:

- The various layers of encryption, authentication, and key protection used.
- Keys are randomly encrypted and time-stamped.
- The nonce is a number such that the values can never repeat.
- The enabling process of the tape drives is encrypted and the keys kept secure.
- The tape drive stores the media keys in volatile memory; whenever the drive is powered-off or removed from the library the media keys will be erased from the drive's memory.

Question: Does T10000 encryption require special media?

Answer: No, encryption is a feature of the drive and it does not require special T10000 media.

Question: Could there be issues with exchanging keys between US and Europe as in the past there were export restrictions on keys in the US?

Answer: No. They are private keys.
Once encryption products are installed, key movement is not regulated.

There has also been a significant reduction in the import/export restrictions on encryption technology in the last few years.

Note: We have received Export Certification from the Department of Commerce.
At FRS, we are only excluded from shipping to Taiwan.

Question: Does encryption require visually unique labels on the cartridge?

Answer: No, encryption uses the same label format as regular T10000 cartridges.

Question: What happens if an unencrypted cartridge is put into a crypto-active drive?

Answer: It can be read or scratched but encrypted data cannot be appended to plain text data.

Question: What happens if the cartridge is encrypted with a key that the drive does not have?

Answer: The drive will report an illegal format error to the operating system and token.

Then, the drive reports the specific Key ID required so the user can determine if the required key value can be supplied.

Question: What happens when an encrypted cartridge is put in a drive without the encryption capability or with the capability but not enabled?

Answer: The drive will report an illegal format error through the data path.

Question: Can an encryption-capable tape drive write without encrypting?

Answer: No, not after the drive is enabled for encryption.

Question: Is there a way to verify that the token used to load the keys into the library switch is the genuine token? Or that the keys are the ones intended?

Answer: Tokens are written at the KMS with specific information from that KMS and a time stamp. So, non-authenticated tokens would not be recognized by drives or the KMS.

Question: Why do I need the token if I have a direct connection from the KMS to the tape drives?

Answer: The primary advantage is that the token acts as a secure local store of keys so that a drive can recover its media keys following a power cycle without any KMS or user intervention. To move keys to third party sites and to suddenly evacuate your facility, you can remove the token and power down the library. At that point data is secure because the keys are gone from the drives until the token is re-inserted.

Question: How are the keys transmitted to the drives?
What are the differences, and who would likely use which method?

Answer: Keys are created in the Key Management Station, and are transmitted to the drives in one of two ways:

- Keys are transmitted through a direct connection to a token attached to a token bay in a library through an Ethernet cable.
Customers utilizing this method are typically in commercial environments and consider their data center secure.
 - The key management station is kept in a secure room away from the library. The token is created there, and then hand-carried to the configuration where the keys are transmitted using a second token bay.
Customers who require the highest level of security will likely use this method.
-

Question: What happens if you lose a key?

Answer: The benefit of electronic keys is that this is an extremely unlikely scenario. The KMS automatically updates the database on an external drive. Best practices dictate that a backup copy is periodically secured in a vault, at another location, to ensure key retrieval should a disaster happen at the site. In the unlikely scenario that the KMS and all backup copies of the database are permanently lost, losing a key means data encrypted with that key is irretrievable.

Glossary

Term	Description
AES	<p>Advanced Encryption Standard</p> <p>Name of Standard: Advanced Encryption Standard (FIPS PUB 197).</p> <p>Category of Standard: Computer Security Standard, Cryptography.</p> <p>Explanation: The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a <i>symmetric block</i> cipher that can encrypt (encipher) and decrypt (decipher) information.</p> <p>The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.</p>
CBC-MAC	Cipher Block Chaining Message Authentication Code.
CCM mode	Counter with CBC-MAC, a mode of operation for cryptographic block ciphers. This mode of operation is an authenticated encryption algorithm.
Communications key	Adds another layer of encryption and authentication during transmission over a LAN from the token to the drive.
Crypto-active	Enterprise tape drive that has had the encryption feature turned on in the drive, and all data will be encrypted when written to media.
Crypto-ready	Enterprise drive that has the ability to turn on in-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 <i>key</i> can decipher (decrypt) the message into its original form.
Device key	Enables the tape drive for encryption.
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.
EKT	Enabling key token (write device key).
FIPS	<p>Federal Information Processions Standards</p> <p>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:</p> <ul style="list-style-type: none"> • Computer Security Division and Resource Center (CSRC) • Federal Information Processing Standards (FIPS) <p>For more information visit: http://www.nist.gov/</p>

Term	Description
Keys	<p>A random string of bits generated by the key management station, entered from the keyboard, or purchased. Types of keys include:</p> <ul style="list-style-type: none"> • Media keys encrypt and decrypt customer data on a tape cartridge. • Device keys enable the tape drive encryption feature. • PC or enable key enables the tape drive for encryption. • Wrap keys encrypt the media key on the LAN and the token. • Split keys are unique to each drive and work with the wrap key for protection. • Communication key adds another layer of encryption (authentication) to the media key during transmission over the LAN from the token to the drive.
KMS	<p>Key management station: The hardware, workstation, token bay. Key management system: The software application</p>
Media key	Encrypts and decrypts customer data on a tape cartridge.
NIST	National Institute of Standards and Technology.
Nonce	<p>A value that changes for every block written. The structure of the nonce guarantees that the nonce value will never repeat no matter how many blocks are written or repeat from one drive to another.</p> <p>So, even if you were to have a huge number of drives encrypting the same data over and over again, there would be no repetition in the cipher text.</p> <p>Each block uses a different nonce value and this value is recorded on tape as part of the encryption header.</p>
OKT	Operational key token (Write Media Key).
PC Key	Enables the tape drive to read and write in encrypted mode.
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.
Token	<p>Tokens are handheld, intelligent devices that connect to a token bay with an Ethernet connection. The two roles of the tokens are:</p> <ul style="list-style-type: none"> • Enabling key token • Operational key token
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.

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

SUN™ THE NETWORK IS THE COMPUTER

©2006 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, and the Sun logo; StorageTek and the StorageTek logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.



Part Number: TT0018E 11/11/2006