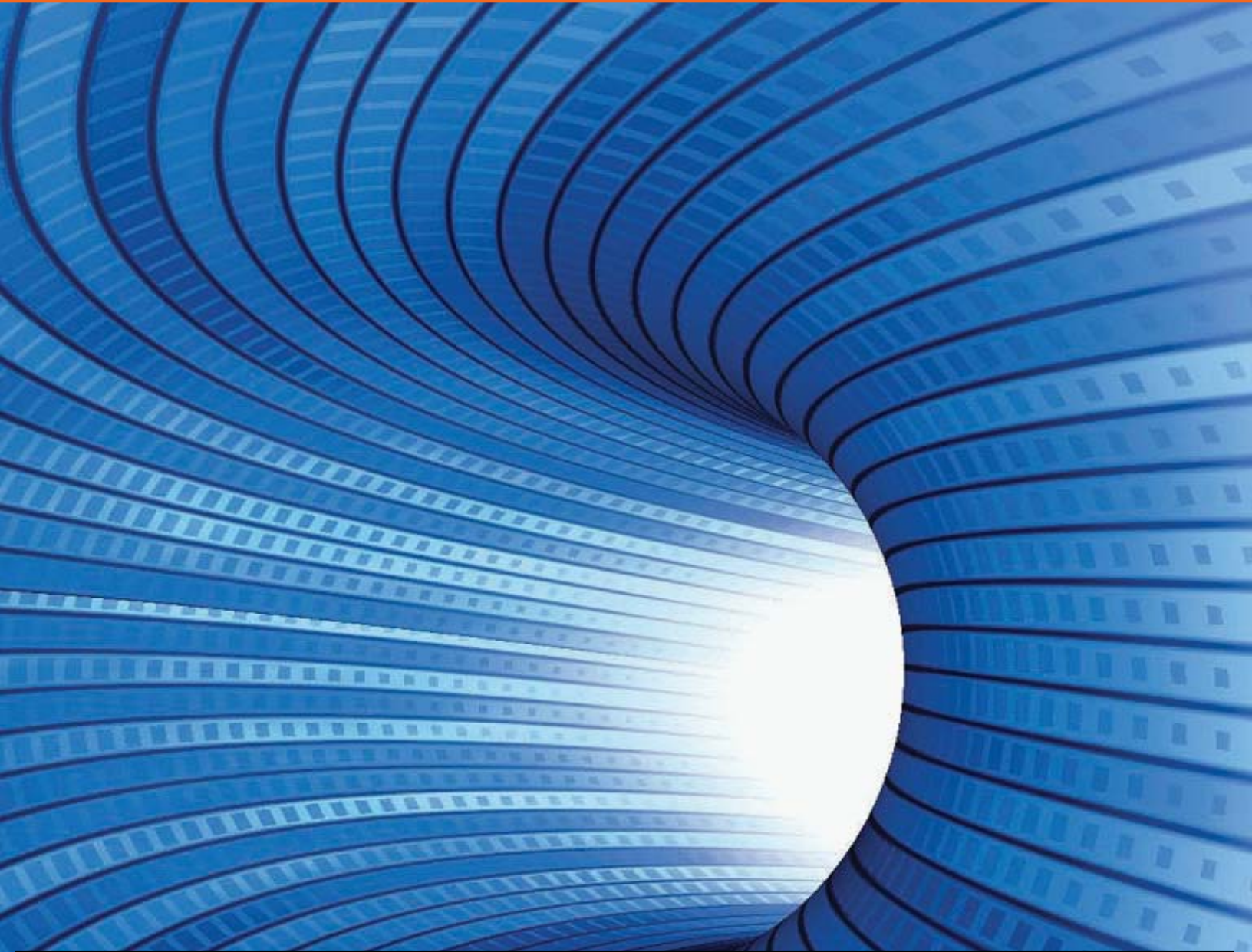


Key Management System



dice
PROGRAM



real testing | real data | real results

Table of Contents

1. Introduction	1
2. Background.....	1
2.1 Offered Capabilities.....	2
3. Key Evaluation Criteria	9
4. Evaluation Setup.....	9
5. Evaluation Results	9
5.1 Software Installation and Setup.....	9
5.2 Management	10
5.3 Functional Testing.....	18
6. Summary.....	24
Appendix A.....	25
Appendix B.....	26
Appendix C	30

High Performance Computing Modernization Program Air Force Research Lab DoD SuperComputing Resource Center

Key Management System
Sun Microsystems, Inc.

1. Introduction

Data centers are beginning to focus their security efforts on more than internet threats. Encrypting hard drives and tapes to avoid data getting into the wrong hands are becoming more and more vital to data center security.

Cryptography based encryption is one of the most effective ways to achieve data security. This method requires access to a key to decipher the file. Since some of the data is required to be kept for decades managing the keys is a challenging problem to solve.

2. Background

The Department of Defense (DoD) High Performance Computing Modernization Program (HPCMP) has formed a Storage Initiative (SI) team to investigate the program's current storage architectures across the centers in search for solutions to utilize aging mass storage systems and tape libraries such as Sun Microsystems servers and StorageTek tape libraries. This Storage Initiative Team has partnered with the DICE (Data Intensive Computing Environment) team to create a systematic methodology for storage security appliance evaluations.

Encrypted tape backup and key management solution could provide capabilities to DoD that would allow data collaborations with known outside entities and secure transport of sensitive data on tape technology from site to site. The data will be unreadable and un-decodable to any foreign entity that does not have authorization or keys available to release the information stored on tape.

Sun Microsystems has developed a solution to accomplish storage security for data-at-rest using encryption technology. This appliance based solution called the Sun Key Management System (KMS) with StorageTek T10000 (T10K) tape drive technology is a comprehensive key management platform designed to address the rapidly growing enterprise commitment to storage-based data encryption. Developed to comply with open security standards, KMS provides the capacity, scalability and interoperability to centrally manage encryption keys over widely distributed and heterogeneous storage infrastructures. This solution can also include the implementation of T9840D and LTO4 tape drives as well. All of these tape drive technologies can be installed in the latest generation Sun storage tape libraries which include the SL3000 and SL8500. The StorageTek SL500 is only supported with LTO4 tape drives. The StorageTek Powderhorn 9310 is supported with StorageTek 10000A and T9840D tape drives. The older generation L180, L700 and L1400 tape libraries are also supported by Sun KMS however the LTO4 drives with encryption enabled are not supported.

Sun Microsystems, Inc. provides network computing infrastructure solutions that include computer systems, software, storage and services. Its core brands include the Java technology platform, the Solaris operating system, MySQL, StorageTek and the UltraSPARC processor.

Since 1982, Sun has maintained that the network is the computer. Sun's vision is to see everyone and everything participating on the network. Sun's mission is to create technologies and fuel communities that enable sharing and participation. Sun's cause is to eliminate the digital divide. Eliminating the digital

divide allows everyone to take part in opportunities and contribute to solutions regardless of their geographic location or economic situation.¹

2.1 Offered Capabilities

Table 2.1 below describes the capabilities of the Sun Key Management System product. The data is generally available on Sun Microsystems website (www.sun.com) through documentation or questions directed toward Sun's personnel.

Table 2.1 Capabilities Summary

Sun KMS 2.1

General	
Name & version of Key Management System	Sun Key Management System 2.1
General architecture	Application running on a minimized and locked-down OS derivative of Solaris 10 operating system
Can function in a heterogeneous environment?	Yes, independent of any HPC system.
Connectivity, Security & Compliance	
File systems supported	Sun KMS is independent of any HPC file system used in conjunction with the storage backup solution implemented thus allowing heterogeneous environment.
Web browsers supported	None. KMS Manager is a fat client on Windows or Solaris platforms.
Tape libraries supported	Sun StorageTek L180, L700e, L1400, SL500, SL3000, SL8500 and PowderHorn 9310
Email support (syslogger, SNMP, email)	SNMP informs
Future support for IPv6	Supported in current release
Service and ports used	KMS Manager-to-Key Management Appliance (KMA) communication requires ports 3331, 3332, 3333, 3335 <ul style="list-style-type: none"> • Agent-to-KMA communication requires ports 3331, 3332, 3334, 3335 • KMA-to-KMA communication requires ports 3331, 3332, 3336.
All communications between services must be properly authenticated and protected from intrusion (i.e., replicate over WAN).	Communication between all elements in the KMS is authenticated using X509 Certificates and protected from attack by either RSA 2048 or AES 256 cryptography.
System functions requiring elevated privilege must be properly documented to allow understanding and limitation of the	At present, user authentication is based on ID and passphrase. Rules for passphrase strength are enforced by the KMS Application. Integration with

¹ <http://www.sun.com/aboutsun/company/index.jsp>

<p>risks.</p> <p>System configurations must meet the DoD ports and protocols guidance and management processes. Static passwords are not permitted by DoD.</p> <p>One of the following three methods must be met to provide/demonstrate proper security protections:</p> <ol style="list-style-type: none"> 1. HPCMP prefers Kerberos protected services to secure information transfer and communications along with SecureID or Common Access Card/Public Key Infrastructure (CAC/PKI) for single sign on authentication. <p>or</p> <ol style="list-style-type: none"> 2. Independent Certification: Meet the requirements set forth by NAIP CCEFS documentation. <p>or</p> <ol style="list-style-type: none"> 3. Systems that do not use Kerberized services and/or SecureID/PKI authentication must be documented and approved to operate in the HPCMP architecture (prior to installation) according to the HPCMP Access Guidelines. 	<p>Kerberos/LDAP is planned for the next KMS release planned for mid-2010.</p>
<p>The tool must apply to one of the security levels. Security Requirement for Cryptographic Modules (FIPS 140-2). There are several levels:</p> <ul style="list-style-type: none"> • FIPS 140-2 Level 1 (the lowest) imposes very limited requirements; loosely, all components must be "production-grade" and various egregious kinds of insecurity must be absent. • FIPS 140-2 Level 2 adds requirements for physical tamper-evidence and role-based authentication. • FIPS 140-2 Level 3 adds requirements for physical tamper-resistance (making it difficult for attackers to gain access to sensitive information contained in the module) and identity-based authentication, and for a physical or logical separation between the 	<p>The Sun T10000B drive has been validated to Security Level 2 of FIPS 140-2 (Certificate 1156.) It is the only tape drive to have achieved this level of validation. T10000A is validated to Security Level 1 (Certificate 1157.) The Sun 9840D has successfully completed testing by the Accredited Test Laboratory to Security Level 1 and, as of 10/23/09, is "In Review" by NIST. When operated in the FIPS-compliant mode, no keys are exposed in plain-text in the KMA outside the crypto-boundary of the SCA6000 Hardware Security Module which is FIPS 140-2 validated to Security Level 3 (Certificate 1050.) The IBM LTO4 drive is validated to Security Level 1 (Certificate 1152).</p>

<p>interfaces by which "critical security parameters" enter and leave the module, and its other interfaces.</p> <ul style="list-style-type: none"> FIPS 140-2 Level 4 makes the physical security requirements more stringent and requires robustness against environmental attacks. 	
IEEE 1619.1 compliance – Standard for Authenticated Encryption with Length Expansion for Storage Devices	Sun Enterprise Drives (T10000A/B and 9840D) conform to the CCM mode of IEEE 1619.1 and LTO4 drives conform to the GCM mode allowed under IEEE 1619.1
IEEE 1619.3 compliance – Standard for Key Management Infrastructure for Cryptographic Protection of Stored Data	The IEEE 1619.3 Standard is under development and the 1619.3 Security in Storage Working Group (SISWG) is chaired by a Sun Engineer. The Sun KMS will conform to the released version of 1619.3 when it is available. It is planned that the 1619.3 Standard will combine the critical features of KMIP with the additional features required for the Enterprise environment such as mutual authentication and automated discovery of components.
Oasis KMIP: The OASIS KMIP TC works to define a single, comprehensive protocol for communication between encryption systems and a broad range of new and legacy enterprise applications, including email, databases and storage devices. By removing redundant, incompatible key management processes, KMIP will provide better data security while at the same time reducing expenditures on multiple products. This has yet to be completed as of December 2009.	KMIP is under development by an OASIS Committee as a lower level protocol to cover a wide range of encrypting devices. Sun has no plans to conform to KMIP for an enterprise system given that the critical KMIP features will form part of IEEE 1619.3.
Performance	
Available benchmark data	No performance impact for encryption since the drive used an embedded cryptographic engine.
Throughput #'s for read/write transactions	No degradation to the transfer rates of the specific encryption enabled tape drives being used. Performance graphs demonstrate this at various compression ratios. See Appendix A for comparisons provided by Sun Microsystems, Inc.
Determine maximum file size - can handle file sizes of 25 TB	Yes, file size is independent of the encryption because the encryption is done on a block by block basis.
Scalability	
Optimizing scalability	All KMAs are linked in an active cluster giving maximum scalability and fault tolerance. Up to 20 KMAs may be linked together in a single cluster.
Reliability and Availability	

Single points of failure	The KMA cluster features automatic load-balancing and failover so no single KMA failure can result in system failure. Library software will mitigate failures in an individual drive or its power supply. The Ethernet connection between drives and the KMS can be mitigated using managed switches thus avoiding single points of failure.
Remote capabilities	Management of the KMS is normally done remotely using a secure and authenticated protocol from the KMS Manager platform only. The KMS Platform can be accessed remotely through Windows Remote Desktop, VNC, X Windows, etc.
Is there any mechanism for detecting data corruption?	Any corruption occurring in key transmission will be detected and reported since all communication is authenticated. Sun Enterprise drives take specific measures to protect against key corruption in the drive by unwrapping and authenticating keys in two independent operations and storing them in independent registers. One register is used to supply the key to the encryption engine while the other key feeds the independent decryptor that is used to authenticate the encrypted data stream. Data written and read by the tape drive is protected via read-while-write and a multi-level CRC and ECC architecture.
File data corruption must be reported, corrected and completely understood if it is the fault of the Key Management framework.	The tape drive has multiple layers of Error Detection and Correction and the un-detected error rate is < 1 undetected error in 10^{30} bits read. The unrecoverable error rate is <1 error in 10^{19} bits read. Unrecoverable data errors are reported in SCSI format over the Data Path. Encryption errors such as Authentication Failures are treated as Hardware Errors and reported as such over SCSI. The tape drive employs powerful Error Correction that makes all possible efforts to recover user data. All key transmissions are protected by one or more layers of encryption and authentication. Typically any failures are the result of hardware failures and recovery is not attempted.
Metadata corruption should be reported, corrected and completely understood if it is the fault of the Key Management framework.	The metadata written to tape as part of the encryption format is covered and protected by the CCM authentication process.
Does the system provide failover capabilities for each component?	Yes, for the servers, the solution has a minimum of 2 KMAs for the required failover capability. The Ethernet connection between the drives and the KMAs can be configured to provide redundant paths. The library Software will mitigate drive failures.
Capacity Planning and Performance Analysis	
What tools are available to determine future capacity needs?	No tool available, since storage capacity is not related to encryption. However, Sun Professional Services offers an Architecture Optimization Service where

	Storage, process, mgmt and performance of Customer's storage infrastructure is reviewed. The output is then reported and specific actionable steps are recommended for the Customer to take to implement and improve reliability, utilization and performance of their storage sub- systems, focused on disk, tape, and networking SAN infrastructure
What is the complexity of adding or removing storage devices?	Tape drives can be enabled for encryption by Sun either prior to or during installation. To add a storage device, the customer enters via the KMS Manager GUI an ID and a passphrase for the new device. The customer or a Sun Engineer submits the corresponding values to the new device using the Sun Virtual Operator Panel (for tape library) along with the IP address of any addressable KMA in the cluster. An automatic challenge/response process then downloads an X509 Certificate to the drive to authenticate all future communication.
Are there tools to see how backup is performing (transactions / minute, # of users / transaction, etc.)?	No, storage backup independent of the KMS.
Key Management Solution Management	
Is there a command line interface?	Only for the Embedded Lights Out Management (ELOM) of the KMA system boot prom.
Is there a GUI provided for administration?	Yes, Fat client for KMA. A GUI is available for the ELOM.
What types of reports are available for administrators?	Audit log can be exported as a report showing up to 33 classes of operations.
What documentation is provided for the installation and setup?	Installation requires a Sun Professional Services engagement. Transfer of information to the customer included as part of the engagement. Installation and Service manual can be found here: http://dlc.sun.com/pdf/316194901A/316194901A.pdf In addition, the Sun KMS supports a well-documented disaster recovery architecture that can complement the user policy for DR. A disaster recovery reference guide for KMS 2.0 can be found here: http://dlc.sun.com/pdf/316197101AA/316197101AA.pdf
What are the staffing requirements?	Up to five separate user roles needed for maximum security implementation plus possible backup users. A user can be assigned for more than one role. It is recommended that a minimum of 3 individuals fulfill the user roles needed with a minimal time required for operations. For more detail on user roles see Section 5.2 Management: Users and Role-based Access Control below.
Manage direct attached storage – delete, move, replicate or consolidate based on a specific action?	Tape drives can be added, replaced and deleted within the KMS.
Diagnostic and Debugging Tools	
Success or error results from all operations, including those on remote	All KMS actions are logged and report Success/Failure on the KMS Manager GUI. Encryption does not

systems, must be available to the administrator at the conclusion of the operation either through the functionality of the tool or some other work around (logged in log files, etc.)	change in any way reporting of data path issues which are covered by the Data Backup Application.
How is notifications sent (success or failure)?	All errors are reported either via the KMS GUI or via the Backup/Archive Application.
Is there any mechanism to detect failure due to access permissions prior to executing an operation?	All login attempts (successful or failing) are logged and reported on the KMS GUI.
Are troubleshooting or diagnostic tools available?	The KMS 2.1 allows the customer to open a support account which gives Sun Field engineering the ability to troubleshoot a KMA but does not provide access to any customer Crypto Sensitive Parameters.
What documentation is provided for the hardware and software troubleshooting?	KMS 2.0 Administration Guide found here: http://dlc.sun.com/pdf/316195101A/316195101A.pdf
Service and Support	
Support Services Available	Next Business Day, 8x5 M-F, 8x8 M-F, 7x24 4 hour and 7x24 2 hour response using Sun personnel
How many service employees are employed?	Sun provides large amount of customer service employees for 24x7x365 support/maintenance across the world.
How often is software and firmware updated and who performs the upgrades?	Sun plans a 6-month cycle for updates to Drive and to KMS Software. Typically these upgrades will be performed by Sun Field Engineering.
Do software and firmware updates require an outage?	KMS and Drive Updates can be performed one at a time without requiring bringing the entire system down although it may be more convenient to accept an outage to perform all updates simultaneously.
Training & Professional Services	
Training Services Available	Yes, 3 day classroom and live virtual training available. See: http://www.sun.com/training/catalog/courses/NWS-3507.xml http://www.sun.com/training/catalog/courses/VC-NWS-3507.xml
Cost	
What is the typical list price for your Key Management solution?	\$50,000 per site that includes the Professional Services implementation – plus \$5,000 per T10KA/B/9840D tape drive and/or \$1,000 per LTO4 tape drive for their crypto activation fee.
What are the ongoing costs over the life of your solution?	Approx. \$5,000 per year of ongoing support/maintenance cost
Vendor Information	
Number of deployed sites?	~600 KMA sold as of CQ4 2009, 250 – 300 sites. 200 customers.
Site Management	
Does the system provide troubleshooting tools to site level administrators (i.e., replicated site unavailable)?	In the KMA Manager, System Management, the KMA list operation shows true or false if nodes are available for the cluster.
Administrator Interface Tool	
Does the tool provide a method to	All tape drives supported by KMS have in-built

compress files and directories?	compression that can be enabled or disabled over using status commands over the data interface. Encryption does not affect this selection functionality and since encryption is performed after compression, encryption does not affect the drive performance in the compressed mode.
Does the tool provide a method to replicate files and directories?	The KMS replicates the database to all component KMAs as well as supporting a backup file to a customer-defined location.
Does the tool provide a method to encrypt files?	The KMS Database and backup are fully encrypted.
Quorum based authentication	The Sun KMS requires Quorum validation for all sensitive security operations. Customer defines number of Quorum members (maximum 10) and required threshold.
Hardware Interfaces	
Does the system manage direct attached system (DAS) (HPC native files)?	No, the system is independent of any DAS, RAID storage.
Communications Interfaces	
Does the system interface with HPC system remotely?	No, the system is independent of any HPC system.
Hardware/Software Requirements	
Does the system function in a heterogeneous hardware environment (i.e., hardware agnostic)? It should not be dependent on what it can interface with.	<p>The encryption system, KMS and drives function independently of the customer hardware environment (server, operating system, HBA etc.).</p> <p>At present, Sun KMS supports Sun Enterprise and Mid-Range (LTO) tape drives through an Open Sourced Interface protocol. Sun provides a protocol freely available to 3rd parties. Both IBM and HP have implemented this in their LTO tape drives. Sun encourages further support for this protocol from other suppliers but it is likely that additional "heterogeneous hardware devices" will base support for the Sun KMS on the pending IEEE 1619.3 Standard.</p> <p>At this time Sun StorageTek Tape Libraries are only supported.</p>
Portability of keys between heterogeneous hardware	This is not supported. Keys can be transported between authorized Sun KMS clusters only.
Ability to enable/disable encryption to a tape drive or complete library	In the Sun encryption architecture, encrypting devices can be configured to be switchable between encrypting and non-encrypting. This is done on a device-by-device basis. For high-security applications, the device can be configured such that, once set in the encrypting mode, it cannot be returned to a non-encrypting mode.
Database	
The database must provide clustering in order to improve of performance.	For robustness of implementation, KMAs can only be operated with a minimum of 2 KMAs in a clustered configuration. For performance optimization, automated load-sharing between KMAs in the cluster is provided.
The database must provide failover	The KMS cluster provides automated fail-over.

capabilities	
The database must be able to handle record locking	Keys with write access are only accessible by one tape drive at a time.
Operational Requirements	
Does data retain its normal structure in order to maintain interoperability with other systems?	Yes, data is streamed to and from tape in native format.
Determine the limitation in the number of files, where metadata is stored and hash table growth. Number of keys associated with file base, file system, etc.	The KMA stores its database on a 500GByte drive. Since the data structure for each key is minimal, there is no effective limit on the number of keys that can be stored. Each tape will have its own unique key. Keys will not span across more than 1 tape, but key groups can be defined along with key policy to span a customer defined set of tapes. The Sun KMS has been characterized to over 1,000,000 keys. The Sun KMS solution has been tested for > 3000 tape drives.
Audit Trail	
Does the system keep an audit trail of administrator transactions?	Yes, Audit log tracks all user activity.

3. Key Evaluation Criteria

The following evaluation criteria are assessed:

1. The ability for the software to interface with HPC hardware (HSM, HPC, Tape libraries, etc.)
2. The security and privacy of other users – permission management
3. The ability to secure data-at-rest for physical transport among approved sites
4. Whether it follows the cryptographic standards for data-at-rest
5. The ability to have complete failover and recovery capabilities
6. The ability to retain data integrity and provide audit capabilities

4. Evaluation Setup

The testing for the Sun KMS solution was conducted at the Sun facility in Broomfield, Colorado. This allowed the evaluation to be completed in a short time period and work with a setup that was already up and running. Normally as part of a DICE evaluation, testing the setup and installation would be performed as well as the functional requirement testing. However, this solution required Sun PS personnel to conduct professional engagement which includes the setup and installation. This Sun PS engagement that is very comprehensive and ensures that the solution will operate smoothly for the customer. Due to the short time frame available conducting a Sun PS engagement was not possible for this proof of concept. As a result, the setup and installation was previously completed at the Sun facility by the KMS development engineers. A complete list of Sun PS services are outlined in Appendix C.

5. Evaluation Results

5.1 Software Installation and Setup

System Setup

For this evaluation, the user data was stored on a Sun SAM-QFS managed file system on a storage area network. The Sun StorageTek T10000B tape drive with encryption enabled was used in a Sun StorageTek L700 library.

Figure 1-1 below depicts the use of SAM-FS as the disk storage backup application and Sun StorageTek Automated Cartridge System Library Software (ACSL) for robotic control of the StorageTek L700 tape library.

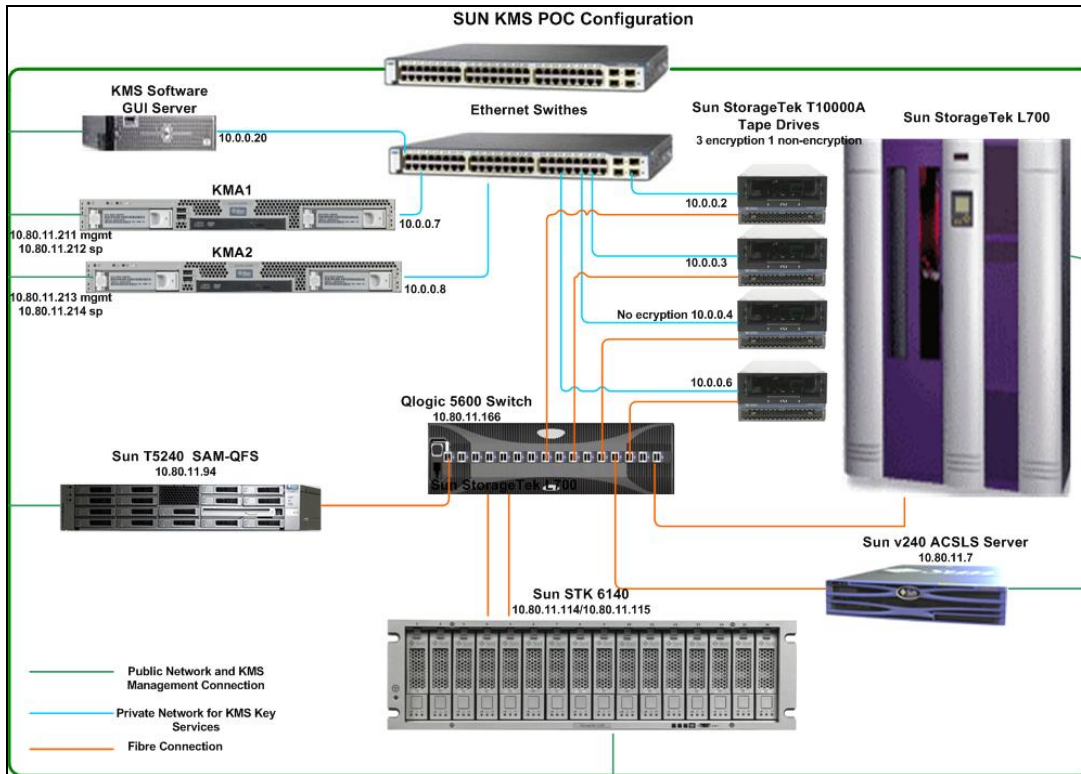


FIGURE 1 – 1 Configuration

Problems Encountered / Resolution

Security guidelines set forth by the AFRL required all network services to be up to date on known security issues. In order for a product to be used in a proof of concept or production, a security advisory scan is performed against the product. In order to conduct the security advisory scan, NMAP version 5.21 security software is used to do remote scanning of the Sun KMS servers. The Sun KMS server is an appliance-based server with a locked down operating environment based on Solaris 10. No third-party software is permitted to be loaded on the appliances. As a result, security scan software cannot be installed and executed. However, NMAP open source security software was used to scan the open ports on the KMS server installation from another platform. The NMAP was executed to scan the KMS server in two ways: the server that runs the KMS application and the embedded lights out management (ELOM) processor that controls the very basic system boot up and shutdown functions. The NMAP output in Appendix B shows that the server running the KMS software is secure and has only 1 TCP port open for SunSSH (this is by default closed at a customer site). On the ELOM interface The NMAP showed older versions of OpenSSH, OpenSSL and Apache running, but this interface should have restricted access on an internal management network.

5.2 Management²

² Information from Section 5.2 Management provided by the Sun KMS 2.0 Administration Guide

Overview

The Crypto Key Management System (KMS) creates, stores and manages encryption keys. It consists of the following components:

- Key Management Appliance (KMA) — A security-hardened box that delivers policy-based Lifecycle Key Management, authentication, access control and key provisioning services. As a trust authority for storage networks, the KMA ensures that all storage devices are registered and authenticated, and that all encryption key creation, provisioning and deletion are in accordance with prescribed policies.
- KMS Manager GUI — A Graphical User Interface that is executed on a workstation and communicates with the KMA over an IP network to configure and manage the KMS. The KMS Manager GUI must be installed on a customer-provided workstation running Solaris 10 x86 update 3, Solaris 10 x86 Update 4 or Microsoft® Windows XP.
- KMS Cluster — The full set of KMAs in the system. All of these KMAs are aware of each other and replicate information to each other.
- Agent — A device or software that performs encryption, using keys managed by the KMS Cluster. For KMS 2.1, these are the StorageTek encrypting tape drives. Agents communicate with KMAs via the Agent API. This is a set of software interfaces that are incorporated into the agent hardware or software.

KMS Concepts

KMS Clusters

KMS supports clustering multiple KMAs, which provides load balancing and failover. All KMAs in a KMS Cluster act in an active/active manner. All KMAs can provide all capabilities to any agent. Actions performed on one KMA are quickly replicated to all other KMAs in the cluster.

Agents

Agents perform cryptographic operations, specifically, encrypting data as it is written and decrypting data as it is read. Agents contact the KMS cluster in order to create and retrieve keys used to perform the cryptography.

Network Connections

The KMS uses TCP/IP networking for the connections between KMAs, Agents and machines where the KMS Manager GUI is running. In order to provide flexible network connections, two interfaces are provided for network connections on the KMA:

- The management connection, intended for connection to the customer network
- The service connection, intended for connection to the tape drives

With production KMA installation, library-specific accessory kits are available that include switches and cables for connecting to the drives and the KMA. This is shown in FIGURE 1-2 below.

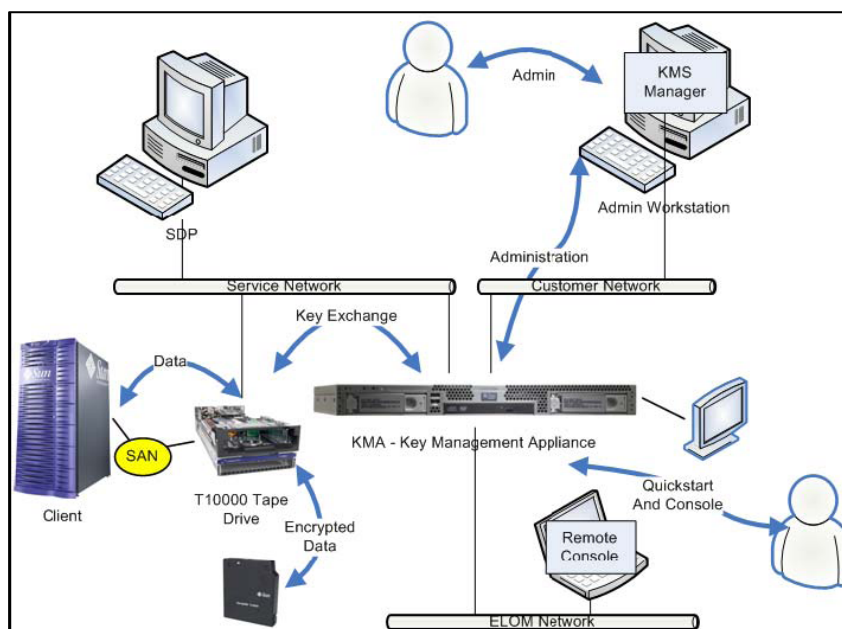


FIGURE 1 - 2 Connections to the KMA

Key Lifecycle

Keys undergo a lifecycle based on the key policy. The lifecycle periods and transitions are imposed by the KMS are based on the NIST SP800-57 guidelines and described briefly below. A few additional states are added to deal with nuances of the KMS.

The key lifecycle is based on two time periods (see FIGURE 1-3) defined in the key policies:

- Encryption period
- Cryptoperiod

The encryption period is the period of time after a key is assigned that it can be used to encrypt data. The cryptoperiod is the time period it can be used for decryption. It is assumed the two periods start at the same time when the key is assigned. Currently, the maximum cryptoperiod length is approximately 68 years.

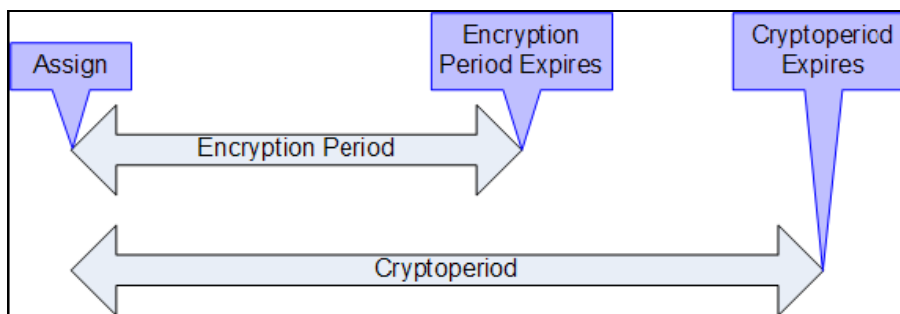


FIGURE 1 - 3 Key Lifecycle Periods

State Transition

These encryption period and cryptoperiod time periods, combined with other functions of the KMS, define a state transition for keys as shown in FIGURE 1 - 4. In this diagram, states and transitions shown in blue are defined by NIST SP800-57. The states and transitions are shown in red are added by the KMS. When examining keys in the KMS Manager, only the innermost state is listed. KMS states are listed below.

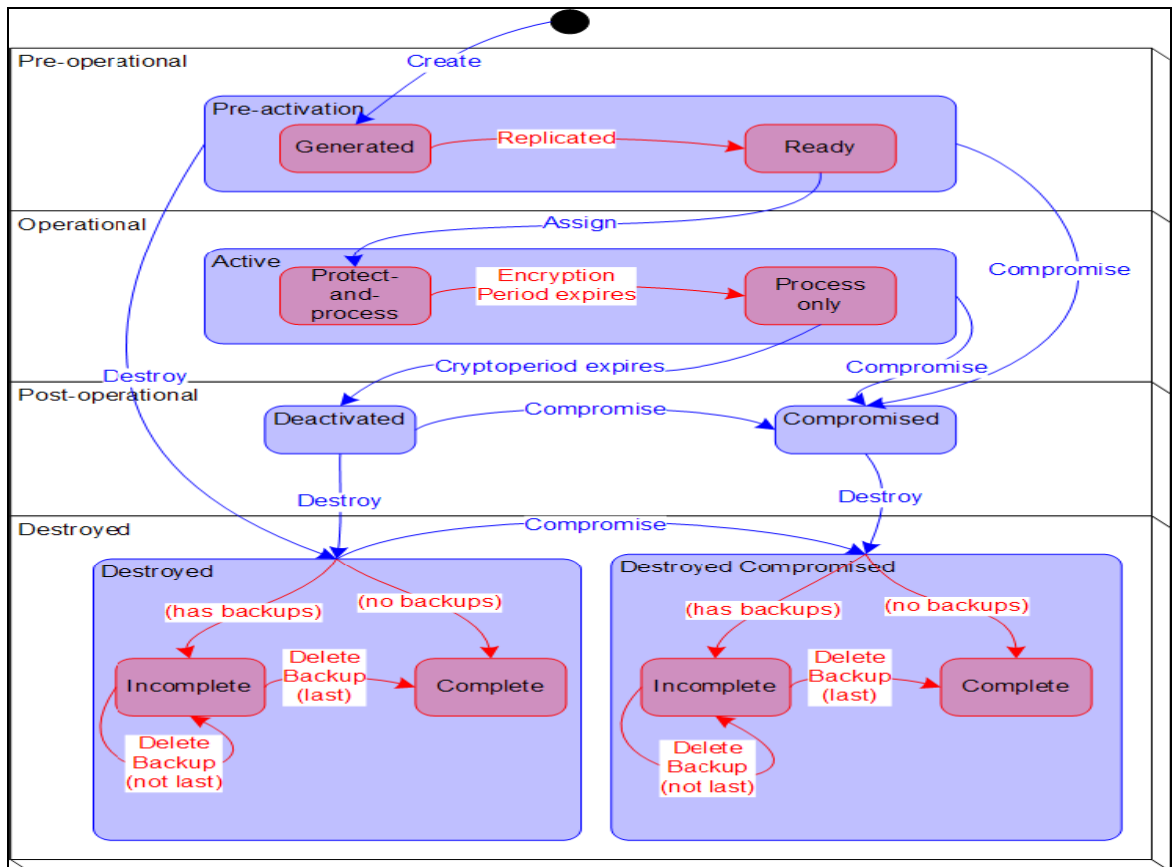


FIGURE 1- 4 State Transition Diagram

Pre-activation

The key has generated but is not yet available for use. Within the pre-activated state, the KMS adds two more detailed states, generated and ready.

Generated

A generated key is a key that has been created on one KMA in a KMA cluster. It remains generated until it has been replicated to at least one other KMA in a multi-KMA Cluster. In a Cluster with only a single KMA, a key must be recorded in at least one backup to transition out of the generated state.

Ready

A ready key is one that has been protected against loss by replication or a backup. A ready key is available for assignment. The “replicated” transition occurs when the key is replicated or (for a single KMA Cluster) backed up.

Active

The key may be used to protect information (i.e., encrypt) or to process previously protected information (i.e., decrypt.) NIST states that an active key may be designated for protect only, process only, or protect and process. Further, it specifically states that for symmetric data encryption keys, a key may be used for some time period to protect and process information and once this time period expires, the key may continue to be used for processing only.

Within the active state, the KMS adds two substates. These states are described in NIST, but are not specifically identified as states.

Protect-and-process

A key in this state can be used for both encryption and decryption. A key is placed into this state when it is assigned. The assignment is done when an encryption agent requests a new key to be created.

Process only

A key in this state can be used for decryption but not encryption. When an agent determines that none of the keys available to it (e.g., for a specific data unit that is being read or written) are in the protect-and-process state, it should create a new key. Keys transition from protect-and-process to process only when the encryption period for the key expires

Deactivated

The key has passed its cryptoperiod but may still be needed to process (decrypt) information. NIST specifically states that keys in this state may be used to process data.

Strictly speaking, the NIST guidelines state that if post-operational keys, including deactivated and compromised keys, need to remain accessible, they should be archived. This is a key recovery process that allows keys to be recalled from an archive and made available for use.

The KMS provides archives in the form of KMA backups but cannot recall a single key from a backup. Therefore, the KMS retains post-operational phase keys in the KMS. Cluster and delivers them upon request from an agent.

Compromised

Keys are compromised when they are released to or discovered by an unauthorized entity. Compromised keys should not be used to protect information but may be used to process information.

Destroyed

Destroyed keys no longer existent, however, information about the key may be retained. In KMS 2.1, key material from destroyed keys is removed from the KMS Cluster. Destroyed keys will not be delivered to an agent.

Note – The only way to destroy a key is through the GUI or the management API.

The NIST guidelines do not appear to provide any basis for destroying keys based on time.

Within the Destroyed and Destroyed Compromised states, the KMS defines two substates. These states are created because the KMS does not control the backups that it creates. A customer administrator must inform the KMS when a backup has been destroyed. Only after all backups have been destroyed can a key be considered truly destroyed. These substates are incomplete and complete.

Incomplete

At least one backup still exists that contains the destroyed key. In this substate, the key does not exist in any KMA in the KMS Cluster. Keys in this state cannot be delivered to agents.

Complete

All backups containing the key have been destroyed. The key does not exist in any KMA, nor in any backup. Strictly speaking, backups that contain the key may well still exist. All the KMS knows is that it has been told the backups have been destroyed. It is the responsibility of the user to ensure these backups have actually been destroyed.

It is worth noting again that the “destroyed” transition occurs only as the result of an administrative command. Further, keys may still be delivered to an encryption agent when the key is in the post-operational phase (Deactivated and Compromised states.) This interpretation is consistent with NIST’s descriptions for the post-operational phase. The NIST guidelines specify that a post-operational key should be destroyed when it is “no longer needed.” We believe that only a user can determine when a key is “no longer needed,” so only an external entity can initiate the destroyed transition.

Destroyed Compromised

This is the same as destroyed, but the key was compromised before or after destruction.

Users can be assigned one or more roles based on the NIST SP800-60 role based access standard.

Each user will only see functions available for the privileges assigned that role in the Fat client software GUI.

Users and Role-Based Access Control

The KMS provides the ability to define multiple users, each with a user ID and passphrase. Each user is given one or more pre-defined roles. These roles are as follows:

- Security Officer — performs KMS setup and management
- Operator — performs agent setup and day-to-day operations
- Compliance officer — defines key groups and controls agent access to key groups
- Backup operator — performs backup operations
- Auditor — can view system audit trails

In the GUI and the console, only the allowed operations are shown. It is possible for an operation to be displayed, and then to fail when attempted. This can occur if roles are removed from a user between the time the display is shown and when the operation is attempted. All roles except auditor are required to create a functioning encryption system. Distinct users may be created, each with one role. Or, multiple roles may be given to a user.

Quorum Protection

The KMS also provides quorum protection for certain operations. A quorum of up to 10 users can be defined. A threshold from one to the number of quorum users is also defined. This information is called the Key Split Credentials. The user IDs and passphrases are distinct from the user IDs and passphrases used to log into the system. When attempting an operation that requires quorum approval, a screen will be displayed that allows each quorum user to input their user ID and passphrase. At least the specified threshold of user ID and passphrases must be supplied for the operation to be allowed. All quorums need to be present in order to complete the operation in KMS 2.1. For the next release a distributed quorum is implemented making it easier for multiple quorum members to make approvals at different times.

Data Units, Keys, Key Groups, and Key Policies

Data units are used to represent data that is encrypted by agents. For tape drives, a data unit is a tape cartridge, and data units are always present. This is not a fundamental requirement, and future agents may operate without defining data units.

Keys are the actual key values (key material) and their associated metadata.

Key policies define parameters that govern keys. This includes lifecycle parameters (encryption period and cryptoperiod) and export/import parameters (import allowed, export allowed.)

Key groups associate keys and key policies. Key groups have a specific key policy and are assigned to agents. Each agent has a list of allowed key groups. Agents are allowed to retrieve only the keys that are assigned to one of the agent's allowed key groups. Agents also have a default key group. When an agent creates a key (more specifically, assigns it to a data unit), the key is placed into the agent's default key group. There is functionality in place to allow more sophisticated control of key groups by agents. However, existing agents cannot leverage this functionality.

In order for the system to function, at least one key policy and one key group must be defined. That key group must be assigned as the default key group for all agents.

Client

The client (end-user) will see no changes in their daily operations. Due to the Sun KMS independent nature, the solution will drop into any disk-based storage and backup infrastructure.

Administration

Configurable Security Parameters

Management Session Inactivity Timeout

Displays the maximum length of time (in minutes) a KMS Manager or Console login session can be left idle before being automatically logged out. Changing this value has no effect on sessions that are already in progress. The default is 15 minutes. The minimum value is 0, meaning no time is used; the maximum value is 60 minutes.

Login Attempt Limit

Indicates the number of failed login attempts before an entity is disabled. The default is 5. The minimum value is 1; maximum value is 1000.

Passphrase Minimum Length

The default is 8 characters. The minimum value is 8 characters; the maximum value is 64 characters.

Audit Logs

The Sun KMS server logs every event occurrence in the audit log and is accessible through a query tool that will also allow creation of an external report. Medium Term Retention Audit Log displays the amount of time (in days) that Short Term Audit Log entries are retained before they are truncated. The default is 90 days. The minimum value is 7 days; maximum value is 24,855 days. There is also a Long Term Retention Audit Log is configurable from 1000 to 1,000,000 entries. The retention lifetime can be configured from 7 to 24,855 days with a default of 730 days.

Other features

Enabling the Technical Support Account

The Technical Support menu option allows an operator to enable/disable the Operating System's support account and SSH access for that account. By default, both the Technical Support account and SSH access are disabled. Since the passphrase for the support account is only known by Sun Support, enabling of this account does not grant the Console user any further access to the KMA.

Problem Resolution

The System Dump menu in the KMS Manager creates a system dump for problem resolution and downloads it to a compressed file on the system where the KMS Manager is running. The downloaded file is in a format that can be opened with compression utilities. The dump does not include any key material or information from which keys can be inferred.

KMA Backup

A backup of a KMA can be saved to the KMS Manager platform by the Backup Operator. The backup can then be saved to external media. A restore operation can only be initiated a quorum.

Server Operation

The Embedded Lights Out Manager (ELOM) system contains a separate processor from the main server. As soon as power is applied (plugged-in), and after a one or two minute boot period, ELOM provides a remote connection to the console allowing you to perform server functions.

Compatible web browser and Java version with ELOM:

- JRE 1.5 (Java 5.0 Update 7 or later)
- Internet Explorer 6.0 and later for Microsoft Windows XP Pro I
- Mozilla Firefox 1.0 for Red Hat Linux 3.0 and 4.0 or Microsoft Windows XP Pro
- Mozilla 1.7.5 or later for Solaris, Red Hat or Microsoft Windows XP Pro

The KMS Manager

To run the KMS Manager, you need a workstation that is running Microsoft® Windows XP, Solaris 10 x86 update 3 or Solaris 10 x86 update 4. The KMS Manager includes comprehensive online help.

The KMS Console

The KMS Console is a terminal text-based interface that allows a user to configure basic function of the KMA. It is accessed by physically connecting a video monitor and keyboard to the KMA or by the “remote console” function in the ELOM web browser interface.

The KMS Console automatically launched by the operating system when the KMA boots up and cannot be terminated by a user. Depending on the roles that a user is assigned, the options in the KMS Console differ.

Before a user can log in to the KMS Console, the user accounts must be created in the KMS Manager. The user must use the same username/passphrase that was used for authentication in the KMS to log in to the KMS Console.

Note – Only the first Security Officer account is created when the QuickStart (for initial configuration) program is launched.

Key Sharing Among Approved Sites

Key Transfer, also called Key Sharing, allows keys and associated data units to be securely exchanged between Partners and is required to exchange encrypted media. This process requires each party in the transfer establish a public/private key pair and then provide the public key to the other party.

Each party enters the other party’s public key into their own KMS cluster. Once this initial configuration is complete, the sending party uses Export Keys to generate a transfer file, which is sent from the sending party to the receiving party. The receiving party then uses Import Keys to import the keys and their associated data units into their KMS Cluster.

The transfer file is signed using the sending party's private key and encrypted using the receiving party's public key. This allows only the receiving party to decrypt the transfer file using their own private key. The receiving party can verify the file was in fact produced by the expected sender by using the sender's public key.

Key Transfer Partners Feature

The Key Transfer Partners feature allows keys to be moved from one KMS Cluster to another. Typically, this feature can be used to exchange tapes between companies or within a company if multiple clusters are configured to deal with large numbers of sites.

The Key Transfer process involves these steps:

- Each KMS Cluster configures the other Cluster as a Transfer Partner. This is usually done once.
- The user exports keys from one KMS Cluster and imports them into the other. This step can be done many times.

Core Security

The primary element of the Core Security component is the Root Key Material. It is key material that is generated when a Cluster is initialized. The Root Key Material protects the Master Key. The Master Key is a symmetric key that protects the Data Unit Keys stored on the KMA.

Core Security is protected with a key split scheme that requires a quorum of users defined in the Key Split Credentials to provide their usernames and passphrases to unwrap the Root Key Material.

This security mechanism enables two operational states for the KMA: locked and unlocked.

A KMA in the locked state is not able to unwrap the Root Key Material, and thus is unable to access the Data Unit Keys. As a result, the KMA is unable to service Agent requests to register new Data Units or retrieve Data Unit Keys for existing Data Units.

A KMA in the unlocked state is able to use the Root Key Material to access the Data Unit Keys and service Agent requests for Data Unit Keys.

System Time

It is important that all KMAs in a cluster have the same time. A Network Time Protocol server can be configured for accurate time for the KMA cluster.

Note: The information in Section 5.2 Management was provided by the Sun StorageTek Crypto Key Management System Administration Guide.

5.3 Functional Testing

Table 5.3 below describes the test requirement, evaluation results and evaluation ranking for the critical and high requirements defined by the Storage Initiative team.

The following criteria are used for the evaluation ranking:

Met	The solution offered the minimum or required functionality.
Surpass	The solution offered more than expected functionality.
Missed	The solution offered less than minimum functionality.
N/A	Requirement does not apply to solution being evaluated or functional testing could not be performed due to a configuration limitation.

Requirement	Evaluation Results	Evaluation Ranking
Functionality		
Site Management		
The system should provide the ability to report status back to each of the sites regarding storage usage for the system administrators to manage.	The encryption infrastructure operates independently of the data structure. It can report on any aspect of security via a detailed log of key and user transactions but has no knowledge of how these keys are used on customer data processed by the Backup Application	N/A

Interface Tool		
The tool must be able to perform configuration modifications (add systems, files, directories).	The KMS is designed as a highly automated system for use in a lights-out data center. Once set up (using documented procedures provided by Sun) all configuration changes to the system can be performed using the KMS Manager, a fat-client GUI. The KMS Manager does a multitude of modify operations, but the modify operations are only available to user roles with that permission. Some of the entities that can be modified include user, key policy key group, transfer partner and agent.	Met
The tool must be able to modify the status of keys regarding files and devices.	In the Sun KMS, each tape is automatically assigned a unique key that is managed through a life-cycle based on NIST SP-800 57 using customer-defined policies. The GUI may be used to compromise keys and, once keys become "post-operational" either through a manual compromise decision or an automated policy driven "crypto-period expiration, keys can be manually destroyed.	Met
The tool must be able to operate on single file/directory, lists of files/directories or directory tree.	One feature of the Sun Tape Encryption implementation is that key assignment is performed independently from any other component of the customer environment such as Backup Application or backup server. This means that the Key Manager has no knowledge of file structure on tape and does not operate at per-file basis. The Backup Application and Library Management Software will direct customer data to an appropriate cartridge and the Key Manager will provide the required key or keys to that cartridge. For this scenario we used Sun SAM/QFS as the storage management and backup and selected a file or set of files to be saved to tape. Sun SAM/QFS manages the knowledge of where and what is saved to tape. The KMS only manages the keys for each tape. So existing or other storage management tools will provide this functionality.	N/A
Role Based Access Control, Support NIST SP800-60 operational roles (ie general user, administrator, security officer)	Sun KMS supports RBAC as required by NIST SP800-60. Available roles are Security Officer, Compliance Officer, Operator, Backup Operator and Auditor. A user can be assigned	Met

	multiple roles,	
Diagnostic tools specific to the key management system should be available to the administrator - determine such things as cache full.	Sun KMS supports such diagnostic tools as are compatible with a locked-down, secure architecture. SNMP Informs are supported (to a customer furnished SNMP Manager) and Support Account access is allowed. Access to the support account is enabled by the customer (if allowed) and provides information on the processes being run by the KMA without exposing any cryptographic-sensitive functions or parameters.	Met
Hardware / Software Interfaces		
The system must be able to have Tape Encryption and Key Management actions available from the HPC file systems.	Tape Encryption and Key Management functions are handled independently from data handling. Once tape drives have encryption enabled, data streamed by desired transport from HPC file system is encrypted. Files restored from encrypted tape to HPC file system are decrypted.	Met
The system should be able to manage direct attached storage (HPC native files).	Encryption and key management are independent of any customer file system.	N/A
The system must interface with a remote or network file system link to HPC systems (like NFS), an HSM archival storage manager or a direct attached file system with a client.	Tape Encryption and Key Management functions are handled independently from data handling. Sun SAM/QFS was used in this scenario as the HSM archive manager.	N/A
Communications Interfaces		
The system must interface with HPC system remotely (disaster recovery)	This capability is available for the Sun KMS solution. However, due to limitations on the test scenario configuration for this could not be tested.	N/A
The communication software must be configured to run on IPv4.	The KMA and Sun drives support IPv4. The evaluation was conducted on an IPv4 configuration.	Met
Hardware / Software Requirements		
The system must support Linux and Unix operating system(s) – POSIX compliant.	The Sun Key Management architecture compatible with and independent of any customer Operating System. The KMA is an appliance implemented on a minimized and locked-down derivative of Solaris 10. Solaris is fully POSIX compliant. The KMS manager can also run on Solaris x86 and Microsoft Window XP.	Met
The software must be commercially available at the time	The Sun KMS hardware and software are robust and field-proven. First	Met

of the installation.	shipments were made in March 2008 and over 500 systems are in the field at customers including Governmental Agencies and Fortune 50 Financial customers.	
Must provide Remote/Centralized Control	The Sun KMS is designed to operate in a lights-out Data Center with centralized control from a KMS Manager GUI that can be run securely from any remote location with network access to the KMA cluster.	Met
Must provide Key Sharing with multiple libraries	A KMS cluster can encompass multiple libraries. Due to hardware limitations we could not test this requirement. Sun has many customers who use this functionality including one large customer whose KMS controls 9 remote data centers with multiple enterprise libraries.	N/A
Interoperability with Current Backup solution (SAMFS)	The Sun KMS operates with backup applications and was tested with Sun SAM-QFS.	Met
Key Replication	A Sun KMA will not issue a key to an encrypting device unless it has been replicated to at least one other KMA. Replication occurs automatically and transparently to the user. The audit log will show a successful key generation. Each KMA in the cluster holds an identical replicated version of the entire database.	Met
Several levels of encryption key granularity (i.e. single tape, pool of tapes)	The Sun KMS provides granularity such that each tape has a unique key or set of keys. The same key is not used on more than one tape.	Met
The Key Management system must provide recovery capabilities	In the event of global failure, the KMS can be reconstructed (after Quorum validation) from a secure and authenticated backup of the key data base. For less catastrophic failures, a new, or replacement, KMA can be added to the cluster and will automatically configure itself to replicate the policies and database assigned to the cluster.	Met
Operational		
Data should retain its normal structure after encryption in order to maintain interoperability with other systems.	In both Sun Enterprise and mid-range tape drives, user data is encrypted on a block-by-block basis so the original data structure is preserved.	Met
The data portion of all unencrypted files must be identical to the original file. De-encryption validation.	Tape drive encryption both authenticates the decrypted file and also preserves the ECC/CRC protection afforded by the native tape format. Data written to tape from SAM-	Met

	QFS was successfully restored to SAM-QFS.	
Encryption method should have minimal impact on storage. How does it handle compressed files?	Tape drive encryption adds a minimal amount of metadata to the file as recorded on tape – typically 100 bytes – and, since block length recorded on tape is typically 256KB, this has imperceptible effect on storage capacity. Files are compressed prior to encryption so compression will not be degraded by the encryption process.	Met
Security and Privacy		
The Key Management administrator (if not system administrator) must be able to perform functions without having system level root privileges.	The Sun Key Manager is architected as a locked down application. Root access is not available to any user. All administration access is based on one of the five available roles that user has been assigned.	Met
The system must be able to detect data corruption and react either automatically or reporting to the site system administrator.	All key communications use authentication and will report errors should any corruption occur. All cryptography used in KMS and in Sun Enterprise drives are subject to Known Answer Tests (KAT) at Power-on. Data written to tape is subject to all standard ECC and CRC protection. In addition, all encrypted data is authenticated in a loop-back decryption and authentication process as it being written to tape. All errors are reported either via the KMS GUI or via the Backup Application.	Met
The system must be able to detect intrusion (unauthorized access) to their devices and/or file system and react either automatically (log entry) or reporting to the site system administrator.	All login attempts (successful and failing) are logged and reported in the KMS Audit log. Passive Tamper-evident labels are used on the KMA and on the T10000B drive.	Met
The system must be able to pass security scripts along with meet compliance testing prior to deployment and/or redeployment.	Appendix B shows NMAP scan output of a KMS Appliance. The KMS Appliance by default has no TCP ports open and the SSH port 22 is only open upon enablement for debugging purposes by Sun engineers.	Met
The system must provide the ability that all operations are subject to access permissions, authorizations of target objects, and user privileges on accounts	All users on the System can only access functions appropriate to their roles. Roles are assigned by a Security Officer and must be validated by the Quorum. The system	Met

for all systems involved in any operation.	authenticates each user at sign-on based on their ID and passphrase.	
Assurance that the software is properly using and protecting those privileged actions and credentials is required.	Fat client only shows actions available based on role user has been assigned. If access to actions for that user change during user session then those actions are denied by the KMS. (i.e., Security officer denies user operator privileged while user is still logged in. KMAs are notified and those operator privileges no longer take any action due to change in permissions.)	Surpass
Audit Trail		
The system must keep log files on the key management appliance/server	The audit log tracks all operations attempted on any KMA in the cluster.	Met
The system must keep an audit trail of administrator transactions.	The log includes all user transactions with detailed user ID.	Met
Reliability		
File data corruption must be reported, corrected and completely understood if it is the fault of the Tape Encryption and Key Management framework.	The tape drive has multiple layers of Error Detection and Correction and the un-detected error rate is < 1 undetected error in 10 ³⁰ bits read. The unrecoverable error rate is <1 error in 10 ¹⁹ bits read. Unrecoverable data errors are reported in SCSI format over the Data Path. Encryption errors such as Authentication Failures are treated as Hardware Errors and reported as such over SCSI.	Met
Key corruption must be reported, corrected and completely understood if it is the fault of the Tape Encryption and Key Management framework.	Any corruption occurring in key transmission will be detected and reported since all communication is authenticated. Sun Enterprise drives take specific measures to protect against key corruption in the drive by unwrapping and authenticating keys in two independent operations and storing them in independent registers. One register is used to supply the key to the encryption engine while the other key feeds the independent decryptor that is used to authenticate the encrypted data stream.	Met
Recoverability		
The system must provide a method to recover a file, directory or key that has been identified as	The tape drive employs powerful error correction that that makes all possible efforts to recover user data. All key	Met

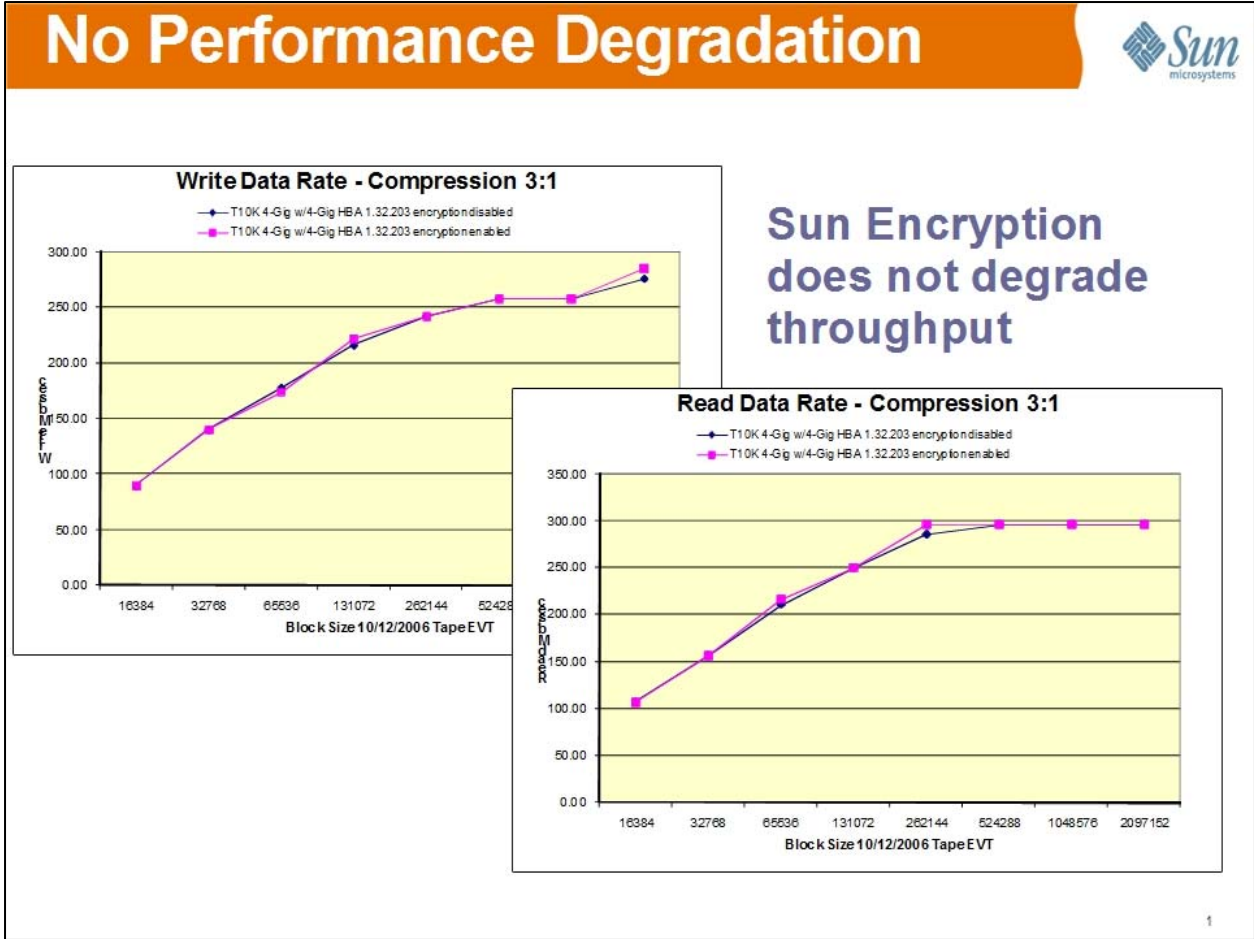
corrupt.	transmissions are protected by one or more layers of encryption and authentication. Typically any failures are the result of hardware failures and recovery is not attempted.	
General Performance		
The system must be able to handle multiple simultaneous transactions without effecting performance (single stream vs. multiple streams).	Sun encryption architecture does not affect the performance of data streams in the data path. Encryption keys are generated well before tape drives will need to acquire them.	Met
The system must be able to handle file sizes of 2 TB.	Encryption is performed on a block-by-block independent basis. The Backup Application will parse user data into the block sizes supported by the drive format (typically 2MBytes maximum) AES-256 encryption in either CCM mode (Sun Enterprise drives) or GCM mode (LTO4) are valid for data block lengths of up to 2^{64} (1.84×10^{19}) bytes.	Met
Error Handling		
Success or error results from all operations, including those on remote systems, must be available to the administrator at the conclusion of the operation either through the functionality of the tool or some other work around (logged in log files, etc.).	The KMS Audit log displays success or failure (with mode of failure) for all transactions.	Met

6. Summary

The Sun Key Management System 2.1 has proven to help protect sensitive information for data-at-rest. Administration of the software came with ease as the GUI provides a user-friendly interface. Implementation into an existing storage backup solution such as SAMFS did not require any changes to the storage backup procedures. This evaluation concluded that the majority of the functionality met the requirements defined by the Storage Initiative team. The DICE team identified four key requirements which were not applicable (N/A) to the solution because the Sun KMS solution is decoupled from any storage management functionality. Decoupling the storage management from the encryption key management provides the ability for Sun KMS to be implemented into existing storage infrastructures. Additionally, two key requirements could not be tested because the system configuration used for this evaluation did not include multiple libraries or a remote site to interface with.

The Sun KMS system has made advancements to the challenging efforts of managing encryption keys. The security of the encryption keys that this solution provides is a closed system solution and no encryption key is ever visible by any user interface, debugging interface, or external interface of the Sun KMS solution. In addition, Sun KMS offers 5 user roles (Security Officer, Operator, Compliance officer, Backup Operator and Auditor) where these roles can be assigned to either multiple or one individual. This achieves security requirements for operation but also gives flexibility for those situations when personal availability may become an issue during specific times of the year, by assigning available personal multiple roles during that time.

Appendix A
Performance Comparison provided by Sun Microsystems, Inc.



Appendix B

Comprehensive scan summary for ELOM interface on KMS server

nmap was initiated at December 14, 2009 - 07:33 with these arguments:

```
nmap -sS -sU -T4 -A -v -PE -PP -PS21,22,23,25,80,113,31339 -PA80,113,443,10042 -PO --script all 10.80.180.134
```

The process stopped at . Debugging was disabled, the verbosity level was 1.

10.80.180.134 / ELOM(online)

ping results

-

address

- 10.80.180.134 (ipv4)
- 00:16:36:DA:8D:80 (mac)

hostnames

- blairathol2.Central.Sun.COM (PTR)

ports

The 1988 ports scanned but not shown below are in state: closed

Port	State	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	OpenSSH	4.3 protocol 1.99
80	tcp	open	http	syn-ack	Apache httpd	1.3.33 (Unix) PHP/4.1.2 mod_ssl/2.8.24 OpenSSL/0.9.7g
443	tcp	open	http	syn-ack	Apache httpd	1.3.33 (Unix) PHP/4.1.2 mod_ssl/2.8.24 OpenSSL/0.9.7g
9000	tcp	open	cslistener	syn-ack		
13	udp	open filtered	daytime	no- response		
161	udp	open	snmp	udp- response	SNMPv1 server	public
623	udp	open filtered	asf-rmcp	no- response		
21524	udp	open filtered	unknown	no- response		
22053	udp	open filtered	unknown	no- response		
40441	udp	open filtered	unknown	no- response		
44968	udp	open filtered	unknown	no- response		
53838	udp	open filtered	unknown	no- response		

remote operating system guess

- used port 22/tcp (open)
- used port 1/tcp (closed)
- used port 2/udp (closed)
- os match: **Linux 2.6.9 - 2.6.28**
- accuracy: 100%
- reference fingerprint line number: 22026

system uptime

- uptime: 4725825 sec
- last reboot: (null)

tcpsequence

- index: 197
- difficulty: Good luck!
- values: FE2DFB84,FE098771,FE85A6CC,FDFFA98B,FE3F02A6,FDFCBAE6

ipidsequence

- class: All zeros
- values: 0,0,0,0,0,0

tcptssequence

- class: 100HZ
- values: 1C2B05D2,1C2B05DD,1C2B05E8,1C2B05F3,1C2B05FE,1C2B0608

runstats

- 1053 sec. scanned
- 1 host(s) scanned
- 1 host(s) online
- 0 host(s) offline
- nmap version: 5.00
- xml output version: 1.03
- nmap.xsl version: 0.9b

Comprehensive scan summary for KMS server

nmap was initiated at December 14, 2009 - 05:34 with these arguments:

nmap -sS -sU -T4 -A -v -PE -PP -PS21,22,23,25,80,113,31339 -PA80,113,443,10042 -PO --script all 10.80.180.133

The process stopped at . Debugging was disabled, the verbosity level was 1.

10.80.180.133 / KMS(online)

ping results

-

address

- 10.80.180.133 (ipv4)
- 00:16:36:D5:FD:52 (mac)

hostnames

- blairathol.Central.Sun.COM (PTR)

ports

The 1996 ports scanned but not shown below are in state: **closed**

Port		State	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	SunSSH	1.1	protocol 2.0
3333	tcp	open	dec-notes	syn-ack			
68	udp	open filtered	dhcpc	no-response			
123	udp	open	ntp	udp-response	NTP	v4	

remote operating system guess

- used port 22/tcp (open)
- used port 1/tcp (closed)
- used port 2/udp (closed)
- os match: **Sun Solaris 9 or 10 (SPARC)**
- accuracy: 100%
- reference fingerprint line number: 34332

system uptime

- uptime: 3960974 sec
- last reboot: (null)

tcpsequence

- index: 255
- difficulty: Good luck!
- values: 8536BDE8,50185972,F8FD5B4D,2735AC63,8FE5DBF5,338AC308

ipidsequence

- class: Incremental
- values: CDEE,CDEF,CDF0,CDF1,CDF2,CDF3

tcptssequence

- class: 100HZ
- values: 179BF4B4,179BF4BF,179BF4CA,179BF4D5,179BF4E0,179BF4EB

runstats

- 192 sec. scanned
- 1 host(s) scanned
- 1 host(s) online
- 0 host(s) offline

- nmap version: 5.00
- xml output version: 1.03
- nmap.xsl version: 0.9b

Appendix C

Installation & Setup using Sun Professional Services

With the purchase of the Sun KMS solution a Sun Professional Services engagement will conduct the following services for installation and setup:

A. Scope

Under this service, Sun will provide integration services of two KMAs (Key Management Appliances) and encryption enablement service for up to 64 T10000, 9840D and/or LTO4 tape drives at one Customer data center (collectively the "Service").

B. Sun's Tasks and Deliverables

Service Initiation. Sun will conduct a project kick-off meeting with the relevant stakeholders in order for Sun to document the following:

- Determine encryption requirements
- Identify content storage environment
- Determine the implementation service tasks and expectations
- Identify and schedule Customer's staff to participate in workouts and knowledge transfer

C. Implementation

Sun will train and assist the Customer to perform the following implementation tasks:

- Key management workouts
- Key configuration
- Drive pool configuration
- Key-group configuration
- Drive pool to key-group mappings
- Key Life-Cycle Management

D. Functional Testing

Sun will demonstrate functionality of the following:

- Read/write encryption testing and validation
- Backup and recovery of KMS configuration and database
- Hardware configuration after KMA replacement
- Load-sharing between one KMA to another

E. Knowledge Transfer

Sun will provide information on the following:

- Installation and use of the KMS Manager
- Responsibilities for the different KMS roles
- Optimum setup of the Management and Service Networks
- Management Network is the Customer's wide area network for KMA-to-KMA communication and for the Customer to manage KMAs with the KMS Manager Service Network is the private network from the KMA to the tape drives
- Actions required to add more drives to the system

F. Other Deliverables

Sun will conduct a formal closure meeting to:

- Review the tasks and deliverables for this Service which Sun completed
- Review any applicable support arrangements and obligations of Sun

A Sun KMS minimum configuration will include the following components:

- Quantity 2 Sun KMS servers
- Sun KMS GUI Fat client software (Windows or Solaris)
- Purchased licenses for encryption enablement of Tape Drives

Customer-provided infrastructure or additional purchase:

- Encryption capable tape drives
- Supported Tape Libraries and ACSLS support system
- Network Infrastructure for private and public networks
- Fiber Network infrastructure for data storage
- System to run KMS Fat Client software