

# Sun™ Crypto Key Management System 2.0

Simple, secure, scalable encryption key management



Compliance with legal, financial, and regulatory requirements is dependent on secure data. If you lose data and it's not encrypted, your business is subject to sanctions and penalties. The designed-for-the-long-haul Sun™ Crypto Key Management System 2.0 makes it easy for growing companies to implement storage-based encryption—for operational and archive data—without unnecessary cost and complexity.

## Highlights

- **Simple** – Get up and running quickly—a day or two for many companies—and manage keys easily with user-defined policies
- **Secure** – Protect encryption keys for full data lifecycles throughout distributed and heterogeneous storage environments
- **Scalable** – Grow without worry since you can manage thousands of storage devices and millions of encryption keys

## Near, far, and wide key management

Distributed and heterogeneous storage infrastructures are a given, so the Sun Crypto Key Management System (KMS) 2.0 provides a comprehensive key management platform for tape-based storage in the most diverse environments. Developed on open security standards, the KMS consists of these integrated parts:

- **Key Management Appliance (KMA)** – a security-hardened x-series rackmounted server. Multiple KMAs can be connected via an IP network to form a KMS cluster. A minimum of two KMAs are required per installation site. A trust authority for storage networks, the KMA delivers the following results:
  - Registers and authenticates storage devices
  - Creates, provisions, and deletes encryption keys in accordance with policies

- **KMS Manager** – a graphical user interface (GUI) that is executed on a workstation. It communicates with the KMS cluster over an IP network to configure and manage the system.

## Protection to last a lifecycle

KMS 2.0 is designed with an emphasis on simplicity, security, and scalability:

- **Secure key retention.** Access archived data when you need it. The KMS securely retains encryption keys for the full data lifecycle, which can exceed a decade
- **Interoperability.** Open standards architecture supports diverse storage devices—main-frame to open systems—under a single storage key management system

In 2003, California Senate Bill 1386 created rules requiring companies to self-report situations where confidential data may have been lost or stolen, to alert the media, and to make direct contact with all the potentially affected individuals. More than 38 states have adopted this legislation. However, if a tape is encrypted, these requirements do not apply.

- **Manageability.** Ensure high availability with active n-node clustering, dynamic load balancing, and automated failover. User-defined, policy-based key management via a secure client GUI makes it easy to administer the solution in one room or worldwide
- **Scalability.** A single clustered KMS 2.0 appliance pair you can manage thousands of storage devices and millions of encryption keys. Scale your solution easily and non-disruptively

### Start fast and right

Sun professional services are required for KMS 2.0 implementations. Our expert team provides set up, configuration, and training—a fast, efficient way for you to get up and running quickly.

### About Sun

A singular vision, The Network is the Computer™, drives Sun in delivering industry-leading technologies that focus on the whole system – where hardware, software, and services combine. With a proven history of sharing, building communities, and innovation, Sun creates opportunities, both social and economic, around the world. You can learn more about Sun at [sun.com](http://sun.com).

KMS 2.0 Supported Tape Drives and Libraries

Drive Types	Sun StorageTek PowderHorn™ 9310	Sun StorageTek SL500	Sun StorageTek SL3000	Sun StorageTek SL8500
HP LTO 4	No	Yes	Yes	Yes
Sun StorageTek T10000A	Yes	No	Yes	Yes
Sun StorageTek T9840D	Yes	No	Yes	Yes
Sun StorageTek T10000B	No	No	Yes	Yes

Features	Benefits of Sun Crypto Key Management System 2.0
FIPS-Certified Cryptography	Utilizes FIPS 140-2 certified cryptography to provide AES-256 bit encryption keys for stored data
Role-based Access Control	Supports NIST SP800-60 operational roles to segregate operational functions
Quorum	Requires quorum to activate and can be invoked as an option to restore KMS 2.0 data backups. Quorum parameters are fully configurable
Active Clustering and Failover	Provides high availability through active n-node clustering of Key Management Appliances with fully automated failover
Near-synchronous Replication	Provides near-synchronous, secure replication of transaction data among appliances within the cluster
Granular Role Segregation	Provides operational segregation through five role definitions — Security Officer, Compliance Officer, Operator, Backup Operator and Auditor. Each role is access controlled and functionally restricted, although users can have multiple roles
Centralized Policy Management	Data encryption policies are managed centrally through the Compliance Officer role. Policies are automatically replicated for disaster recovery purposes
Audit Logging	Maintains audit logs for all operational and key material events and transactions
Open Standards	Developed on open standards including X.509v3 certificates, Simple Object Access Protocol (SOAP), and Transport Layer Security (TLS)
Secure Management Client	Provides a rich cross-platform compatible client for local and remote management via secure client GUI
Multi-vendor Device Support	Capable of providing encryption key management support to Sun's most popular tape drives including the StorageTek T10000, StorageTek T9840D, and StorageTek LTO 4

## Key Management Appliance Specifications

Based on Sun X-Series Rackmounted Servers (Specifications Will Vary)

### Processor

- One dual-core AMD Opteron™ processor. 2.2 GHz. Up to 1 MB level 2 cache

### Crypto Processor

- Sun Crypto Accelerator 6000 (SCA6000)

### Memory

- Four memory slots, up to 8 GB

### Mass Storage

- Up to two SATA disk drives (1.5 TB capacity)

### PCI Slots

- Two PCI-Express slots (PCIe)

### Removable Media

- One EIDE DVDD-ROM or DVD+ / -RW DL drive

### Networking

- Four USB 2.0 connectors on the rear panel. Two USB 2.0 connectors on the front panel. One serial RS-232 port and One VGA port. Four 10 / 100 / 1000 Base-T Ethernet ports

### Height

- 43 mm (1.7 in.) 1U

### Width

- 425.5 mm (16.8 in.)

### Depth

- 633.7 mm (25 in.)

### Weight (max.)

- 10.7 kg (23.45 lb)

### Mounting Options

- 19-in. rackmount kit. Compact 1 RU (1.75 in.) form factor.

### Learn More

To learn more about the Sun Crypto Key Management System, go to [sun.com/storagetek](http://sun.com/storagetek). For more information on Sun encryption offerings, go to [sun.com/encryption](http://sun.com/encryption)