Cisco MDS 9000 Storage Media Encryption Package

Package Description

Cisco Storage Media Encryption (SME) secures data stored on heterogeneous tape drives and virtual tape libraries in a SAN environment using secure IEEE standard Advanced Encryption Standard (AES) 256-bit algorithms. Cisco SME is built upon FIPS level-3 system architecture, and offers secure, comprehensive key management, with support for offline media recovery.

Cisco SME uses cryptographic engines on the Cisco MDS 9222i Multiservice Modular Switch and Cisco MDS 9000 18/4-Port Multiservice modules (MPS-18/4), each providing enough throughput to sustain streaming continuously to multiple tape drives. Multiple encryption engines can be deployed in a Fibre Channel fabric to easily scale performance, enable load balancing, and increase availability.

Cisco SME hardware and software integration with the Cisco MDS 9000 family makes it easier to deploy and manage sensitive data on SAN attached storage devices. Unlike competitive offerings, Cisco SME requires no down time to deploy and no host agents. The Cisco MPS-18/4 modules are hot swappable, allowing them to be installed while an existing SAN is in use. No rewiring or SAN configuration changes are required, and encryption provisioning can be performed without shutting down applications.

The Cisco MDS 9000 Storage Media Encryption Package includes the following features:

- Encryption of Storage Media—Cisco SME secures data stored on heterogeneous tape drives and virtual tape libraries in a SAN environment using secure AES 256-bit algorithms.

- Rapid Deployment—The innovative Fibre Channel redirect capabilities in Cisco MDS 9000 SAN-OS enable traffic from any switch port to be encrypted without SAN reconfiguration or re-wiring, eliminating down-time and simplifying deployment.

- VSAN Independence—Traffic in any virtual SAN (VSAN) can fully utilize Cisco SME encryption capabilities, providing unparalleled flexibility for provisioning, and load balancing with this transparent fabric service.

- Scalable Performance—As SAN attached storage grows and encryption performance increases, Cisco SME throughput can be scaled up proportionally to meet these needs by simply adding more MPS-18/4 modules or Cisco MDS 9222i fabric switches to SANs.

- Data Compression—To maximize tape media utilization, Cisco SME provides an option to compress tape data before encrypting it.

- High Availability—Cisco SME is a distributed fabric service that employs clustering technology to create a highly available solution. The cryptographic cluster formed enhances reliability, availability, enables automated load balancing with failover capabilities, and simplifies provisioning as a single service rather than as individual switches or modules.

- Secure Solution—Strong, IEEE compliant AES-256 encryption algorithms are used by Cisco SME to protect data at rest. Cisco MDS 9000 family SAN-OS security features, such as Secure Shell, Secure Sockets Layer, RADIUS protocol, and Fibre Channel Security Protocol provide the foundation for a secure FIPS level-3 architecture.

- Integrated Management—Cisco SME is configured and provisioned using Cisco MDS 9000 CLI and Cisco Fabric Manager; no new management software is needed. In addition to consistent management interfaces, Cisco SME supports role based access control (RBAC) and RADIUS/TACACS+ servers for unified credentials management.

- Comprehensive Lifecycle Key Management—The Cisco Key Management Center (KMC) provides dedicated key management for Cisco SME, with support for single and multiple site deployments. Cisco KMC provides essential features such as key archival, secure export/import and translation for distribution, and key shredding. Enterprisewide lifecycle key management is also available using industry leading software integrated through an open API included with Cisco SME.

- Smart Cards—For increased operational security, smart cards with M of N key recovery are offered to protect master keys, facilitate master key escrow, and help prevent unauthorized cryptographic cluster formation and key recovery. See Cisco Storage Media Encryption Data Sheet for more information.

- Exceptional Investment Protection— In addition to supporting heterogeneous storage devices, the Cisco MDS 9000 family hardware used by Cisco SME supports other storage networking functions, such as SAN Extension over IP for flexibility and solid investment protection.

Software Release

To use the Cisco MDS 9000 Family Storage Media Encryption Package, Cisco MDS 9000 SAN-OS Release 3.2(1) or later must be installed on a Cisco MDS 9200 series or MDS 9500 series switch.

License Information

The Cisco MDS 9000 Family Storage Media Encryption Package is licensed on a per-module basis. The total number of licenses needed for a SAN fabric is equal to the number of MPS-18/4 modules plus the number of fixed slots on Cisco MDS 9222i switches used for Cisco SME.

Ordering Information

The product identification numbers associated with this package are as follows:

M9500SME1MK9	• Storage Media Encryption Package for one MPS-18/4 or one MPS-18/4 FIPS module on a Cisco MDS 9500 series switch
M9500SME1MK9=	• Spare
M9200SME1MK9	• Storage Media Encryption Package for one MPS-18/4 or one MPS-18/4 FIPS module on a Cisco MDS 9200 series switch
M9200SME1MK9=	• Spare
M9200SME1FK9	• Storage Media Encryption package for Cisco MDS 9222i Multiservice Modular Switch fixed slot
M9200SME1FK9=	• Spare

Additional References

For more information on the Cisco MDS 9000 SAN-OS, the Cisco MDS 9222i, and MPS-18/4 module, view the data sheet at:

http://www.cisco.com/en/US/products/hw/ps4159/ps4358/products_data_sheets_list.html.

Printed in USA

C78-388977-00   01/07