# QuickSpecs

Overview

What would happen if your backup tapes and disposed disk drives were lost or stolen? When data at rest encryption keys are secure, the threats of financial loss and damage to your company's reputation are significantly lowered.

The HP Secure Key Manager reduces your risk of a costly data breach and reputation damage while improving regulatory compliance with a secure centralized encryption key management solution for HP LTO-4/LTO-5 enterprise tape libraries and Encryption SAN Switches. The Secure Key Manager automates key management based on security policies for multiple encryption clients. This occurs transparent to ISV backup applications. The Secure Key Manager is a hardened server appliance delivering secure identity-based access, administration and logging with strong auditable security meeting the rigorous FIPS 140-2 security standards. Additionally, the Secure Key Manager provides reliable lifetime key archival with automatic multi-site key replication, and high availability clustering. Encryption clients can access the cluster using flexible path and node failover capabilities.

The HP Secure Key Manager provides centralized key management for HP Enterprise Storage Libraries (ESL) E-series Tape Libraries, HP Enterprise Modular Library (EML) E-series Tape Libraries and the HP Encryption SAN Switch. In addition to the clustering capability, the Secure Key Manager provides comprehensive backup and restore functionality for keys, as well as redundant device components. The Secure Key Manager supports policy granularity such as a key per library partition to a key per tape cartridge and allows for additional client types in the future needing key management services. Keep your confidential data secure yet highly available with automated management for your encryption keys using the HP Secure Key Manager, a member of the "HP Secure Advantage" portfolio.
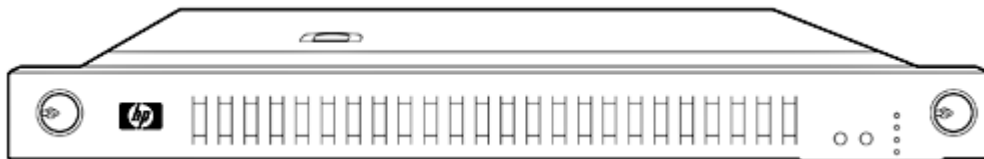
HP Secure Key Manager

What's New

- Solution integration with HP Encryption SAN Switch. The Secure Key Manager acts as a key repository and key manager for the Encryption SAN switch to deliver data at rest privacy in the SAN.

Models

HP Secure Key Manager	HP Secure Key Manager	AJ087B
Models	HP Secure Key Mgr Storage Client License	AN584A
	NOTE: ESL/EML tape libraries and Encryption SAN Switches are purchased separately from Secure Key Manager.	

Standard Features

Secure Key Manager Customer benefits	• Enables effective privacy of data • Reduced complexity and effort to manage encryption keys • Verification for compliance and audit • High availability of archived keys for long term rapid access

---

Key Features	• Centralized encryption key management
	    ○ Automatic policy-based key generation and management supporting key/cartridge granularity for HP LTO-4/LTO-5 enterprise tape libraries
	    ○ ISV transparent key archival and retrieval
	    ○ Key repository and key manager for the Encryption SAN switch to deliver data at rest privacy in the SAN. Key/LUN, key/tape pool and key/tape granularity
	    ○ Capacity of 2 million keys per cluster
	• Strong auditable security for encryption keys
	    ○ Security hardened Linux-based server appliance with pick resistant locks
	    ○ Secure identity-based access, administration and logging
	    ○ FIPS 140-2 Level 2 validated, Certificate #1102
	• Reliable lifetime key archival
	    ○ Automatic multi-site clustering and key replication
	    ○ Flexible path and node failover options (client configurable)
	    ○ Comprehensive backup and restore functionality for keys
	    ○ Redundant device components

QuickSpecs

Product Highlights

Mitigate data breach risk Mitigate your risk of data exposure. Keep your tape encrypted data private and protect the company reputation with Secure Key Manager while improving regulatory compliance and avoiding financial consequences of a breach. Proactively avoid situations requiring disclosure of unauthorized access to unencrypted private information.

Centralized automated key management The Secure Key Manager reduces the complexity of managing encryption keys across a distributed infrastructure with a single point of management. Independent of tape drive count in a library, Secure Key Manager supports multiple encryption clients per node further boosting investment protection. Secure Key Manager cluster nodes and key management clients may be deployed at different geographic sites; only network connectivity is required.

Strong auditable security The Secure Key Manager features a security hardened Linux kernel, dual locking bezel with durable pick-resistant locks and tamper-evident enclosure seals to provide platform security substantially beyond a general- purpose server key repository.
The Secure Key Manager also provides a trusted infrastructure for enforcement of internal security policies/controls and a trusted audit trail of encryption and key management activities as evidence for compliance and audit verifications. This product is appropriate for stringent cryptographic installations and supports AES-256 key generation. It has FIPS 140-2 Level 2 security validation with Certificate #1102. The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government standard used to validate cryptographic modules.

Reliable lifetime key archival High availability and reliability are paramount because keys must be retained for the life of the data which may be for decades. The Secure Key Manager delivers high availability of archived keys for same or multi-site coverage. Key replication occurs automatically in a clustered configuration. Encryption clients may support flexible, tiered, path and node failover.
For improved overall hardware reliability, the Secure Key Manager has redundant dual fans, power supplies and disk drives with RAID 1 (mirroring). It also features health checks to maintain uptime.

OS Support The Secure Key Manager is a dedicated, hardened server with a hardened Linux kernel supporting the key management operations. The Secure Key Manager interfaces with its clients via secure Ethernet communications.

Backup Software Support and Compatibility Reduce impact to existing backup and recovery processes. Secure Key Manager key management operations occur transparent to backup application. The data can be decrypted on any Secure Key Manager library client that has permission to access the key. Note that the LTO-4/LTO-5 Utrium drives require backup application ISV support. Check the Enterprise Backup Solutions (EBS) matrix and/or go-connect for support information for the LTO drive.
http://www.hp.com/go/EBS
http://www.hp.com/go/connect

Service and Support, HP Care Pack, and Warranty Information

Warranty and Services Included with the Product	Hewlett-Packard provides Advance product exchange; Next coverage day; Customer delivers, HP ships return 12 month warranty for the HP Secure Key Manager hardware, plus 9x5 phone support for the duration of the warranty. For more information about HP's Global Limited Warranty and Technical Support, visit: http://h18006.www1.hp.com/products/storageworks/warranty.html

---

HP Care Pack Services	Scalable, Flexible, Dependable. Like your storage. Your storage is evolving. Get scalable support that evolves with it. HP Care Pack Services is an easy-to-buy, easy-to-use portfolio of packaged services covering your lifecycle needs. You can rely on our highly skilled, HP certified professionals to offer a breadth of expertise across leading storage technologies, and work side by side with you for optimal results. Push services beyond expectations and choose support that meets the changing needs of your business with the same reliability, scalability and flexibility you demand of your storage. Protect your business beyond the warranty Standard warranty protects against product defects and some causes of downtime. HP Care Pack Services helps you proactively guard against unplanned downtime which can reduce your productivity and profitability. By using a standard approach to warranty uplifts, such as HP Care Pack Services, customers can be more sure of consistency of operations for both mission-critical and standard business computing. Extending warranties with HP Care Pack Services The key to normalizing the warranty of combined solutions-is making service uplift simple: HP Care Pack Services. This portfolio of predefined packages, extending across the entire IT lifecycle, offering consulting, education, technical support, optimization, risk assessment, and more. It's entirely flexible allowing customers to extend the cover to the precise level of support required. Customer's standard hardware warranty, for example, can be upgraded to next-business-day response, to same-day coverage, or even to a committed six-hour call-to-repair service available 24 hours every day of the week. - Provide consistent, predictable levels of support across your entire department or business - Give you direct access to proven technical and problem-solving expertise - Offer a choice of response-time and repair-time commitments - Are available whenever and wherever you do business For many products, post-warranty HP Care Pack Services are available when your original warranty has expired. Choose the support levels that meet your business requirements. http://www.hp.com/services/storage **NOTE:** Care Pack Services availability may vary by product and country.

Service and Support, HP Care Pack, and Warranty Information

Recommended Services	HP Care Pack Services recommended for optimal satisfaction of all deployments of your product.	
	3-Year HP Support Plus 24	24x7x365 hardware and software services - plus cost-saving software updates and more

HP Support Plus 24 helps you increase performance and availability with comprehensive, consistent hardware and software services. Working with your IT team, HP Services engineers deliver onsite hardware support and over-the-phone software support around-the-clock 365 days per year. Service coverage encompasses HP products and selected multivendor hardware and software.

In addition, this convenient HP Care Pack packaged service makes software updates available to you at substantial savings.

Choose Support Plus 24 when you need to:

Improve uptime with responsive hardware and software services available anytime
Cost-effectively obtain expert 24x7 multivendor hardware and software support
Enjoy consistent service coverage across geographically dispersed sites
Update HP and selected third-party software at a predictable cost
Take advantage of subscription savings on software updates |
| | **HP Installation and Startup Service for Secure Key Manager** | HP Installation and Startup Service for Secure Key Manager provides for the installation and implementation of the HP Secure Key Management Appliance, enabling secure end-to-end data management.

This service provides design, implementation, and testing services to help deploy real-time Secure Key Management functionality between two HP Secure Key Management Appliances.

With help from your designated IT security officer, an HP storage specialist will engage in a discovery process designed to aid in understanding your business, security management, and policy management needs. This collaboration provides the groundwork to plan, design, and employ your personalized system configuration. |

Product Number	Product Name	Service Name	Care Pack Services Product # and Band	Alternate Care Pack Services Product #
AJ087B	HP Secure Key Manager	3 Year HP Support Plus 24	HA110A3-9L2	-
-	-	HP Installation and Startup Service for Secure Key Manager	Contact your HP sales rep or Channel Partner for assistance	-
AN584A	HP Secure Key Mgr Storage Client License	3 Year HP Support Plus 24	HA110A3-9L3	-

QuickSpecs

Service and Support, HP Care Pack, and Warranty Information

eSupport	Limited eSupport for Secure Key Manager
Customer Technical Training	There is no Customer Technical Training available at this time
HP Services Awards	HP Services continues to be recognized for service and support excellence by customers, partners, industry organizations and publications around the world. Recent honors and award reflect our services team's dedications, technical expertise, professionalism and uncompromising commitment to customer satisfaction. For a list of all our awards, please visit http://h20129.ww2.hp.com/services/cache/77318-0-0-225-121.html.
Additional Services Information	For more information about HP Care Pack Services for Storage, please visit: http://www.hp.com/services/storage If you have specific questions, contact your local HP representative. Contact information for a representative in your area can be found at "Contact HP" http://www.hp.com

Kit Contents

Model	Description	Part Number
HP Secure Key Manager	**HP Secure Key Manager**	AJ087B
	Supplied with each Secure Key Manager	
	• One HP Secure Key Manager node or appliance • One Client License Entitlement Certificate AN584A • HP Secure Key Manager Documentation CD	
	NOTE: Requires quantity 2 of AJ087B to configure a 2 node cluster for high availability of the keys. The capacity is 2,000,000 keys. **NOTE:** This SKU includes one client license per node, however, it is possible to scale up to five client licenses per node. Additional licenses must be purchased to scale beyond one client per node. Each ESL or EML consumes only one license (AN584A) independent of number of drives. Each Encryption SAN Switch consumes only one license (AN584A) on the SKM.	
HP Secure Key Mgr Storage Client License	**HP Secure Key Mgr Storage Client License**	AN584A
	Supplied with each HP Secure Key Mgr Storage Client License	
	• One Client License Entitlement Certificate	
	NOTE: This SKU entitles one encryption client for the AJ087B. Each ESL/EML only consumes one license (AN584A) independent of the number of drives. Each Encryption SAN Switch or Blade consumes only one license (AN584A) on the SKM.	

Related Options

HP Enterprise Class Libraries	ESL and EML Tape Libraries For details please visit: http://www.hp.com/go/tape
LTO Encryption	HP LTO-4/LTO-5 Ultrium Tape Drives For details please visit: http://h10010.www1.hp.com/wwpc/us/en/sm/WF04a/12169-304612-3446236-3446236-3446236.html
Encryption SAN Switch	HP Encryption SAN Switch For details please visit: http://h18006.www1.hp.com/storage/networking/b_switches/index.html
HP Compliance Log Warehouse	(Optional) For additional compliance reporting capability consider the HP Compliance Log Warehouse (CLW) to transform security and compliance log event data into valuable information. By understanding the detailed event data that IT systems already produce, organizations can better manage, investigate, and protect these systems. HP CLW collects and analyzes data such as system and application log files, database event records, and operating system event logs. With powerful compliance reporting tools, it turns this data into actionable intelligence, providing rapid time-to-value at a fraction of the cost of traditional data warehousing and security solutions. Visit: http://www.hp.com/go/clw to verify log adaptor support options for HP Secure Key Manager

Power Cords
(for connection to standard wall outlets)

Power Cord, North American C13-Nema 5-15P	AF556A
Power Cord, Euro, 10A 250 V Straight (12 ft/3.7 m)	157215-021
Power Cord, UK, 10A 250 V Straight (12 ft/3.7 m)	157216-031
Power Cord, Danish, 10A 250 V Straight (12 ft/3.7 m)	157218-081
Power Cord, Swiss, 10A 250 V Straight (12 ft/3.7 m)	157219-111
Power Cord, Italian, 10A 250 V Straight (12 ft/3.7 m)	157217-061
Power Cord, South Africa, 10A 250 V Straight (12 ft/3.7 m)	157220-AR1

NOTE: Each Secure Key Manager node ships with redundant power supplies and two (2) IEC-IEC power cords intended for rack mounting with Power Distribution Units (PDUs) and/or Uninterruptible Power Systems (UPS) for highest availability. Alternatively, each Secure Key Manager mode may be powered using two (2) optional power cords connecting to two separate wall receptacles provided on separate branch circuits and mains for highest availability. Two (2) such optional power cords must be ordered for each Secure Key Manager node.

QuickSpecs

Configuration Information

NOTE: Only rack-mount units are available

Step 1 - Select quantity of nodes (2 nodes minimum required for a cluster)

HP Secure Key Manager   AJ087B

Step 2 - Add additional client licenses (optional)

HP Secure Key Mgr Storage Client License   AN584A

NOTE: AJ087B includes one client license per node, however, it is possible to scale up to five client licenses per node. Additional licenses must be purchased to scale beyond one client per node. Each ESL or EML consumes only one license (AN584A) independent of number of drives. Each Encryption SAN Switch consumes only one license (AN584A) on the SKM.

Step 3 - Select appropriate clients -- (optional)

- Add additional HP Enterprise Tape Library LTO-4/LTO-5 or encryption SAN Switch clients that require key management unless you already have them
- See the Enterprise Tape Library QuickSpecs at: http://h18006.www1.hp.com/storage/tapestorage/enterprise_class/index.html
- Add additional HP Encryption SAN Switch clients that require key management
  http://h18006.www1.hp.com/storage/networking/b_switches/index.html

NOTE: New or exiting tape library must be at the current supported level of the latest ETLA firmware, patches and software updates etc to support HP Secure Key Manager. Consult: http://www.hp.com/go/ebs for the minimum revision numbers required
NOTE: Each ESL/EML E-series Tape Library in the solution requires at least one LTO-4/LTO-5 encrypting tape drive, LTO-4/LTO-5 media and an ETLA Secure Manager License (343376-B21 for ESL or T3664A for EML).

Step 4 - Select appropriate Services/Support

- Choose required Installation and Startup service. This service requires a FAN override approval for removal. (More information on Installation and startup Service in service section.)
- Choose support uplift type. There are different service uplifts uplifting years of service, hours of availability and response time. HP recommends the three year HP Support Plus 24 support uplift. (Details of specific part numbers in service section.)
- Consider Consulting and Integration enterprise security services: http://www.hp.com/hps/security

Application Overview (tape library encryption client example)

Configuration Information
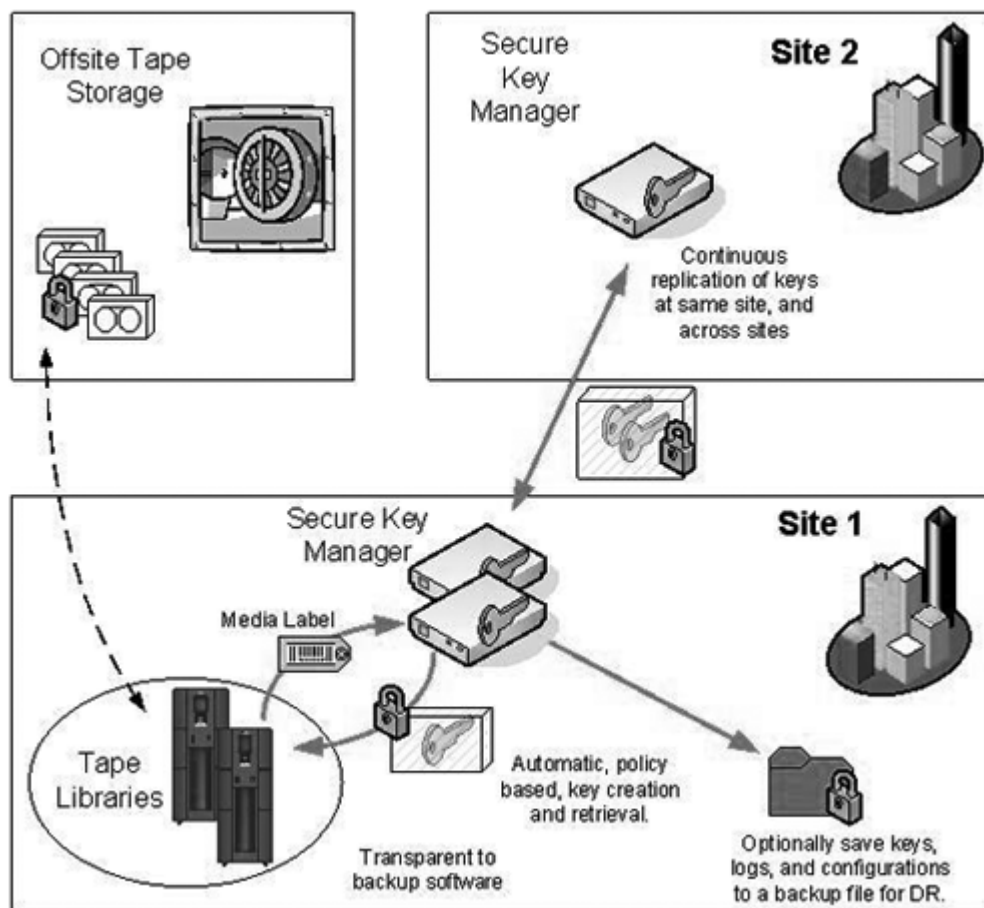
Using the HP Secure Key Manager with tape libraries as encryption clients

This section summarizes the usage and applications of the HP Secure Key Manager.

1. **Installing and configuring the Secure Key Manager**

   - Define your security policies and the roles for those who will administer the devices. For example, the security policies on the Secure Key Manager may be administered by a Security Officer. This role might direct security policy across all your storage products, not just tape. It is not necessary that this role overlap with existing roles, such as the Tape Library Administrator. The Secure Key Manager and the ETLA libraries that use it, both support the separation of roles, with each having separate logins and credentials.
   - Determine which tape libraries and drives will be used for encryption. You can configure keys to be shared among all libraries or restrict keys to one library. Configure the key generation policies that best fit your business needs (key per cartridge or key per library/partition).
   - Setup the Secure Key Manager cluster. The cluster can span multiple sites if necessary.
   - Configure the ETLA tape libraries that will use the Secure Key Manager. The supported clients are HP ESL and EML E-series tape libraries (confirm at: http://www.hp.com/go/ebs). The configuration process is guided by a wizard in the tape library CommandView GUI. You can also use this wizard to modify the configuration later.
   NOTE: An Advanced Secure Manager license is required for each ETLA library that will use the Secure Key Manager.

2. **Encrypting your data backups and decrypting your restored data**

Configuration Information

- Each partition of each library may have a separate key generation policy. The library will automatically retrieve keys to the HP LTO-4/LTO-5 Ultrium Tape Drives.
- These operations are transparent to the backup software and therefore do not affect your existing backup/restore processes.
- When a tape is written for the first time, the library obtains a key based on the key generation policy you established for it. The keys are assigned unique names, based on a media ID, the barcode value, and a timestamp.
- When a tape is read, the library retrieves the key from the Secure Key Manager. If the tape is moved to a different library before it is read, the two libraries must be part of the same security group so the key can be shared. Security groups are easily configured at the Secure Key Manager GUI.
- Keys are passed between the library and the Secure Key Manager via an SSL connection. This is more secure than using a backup application and the SAN where keys are passed in the clear. The path is secure between the library and the Secure Key Manager.
- Encrypted media may be re-used or overwritten again at a later time using a different key. Tape cartridge re-cycling is common in backup applications.

3. **Backing up keys, logs, and configuration data**

- All the nodes of a Secure Key Manager cluster will continuously replicate, so all keys are stored on and available from each node. If a node fails, the other nodes continue to operate, and will serve keys to the tape libraries without interruption.
- You can also periodically backup all the keys, logs and node configurations on each node. These backups are typically stored on a server in your network. These backup files are encrypted and can only be restored to a Secure Key Manager.
- The Secure Key Manager will support multiple libraries. Each node in the cluster can support 5 HP ESL or EML tape libraries, so a 2-node cluster will support 10 libraries. The Secure Key Manager has capacity to support the largest ESL configuration (44 drives). Each library requires a valid license: AN584A - HP Secure Key Manager Storage License.

4. **Auditing and Validation Features**

- The Secure Key Manager maintains an audit log of all key creation and usage. This can be used to support your auditing and security validation policies. This log is digitally signed, which facilitates non-repudiation.

5. **Key Deletion**

- The Secure Key Manager supports manual key deletion, through the Secure Key Manager GUI. This operation can be used if a tape is lost or if the data on the tape is no longer needed. Key deletion is only possible as a manual process by an administrator with the proper authority. The tape library clients cannot delete keys.

Technical Specifications

HP Secure Key Manager	
Security	
Key Generation	AES-256 (Advanced Encryption Standard with 256-bit keys)
Security Standards	FIPS 140-2 Level 2 (Validated Certificate #1102)
Operating System	Hardened embedded Linux OS
Authentication/Quorum Control	2-factor client device authentication, multiple credentials administration
Configurable Security Policies	Customizable security settings for device and key generation
Physical Security	Dual locking bezel with high-security pick-resistant locks and tamper-evident enclosure seals
Secure Audit Logs	Digitally signed logs
Scalability	
Number of Clients Supported	1 storage client license included per node, scales to 5 clients per node
Encryption Key Capacity per Cluster	2,000,000
Attribute Bytes per Key	2048
Key Granularity	Key per cartridge, Key per library partition, Key per LUN and Key per tape pool
Client IOP	Contact HP for latest list of supported clients
Management	
System Administration	Secure simple to use Web-GUI (HTTPS communications) and SSH/Serial CLI
Certificate Management	Local and external certificate authorities. Create and sign client and server certificates
Key Management	Centralized, automated key generation, archival and retrieval
Network Management	SNMP, NTP, health checks, log rotation, backups, upgrades and statistics
Redundancy and Failover	
Hardware Redundancy	Dual fans, power supplies and disk drives (RAID 1 mirroring)
Clustering and Failover	Multi-node multi-site clustering, automatic key and policy synchronization; > 20 nodes supported Flexible, configurable path and node failover support (client dependent)
Data Protection	Secure encrypted and integrity checked backups of the keys, logs and all key manager configurations

QuickSpecs

Technical Specifications

Dimensions and Physical Characteristics	HP Secure Key Manager		
	Form Factor		
	Physical Dimensions (HxWXD): **NOTE:** 1 node	Node	1.7 x 19.0 x 29.1 in (4.3 x 48.2 x 74.0 cm)
		Shipping	11.5 x 23.8 x 36.0 in (29.2 x 60.3 x 91.4 cm)
	Out of Box Weight	Node	37 lb (16.78 kg)
Power Consumption by component			
Secure Key Manager AJ087B	336W		

Dimensions and Physical Characteristics	HP Secure Key Mgr Storage Client License	
	Form Factor	
	Physical Dimensions (HxWXD):	1.7 x 19.0 x 29.1 in (4.3 x 48.2 x 74.0 cm)
		8.5 x 11.0 in (21.6 x 27.9 cm)
	Shipping Weight	1 lb (0.5 kg)

Environmental	Operating temperature range	10°C to 35°C (50°F to 95°F)
	Shipping temperature range	-40°C to 66°C (-40°F to 150°F)
	Operating Humidity (non-condensing)	10 - 90 % RH