Hewlett Packard
Enterprise

HPE 3PAR StoreServ Data-At-Rest Encryption

Technical white paper

Contents

Executive summary

As technology moves forward and the requirement to protect user data becomes more of an everyday need for commercial users who store customer data, it is paramount that the storage manufacturers provide a safe method to protect the data stored on storage mediums. These protection standards should comply with the standards set forth by the National Institute of Standards and Technology (NIST) and be FIPS 140-2 (Federal Information Processing Standard) compliant.

To answer the need for securely storing data, all currently supported HPE 3PAR StoreServ Storage arrays including the 3PAR StoreServ 7000 and 3PAR StoreServ 10000, support the use of Self Encrypting Drives (SED). To support the use of SED drives the HPE 3PAR StoreServ Storage array must use HPE 3PAR OS 3.1.2 MU2 or above. The SED is a hard drive or solid state disk drive with a circuit (ASIC) built into the drive controller's chipset which encrypts/decrypts all data to and from the drive media automatically.

Hewlett Packard Enterprise has continued to enhance the encryption support on the HPE 3PAR StoreServ arrays by offering FIPS-2 compliant SED drives with a subsequent release of HPE 3PAR OS and is now offering with HPE 3PAR OS 3.2.1 the ability to use an external Enterprise Key Manager (EKM). An enterprise secure key management solutions that offer the flexibility of local, remote, and centralized controls over keys will include a number of defining characteristics. It's important to consider the aspects that will help match the right solution to an application environment for best long-term reusability and ROI—relative to cost, administrative flexibility, and security assurance levels provided.

These combined offerings of FIPS 140-2 validated components allows the HPE 3PAR StoreServ arrays to be FIPS 140-2 compliant. FIPS 140-2 compliance ensure the customer the satisfaction of knowing their data is securely stored on the HPE 3PAR StoreServ array. Key Management on the array with either Local Key Manager (LKM) or EKM coupled with FIPS drives, offers the customer a safe secure environment in which to securely store their data.

Features of Secure Data Encryption

FIPS 140-2 Standard

FIPS 140-2 is a U.S. Government standard which describes encryption methodology used to accredit cryptographic modules. NIST issued the standard for FIPS 140-2 so as to publish the requirements for cryptography modules which include both hardware and software components.

Security levels within FIPS 140-2 Standard

FIPS 140-2 defines four security levels by which a product will adhere to.

- Level 1, is primarily used for software-only encryption, this level imposes very limited security requirements.
- Level 2, improves on level 1 by requiring features that show evidence of tampering. On an SED disk this typically is seen by a tamper proof cover over the electronics section on the bottom of the disk and the placement of tamper proof seals on the mating surfaces of the disk drive.
- Level 3, adds physical tampering resistance to disassembly of the SED, furthermore if tampering is detected the device must be able to erase critical security parameters (CSP). Physical security mechanisms may include the use of strong enclosures and tamper detection response circuitry.
- Level 4, provides the highest level of security. The physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent detecting and responding to all unauthorized attempts to physical access.

All FIPS 140-2 disk drives on the encrypted ready HPE 3PAR StoreServ arrays are level 2 certified.

AES 256

The Advanced Encryption Standard (AES) is a specification for the encryption level of electronic data established by the U.S., NIST in 2001. AES is a symmetric key algorithm which uses the same key for encrypting/decrypting the data on the disk drive.

All data is encrypted prior to be written to disk as illustrated in figure 1. Data enters the disk as a readable clear text, upon being sent to the disk the data enters special chipset only found on SED disks. This chipset then encrypts the data prior to being written to the disk drive.

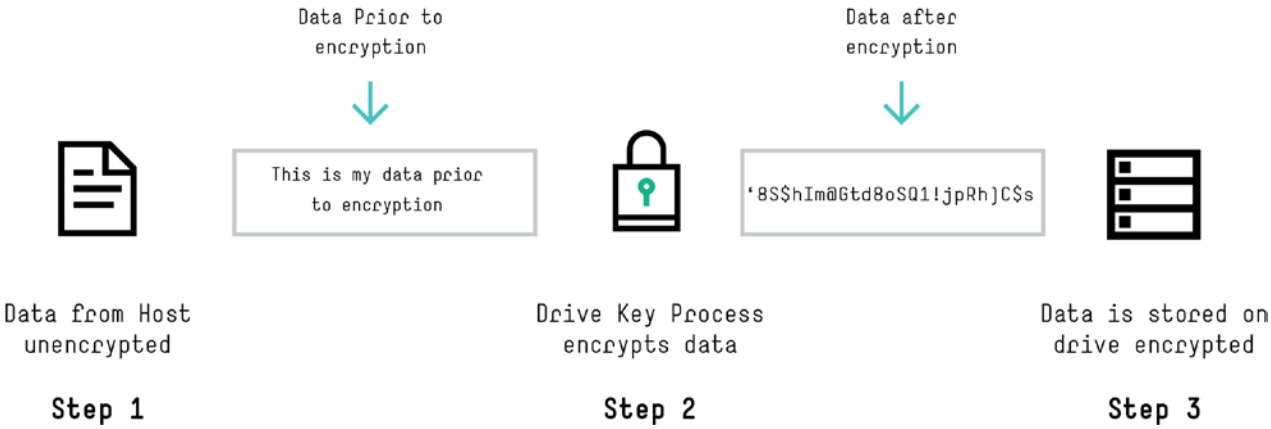


Figure 1. Data encryption

All data written to each FIPS 140-2 disk uses Full Data Encryption. All data encryption is handled at the drive level and no external software or hardware is needed to encrypt data. The benefits from FDE encryption are as follows:

- Government Standard based encryption—industry wide standard
- Uses AES-256
- Dedicated engine for full speed encryption contained on every drive
- Encryption key is unique and protected on the media
- Encryption key itself is encrypted and stored on the media

FIPS 140-2 Self Encrypting Drive

A SED is a self encrypting disk drive with on board circuitry which will encrypt/decrypt all data to the media without any user intervention. The FIPS 140-2 standard for SED ensures that a product uses sound security practices, such as approved, strong encryption algorithms and methods. Each FIPS 140-2 SED disk which is deployed within the HPE 3PAR StoreServ Storage array meets the level 2 requirement of FIPS 140-2 Standard. Other features built-in include:

Security

- Protect data from exposure due to loss of equipment—in the event a drive failure or the drive is removed from the HPE 3PAR StoreServ Storage array, the data resident on the disk drive is protected from any unauthorized use due to an encrypted data key which is generated on the drive. Data is protected from unauthorized use since the drive is set to lock on powerfail (drive removal) and the user would need an authorization key to unlock the disk.
- Enable instant and secure erasure of the SED through the administrative processes

Closed Encryption Device

- Dedicated engine for full interface speed encryption—this equates to the encryption engine being built into the drive electronics which guarantees no data delays
- Key is generated on the drive
- Encryption key never leaves the drive
- Encryption cannot be turned off
- Drive exposes an open interface for key management—key management is done at the array level and implemented by a LKM or EKM

Cryptographic Drive Key

Each SED manufactured drive contains a unique cryptographic key to unlock drive access when array encryption is enabled. This unique key is exchanged with a Key Manager (which is discussed later in this paper) and enables data protection of the SED drive. This unique key is stored on a single band of the disk drive. If the SED is removed from the array after encryption has been enabled, the SED drive is automatically locked from any external access unless the unique cryptographic key of the drive is entered. All other attempts to access data will result in failure.

Cryptographic erase

Each SED drive contains the function to cryptographically erase data stored on the SED drive within a matter of milliseconds. The methodology to erase the data destroys the cryptographic key stored on the SED drive which effectively wipe all accessible data on the drive. A cryptographic erase occurs on a SED drive when either the drives is admitted to the HPE 3PAR StoreServ array (admitpd) or when the drive is removed by the HPE 3PAR OS (dismisspd). Any attempt to remove the drive in an unauthorized method results in the SED drive entering a locked state as outlined previously.

Self Encrypting Disk (SED)

The SED is at the heart of data encryption and customer data security. Each SED drive contains an ASIC used in the encryption and de-encryption of data. The ASIC referenced here is not the HPE 3PAR ASIC contained within the array controller. It is important for the consumer to understand, as is illustrated in figure 3 that data encryption/decryption occurs at the drive physical layer and it is not part of the HPE 3PAR OS. The HPE 3PAR OS is used for Key Management of each disk but does not participate in the encryption/de-encryption of the data. Figure 2 illustrates the 3PAR StoreServ virtualization is separate from disk encryption/decryption, encryption/decryption occurs once data is presented to the disk as write or when a request is received from the host as a read operation.

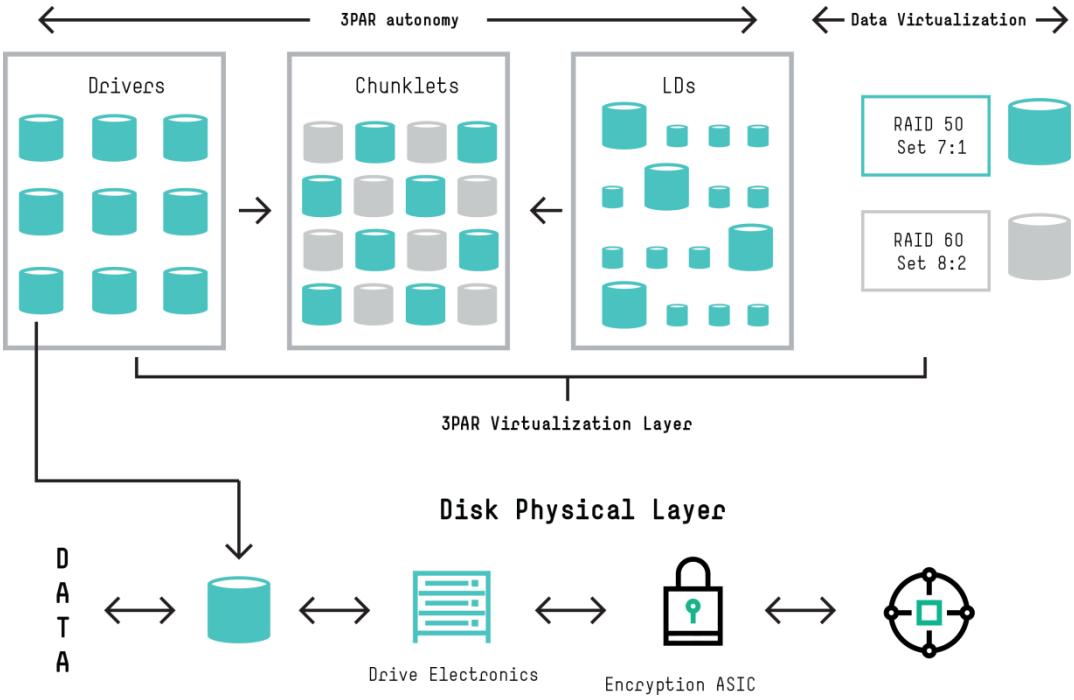


Figure 2. Disk Physical Layer

Once data is presented to the disk as illustrated in figure 3, the disk will perform normal data consistency checks prior to data encryption. These data consistency checks occur within the drive electronics include CRC checks, odd parity, and Disparity and T10-DIF standard. This data would be received from the HPE 3PAR StoreServ storage controllers as part of the virtualization storage request.

Once data is received at the storage medium the disk will act upon the data as a normal data request. The drive electronics are responsible for checking and maintaining data integrity prior to the data entering the data encryption engine. This paper does not discuss other parity generation and checks that occur within the drive electronics.

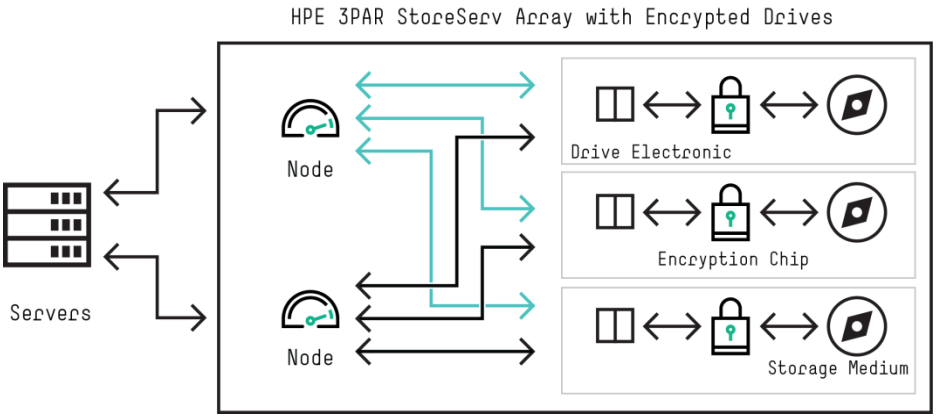


Figure 3. Data checks and encryption

The actual encrypting of data occurs within the logic of the encryption chip as shown in figure 4. As previously mentioned, the encryption engine uses the Advanced Encryption Standard (AES 256) when encrypting data being stored on the physical disk medium.

Shown in figure 4 is the inner band where the secure encryption key resides if array encryption is enabled. The secure encryption key generated by the appropriate key manager (discussed later in this paper) which secures the SED drive to the array in which the key was generated. Unauthorized removal of the disk drive will result in the SED drive being locked and no data access can be gained.

Destruction of the key renders the disk drive as blank, if the key is destroyed all data on the disk drive is unintelligible.

Note

On SED drives, data is always encrypted on the storage medium, no license is necessary. Enabling encryption on the array protects the SED drives from any malicious intent by locking the disks to the array in which encryption is enabled. The same array encryption locking key is used for all disks within the same encrypted storage array.

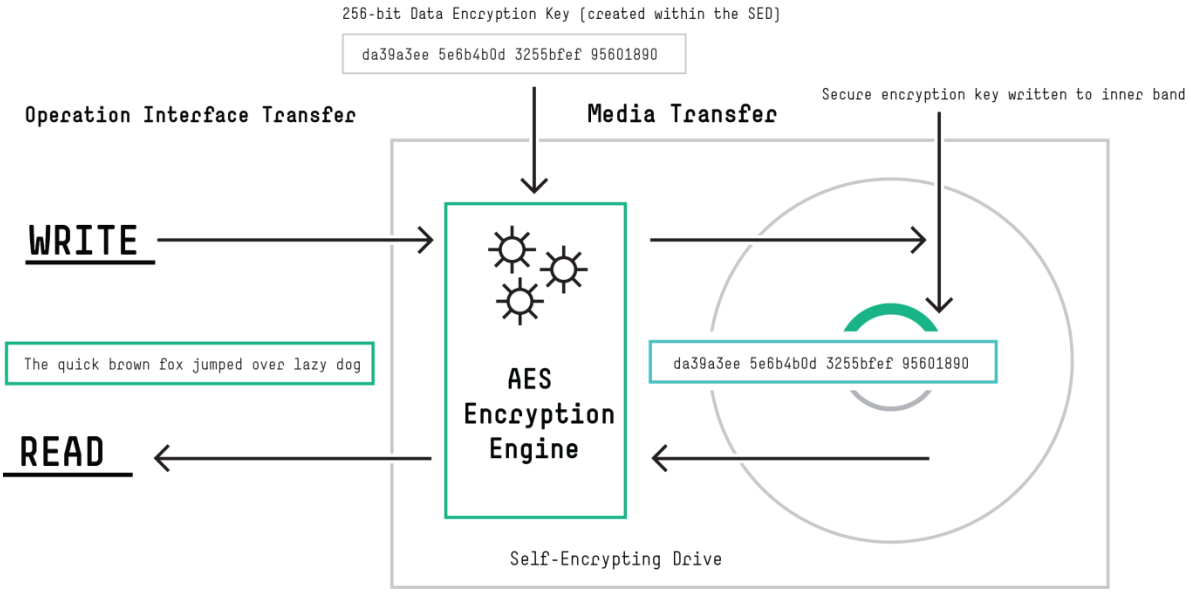


Figure 4. Drive Encryption Engine

Supported Storage components

The following StoreServ Storage arrays and disk drives and HPE 3PAR OS are supported for use as an encrypted array.

Storage Arrays

All HPE 3PAR StoreServ Storage arrays support encryption.

- HPE 3PAR StoreServ 7000 Series
- HPE 3PAR StoreServ 10000 Series
- HPE 3PAR StoreServ 20000 Series
- HPE 3PAR StoreServ 8000 Series

For each of the listed HPE 3PAR StoreServ arrays to support encryption the array must be populated with encryption supported disk drives and cannot have a mix of encrypted and non-encrypted. The above list is inclusive of supported HPE 3PAR StoreServ at the time of the writing, any new HPE 3PAR StoreServ arrays which are developed after publication of this paper will also be supported for encryption.

Supported HPE 3PAR OS

The following HPE 3PAR OS versions are supported along with supported hardware components:

- HPE 3PAR OS 3.1.2 MU2—Supported SED disk drives and Local Key Manager
- HPE 3PAR OS 3.1.3 MU1—Supported FIPS SED disk drives
- HPE 3PAR OS 3.2.1—Supports Enterprise Secure Key Manager
- All current versions of HPE 3PAR OS

Note

All supported HPE 3PAR OS versions must have a valid Encryption license to enable encryption.

Supported HPE 3PAR StoreServ Drives

The following disk drives are supported when enabling encryption on the HPE 3PAR StoreServ array. The current list below was as of the writing of this paper, please refer to HW QuickSpecs of the appropriate HPE 3PAR StoreServ array for current list of supported encrypted drives.

Note

It should be noted that all disks are supported in a configuration of array encryption, whether the encryption method is LKM or ESKM. The user can mix encrypted drives within the architecture. Mixing of drives must follow HPE 3PAR OS standards whereas different CPG's will be associated to different classes or drives. As in the case where the user deploys Nearline, Fast Class and SSD drives within the same array. Each class of drives must reside within a separate CPG associated with drive class.

Although an array can have a mix of non-encrypted disks and encrypted disks within the same array, the array cannot enable encryption in this mode. At the current time the mixing of non-encrypted and encrypted disks, is supported with HPE 3PAR OS 3.2.2 but encryption cannot be enabled unless all disks are encryption capable.

HPE 3PAR engineering continues to evaluate the process of migrating non-encrypted disks to encrypted disks but as of the publishing of this paper does not support this process. Currently the only supported migration strategy is for another array to be installed and data migrated over to the encrypted array using HPE 3PAR Peer Motion Utility or creating a Federation.

Key management

Enablement of array encryption requires a key manager of the encryption key. Key management of the secure encryption key is accomplished via the use of either the LKM or the EKM.

Management of access to the SED drives is done via one of the two key managers. Specific management features allow control of the encryption features including, locking, unlocking, creation of and removal of authentication keys. The key manager provides the functionality for generating and storing authorization keys with the HPE 3PAR OS system. The key manager also includes backup and restoration for generated keys. Both key managers will include the following functions:

- Encryption enablement
- Backup of keys
- Rekey
- Recovery Management

Local Key Manager

The LKM enables key management at the HPE 3PAR StoreServ array. All key management is local to the HPE 3PAR StoreServ array and is controlled by an internal process of the HPE 3PAR OS. The file in which the encrypted key is kept is identified as a keystore, the keystore is kept locally within the array and also is backed up in the event of a failure or for security purposes the file needs to be changed. The process which interfaces with the encrypted drives is darsvr. Figure 5 illustrates the connection of darsvr to the encrypted drives.

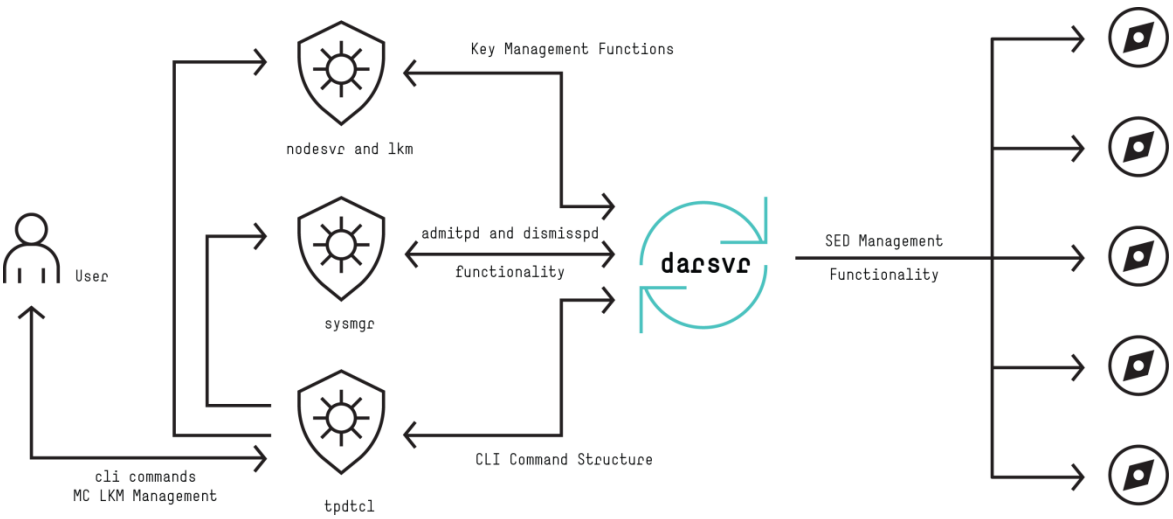


Figure 5. Local Key Management

Darsvr processes includes communication to encrypted drives for unlocking, rekey of drive authentication key and changing ownership of the disk drive. To enable these processes darsvr must communicate with other internal HPE 3PAR OS processes.

Three Par Data Terminal Control Language (tpdtcl) is the internal OS logic which communicates with darsrv to control the following functions. The tpdtcl is the cli of the HPE 3PAR StoreServ Storage array.

- admitpd—process whereby when the physical drive is admitted to the HPE 3PAR StoreServ array for use, this process also includes division of blocks into chunklets
- dismisspd—process which removes the physical drive from the storage array
- controlencryption—five commands associated with the array encryption
  - enable—process which turns on drive protection on the array
  - rekey—new key will be generated all the disks will be updated

- status—command which shows the status of the SED disks and the encryption status
- restore—restore the keystore (LKM Only)
- backup—create a separate backup of the keystore (LKM Only)

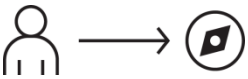
Sysmgr is the system manager of the HPE 3PAR OS, sysmgr is the scheduler service which runs and maintains the HPE 3PAR StoreServ Storage array. One function of the sysmgr is to maintain the list of disk drives within the array. Sysmgr communicates with the darsvr on startup and request the SED info about drives to populate its internal data tables. Sysmgr will also perform its normal admitpd and dismisspd processes.

Nodesvr is where the LKM resides. Nodesvr is the process which handles key management functions and runs on the master node. It tracks the current state and key sequence numbers for the LKM.

Admitting disks with LKM

A question arises as to the process to admit disks into the array used for encryption. The process talks of a single disk with encryption already enabled.

Step 1. User inserts disk into the HPE 3PAR StoreServ Storage array



Step 2. The darsvr will query the disk for disk information. That information is passed to the sysmgr for validation of drive type and a qualified encrypted disk

Step 3. Sysmgr will verify drive is qualified to admit into the HPE 3PAR StoreServ Storage array, if qualified

Step 4. Sysmgr will issue a command to darsvr to admit the disk

Step 5. Darsvr will request a locking key from nodesvr to write on the admitted disk

Note

When a disk is admitted into or dismissed from the system, a unique internal encryption key is created so that all data is destroyed. Neither the encryption key nor data are ever exposed outside the array.

Enterprise Key Manager

As part of FIPS 140-2 compliance, starting from HPE 3PAR OS 3.2.1, HPE 3PAR will support an EKM. EKM provides a complete security solution for unifying and automating an organization's encryption controls by securely creating, protecting, serving, controlling, and auditing the encryption keys.

Starting with, HPE 3PAR OS 3.2.1 will support HPE Enterprise Secure Key Manager v4.0 and SafeNet KeySecure k450 or k150. Either solution will support the HPE 3PAR StoreServ Storage arrays which are supported for encryption. Both solutions meet the NIST Key Management standards are validated for FIPS 140-2 level certification. As there are other EKM's in the industry, HPE has only qualified the above EKM's to function with the HPE 3PAR StoreServ Storage array.

Similar to the LKM the EKM will use a single locking key for all drives in the array. The locking key will be managed by the EKM and is not key manager sensitive, meaning whichever HPE key manager the user deploys, EKM will use the same methodology to provide a secure locking key. In order to protect the key, a new process "fipsvr" will be deployed and will be the only process which has access to the locking key. The key will only be in memory during an operation, otherwise the key is stored in the EKM.

The following two sections will highlight the two EKM's which are supported with HPE 3PAR OS 3.2.1, any further investigation into each of the products is left to the user.

HPE Enterprise Secure Key Manager (ESKM) 4.0[1]

HPE ESKM is designed as a fully integrated solution: an independent lab-validated secure server appliance. Standard capabilities include high availability clustering and failover, secure key database, key generation and retrieval services, identity and access management for administrators and encryption devices, secure backup and recovery, a local Certificate Authority, and strong audit logging for compliance validation.

The HPE ESKM includes:

- Unified, secure, scalable encryption key management services
- Strong auditable security
- Reliable continuous access to business-critical encryption keys
- Management
- FIPS 140-2 Level 2 validation

SafeNet KeySecure[2]

SafeNet offers a broad range of Data Protection solutions that enable organizations to move past silo constrained encryption, and to centrally, and uniformly deploy encryption in a scalable manner that spans the enterprise, and allows them to effectively control their security policies. SafeNet solutions deliver unmatched coverage—securing databases, applications, personal identifiable information (PII), and storage in the physical and virtual datacenter and the cloud. SafeNet also provides the critical key management needed to effectively and efficiently enable protection across the enterprise wherever data resides. With SafeNet, organizations can apply data protection where they need it, when they need it, and how they need it—consistently and effectively.

Fipsvr

As illustrated in figure 6, fipsvr is the integral component within the HPE 3PAR OS when an ESKM is configured. The fipsvr replaces darsvr which was used with the LKM to control access to the FIPS 140-2 certified SED drives. Fipsvr is also the primary interface to the External Key Manager (EKM).

[1] http://www8.hp.com/us/en/software-solutions/asset/software-asset-viewer.html?asset=1586399&module=1817037&docname=4AA5-0654ENW&page=1817049
[2] safenet-inc.com/data-encryption/enterprise-key-management/key-secure

The darsvr process runs on the master node and will handle the unlocking and management functionality, it will be a consumer of events from em_filter. When a locked disk I/O is attempted, an event will be posted and darsvr will automatically issue a request for fipsvr to unlock the drive. The SCSI driver will create an event when the drives are locked and implement a retry after darsvr has had time to unlock the drive. A table holds the External Key Manager (EKM) configuration data.

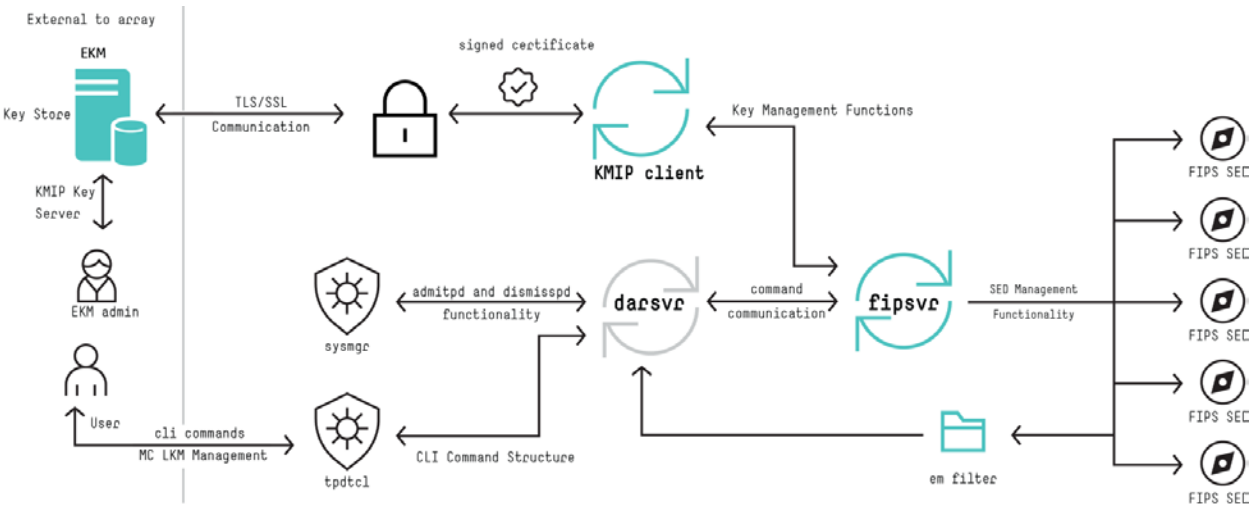


Figure 6. fipsvr and key management

Fipsvr will be the only process that ever has access to the key. It is responsible for communication with either the LKM or EKM to retrieve keys when needed and will securely remove the keys from memory after every operation so that the key is only in memory on the array when an SED operation is in progress. Darsvr will continue to coordinate the operations and keep track of changes at a high level and will issue individual drive requests to fipsvr which will construct the CDB (with the key) and send the request to the drive. Only one instance of fipsvr will run on an array, and in general will run on the node which has the active network interface for the network that can communicate with the EKM. If the active network node changes while a SED operation is in progress, the operation will be completed and then fipsvr will move to the new active network node.

Certificate Authority

Using an external key manager will require additional configuration in order to be able to securely communicate across the network. Both the EKM and the array must have certificates signed by a trusted Certificate Authority (CA). This requires the ability to create a certificate signing request (CSR) on the array, the ability to import the resulting signed certificate and the ability to add a trusted CA. In addition to the certificates, the array must have a username and password to use for accessing the EKM as well as connection information for the EKM (hostname or IP, and port). Fipsvr will communicate with the EKM using the CryptSoft library via TLS connections through a FIPS validated openSSL library on the array.

OASIS Key Management Interoperability Protocol (KMIP)[3]

A KMIP server stores and controls **Managed Objects** such as Symmetric and Asymmetric keys, Certificates, and user defined objects. Clients then use the protocol to access these objects subject to a security model that is implemented by the servers. Objects have core **Base Object** properties such as key length and value, as well as extended **Attributes** that can include user defined attributes.

KMIP enables interoperable communication between cryptographic environments and key managers, reducing the operational, training, and infrastructure costs for key management in the enterprise. KMIP Profiles define functionality sets that address specific scenarios (such as vaulting keys created within a storage environment). KMIP Profiles also define the authentication that must be used to ensure message confidentiality and integrity.

[3] oasis-open.org/committees/tc_home.php?wg_abbrev=kmip

Dismissing disks from an encrypted array

Dismissing a physical disk (pd) with the dismisspd command will remove the active disk from the encrypted HPE 3PAR StoreServ Storage array and destroy all data which resides on the physical disk.

Step 1. User requests to remove pd via cli or SSMC

Step 2. Sysmgr will request an inquiry as to status of pd

Step 3. If pd does not contain user data proceed to Step 5

Step 4. If pd does contain user data, message is returned to user indicating user data must first be removed dismisspd request ends

Step 5. If no user data resides on pd, sysmgr issues a secure erase command to erase the encrypted key from the drive band as shown in figure 4

Note

As stated before and shown in figure 4, once the secure data band is erased, all data on the physical drive is unintelligible and no data can be recovered.

Step 6. Physical disk is removed from the HPE 3PAR StoreServ Storage array table of contents and spun down

Step 7. User can remove disk

HPE 3PAR StoreServ Management Console

Prior to use of encryption on HPE 3PAR StoreServ Storage array the user must obtain a valid license and enter that license through the management console, it is important to note this does not enable encryption on the HPE 3PAR StoreServ Storage array but rather allows the user access to enabling encryption. Figure 7 illustrates the SSMC when an encryption license is entered.

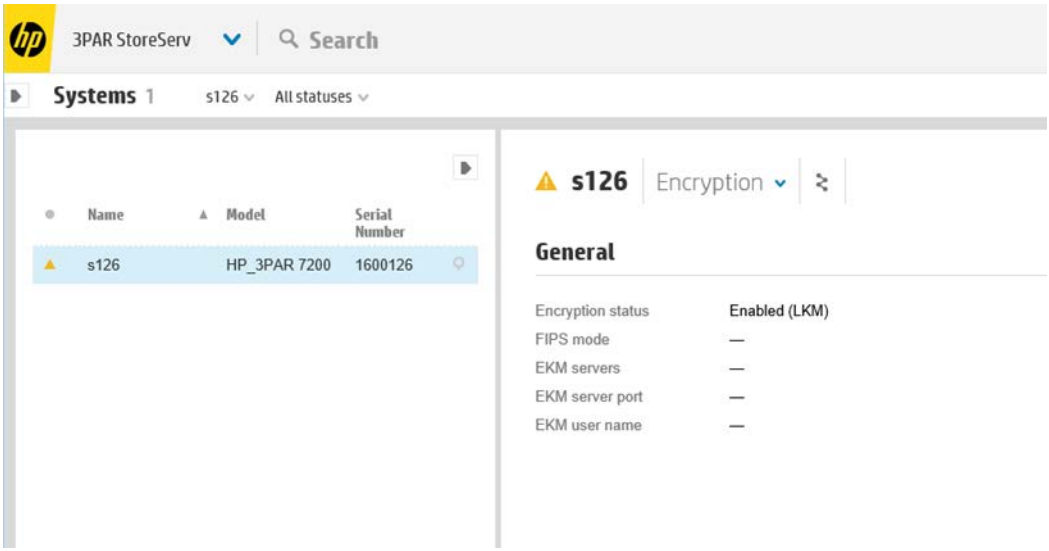


Figure 7. Encryption License enabled

Note

It should be noted that entering an encryption license does not enable encryption. The user must enable encryption from the drop down as illustrated in figure 8 or at the cli prompt enter “controlencryption enable”.

Other functions available from the SSMC include the following:

- Backup Encryption Key—Immediately after encryption is enabled on the HPE 3PAR StoreServ Storage array, the user is required to back up the encryption key. This key should be kept in a safe secure area.
- Restore backup file—Allows the user to restore a previously backed up encryption key.
- Rekey Encryption—Some corporate security polices require a new encryption key be created and backed up on a scheduled basis. This option invokes the process of creating a new encryption key and exporting the new key to all drives in the array.

For all other functions regarding the use of the HPE 3PAR StoreServ Management Console[4] please refer to the appropriate version of HPE 3PAR StoreServ Management Console you are using.

Figure 8. SSMC Encryption drop down menu

Using cli with data encryption

As indicated the user has the choice between using cli for management or SSMC. The current cli include the following commands and are used when working with a Local Key Manager:

controlencryption enable <filename>—allows enablement of the encryption process with the array. Drives in the array must all be SED drives. The user after enabling encryption will be prompted and reminded to back up the encryption key in a separate location.

controlencryption backup <filename>—used to back up the key store. The key store may be backed up as many times as the user feels comfortable with. The password which is required during the backup of the key store is to protect the key store and prevent unauthorized access to the LKM. Example of key store backup to the file myarray. (**LKM Only**)

cli% controlencryption backup c:\keys\myarray

[4] h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c04777556&docLocale=en_US

controlencryption rekey <filename>—New keys will be generated and all of the disks will be updated. There must be no disks in a degraded or failed state on the array at the time of the rekey. Once rekey is initiated the user will be asked to back up the key store.

controlencryption restore <filename>—This command will be used to restore the key management file in the case the encryption is not currently functioning. The restore command will not be permitted on a functional encryption system and can only be used in the case of a failure. An example of a restore of a key store from the directory of keys is:

cli% controlencryption restore c:\keys\myarray.txt

controlencryption status –d—This command can be run to show the status of the SED disks and the encryption status. The only subcommand for this is a –d which provides details for the encryption status. See figure 10 for an example of the controlencryption status command.

Commands added for the use of ESKM (no GUI support)

The following commands were added to support the use of the ESKM. The user may specify more than one EKM IP or hostname, all other configuration options (port, username, password, certificates) are common to all EKMs. To setup an EKM, the user will use the below commands to specify the connection options for one or more EKMs, then run checkekm to verify that the array can connect to the EKMs configured. Once encryption has been enabled with an EKM, any changes to the EKM properties will be verified before committing them. All controlencryption commands will require a backup path to be specified.

importcert ekm-client –ca <certfilename.pem>—will import the certificate of the Certificate of Authority (CA) that signed the server certificate the EKM presents

importcert ekm-server –ca <certfilename.pem>—will import the certificate of the CA that signed the array's client certificate

importcert ekm-client certfilename.pem—will import the signed certificate from the CA

createcert -csr ekm-client—create a Certificate Signing Request (CSR) to be used as a client certificate when communicating with the EKM

controlencryption command will add the following subcommands:

setekm

-setserver—will specify a comma separated list of IP's or hostnames to be used with EKM

-addserver—will add an IP addr or hostname to the current list of configured EKMs

-removeserver—will remove IP addr or hostnames from list of configured EKMs

-port—specify the port to communicate with the EKM

-ekmuser—specify the username to communicate with EKM

-ekmpass—used to set the password for the EKM

checkekm—displays status of the ekm

```
s127 cli% controlencryption checkekm
EKM settings are correct.
```

The enable command will also allow user to transfer from and existing LKM configuration to EKM configuration. The change in this configuration is only one way, meaning the user cannot change back to using LKM without first initializing the array.

showencryption—will display the same information as controlencryption status. FIPS status and EKM configuration will be added to the output of the command. Figure 9 illustrates the output from each command.

```
s127 cli% controlencryption status -d
Licensed Enabled BackupSaved State  FIPS      SeqNum non-FIPS FailedDisks
yes      yes     yes         normal Compliant      1        0           0

Number of EKM servers defined: 1
EKM servers: 15.252.193.189
EKM server port: 9001
EKM username: jason
s127 cli%
s127 cli% showencryption -d
Licensed Enabled BackupSaved State  FIPS      SeqNum non-FIPS FailedDisks
yes      yes     yes         normal Compliant      1        0           0

Number of EKM servers defined: 1
EKM servers: 15.252.193.189
EKM server port: 9001
EKM username: jason
```

Figure 9. Encryption status

Important

Backups when running with an External Key manager are for configuration information **ONLY**! While this file is still important, as it is necessary to recover from a disaster, the keys are stored **ONLY** on the EKM, and must be backed up independently. Also, when configuring the EKM and before encryption is enabled, a backup filename is not required.

Enabling encryption after data population

Best Practice is for the user during the installation of the array to enable encryption through the use of the cli command “controlencryption enable” prior to data being populated on the array. Using this command allows the local key manager the functionality for generating and storing the authentication keys within the system and will include backup and restore functionality.

Data however, is always encrypted at the drive level with or without the enablement of controlencryption. As discussed earlier in this document, the AES chip is in-line with data movement within the SED disk. Data therefore is always encrypted on a SED disk drive. The added functionality of enabling the key within the Local Key Manager, enables the data security on powerfail. Powerfail occurs when a power is loss at the drive level, this power loss could be the sudden loss of power at the array level or the loss of power from an extraction of the disk drive within the array.

Extraction of a SED disk drive within the array without the LKM/ESKM enabled could allow an unauthorized user access to the data stored on the disk. Enabling the LKM/ESKM through “controlencryption enable” controls access to a specific band on the disk drive. The disks have the ability to go into a locked state whenever power is lost to the SED disk. This locked state guarantees any disk removed from the HPE 3PAR StoreServ array will not be accessible except in its original array. When the drive is unlocked, all I/O behaves exactly as a non-SED disk drive as discussed earlier in this paper.

Enabling encryption after data has been populated on the array will allow the extra failsafe measures discussed, Data which is resident on the disks prior to enabling encryption protection at the array level will continue to reside on the disks after the encryption key is enabled. There is a rumor that enabling encryption after data resides on the drives will erase the data on the encrypted disks. This claim is completely false, enabling encryption after data occupancy has been thoroughly tested at HPE and is supported by HPE 3PAR StoreServ Storage. It should be noted though that enabling this feature while data is being processed will have a slight performance impact on the array initially due to the LKM/EKM initial key exchange with the SED disks.

Once key exchange is completed I/O throughput would return to normal.

Note

A user can enable encryption on the array from a non-encrypted state and not lose any data. However, once encrypted the array must always be encrypted. Removing encryption will erase the secure encryption band on each of the physical drives and render all data unintelligible.

Off array data movement

Remote Copy

The user will be warned prior to creating a remote copy session between an encrypted and non-encrypted array. A pop up message will appear warning the user of the intent to link the two arrays, one with encryption and one non-encrypted. A message will be displayed during the RC creation which warns the user of the differences in encryption modes. The user is given the choice to continue with the Remote Copy link.

Peer Motion

Peer Motion between a non-encrypted array and an encrypted array will produce a warning much in the same way as it did with Remote Copy. Prior to any migration occurring the user will need to select Yes or No to data movement. A "NO" answer will dissolve the Peer Motion connection. If moving to an encrypted array be sure to answer "YES."

Movement of data from an encrypted array to a non-encrypted array will result in the data on the non-encrypted array being stored without encryption.

Non HPE 3PAR StoreServ Array Migration

HPE 3PAR offers the ability to migrate data online from supported models of EMC, HDS, IBM, and HPE EVA's online. The ability to migrate data from a supported migration source to an encrypted HPE 3PAR StoreServ Storage array will have no impact on either array. Data movement between a non HPE array and the HPE 3PAR StoreServ Storage array occurs at the block level. There are no dependencies at the disk drive level.

Performance

HPE has verified through extensive testing the SED drives which are used for Data Encryption have no impact on array performance. The following questions and answers are in response to our observations made in our analysis.

Question—Will SED drives have any different behavior at the drive level for any IO profiles compared to non-SED drives (r/w/random/sequential)?

Answer—The drive manufactures that HPE uses in our arrays performed separate tests to characterize performance. Each of the manufacturers concluded there was no performance impact by using an encrypted (SED) drive. HPE also performed separate analysis and agrees with their findings.

Question—Will SED drives behave any differently at the system level for any IO profiles compared to non-SED drives (r/w/random/sequential)?

Answer—HPE found no performance differences when comparing SED to non-SED drives with any I/O profile.

Question—Will a rekey operation have any effect on performance?

Answer—Yes, increases in I/O latency was observed during the execution of system rekey activity. It was observed that random read were impacted more than write operations since write operations are serviced by arrays cache. Write response times were not impacted.

Figure 10 displays the temporary increase in response time during the rekey operation.

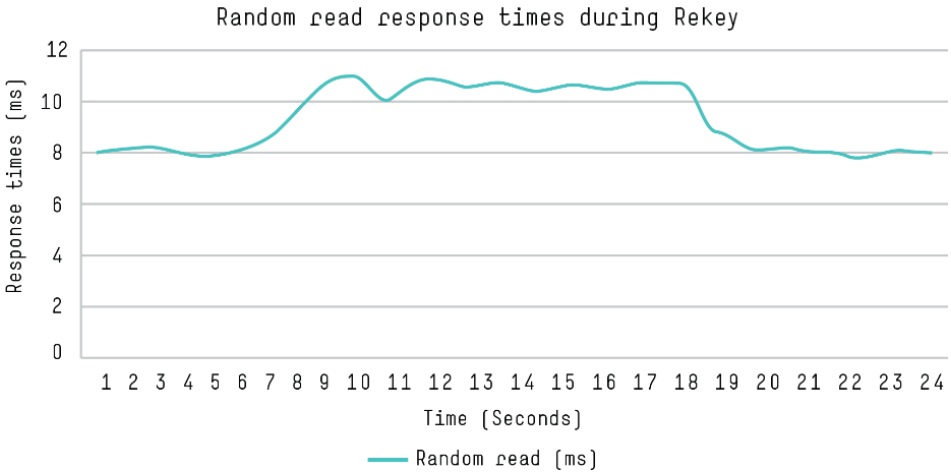


Figure 10. Rekey operation

Power removal scenarios

Power failure on the array

In the event of an untimely power failure within the data center, each drive is protected by a unique encryption key and data cannot be accessed without that unique key. Drives cannot be removed and put into another array for data retrieval. Once power is restored to the data center, a normal startup of the array will restore availability to access data stored on the array by the host systems.

Powering down the array

User should follow standard procedures in powering down the array. There is no special process in powering off the array. Upon powering on the array the appropriate key manager will unlock access to the hosts to allow host access to data. In testing it was found that booting up the array with SED disks could take up to two minutes more due to the key mechanism, in general it was observed that boot time was increased by 20–30 seconds.

De-Installing the array

Removing an encrypted array from service will require the user to initialize the array. Once the array is initialized the secure encryption key will be erased from each drive rendering the data irretrievable. Once this occurs no user data will remain on the array. In order for the array to be encrypted again, the user would need to start encryption as detailed earlier in the paper. It should be noted unless the encryption license is deleted, it would not be necessary to obtain a new license.

It is suggested the user contact HPE services to assist in initializing the array and any services needed to move the array.

Best practices

Booting from encrypted array protected with EKM

Booting a host from an encrypted array prior to the EKM manager startup will result in a failure on the host to boot. The EKM manager must communicate with the array prior to any host activity. The EKM manager will issue the key used to unlock disk drives on the encrypted array.

Terminology

MC—Management Console

SP—Service Processor

VSP—Virtual Service Processor

HPE 3PAR OS—Operating System for HPE 3PAR StoreServ array

LKM—Local Key Manager

KMIP—Key Management Interoperability Protocol

ESKM—Enterprise Secure Key Manager

NIST—National Institute of Standards and Technology

FIPS—Federal Information Processing Standard

SED—Self Encrypting Drive

CA—Certificate Authority

CSR—Certificate Signing Request

HIPAA—Health Insurance Portability and Accountability Act

CSP—Critical Security Parameters

OASIS—Organization for the Advancement of Structured Information Standards

Learn more at

hpe.com/storage/3PAR

4AA4-7605ENW, April 2016, Rev. 4