Dell PS Series Architecture: Self Encrypting Drive Management with PS Series Storage Arrays

Dell Storage Engineering
February 2017

A Dell EMC Technical White Paper

Revisions

Date	Description
May 2013	Initial release
February 2017	Updated to reflect industry changes

Table of Contents

Executive summary

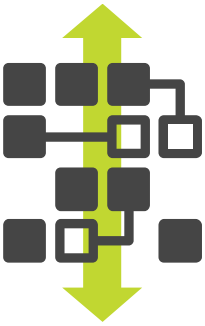
Data and intellectual property are the life blood for a company in the modern information driven economy. Although a considerable amount of money and effort has been spent towards protecting corporate networks from outside intrusions, many security analysts agree that there are still significant vulnerabilities relating to data theft by either physically stealing, misplacing, inappropriate redeployment or disposal of hard drives from corporate computers and storage arrays. An effective solution to ensure that data on hard drives leaving the data center cannot be used to compromise critical information is to employ Self-Encrypting Drive (SED). SEDs, coupled with Dell Storage PS Series arrays, provide an industry leading solution for securing corporate data from hard drive loss or theft.

1 Introduction

Whether it is sensitive customer information, intellectual property or proprietary data that helps a company reach its strategic objectives, company data is often its most valuable asset. If this data is misplaced or stolen, organizations run the risk of lost revenue, legal repercussions and a tarnished reputation. The unfortunate truth is that organization data is becoming increasingly vulnerable as lost, accidentally exposed or breached data is becoming more and more commonplace in our highly connected world. With data security risks on the rise, an influx of government regulations for securing data have been mandated and are becoming part of the corporate business requirements for many organizations. Even in the absence of a government mandate, eliminating exposure of private data is now simply viewed as a sound business practice.

To avoid the high cost and other negative consequences of a data breach or lost data, it is important for organizations to put a comprehensive security strategy in place. A comprehensive strategy requires understanding where data is at all times across the organization and securing it at each of these points. These points, or levels of security, can be broken down into three basic categories: data in use, data in motion, and data at rest.

Table 1 Levels of data to be secured across an organization

	**Data in use**	User, OS, or application utilization of data (for example, print, copy, move)
	**Data in motion**	All data being transferred between two nodes across the network
	**Data at rest**	Data recorded on the storage media

The primary focus of this guide is securing data at rest. While each point in the storage infrastructure provides unique threat models, data at rest presents one of the highest security vulnerabilities. In fact, data spends most of its life at rest on drives. As these drives will eventually leave the data center for repair, retirement, relocation, or maintenance, it is at this time that drives (and the data contained on these drives) are most vulnerable to being lost or stolen.

The emergence of full disk encryption technology and SEDs is timely in mitigating the security vulnerabilities of data at rest. SEDs are also becoming a standardized technology across many top drive vendors, which allows for interoperability and ensures greater market competition and competitive pricing.

To further highlight the importance of SEDs, the Storage Networking Industry Association (SNIA) best practices recommends encryption as close to the information source as possible—which is the media where the data resides. In addition, many safe harbor laws, such as California state regulations CA 1798 (formerly SB-1386), protect organizations that store data in compliance with security encryption requirements. With safe harbor laws such as these, organizations might not have to notify customers of lost data if that data was stored and secured on SEDs. Current SEDs use the Advanced Encryption Standard (AES) encryption algorithm as defined by the National Institute of Standards and Technology (NIST) and has been widely adopted as an encryption standard. The SEDs selected by Dell for use in the PS Series product line are approved for use in applications requiring compliance with FIPS 140-2 Level 2.

2 SED technology overview

An SED is a self-encrypting hard drive with encryption and decryption functions built into the disk drive controller chip that encrypts all data written to the media and automatically decrypts all the data read from the media. All SED solutions have three main parts: the storage subsystem (the PS Series array), the drive electronics and the drive storage media. SEDs encrypt all the time performing like any other hard drive with the encryption being completely transparent to the user.

There are two primary functions of SED technology:

- Protecting hard drive data from unauthorized access to secure data at rest.
- Instant Secure Erase that provides a mechanism to securely erase the data on the drive so that the drive can be repurposed or retired.

Note: SEDs cannot be used to encrypt the contents of individual volumes, in the sense of securing each iSCSI volume with its own key. This level of protection would need to be supplied by the file system using the volume, or by a utility running on the host that is using the volume to store data. SEDs also cannot provide security across multiple PS Series members, so it is up to the administrator to ensure that SED members and non-SED members are not combined in the same pool in order to ensure that data is fully protected by SEDs.

2.1 Protecting data from unauthorized access

To protect the data from unauthorized access, SEDs utilize two sets of keys. One key is called the Media Encryption Key (MEK). In the factory, each SED randomly generates an MEK that is encrypted and embedded within the drive. The MEK is never exposed outside the drive and requires no management by the user. The MEK functions as a password so that the encryption/decryption engine built into the drive knows how to decrypt the user data stored on the physical media.

The second required key is called the Access Key (AK), sometimes referred to as the PIN or BandMaster password. The AK is used to encrypt the MEK, so that the AK must be provided before the MEK can be used to encrypt and decrypt the user data on the drive. Once a SED has been configured with an Access Key, then the Access Key must be provided in order to unlock the drive, and the drive remains unlocked only while powered. The drive locks itself upon losing power or shutting down, and the access key must be provided again before the drive will unlock and participate in I/O operations. PS Series arrays automatically detect SED drives and create the AK when the array is initially configured or reconfigured after a reset command returns the array to factory defaults.

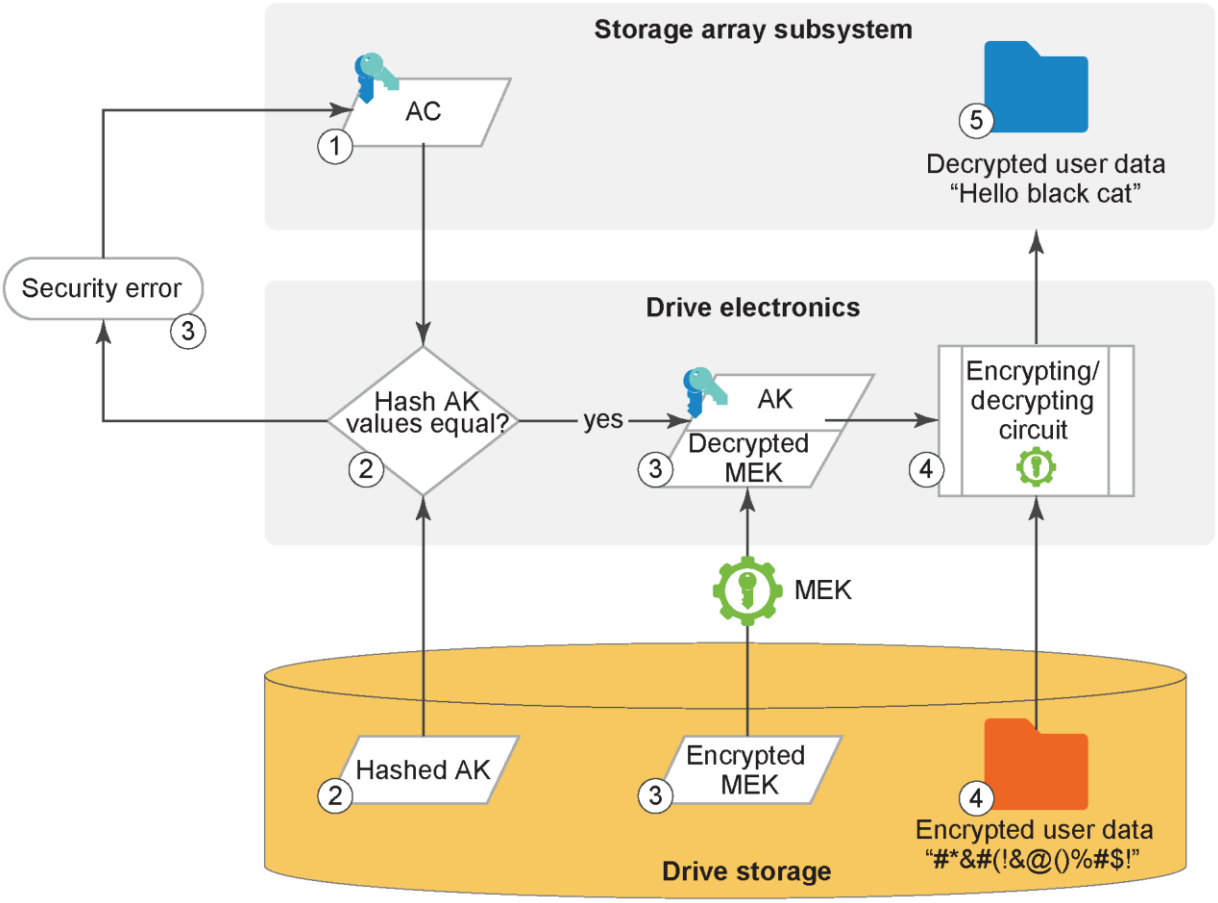


Figure 1 Accessing data on a SED

1. Data is requested from the self-encrypting drive by the storage subsystem. The storage subsystem sends its access key (AK) to the drive electronics.
2. The drive electronics hash the authentication key from the storage subsystem and pull the stored hashed access key from the drive storage. The hashed keys are compared.
3. If the hashed keys do not match, no access is given to the data and an error is passed back to the storage subsystem stating that the drive is locked and that the subsystem does not have authorization to access it. If hashed keys match, then the encrypting/decrypting circuit is granted access to pull the encrypted media encryption key (MEK) from the drive storage. It then uses the access key passed by the storage subsystem to decrypt the MEK.
4. The encrypting/decrypting circuit pulls the requested data from the drive and uses the decoded MEK to decrypt the encrypted user data.
5. The decrypted user data is then passed back to the storage subsystem

In summary, the true value of SEDs is realized when a drive (or drives) is lost, removed, or stolen. In such an instance, the drive becomes locked and the data remains encrypted and unreadable. Because an unauthorized user would not have the appropriate access key, the MEK cannot be unlocked to decrypt the data and without the MEK the data remains inaccessible to any attacker.

2.2 Instant Secure Erase

Another security method available with SEDs is Instant Secure Erase (ISE). Alternative methods, such as degaussing each drive or simply overwriting the data with zeros, are available to permanently erase this data. However, these methods are often expensive, slow or do not provide complete data erasure.

Typically, whenever an SED populated array is reset to factory default condition, each drive in the array is instructed to destroy the stored encrypted MEK, and then lock itself. At this point, a new randomly generated MEK is created by and stored on the drive. Without the original MEK, there is no way to decode the already encrypted data on the drive. Another common occurrence of ISE is when a failing drive is preemptively copied to a spare drive and then removed from use (failed) by the PS Series firmware. After the copy-to-spare action occurs, the failing drive undergoes an ISE so that it may be safely returned to the manufacturer under warranty.

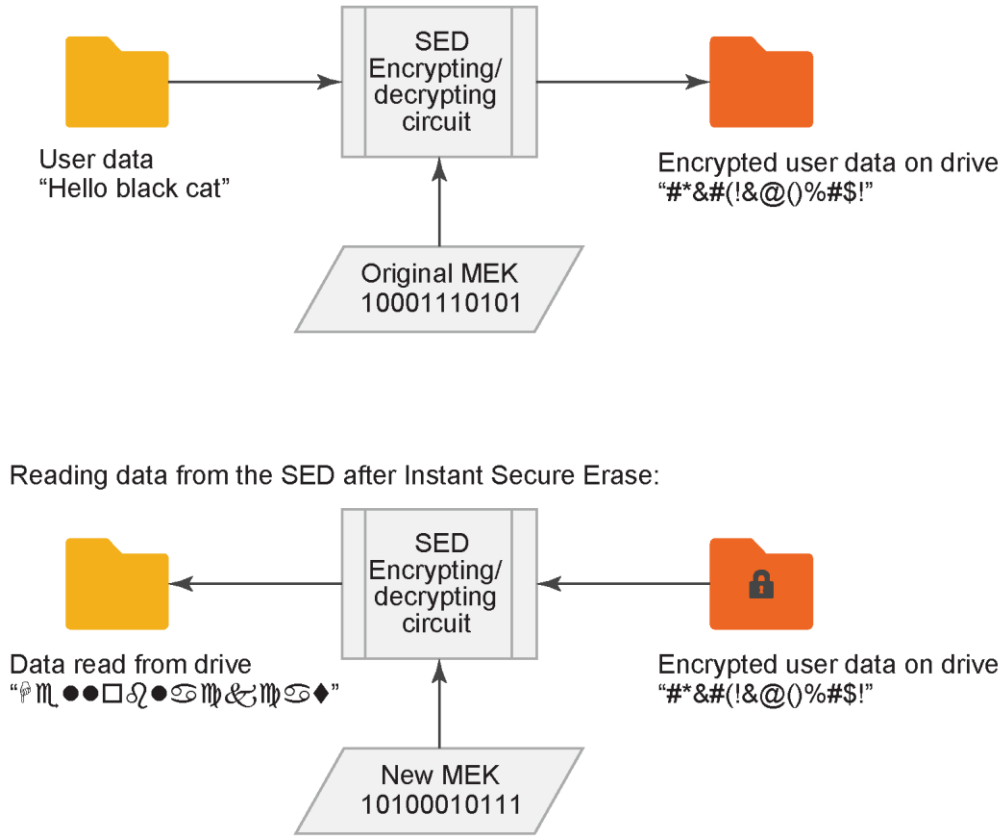


Figure 2 Instant Secure Erase Process

As shown in Figure 2, instant secure erase prompts the SED to permanently erase the current media encryption key and replace it with a new key randomly generated within the drive. When the media encryption key is changed, any data that has been written to the drive using the previous key cannot be decoded by the new media encryption key, in so doing all of the data is rendered unusable. Data that was encrypted with the previous media encryption key is therefore cryptographically destroyed.

3 Securing data with SED technology on PS Series arrays

As the leader in storage technologies, Dell EMC provides support and management capabilities that allow users to safely secure their data-at-rest in PS Series arrays. This support is offered through AutoSED which combines local key management with SEDs. The Dell AutoSED feature provides the all of the benefits of SED security with no special effort on the part of the administrator. An administrator does not need to configure or set up drives, manage encryption, install a Key Management Service (KMS) or ever issue an instant secure erase command. Everything is handled by AutoSED as it is a completely self-contained keying system.

The AutoSED feature is embedded within the PS Series firmware version 6.0 and above. As said above, it does not need to be separately installed. When a PS Series array equipped with SEDs is first powered on, the AutoSED feature immediately engages and begins providing data at rest protection.

3.1 Key management

AutoSED relies on the concept of cryptographic secret sharing as discovered by Adi Shamir. This allows an AutoSED array to unlock itself without revealing the key.

The concept of a SEDset is central to the AutoSED security model. Similar to how RAID groups hard drives into a RAID set for redundancy, AutoSED groups hard drives into a SEDset for security. There is always one SEDset per PS Series member equipped with SED drives, spanning all active drives in the member. The SEDset cannot be unlocked unless it is sufficiently intact. A SEDset is considered intact when at least half of its drives are present (excluding spares, failed, and foreign drives).

The access key is the key that is protected by AutoSED. When a SED PS Series member is initially configured, AutoSED configures a small unsecured band for drive labels, followed by a single secured band spanning the rest of the drive. AutoSED then generates a new and unique AK using a randomized function. Every drive in the array will be locked with this one AK. AutoSED then uses the Shamir algorithm to split the AK into multiple pieces, called shares. AutoSED always chooses to split the key such that one share is written to each of the active drives in the system in the unsecure band on that drive. AutoSED requires that at least half of its drives to be functioning in order to reassemble the AK.

3.2 Instant Secure Erase (ISE)

With AutoSED, a user does not ever issue a secure erase command. If a member is removed from the group – for example, to be repurposed for the use of some other department in a different PS Series group – then the ISE function is invoked on all of the drives in the array, causing all of the MEKs to be regenerated, and whatever data was once on the array is no longer accessible. As discussed above, ISE is also invoked when a failing drive is removed from service by the PS Series firmware before it is marked failed. Drives that fail suddenly, without warning, do not undergo ISE, but are still safe to return since they are still in a locked state and the data cannot be recovered.

Cases when ISE is invoked:

- Array reset (all drives undergo ISE)
- Disk mirror/copy-to-spare (the original drive gets erased by ISE when the copy process is done)

- Reuse of a drive from another array (The drive will be initially marked as a foreign drive ISE is invoked and the drive is converted to a spare after the administrator confirms that the drive should be used)
- A drive that fails, and then comes back to life (ISE is invoked, then the drive is set to history-of-failure)
- A drive that is removed while the array is running (without faulting the system) and then reinserted (ISE is invoked, then the drive becomes a spare)

The AutoSED secure erase function cannot be undone. Once a member is removed from the PS Series group, the data is permanently destroyed and there is no recovery. Having this performed automatically is a major advantage of AutoSED as it saves the user from having to remember to call a separate secure erase command when a drive or member is retired or repurposed.

3.3 Security Scenarios Covered by AutoSED

While using AutoSED is effortless, it is important to understand what protection is provided.

- Loss of a drive. When a powered on drive leaves the SEDset (whether by failure, removal, or otherwise), the drive immediately locks itself. Its contents are inaccessible without the access key. At the same time, the SEDset immediately re-secures itself to exclude the departed drive by creating new key shares, ensuring protection of the access key.
- Loss of fewer than half the drives. When fewer than half the drives in the SEDset are removed, the SEDset remains intact and re-secures itself by creating new key shares to exclude all the removed drives. By doing so, the removed drives permanently lose all knowledge of the SEDset access key, and remain locked to any attacker. If these drives are later re-inserted into either the original or a different PS Series array, AutoSED will perform an ISE on the drives before allowing them to be utilized as part of the new array.
- Insertion and reinsertion into the same array. When an SED is removed and reinserted into the same array, it will invoke an ISE of the SED
- Removal and insertion into a different array. When an SED is removed and inserted into a different array, the drive will remain in a locked state and appear as foreign. The administrator must explicitly bring the drive into service which then will result in an ISE of the SED
- Loss of other array components. The SEDset access key shares reside wholly within the drives. The key cannot be found in the flash cards, channel cards, mid-plane, chassis or any other component including the controllers and controller memory.

3.4 Security scenarios not covered by AutoSED

- Loss of the entire array. An SEDset is a self-contained key management system, which is why the array can unlock itself with no external assistance. A stolen array will continue to unlock itself, just as it did before it was stolen.
- Loss of half the drives. Security may be compromised if half (or more) of the drives are removed at once. These drives can be combined into an intact SEDset of their own, which will automatically unlock itself.

- Insider attack. Any person who possesses the administrator password can access any volume on the array, or change ACLs to allow others to do the same. Similarly, a compromised host can access volumes that the host is authorized to access. SED devices cannot provide protection against improper access to an online data volume.
- Data in flight. SEDs are intended to solely provide protection for data at rest, and thus provide no protection for data in flight on the network. IPsec is also supported by PS Series products and can be used to provide secure connections to the volumes by the hosts.
- Tampering with array hardware. AutoSED is not resistant to modified firmware, hardware probes and other snooping devices, or the removal of a drive without loss of power to that drive.

4 Summary

As demonstrated, AutoSED technology and PS Series arrays provide a robust data-at-rest security solution. This solution further ensures that the provided enterprise level data security is easy to use and fully automatic, requiring no user interaction. In addition, AutoSED injects no performance degradation in storage operations.

Table 2 Key components of the solution

Solution Component	Description	Benefit
Self-encrypting drives (SED)	Storage devices with embedded cryptographic electronics which encrypt/decrypt data on the drive	Data is cryptographically secured and cannot be read by unauthorized individuals. Always on and has no performance impact on drive I/O operations
PS Series AutoSED Key Management	AutoSED is embedded software in PS Series firmware which provides SED access key management	Fully automatic and requires no intervention from PS Series customers. Works from the moment a SED array is powered on. All key management functions are performed in the background transparently and automatically
PS Series AutoSED Instant Secure Erase	AutoSED is embedded software in PS Series firmware which provides SED instant secure erase functionality	Fully automatic and requires no intervention from the customer. The SED ISE function is performed automatically whenever member is reset, for example, when it is removed from a group. The ISE function is also used when a failing drive is removed from service before failure occurs, or when a good SED drive is moved from one array to another. This eliminates the risk of data being inadvertently exposed when a drive is returned under warranty or repurposed

A PS Series SED storage procedures

A.1 Backing up the access key using the PS Series Group Manager GUI

The AutoSED machinery is very robust and remains functional even when severe failures have taken the array offline. The backup is only needed in exceptional circumstances, such as the loss of more than half the drives from an array.

The SED Access Key is never explicitly revealed as part of the backup process. Rather, it is cryptographically rewritten into a set of three unique backup units. Any two backup units from the same backup set can be combined by AutoSED to decode the Access Key. Although the key does not change until the member is reset, each backup set is unique. No two sets are alike, and backup units from different sets cannot be combined to recover the Access Key.

The array will automatically create and present a backup set during initial setup, when the RAID policy is configured. Additional backup sets can be manually requested at any time.

1. Click **Group** and expand **Members**.
2. Click the name of the member identified for encryption key back up.
3. Click the **Maintenance** tab.
4. In the Disk Encryption panel, click **Encryption Key Shares**.
5. Enter the administrative password in the dialog box. The Information dialog will list the names and location of the three files.
6. To download all three backup units as individual text files, click **Download key shares** and choose the location where you want to store them. All three file names have the format membername-backup-unit-N, where N stands for 1, 2 or 3.
7. Click **Copy** above each key share to copy the individual key share (backup unit) and paste it into a file, if desired.
8. If one of the backup units is lost or compromised, refer to “Safeguarding the key backup” in the *Dell EqualLogic Group Manager Administrator’s Guide*.

Note: If you generate a second set of key shares, the first set is not invalidated. Generating a second set of key shares, therefore, does not protect the key shares from being compromised.

A.2 Unlocking a Self-Encrypting Drive

During normal operation, an SED automatically unlocks at startup. When you back up the key shares from the GUI, the three parts of the key are saved as individual text files to the directory that you specify. To unlock a locked drive, you must use the CLI.

1. From the CLI prompt, type `keyd` (but do not press [**Enter**]). This command invokes the keying daemon.
2. Open the first key share file with a text editor (such as Notepad). The key share file name has the form groupname-keyshare-*number*, where *number* represents 1, 2, or 3. The key share file has no file extension.

3. Copy the long string (130 hexadecimal characters) from the file and paste it onto the command line after the `keyd` command. The first 56 characters, the header, is the same for all three pieces. You might have to keep scrolling to the right to see all the characters in the string. This is normal and works as designed.
4. Repeat the process with keyshares 2 and 3.
5. Press [**Enter**].

B Frequently Asked Questions

Why are my key backups always different?

Although the encryption key never changes, the backup will look different each time it is generated. The three backup units are cryptographic images of the key, never generated the same way twice.

Why is there no secure-erase command?

None is needed. Whenever the array is reset, or when the situation warrants it (such as marking a failing drive as failed or reusing a drive in a new array) AutoSED will perform a secure-erase, without intervention. There is no need to perform a manual secure-erase, so there is no command to perform it.

Note: Secure-erase is also known as cryptographic erase or crypto-erase in the general SED literature on the Internet.

What is the difference between a locked drive and a securely-erased drive?

Data that is locked is inaccessible without the SEDset Access Key. Data that is securely erased has been cryptographically destroyed.

Are there any restrictions about mixing SED and Non-SED arrays in the same group or within a pool?

There is no restriction on mixing of SED and non-SED PS Series members in a group, or for that matter in a pool. This means it is easy to deploy SED members without confusing restrictions, but it also means that you don't necessarily gain the benefits of your SED members right away. In particular:

- In a mixed pool, volumes may be unencrypted, partly encrypted or completely encrypted, depending on the PS Series arrays in the pool and the distribution of the volume slices among the available resources.
- In a mixed pool, page movement does not pay attention to SED status. As a result, a page may move from an SED member to a non-SED member, or vice versa, without notice.
- For more details, refer to *Dell Storage PS Series Architecture: Load Balancers*.

There will be a notice when adding a member to a pool changes that pool from homogeneous to mixed, but this is only a notification, it does not block the action. If a pool is entirely SED, that pool will be marked as such in the UI, and all volumes assigned to that pool will also be marked. If a pool is not entirely SED (either mixed, or not SED at all) then the pool will not be marked and neither will the volumes in the pool.

Similarly, there is no restriction on mixing SED and non-SED groups and pools in replication. As a result, even if a pool is entirely SED (and therefore the volumes in it are definitely all encrypted) those volumes may be replicated to a partner that has no SED members, or a mix.

I accidentally removed an SED array from a group. Is there anything that can be done?

No. Every drive in the member has been securely erased. The data has been cryptographically destroyed. Recovery is impossible.

What if the entire array is stolen?

Security is compromised. The array will unlock itself when it boots, as it did before it was stolen.

What if the grpadmin password is stolen?

Security is compromised. The adversary can simply connect to the array over the network and read the data.

Is it safe to discard or return a locked SED?

Yes. Any data that was written to the drive will be locked and inaccessible. When you return a drive to Dell, the only information that remains readable are its operating statistics (S.M.A.R.T. data), the RAID type that the drive was used in, and drive hardware error logs.

Can I add SEDs to a non-SED array, or vice versa?

No. Do not ever mix SEDs and non-SEDs in the same array. If mixed drives are detected while the array is booting, the array will halt until the incorrect drives are removed. If mixed drives are detected while the array is operating, the incorrect drives will be shown as unauthorized.

Does an SED system use RAID also?

Yes. Each drive in a SED-equipped array is managed by both AutoSED and RAID. The SEDset governs the locking of data, and the RAIDset governs the data itself.

Does SED encrypt individual volumes?

No. SEDs cannot be used to encrypt individual volumes, in the sense of securing each iSCSI volume with its own key. AutoSED operates at the level of the physical disk drives within an individual member.

If I create a new set of backup units, does this invalidate the previous set of backup units?

No. Generating a new set of backup units does not affect previously-created backup sets. To invalidate previous backup sets, refer to the Safeguarding the key backup topic.

C Key terms and glossary

Table 3 Key terms

Term	Definition and usage	Location and management	How it is generated
Media Encryption Key	Required to encrypt and decrypt data	Resides on & managed by the drive. It is never transferred from the drive. Every drive has its own unique encryption key.	Generated by the drive at the manufacturer, then regenerated at the customer site if used with the instant secure erase feature.
Access key	Needed to unlock a drive. Automatically provided to the drives by AutoSED, or manually using the backup units.	Resides on the drives in a hashed form, managed by AutoSED.	Created and managed automatically by PS Series AutoSED.

C.1 Glossary

Data-at-rest – Data recorded on the storage media.

Data-in-motion – Data in transit between two nodes.

Data-in-use – Data being used by a person, an application or an operating system.

Instant secure erase – This feature also permanently changes the Media Encryption Key so the drive can be re-used or re-purposed. After instant secure erase is performed, the data previously written to the drive becomes unreadable. The data has been cryptographically erased.

Local key management – Management of the keys and key linkage between the storage array and the SEDs that it contains (as opposed to an external Key Management System).

Locked drive – An SED in which security has been enabled and the drive has been unexpectedly removed from the storage array, or powered down. Data on the drive cannot be read from or written to until the appropriate Access Key is provided.

Re-purpose – Changes the drive from a secured state to an unsecured state so that it can be safely used for another purpose. This task is accomplished using the instant secure erase feature.

Security-capable drive – A SED that is capable of encryption. (However, this type of drive may not reflect its true status -- it can be either enabled or disabled).

Security-enabled drive – Security on a SED is enabled.

Unlocked – Data on a drive is accessible for all read and write operations.

D Technical Support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Dell TechCenter is an online technical community where IT professionals have access to numerous resources for Dell EMC software, hardware and services.

Storage Solutions Technical Documents on Dell TechCenter provide expertise that helps to ensure customer success on Dell EMC Storage platforms.

D.1 Related resources

PS Series Group Manager Online Help: Keyword “SED”

SNIA key management best practices charts:
http://www.snia.org/images/tutorial_docs/Security/WaltHubis-Best_Practices_Secure_Storage.pdf

“Guidelines for Media Sanitation,” National Institute of Standards and Technology, Computer Security Division. http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

SNIA Guidance and Best Practices http://www.snia.org/forums/ssif/programs/best_practices

Registration is required to download the following documents:

Best Current Practices – Broad guidance to organizations seeking to secure their individual storage arrays, as well as their storage ecosystems

Cryptography and Secret Sharing Algorithm References:

Shamir, Adi (1979). "How to share a secret". Communications of the ACM, Volume 22 Issue 11, Nov. 1979. Pages 612 - 613. ACM New York, NY, USA

Internet Draft Threshold Secret Sharing by David McGrew (draft-mcgrew-tss-03).