DELL PowerVault™ MD32x0 and MD32x0i Series of Arrays:

MD Storage Manager and Self-encrypting Drive Overview

Dell

May 2010

Contents

Figures

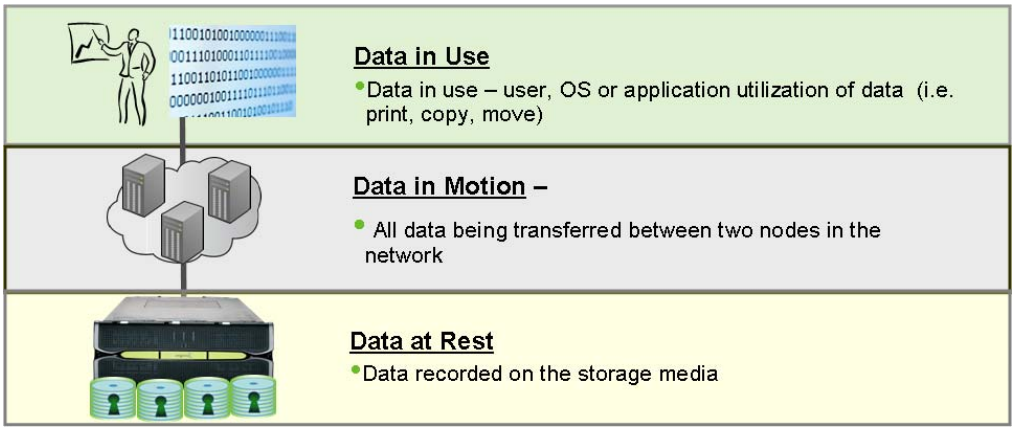
Introduction

Whether it is sensitive customer information, intellectual property, or proprietary data that helps a company reach its strategic objectives, a company's data may be its most valuable asset. If this data is misplaced or stolen, organizations run the risk of lost revenue, legal implications, and a tarnished reputation. The unfortunate truth is that an organization's data is becoming increasingly vulnerable as lost, accidentally exposed, or breached data is becoming more and more commonplace in today's environment. With data security risks on the rise, an influx of government mandates and regulations for securing data have been implemented and are becoming part of the corporate landscape for many. Eliminating exposure of private data is now simply viewed as a sound business practice.

To avoid the high cost and other negative results 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.

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. Data, in fact, 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.

Figure 1. Levels of data to be secured across an organization



The emergence of full disk encryption technology and self-encrypting drives (SEDs) is timely in mitigating the security vulnerabilities of data-at-rest. SEDs adhere to the Trusted Computing Group (TCG) Enterprise Security Storage array Class and provide unparalleled security with government-grade encryption. SEDs are also becoming a standardized technology across many of the world's top drive vendors, which allow for interoperability and ensures greater market competition and competitive pricing.

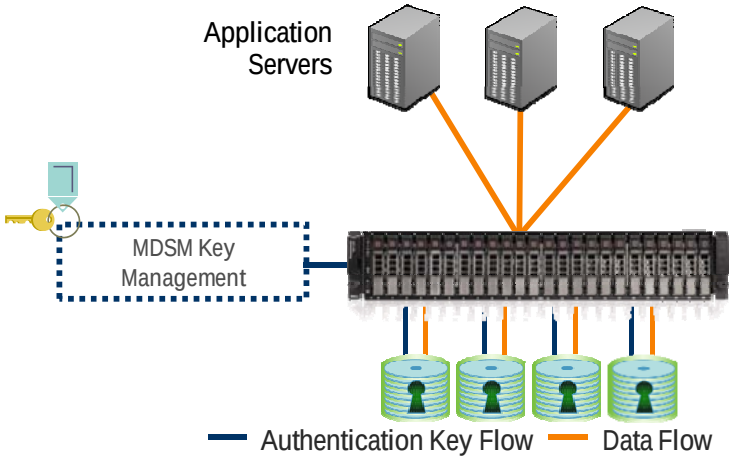
To further strengthen the importance of SEDs, the Storage Networking Industry Association (SNIA) best practices recommend encryption as close to the information source as possible—which is the media where the data resides. In addition, many safe harbor laws, such as California state regulations CA 1798 (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 from the National Institute of Standards and Technology (NIST) which is implemented with a 128-bit encryption key. AES is defined in the NIST publication FIPS 140-2 Level 2(Federal Information Processing Standard) and has been adopted as an encryption standard

MDSM and the SED Solution

While the encryption capabilities of the drives offer high quality security, management of these SEDs is critical to the security's effectiveness. Securing data with SEDs requires a key management service that stores, manages, and serves the appropriate authentications to these drives. In addition to its traditional functions, a storage array's management service also defines secure arrays and invokes the instant secure erase feature when the administrator wants to permanently erase data. In fact, the security capabilities offered with drive-level encryption are only as good as the people and management tools administering them.

As a leader in storage technologies, the PowerVault™ MD3200, MD3220, MD3200i and MD3220i series of storage arrays provide support and management capabilities that secure SEDs allowing users to safely secure their data-at-rest. This support is offered via these arrays with the MD Storage Manager (MDSM) which combines local key management with SEDs. By turning on encryption protection the locking junction has been enabled on the MDSM. The locking function is configured by selecting the appropriate feature on the MDSM console.

Figure 2. MD3220 / MD3220i SED management with MDSM



Together, Dell MDSM and SEDs provide the following benefits:

Assured Security

By embedding the intelligence to manage SEDs in the MDSM, the MD32x0 and MD32x0i series of arrays remove the administrator from most of the daily tasks of securing data, thereby reducing user error or the compromising of data.

High performance

The MD32x0 and MD32x0i series of arrays performance-optimized architecture with SEDs allow for exceptional data security with virtually no performance impact.

Simple

MDSM provides the necessary administration and protection of SEDs by using a single authorization scheme with a simple pass phrase, security key identifier, and security key file that can be set and applied to all SEDs within a MD32x0 and MD32x0i storage array. This process removes the complexity of managing each SED's unique encryption key.

Flexible

For maximum utilization of drive inventory, organizations may continue to use their non-SEDs for data that is deemed not confidential. Having the flexibility to support both SEDs and non-SEDs, the MD32x0 and MD32x0i series of arrays address the needs of tiered and classified data within a single storage device. And when it becomes necessary to secure data residing in a non-SED, the data can be simply migrated to secured SEDs.

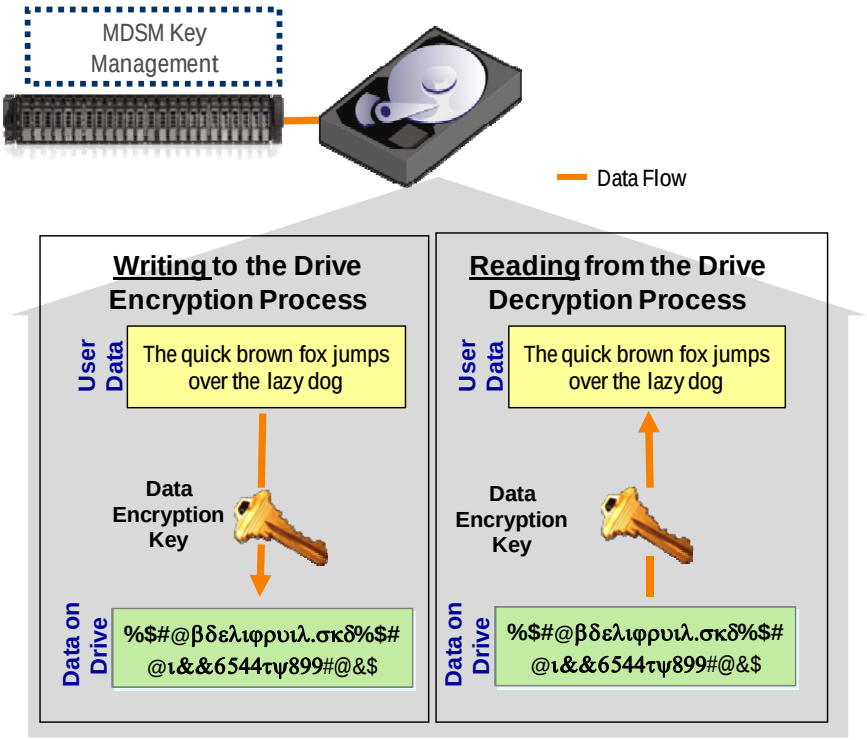
Two methods of data protection

Secure data against a breach

The first method secures data against a breach. Should unauthorized users find themselves with a security-enabled SED that has been removed from the data center; they will find that encryption has rendered the data unreadable.

Each SED randomly generates an encryption key in the factory that is embedded on the drive. The SED automatically performs full drive encryption; when a write is performed, clear text enters the drive and is first encrypted (using the encryption key embedded within the drive) before being written to the drive. When a read is performed, the encrypted data on the drive is decrypted before leaving the drive. If the security is not yet enabled, this process takes place without any authorizations needed.

Figure 3. SEDs at work – Encryption and decryption of the data takes place at all times

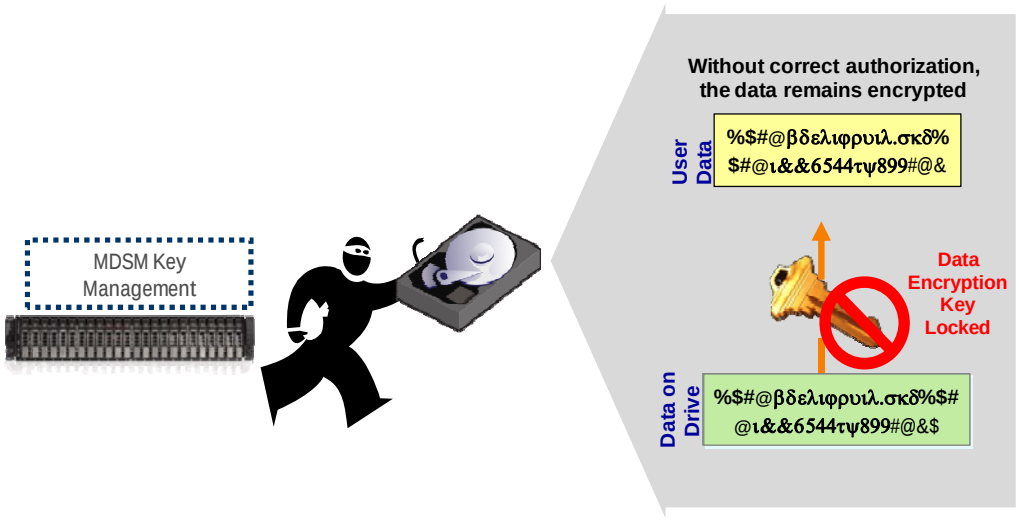


When an administrator decides that data must be protected against a security threat, the administrator would secure the SED. With MDSM, the administrator first enables security on the MD3200 or MD3200i storage array and then secures the specific arrays where the data to be secured resides.

Enabling security on the MD32x0 and MD32x0i array in which an authorization schema is set by the data center administrator can be a simple and one-time process (unless the administrator decides to change the authorization variables at a later date).

After the authentications are set up and security is enabled on an array, the security operations that are taking place across the MD3200 or MD3200i array is transparent to the administrator. The true value of enabling security on SEDs comes when the drive or drives are lost, removed, or stolen. In such an instance, the drives become locked with data being encrypted and unreadable. Because an unauthorized user would not have the appropriate security key file and pass phrase, gaining access to the data is impossible.

Figure 4. A security-enabled SED is removed from the storage array without the correct authorizations



As noted in Figure 4, if the drive is removed from the MD3200 or MD3200i, that drive then becomes locked. Authorizations then must be provided to unlock the drives and read the data. Because an unauthorized user does not have this information, this person is not able to decrypt the data. The drive becomes useless because data cannot be read from or written to the drive.

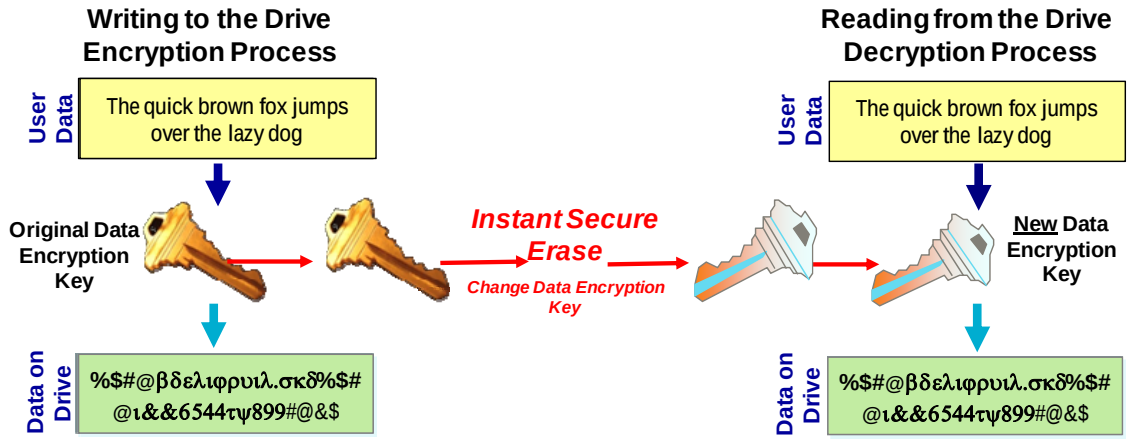
Instant secure erase

Another security method that is available with MDSM and SEDs is instant secure erase. This method protects SEDs from security threats when they are eventually retired, disposed of, sent out for service or repurposed. As these drives are moved from the data center or re-used, it is critical that the data on them is permanently erased and not vulnerable to the recovery of supposedly deleted data. Often times, disposed-of drives still have residual data that can be reconstructed by an unauthorized user. Instant secure erase protects against such threats by permanently encrypting data on the drive.

Alternative methods are available to permanently erase this data; however, these methods often proved to be expensive, slow, and not the highest level of data erasure when the drives were out of the control of the data center administrator and susceptible to a data breach.

Instant secure erase is just that—instant–and it allows for the immediate erasure of data without the drive being removed from the data center or relying on human intervention that is open to error and makes the data vulnerable. With just a few clicks, instant secure erase quickly and simply lets an administer reprovision or dispose of a drive. Cost savings with instant secure erase are often realized because drives are no longer destroyed but instead are reprovisioned to be used again and again. Reprovisioning eliminates the need to destroy a drive, which can now be reused, while still securing warranty and expired lease returns. Instant secure erase can save an organization thousands of dollars in spending on new drive hardware as replacements.

Figure 5. Instant secure erase process



As demonstrated in Figure 5, instant secure erase prompts the SED to permanently erase the current encryption key and replace it with a new one randomly generated within the drive. The encryption key is similar to a decoder key. When the encryption key is changed, any data that has been written to the drive cannot be decoded by the new encryption key rendering the data unreadable. Data that was encrypted with the previous encryption key is now permanently decrypted.

Frequently Asked Questions

Securing and the unsecuring of disk groups

1. When I enable security on a disk group, will the data previously written to that disk group be lost or erased?
   - No, unless you perform an instant secure erase on the drive, this data will remain intact.

MD3200 AND MD3200i supported SEDs

- 146GB 2.5" 15K
- 300GB 2.5" 10K
- 450, 600 GB 3.5" 15K
- 500GB 2.5" NLSAS
- 1TB, 2TB 3.5" NLSAS

2. Can I make a secure disk group with SEDs a non-secure disk group?
   - No, this option is not supported. It is recommended that you make a Virtual Disk Copy of the secure data to a non-secure disk group. If you would like to return this data to the original drive, you would then delete the original disk group and perform an instant secure erase on the drives, which makes them unassigned drives. You then can create a virtual disk copy of this data back to these drives after creating a new disk group.

3. If I have a disk group with SEDs that is secured, can I create another disk group across these same drives and not enable security?
   - No, this function is not supported. Any disk group or logical drive that is created in security-enabled SEDs must also be secured.

4. When a secure disk group is deleted, does the drive security remain enabled?
   - Yes. The only way to disable security is to perform an instant secure erase that will re-provision these drives.

5. If I create a new virtual disk on a set of security-enabled SEDs (secured virtual disk group, will they automatically become secure?
   - Yes.

Instant secure erase

1. With instant secure erase, what can I erase…an individual drive, a disk group?

- Instant secure erase occurs on a drive-by-drive basis. It is not possible to perform an instant secure erase on an SED that houses part of a secure disk group. You must first delete the disk group. After the disk group is deleted and the drives then become unassigned, you can erase the drive. You can erase multiple drives at the same time by holding down the Ctrl key.

2. If I want to use only the instant secure erase feature, do I still need to set up a security key ID, pass phrase and security key backup file?
   - Yes.

3. After instant secure erase is applied to a drive, will security be enabled or disabled on that drive?
   - Because the drive will be returned to the factory state when the instant secure erase feature is applied, it will be security disabled.

Access to data, keys, and pass phrases

1. Can I get to the security keys through the MDSM or the controller?
   - SED covers the data-at-rest level of security only. It is, therefore, recommended to address prudent security features for the storage array management. The MDSM will force a strong password, but an administrator's access should have stringent controls in place.

2. What if I forget my security key identifier, pass phrase and security key backup file?
   - If the user has access to the MDSM, they can change the security key pass phrase and file. Select **Storage array >> Physical Disk Security >> Change Security Key**. Additional steps will then prompt the user to change both the security key pass phrase and the security key file. Record and track this information. It is recommended to keep more than one copy of the pass phrase and security key backup file.

3. What if I lose a drive that is unlocked or security disabled? Can that data be accessed even though the data is encrypted?
   - Yes. This data is still accessible because the drive's security has not been enabled. The drive remains unlocked, and the data is accessible.

4. What if my security key falls into the wrong hands, can I change it without losing my data?
   - Yes. If the drive is still powered on and residing in a MD3200 or MD3200i, it can be rekeyed. Refer to the response to question 2 in this section.

Premium features

1. Can I make a Virtual Disk Copy of a “secure” virtual disk to a non-secure one? If so, what is preventing someone from doing that first, and then stealing the non-secure copy?
   - Yes.
     To prevent someone from stealing the data using this method, it is recommended to address prudent security features for the storage array management. The MDSM will force a strong password, but an administrator’s access should have stringent controls in place.

2. Can Snapshot and Virtual Disk Copy data be secured? Any recommendations?
   - Yes.
     For Snapshot, the Snapshot repository data must be secured if the target Snapshot data is secured. The MDSM will enforce this. There are no specific recommendations for Virtual Disk Copy beyond the standard best practices and processes.

Hot spares

1. Because the hot spare in a secured disk group is a non-secured SED, does this drive automatically become secured after a secured SED fails and that data is written to the hot spare?
   - The security on a hot spare SED is enabled before the rebuild is started. A rebuild cannot be initiated on a non-SED for a secure disk group. Therefore, the data is secured both in terms of availability (RAID) and in terms of secure access (SED).

Boot support

1. Is there a special process for booting data from a security-enabled drive?
   - No. The only requirement is that the storage array must be running (which is required in any booting process).

2. Are my SEDs susceptible to cold boot attacks?
   - This event occur more on the server side as an individual can come up with his or her own boot image to gain access to the server. This event does not apply to SEDs. SEDs do not use the type of memory that is susceptible to a “cold-boot” attack.

Locked and unlocked states

1. When does a security-enabled drive go into a locked state in which it will require the pass phrase, and so on?
   - The drive is locked whenever the drive is powered down. In other words, the moment that the SED is switched off or unplugged, it automatically locks down the drive's data.

Backup and recovery

1. How can I ensure that my archived data is secure?
   - This problem is outside the scope of this document. Refer to SNIA secure backup, which provides more tape-related recommendations.

Other

1. What encryption algorithm is used by SEDs?
   - The Advanced Encryption Standard (AES) from National Institute of Standards and Technology (NIST) is implemented with a 128-bit encryption key. AES is defined in the NIST publication FIPS (Federal Information Processing Standard) and has been adopted internationally as an encryption standard.

2. Why was AES-128 implemented instead of AES-256?
   - Both the United States National Security Agency NSA and NIST have asserted that AES-128 provides sufficient protection. There are 2^128 = 3.4 x 10^38 possible keys with 128 bits, which is a huge key space. NIST estimates that AES 128 is safe from key-search techniques for at least the next 30 years. In addition, AES-256 requires four more iterations of the core AES algorithm than does AES-128, which would slightly reduce the throughput and increase the cost of the product.

3. Does the SED functionality affect drive performance?
   - No. Because the AES algorithm was chosen by NIST as optimal for hardware implementations, and the SED has its AES engine built into the electronics, the throughput affect is imperceptibly small (a few millionths of a second). SEDs operate at the same throughput and response time levels as non-SEDs. Furthermore, the incorporation of the encryption into the drives (versus other encryption methods) means that encryption horsepower scales perfectly with the number of drives in the system.

4. How many bits of encryption reside on the drive?
   - Refer to the drive vendor specifications.

5. Is DACstore information still written to the drive?
   - Yes.

6. Is data on the controller's cache secure with SED and MDSM?
   - No, because this is a security issue of the physical access to the hardware. It is recommended that the administrator have physical control and security of the storage disk group itself.

7. What about data classification?
   - Because all data written to an SED is encrypted, the requirement for data classification may be reduced. Refer to SNIA best practices, which are provided in an appendix of this guide.

8. Can I mix SED and non-SEDs if I do not secure the drives?
   - Yes, however, this action is not cost-effective or a good use of SEDs and is not recommended.

9. Do SEDs have lower usable capacity because the data is encrypted or capacity is needed for the encryption engine and keys?
   - No. There is no capacity difference (i.e., 1 GB unencrypted = 1 GB encrypted).

Appendix A – Key Terms and Glossary

Key terms

Term	Definition and how is it used	Where is it located and managed	How it is generated
Encryption key	Required to encrypt and decrypt data ▪ Similar to a decoder	Resides on and is 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 and then regenerated at the customer site if desired with the instant secure erase feature (this action ensures that the key was not compromised prior to use)
Security key	Needed to unlock a drive ▪ Its hashed version can be provided to the drive from the storage disk group after the user provides the correct security key identifier, pass phrase and backup file. The drive then confirms if its hashed security key and the provided hashed security key are one and the same to allow encrypting/decrypting.	A hashed version of the key is housed on both the drive and controller (to protect it from hackers) A single lock key is synchronized across the controllers	Created and negotiated by the controller and the drive
Security key identifier	Needed to unlock a SED	Saved in the security key backup file and the administrator to record in a safe location	Generated by the administrator and the storage disk group adds a WWID and a randomly generated number

Pass phrase	Needed to unlock a SED	The administrator to record in a safe location	Generated by the administrator and storage disk group
Security key file	Needed to unlock a SED ▪ A file location where the security key identifier and pass phrase are saved	Created by the administrator	The file location is determined after the creation of the security key ID and the pass phrase

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.
- SED – A custom chip or ASIC on every drive that requires the correct authorization information (sometimes referred to generally as the key) to let activity begin. SED encrypts all of the data on a drive. The secured SED requires a secret password to be supplied by the initiator before any read or write operation can be performed. The encryption and decryption of data is processed entirely by the drive and appears transparent to the array.
- Hash – Hashing creates a constant-length hash representing a checksum for the data. You cannot re-create the original data from the hash, but you can hash the data again to see if the same hash value is generated.
- Instant secure erase – Permanently encrypts data (erased) when the encryption key is changed, which also changes the encryption algorithm permanently drive can be serviceable or repurposed. After instant secure erase, the data that had been written to the drive is unreadable and the drive is in an unsecured state, just as it was delivered from the factory.
- Local key management – Management of the keys and key linkage between the storage arrays and the SEDs.
- Locked drive – An SED in which security has been enabled and the drive has been removed from the storage array or powered down. Data on this drive cannot be read from or written to until the appropriate authorization information is provided.
- Re-provision – Makes drives fully reusable. Previous data and key are not accessible.
- Repurpose drive – Change the drive from being in a secured state to an unsecured state so that someone else can use the drive. This task would be accomplished using instant secure erase.
- Secure disk group– Any disk group residing 0n secured SEDs.

- Security capable drive – A SED that is capable of encryption (however, this type of drive does not reflect its status as it can be enabled or disabled).
- Security-enabled drive – The security on a SED is enabled.
- Security locked state – Occurs whenever the power is turned off and turned on again, all of the security enabled drives change to a security-locked state in which the data is inaccessible until the correct security key information is provided by the controller.
- Unlocked – Data on the drive is accessible for all read and write operations.

Appendix B – Next steps and Additional Resources

SNIA key management best practices charts are in
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 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