Overview of Self-Encrypting Drive Management on Dell PowerVault™ Storage Arrays

Dell PowerVault™ MD3 Series of Arrays

Dell Engineering
June 2015

A Dell Technical White Paper

A Dell Technical White Paper

Table of contents

1 Introduction

Whether it is sensitive customer information, intellectual property, or proprietary data that helps a company reach its strategic objectives, a company's data is often 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. 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.

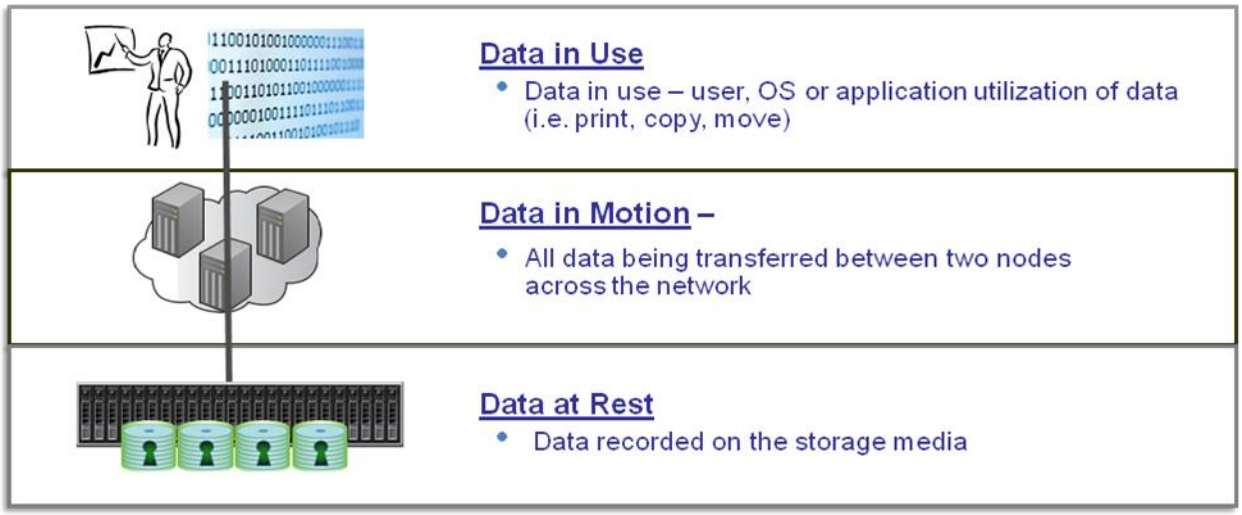

Figure 1 Levels of data to be secured across an organization

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 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 from the National Institute of Standards and Technology (NIST). AES is defined in the NIST publication FIPS 140-2.

Level 2 (Federal Information Processing Standard) and has been adopted as an encryption standard. The SEDs are also approved for FIPS 140-2 Level 2 and found acceptable by the National Security Agency NSA for use with sensitive and or classified national security data.

2 MD Storage Manager 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 Dell PowerVault™ MD3 Series of Arrays provide support and management capabilities that allow users to safely secure their data-at-rest. This support is offered via MD Storage Manager (MDSM), which combines local key management with SEDs. By turning on encryption protection, the locking junction is enabled in MDSM by selecting the appropriate option in the MDSM user interface.

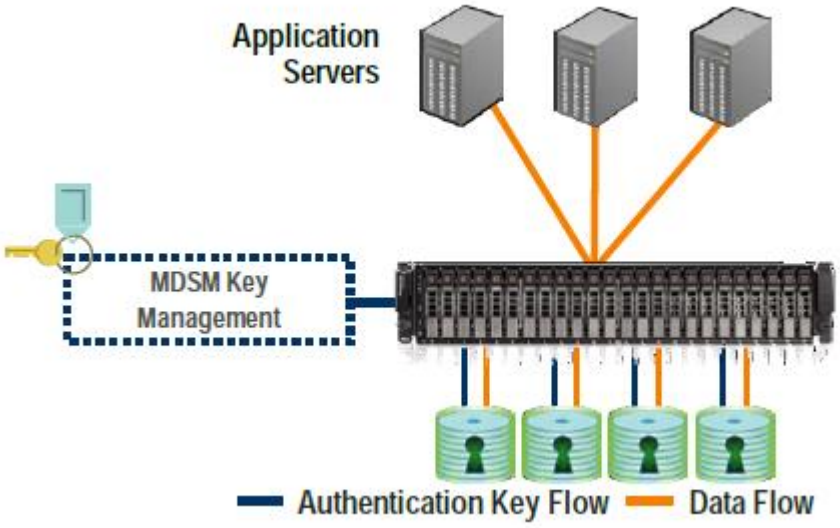

Figure 2 Dell PowerVault MD3 Series of Arrays' SED Management with MDSM

Together, Dell MDSM and SEDs provide benefits including assured security, high performance, simplicity, and flexibility.

2.1 Assured security

By embedding the intelligence to manage SEDs in MDSM, the Dell PowerVault™ MD3 Series of Arrays remove the administrator from most of the daily tasks of securing data. This reduces the likelihood of user error and inadvertent data compromise.

2.2 High performance

The Dell PowerVault™ MD3 Series of Arrays' performance-optimized architecture, combined with the use of SEDs, provides exceptional data security with virtually no performance impact.

2.3 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 any of the Dell individual arrays. This process removes the complexity of managing each SED's unique encryption key.

2.4 Flexible

For maximum drive utilization, organizations may continue to use their non-SEDs for data that is non- confidential. This flexibility in supporting both SEDs and non-SEDs allows the Dell PowerVault™ MD3 Series of Arrays to address the needs of both tiered and classified data within a single storage device. Should it become necessary to secure data residing in a non-SED, that data can be simply migrated to a secure SED.

3 Two methods of data protection

3.1 Secure data against breach

The first method of data protection secures data against a breach. Should unauthorized users come into possession of a security-enabled SED that has been removed from the data center; an embedded encryption key on the drive itself will render its data unreadable.

Each SED randomly generates its own encryption key and self-embeds that key before leaving the manufacturer.

The SED is then able to automatically perform full-drive encryption in the following way:

1. When a write is performed, clear text enters the drive and is encrypted (by the drive's own encryption key) before being written to the drive.
2. When a read is performed, the encrypted data on the drive is decrypted before leaving the drive. If the security is not yet enabled on the storage array, this process takes place without requiring any authorizations.

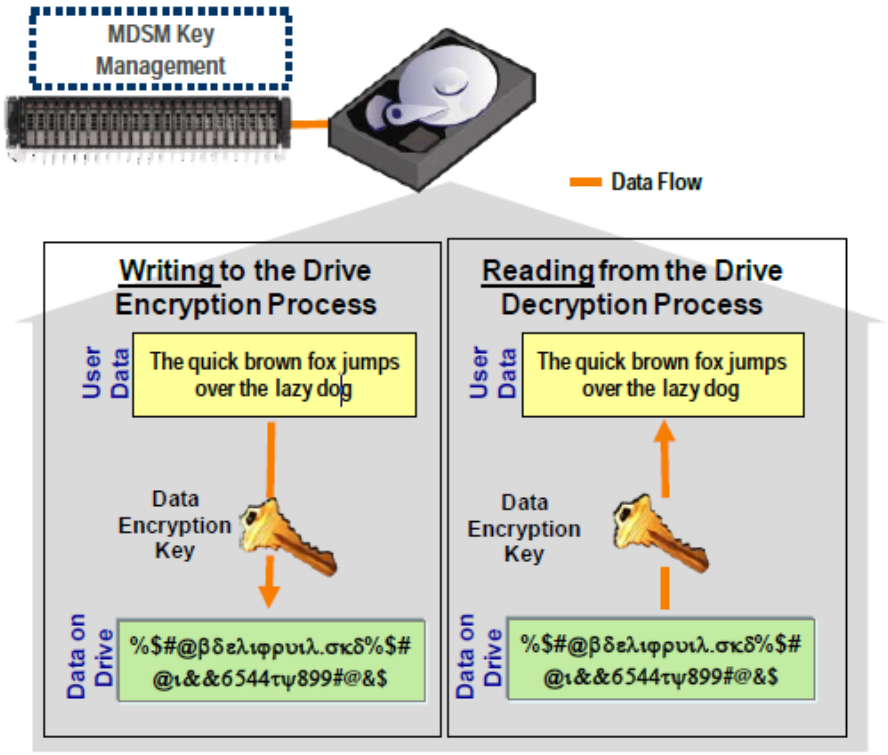

Figure 3 SEDs at work – Encryption and Decryption of the data takes place at all times

When an administrator decides that data must be protected against a security threat, the administrator secures the SED. Using MDSM, the administrator first enables security on any of the Dell PowerVault™ MD3 Series of Arrays, then secures the specific arrays where the data resides.

Enabling security on any of the Dell PowerVault™ MD3 Series of Arrays in which an authorization schema is set by the data center administrator can be a simple, 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 taking place across all of the Dell PowerVault™ MD3 Series of Arrays are transparent. The true value of enabling security on SEDs comes 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 security key file and pass phrase, gaining access to the data is impossible.

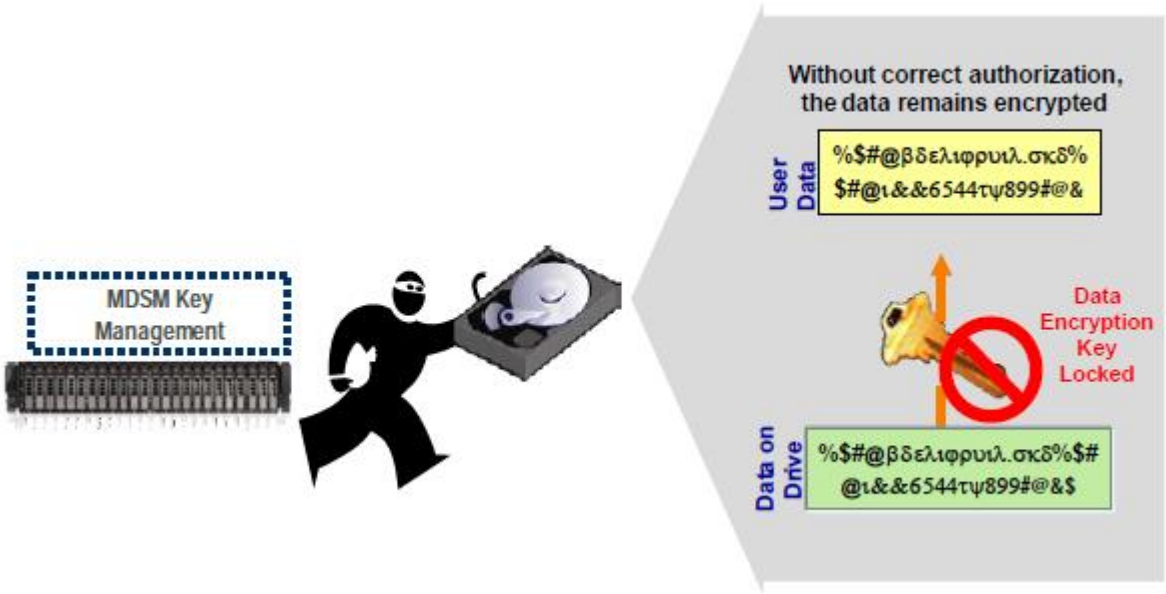

Figure 4 A removed security-enabled SED without the correct authorizations

Once a drive is removed and becomes locked, specific authorization must be provided to unlock the drive and read the data.

3.2 Instant Secure Erase

Another security method available with MDSM and SEDs is instant secure erase. This method protects SEDs from security threats when they are retired, disposed of, sent out for service, or re-purposed. 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 recovery, even when supposedly deleted. Often, 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 are expensive, slow, or do not provide the highest level of data erasure.

Instant secure erase is just that – instant – and allows for the immediate erasure of data without the drive being removed from the data center or relying on human intervention. With just a few clicks, instant secure erase will quickly erase all the data on the drive and the administrator can re-provision or dispose of a drive. Cost savings are realized since drives no longer need to be destroyed, but instead can be safely re-provisioned for re-use. Re-provisioning can help maintain warranty life and extend the lifespan of expired lease returns, saving an organization thousands of dollars in hardware replacement costs.

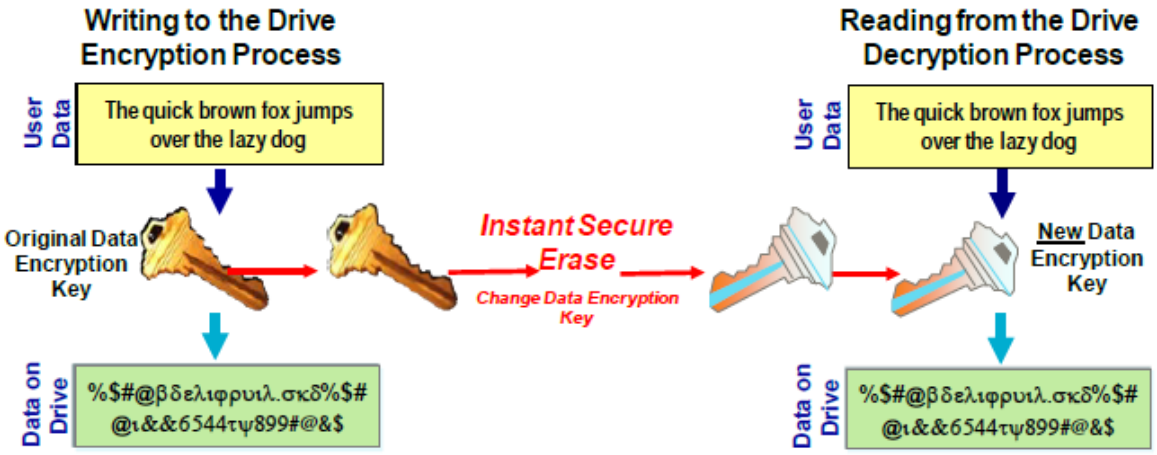

Figure 5 Instant Secure Erase Process

As demonstrated in Figure 5, instant secure erase prompts the SED to permanently erase the current encryption key and replace it with a new, randomly generated key 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 deleted.

4 Frequently asked questions

4.1 Securing and unsecuring 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.

2. Can I make a secure disk group with SEDs a non-secure disk group?

   No, this option is not supported. Alternatively, you can make a Virtual Disk Copy of the secure data to a non-secure disk group. To return the copied data to the original drive, delete the original secure disk group and perform an instant secure erase on the drives. This will make them unassigned drives. You can then create a new non-secure disk group and perform another Virtual Disk Copy of the original, once-secure data back to those drives.

3. If I have a disk group with SEDs that is secured, can I create another disk group across these same drives but 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 drive 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.

4.2 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. Instead, you must first delete the disk group. After the disk group is deleted, the drives will become unassigned. Then, you can erase the drive.

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?

   Applying instant secure erase to a drive returns it to its factory state. Therefore, it will be security disabled.

4.3 Access to data, keys, and pass phrases

1. Can I access the security keys through the MDSM or the controller?

   Yes. SED covers the data-at-rest level of security only. It is, therefore, recommended to address prudent security features for the storage array management.

2. What if I forget my security key identifier and/or pass phrase, and cannot access my security key backup file?

   If the user has access to 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 any of the Dell PowerVault™ MD3 Series of Arrays, it can be rekeyed. Refer to the response to question 2 in this section.

4.4 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, then stealing the non-secure copy?

   Yes. SEDs only protect data that resides on them. To prevent someone from stealing the data using this method, it is recommended to address prudent security features for the storage array management.

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. MDSM will enforce this. For Virtual Disk Copy, the data must be secured after the copy has finished. MDSM does not force this.

4.5 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 in terms of availability (RAID) and secure access (SED).

4.6 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 (required in any booting process).

2. Are my SEDs susceptible to cold boot attacks?

   These attacks occur more frequently on the server, where an individual can generate a boot image to gain access. SEDs do not use the type of memory that is susceptible to a "cold-boot" attack.

4.7 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/or other security credentials?

   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.

4.8 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 the Storage Networking Industry Association (SNIA) secure backup best practices, which provide tape-related recommendations.

4.9 Other

1. What encryption algorithm is used by SEDs?

   The Advanced Encryption Standard (AES) from National Institute of Standards and Technology (NIST) is implemented. AES is defined in the NIST publication FIPS (Federal Information Processing Standard) and has been adopted internationally as an encryption standard.

2. 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 its electronics, the throughput effect 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.

3. How many bits of encryption reside on the drive?

   Refer to the drive manufacturer's specifications.

4. Is data on the RAID controller cache secure with SED and MDSM?

   No. This is a security issue surrounding physical access to the hardware. It is recommended that data administrators maintain strict control over access to the storage disk group array hardware.

5. 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 to this guide.

6. Can I mix SED and non-SEDs if I do not secure the drives?

   Yes. However, it is not recommended and is neither cost-effective or a good use of SEDs.

7. Do SEDs have lower usable capacity because the data is encrypted, or because capacity is needed for the encryption engine and keys?

   No. There is no capacity difference.

5 Appendix A: Key terms and glossary

See table below for key terms.

Term	Definition and Usage	Location and Management	How it is Generated
Encryption key	Required to encrypt and decrypt data • Similar to a decoder	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 (ensures 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 before allowing encryption/decryption	Hashed version of the key is contained on both the drive and RAID controller (to protect it from hackers) A single lock key is synchronized across the controllers	Created and negotiated by the RAID controller and drive
Security key identifier	Needed to unlock SED	Saved in the security key backup file and recorded by administrator in safe location	Generated by the administrator, storage disk group adds a WWID and randomly generated number
Pass phrase	Needed to unlock SED	Recorded by administrator in a safe location	Generated by the administrator and storage disk group

Security key file	Needed to unlock SED	Created by the administrator and saved to file location with the security key identifier and pass phrase	File location determined after creation of the security key ID and pass phrase

5.1 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.

SED – A drive that encrypts all of the data sent to it. The secured SED requires a secret password to be supplied by the initiator before any secured read or write operation can be performed. The encryption and decryption of data is processed entirely by the drive and is 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 (in effect, erasing it) when the encryption key is changed. This feature also permanently changes the encryption algorithm 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 and the drive reverts to an unsecured state, just as it was delivered from the manufacturer.

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 the 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.

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.

Secure disk group– Any disk group residing on secured SEDs.

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.

Security-locked state – Occurs whenever power to a drive is turned off and turned on again. When this happens, all security-enabled drives are changed to a security-locked state in which the data is inaccessible until the correct security key information is provided by the RAID controller.

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

6 Appendix B: Next steps and additional resources

Guidelines for Media Sanitation National Institute of Standards and Technology, Computer Security Division.

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