WHITE PAPER

NEXSAN™
by imation

E-SERIES ENCRYPTION

imation

INTRODUCTION

This paper describes the use-cases and implementation of self-encrypting drive (SED) support in the E-Series V software, implemented in version R011.1204 and later. SEDs can provide protection for data when drives leave the control of the user, whether intentionally or if stolen. As a consequence of encryption, data can also be securely erased in the event of repurposing of a drive or set of drives.

OVERVIEW

E-Series software supports SEDs to provide data-at-rest protection of user data on supported SAS HDDs or SSDs, once a drive has left the control of the user. This is enabled on a per-RAID set basis, and the complete system can include both SED and non-SED arrays. All drives in an encrypted array must be SEDs. It is possible to enable or disable array encryption at any time, without affecting the user data on the system.

SED OVERVIEW

SEDs are available from all major HDD and SSD vendors. A SED always performs encryption of all data as it is written to the media, regardless of any system or user involvement. At manufacturing time (or on demand) the drive creates a Data Encryption Key (DEK) that it stores internally to the drive, and it uses this key to encrypt and decrypt all data as it is written or read. By default, all SEDs operate identically to a non-SED drive, and can be used in non-SED mode. Since all encryption is handled in hardware, there is no performance impact to using the encryption feature.

To use the drive in a secure mode, it is necessary to lock the drive. To do this, an Authentication Key (AK) is created by the drive management software (controller software in the case of E-Series V). This AK is used to encrypt the DEK, which is also typically changed at the time of locking. For more details on this process, refer to page 4.

USE CASES

There are a number of common use cases for SEDs, all associated with protecting data in various situations. The most typical use cases are described below. All drives in an encrypted array must be SEDs. It is possible to enable or disable array encryption at any time, without affecting the user data on the system.

PROTECTION OF DATA ON DRIVES RETURNED FOR RMA

When drives fail in an array during the warranty period, they are typically returned to the manufacturer for replacement. Often, data is still present and recoverable on the drives. Even drives that have been used in a RAID level that uses striping can have significant amount of recoverable user data, since the large stripe sizes used are sufficient to contain large fragments of files or databases. If these drives are part of an encrypted array, then any data on them is not accessible without the key, which is not stored on the drive. Therefore access to the drive's user data is prevented.

PROTECTION OF DATA ON STOLEN DRIVES

If one or more drives from an encrypted array are stolen, then any data on them is not accessible without the key, which is not stored on any of the drives. This prevents access to the user data. Note that physical or administrative access to the complete system including the controllers does not protect from unauthorized access, since the storage system controller automatically unlocks the drives once the system is powered on. Appropriate security practices must still be employed to secure data path access to the storage system.

DRIVE RETIREMENT OR REPURPOSING

If an encrypted array of drives is deleted, part of the deletion process ensures the drive's encryption key (DEK) is changed. This immediately ensures that the contents of the drive cannot be read, and the drive can be safely repurposed or removed from the system with no risk of exposing previous user data. An individual unused drive can also have its encryption key (DEK) changed to perform a secure erase. Without SEDs, drive retirement can take a significant amount of time to overwrite the data, and there is no guarantee that all data is erased. Secure warehousing of the drive is expensive and means the drive cannot be reused and physical destruction before the end of its useful life is wasteful.

SECURE SHIPMENT

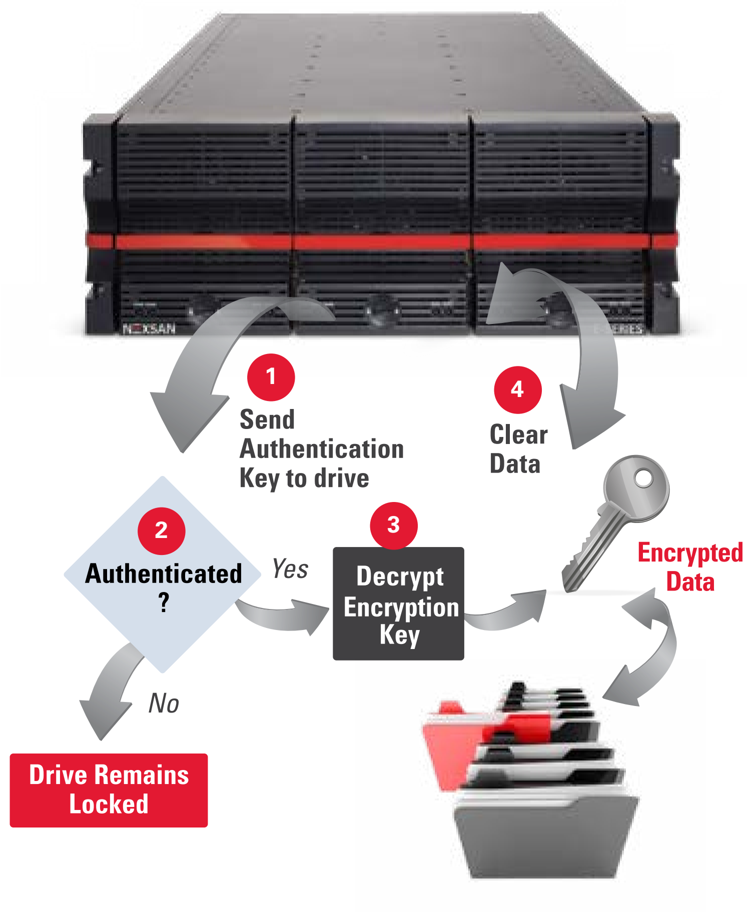
Company mergers and consolidation can often lead to a requirement to move storage systems between datacenters. This poses a challenge where confidential data is stored on the drives. Using SEDs, it is possible to securely ship the drives without using secure shipping solutions and incurring the associated additional shipment costs. To ensure security of the data if drives are stolen in transit, controllers that contain the keys must be shipped separately.

(Rev. 09/11/15)

DRIVE UNLOCKING

The diagram below illustrates the process of unlocking and accessing data on a locked SED. The E-Series software automatically unlocks an array when it is powered on, so no additional user interaction is required to use the array encryption functionality. The drive stores the encrypted copy of the DEK internally, and uses the AK to validate whether to unlock the drive. Once unlocked, the drive remains unlocked until it is powered off. Every time the system needs to unlock the drive, it must provide the AK. The AK can be changed at any time, and since it is only used to encrypt the DEK, the underlying data remains unaffected. For ease of management, the same AK may be used for a number of drives. The drive does not store the AK internally, it stores a hash of the AK to use for validation, and once the AK is validated, it uses the provided AK to decrypt the DEK.

1. The controller sends the Authentication Key (AK) to the drive.
2. The drive hashes the authentication key and compares it with its stored hash to validate.
3. If the authentication is validated, the drive uses the provided authentication key to decrypt the DEK, stored on the drive media.
4. From this point, the drive automatically encrypts and decrypts all data passing through it.



(Rev. 09/11/15)

KEY GENERATION AND STORAGE

The per-array authentication key (AK) is generated internally on the controller, and is stored in a private area on each controller. For redundancy, this is mirrored in the partner controller, so the system can automatically unlock the array in the event of controller failure. A replacement controller will automatically have the necessary keys installed.

When an encrypted array is created or an array's AK is changed, it is strongly recommended to download and make a backup of the key. This key should be securely stored in compliance with the user's normal security practices, and a fresh backup made as it is changed. The AK can be changed at any time, if this is necessary for compliance with security practices. Whenever a key is created or changed, the user is prompted to download the key file for storage. Access to this file should be restricted to ensure the keys are kept private.

REFERENCES

Trusted Computing Group (TCG) SED specifications:

http://www.trustedcomputinggroup.org/solutions/data_protection

ABOUT IMATION

Imation is a global data storage and information security company. Imation's Nexsan portfolio features solid-state optimized unified hybrid storage systems, secure automated archive solutions and high-density enterprise storage arrays. Nexsan solutions are ideal for mission-critical IT applications such as virtualization, cloud, databases, and collaboration; and energy efficient, high-density storage for backup and archiving. There are more than 11,000 customers of Nexsan solutions worldwide with more than 33,000 systems deployed since 1999. Nexsan systems are delivered through a worldwide network of cloud service providers, value-added resellers and solutions integrators. For more information, visit www.imation.com/nexsan.

(Rev. 09/11/15)