Storage Security Capabilities of AES-256 Self Encrypting Drives

Abstract

StorePak and StoreEngine provide a variety of features that help protect stored data, also known as data-at-rest. These features leverage the capabilities of AES-256 Encrypted SSDs along with Critical I/O provided security and authentication management software utility.

Note that the specific program requirements for securing data-at-rest vary dramatically from project to project. The purpose of this paper is to describe the security capabilities available within the StoreEngine and StorePak products. It is always up to user to determine the applicability of these capabilities to their individual program.

Data Security Features of StoreEngine and StorePak

StorePak and StoreEngine provide a variety of features that help protect stored data, also known as data-at-rest. These features leverage the capabilities of AES-256 Encrypted SSDs along with Critical I/O provided security and authentication management software utility.

Data-at-Rest Security

There are two protection concerns with respect to data-at-rest. The first and most obvious is to protect the data against theft or compromise. The second is to protect data against unintended alteration or deletion (whether accidental or otherwise). Both of these goals can be addressed to varying degrees by using one or both of two main techniques:

***Physical* Protection** – This protection is facilitated either by: 1) ensuring that the data storage media is used and permanently located in an appropriately secure facility, or 2) physically transporting the data storage media as needed to a secure facility for storage of the media.

***Encryption/Key* Protection** – This protection is facilitated by storing data on the media using an appropriate encryption method, with auxiliary mechanisms to "lock" access to the media, and to require a appropriate key to be provided to attain access to the media.

Critical I/O's StorePak products facilitate physical protection via their easily removable and hot-swappable SSD storage cartridge. Critical I/O StorePak and StoreEngine products also provide Encryption/Key protection through the use of Self-Encrypting Drive SSDs (SEDs) combined with storage and key management utilities.

SSD Based Security Implementation and Conformance/Certification Levels

Storage security can be thought of as having two largely orthogonal aspects. First, the *specific mechanisms* that are provided by the storage hardware (including self-encrypting SSDs). And second, the *conformance/certification* aspects of the implementation of these mechanisms (i.e. TCG, FIPS, NSA, etc.).

Solid State Drive (SSD) Built-in Security Mechanisms

The level of SSD security implementations fall into three main categories:

None – Self-explanatory. No encryption or password capability. This category of SSDs is not recommended for data sensitive applications.

Password Protection – The SSD implements an ATA drive password. Drives that implement password only capabilities are resistant only to a casual attempt to gain access to stored data. They are not considered secure in the face of any serious attack for two reasons: 1) possible existence of backdoors that are sometimes provided by drive manufacturers for data recovery purposes, or 2) their vulnerability to physical removal or probing of flash chips, as the data in these SSDs is stored in plain unencrypted form. This category of SSDs is also not recommended for data sensitive applications.

Full Drive Encryption - (FDE, also known as Self Encrypting Drives or SEDs) – SEDs also implement a password (aka Authentication Key), but in addition they implement an encryption mechanism based on a Media Encryption Key which is used to encrypt all data stored on the SSD, typically using an AES-256 encryption algorithm. This category of SSDs can be suitable for selected data sensitive applications.

Solid State Drive Security *Assurance/Certification* Levels

There are several standards the deal with the implementation and validation of the security aspects of data transmission and storage systems. These standards are relevant to varying degrees to SSD based data storage systems.

TCG-Opal – The Trusted Computing Group (TCG) Opal specification defines standards specifically for the implementation of security features for self-encrypting drives (SEDs). These standards are designed to protect the confidentially of data stored on the SSD device. The Opal specification encompasses these main aspects of security implementation:

- Cryptographic features
- Authentication features
- Access control features

FIPS-140-2 – The Federal Information Processing Standard (FIPS) Publication 140-2 is defines requirements to accredit cryptographic modules. FIPS-140-2 goes beyond TCG-Opal in that, in addition to defining security functional requirements (as does TCG-Opal) it also defines a strict certification process to which a device must be subjected prior to claiming FIPS certification. FIPS-140-2 provides four levels of security. Level 1 is the lowest level and covers only the basic security algorithm implementation. Higher levels 2 through 4 add increasingly extensive physical security requirements such as tamper detection. A small selection of encryption capable FIPS-140-2 approved SSDs is available.

NSA Type 1 – A National Security Agency (NSA) categorizes encryption products into four product types. A NSA Type 1 product provides the highest level of data security. A NSA Type 1 certified product, when appropriately keyed, is approved by NSA for the encryption and decryption of classified information. Type 1 security capabilities are not currently available as "built-in" features of SSDs.

Overview of Self-Encrypting Drives (SEDs)

Critical I/O's StoreEngine and StorePak products can leverage Self Encrypting Drive (SEDs) to help protect sensitive data. A self-encrypting SSD has logic built into the SSD controller that encrypts all data to the flash media, and automatically decrypts all the data from the media using an AES-256 algorithm. SEDs encrypt all data all the time, with the encryption being completely transparent or invisible to the user, and SSD performance unaffected.

SEDs can be used as an integral part of a data-at-rest security implementation. Depending on the specific model, an SED may be TCG-Opal compliant, ensuring the implementation of common set of security features. Or, it may be FIPS-140-2 certified ensuring that the implementation of these features has been fully validated. Or, an SED SSD may have no particular compliance at all but simply implement a set of encryption and authentication features.

The mechanization of the SSD security features as described in this paper is typical of currently available SSDs, with minor variations in the details of the implementation dependent on the specific SSD supplier.

Use of SEDs within StoreEngine and StorePak

When StoreEngine or StorePak are configured to use SEDs, they provide automatic full AES-256 encryption of all stored data. This basic encryption capability is supplemented with mechanisms to set a SSD Authentication Key (A-key), to lock and unlock drives using the user defined A-key, and to initiate a secure cryptographic erase of the SSDs. These mechanisms are implemented in the form of a Security Manager

utility that runs on the StoreEngine (for Recording and NAS applications) or on the user's SBC (for DAS applications)

The Security Manager utility provides for these capabilities:

- Set/change/remove SSD Authentication Keys
- Ability to receive it via Ethernet network command or from a USB drive
- Ability to optionally store A-key locally in non-volatile storage
- Ability to erase locally stored A-key
- Lock/unlock SSDs
- Initiate secure cryptographic erase of SSDs

All of the Security Manager operations may be invoked via several methods:

- StoreEngine web-based storage management interface
- Ethernet commands
- For DAS applications, a local API that the user's application can call directly

Figure 1 below illustrates the Security Manger utility in the context of unlocking and using encrypted SSDs in a StoreEngine/StorePak application. In this example, the StorePak SSDs have previously been set with an Authentication Key. Thereafter, when powered up the StorePak SSDs will be locked and data on them will be inaccessible. Before the SSDs can be accessed, they must each be provided the correct A-key. This is done via the Security Manager, which either retrieves the key locally from flash storage (optional) or receives the key via a network command, or retrieves the key from a removable USB drive.

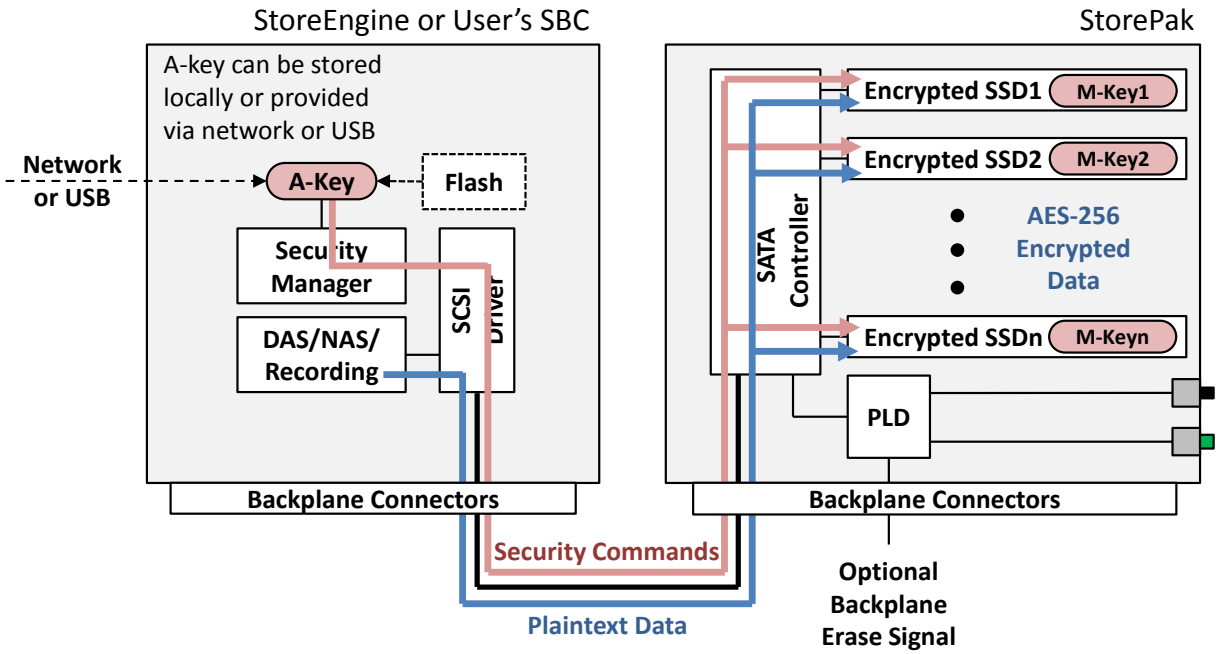

Figure 1: Use of Self Encrypting Drives (SED) within a StorePak

How SEDs Help to Provide Data-at-Rest Security

SEDs automatically encrypt all user data using an AES-256 encryption algorithm. The data encryption key used in SEDs is called the Media Encryption Key (M-key). Locking and unlocking a drive requires a different 32 byte key, called the Authentication Key (A-key) which is defined and supplied by the user (or the host platform, or the network).

SEDs do all the cryptography within the SSD controller, which means the disk encryption keys are never present in the computer's processor or memory, where they could be compromised. Authentication of the user provided Authentication Key is also done within the SED and never exposed within the memory or operating system of the host StoreEngine or SBC.

The contents of an SED are always encrypted and the encryption keys themselves are always stored encrypted on the SED. Neither the M-key nor the A-key can ever be retrieved from the SED by the user.

The specific security operations supported by SEDs include:

- Set Authentication Key (A-key)
- Lock (both upon command and after power cycle)
- Unlock (using A-key)
- Write/Encrypt user data using Media Key (M-key)
- Read/Decrypt user data using M-key
- Change Authentication Key
- Secure Erase (cryptographic erase)

A SED will always encrypt all data that is written to the SSD flash media. Data is encrypted using an AES-256 Media Encryption Key. The M-key is generated by the SSD and never leaves the SSD, and is always stored on the SSD only in an encrypted form. Thus, even if the SSD is physically compromised and access to the internal flash chips is gained, the unencrypted M-key cannot be accessed, as it is stored only in an encrypted form.

The stored version of the M-key is encrypted using the 32 byte Authentication Key (A-key). The A-key is used in two ways to “unlock” the drive and gain access to data. First, the A-key must be provided after each power-up to gain access to the drive. When the SSD receives the A-Key (as part of the drive unlock operation), it first performs a one-way cryptographic hash on the key, and then compares the result to the crypto hashed version of the key that was previously stored on the drive. If the hashed key values do not match, further access to the drive is denied. If the hashed keys do match, then the “clear” version of the A-key is used to decrypt the stored encrypted M-key. The decrypted M-key is then provided to the AES encryption engine to enable encryption of new user data and decryption of previously stored user data.

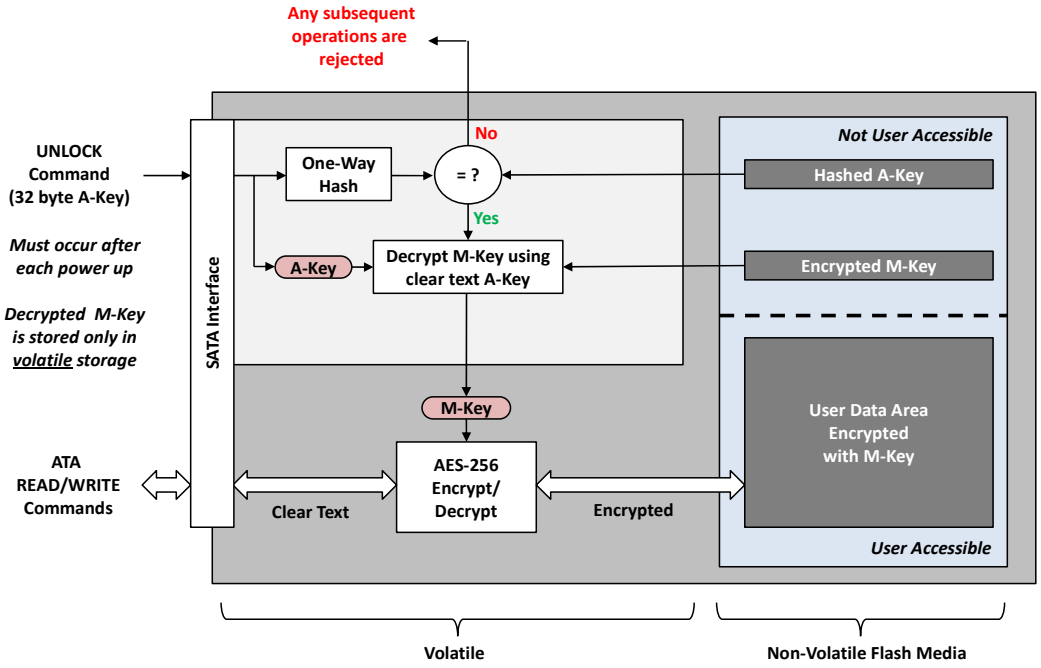

Figure 2. Self-Encrypting Drive Unlock, Followed by Normal Operation

SED Secure Erase (aka Cryptographic Erase) Operation

A SED can be cryptographically erased by performance a SSD secure erase. This operation generates a completely new M-key, which renders data that had been encrypted with the previous M-key un-decryptable. This process of generating a new M-key to render existing data un-decryptable is also known as a cryptographic erase. In most SED implementations the SSD controller will also erase all of the flash pages and clear the flash mapping table as part of the secure erase. But this extra step is done only for flash management convenience and SSD performance optimization, and is not actually needed from a security point of view. The typical mechanization of a SED secure erase operation is shown in figure 3 below.

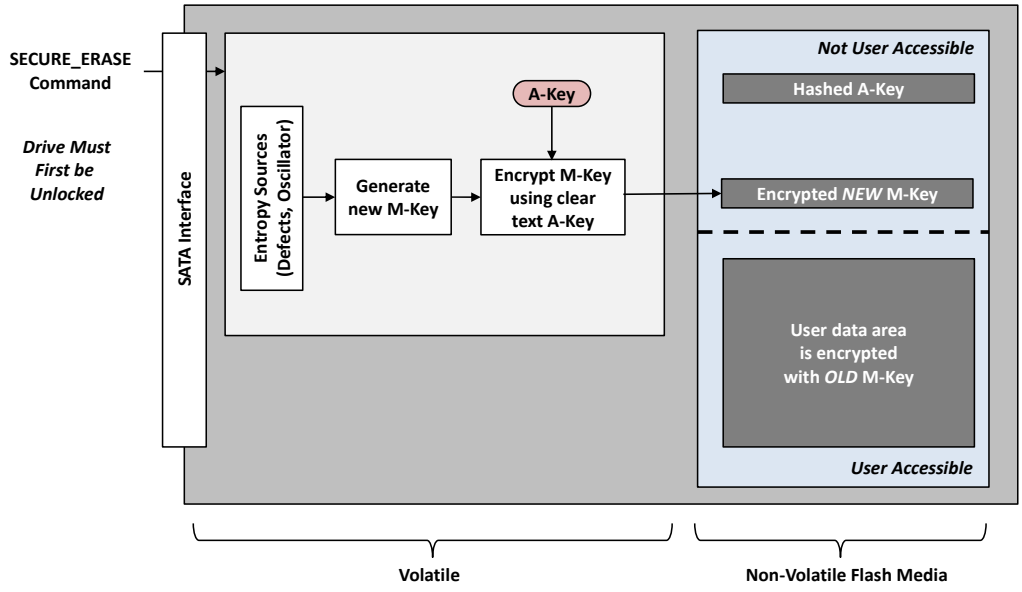

Figure 3. Self-Encrypting Drive Secure Erase Operation

Changing the User-Defined Authentication Key

A key capability of an SED is the ability to change the drive's Authentication Key without the time-consuming need to decrypt and re-encrypt the existing data stored on the SSD (which could be hundreds of GBytes). This leverages the fact that the M-key stored on the SSD is itself encrypted using the A-key. To change the A-key, the encrypted M-key is first decrypted (using the old A-key), then it is re-encrypted (using the new A-key), and the newly encrypted M-key is stored. Figure 4 below illustrates this process.

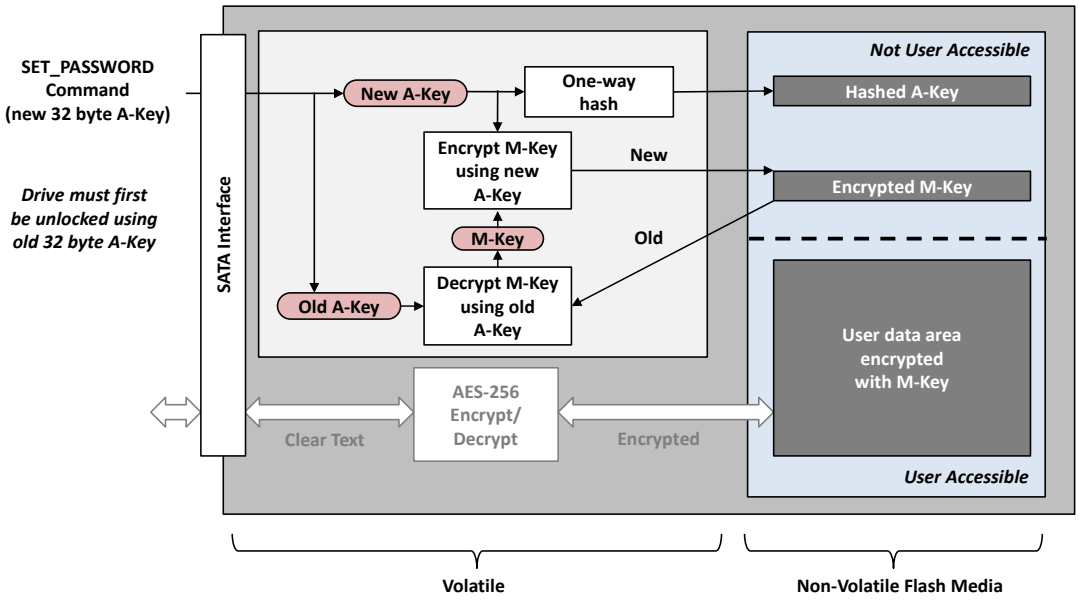

Figure 4. Changing the User Defined Authentication Key

Summary

Critical I/O's StoreEngine and StorePak can optionally be configured with Self-Encrypting Drives (SEDs). SEDs provide features including authentication and AES-256 encryption that can be used as the basis of a secure storage system to help protect sensitive data. SSDs may comply with different levels of assurance/certification ranging from TCG-Opal compliance to FIPS-140-2 certification. Critical I/O supplements the use of SEDs with a Security Manger utility which runs on StoreEngine or the user's SBC. This utility provides capabilities to control and manage the security features of the SEDs, and in particular to manage the user-defined Authentication Key to control access to stored data.