Enterprise SED Presentation

- TCG Storage WG Marketing

Goal of this Presentation

High Level description of how Self-Encrypting Drives (SEDs) utilize cryptography to protect user data

- Target Use Cases for Self-Encrypting Drives
- Encryption practices used in Self-Encrypting Drives
- Key Handling within the Self-Encrypting Drive
- Key Management examples with Self-Encrypting Drives

The Need for Encryption

- All Drives eventually leave the data center
  - IBM estimates 90% have some readable data
  - Need to prevent loss of data on those drives
- Laws & Regulation
  - PCI, HIPAA regulations require data privacy
  - 46+ states have data privacy laws with encryption safe harbor

The Problem SEDs solve

- Stored Data Protection
  - Should equipment be lost, data is not exposed
  - All user data is always encrypted
  - Encryption function cannot be turned off
- Immediate Data Erasure
  - When drives are to be retired, relinquished or repurposed
  - Data can be destroyed instantaneously
  - Even if drive is inoperable
- Not addressed
  - Protecting data in flight
  - Prohibiting unauthorized user access after drive is unlocked

What keys are in the SED?

- Data Encryption Key (DEK)
  - The key used to encrypt all of the user data on the drive
  - Generated by the drive and never leaves the drive
  - This key is stored in an encrypted format somewhere in the Drive
  - When the DEK is changed or erased, no prior existing data can be decrypted
- Authentication Key (AK)
  - The key used to unlock the drive
  - A hash of this key may be stored on the drive
  - Once confirmed, this key is used to decrypt the DEK

Self-Encrypting Drive Basics

Locking + encryption = security

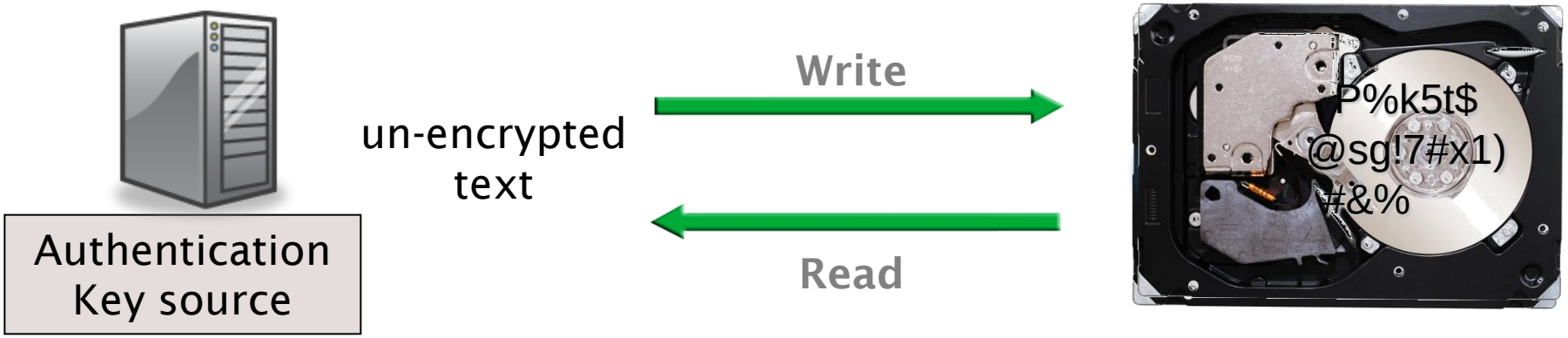
- Locking only is easily hacked (ATA has had this for years)
- Encryption-only does not prevent access to data

Power OFF: SED LOCKS automatically

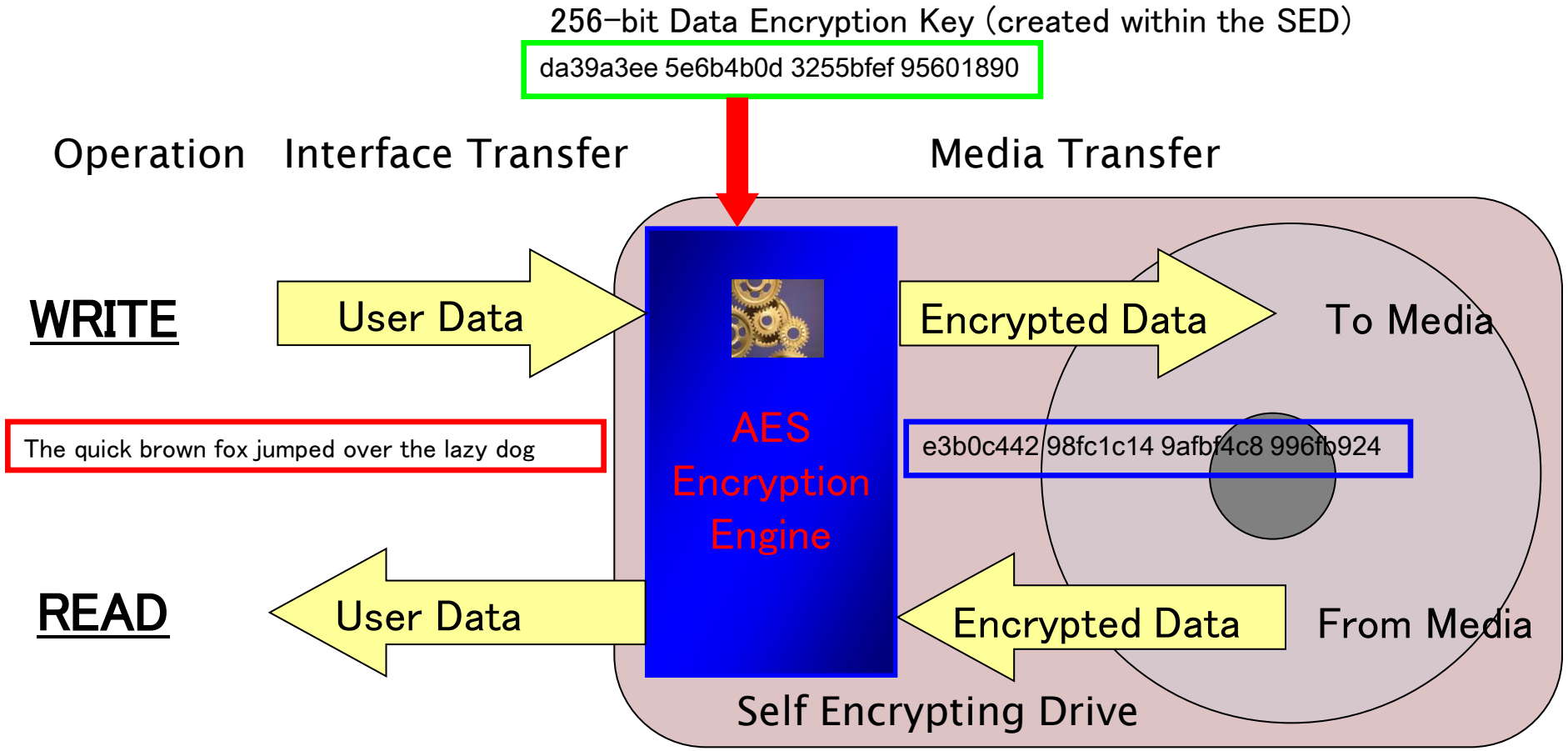
Power ON: SED remains LOCKED

Authentication Key (Password) Unlocks the drive

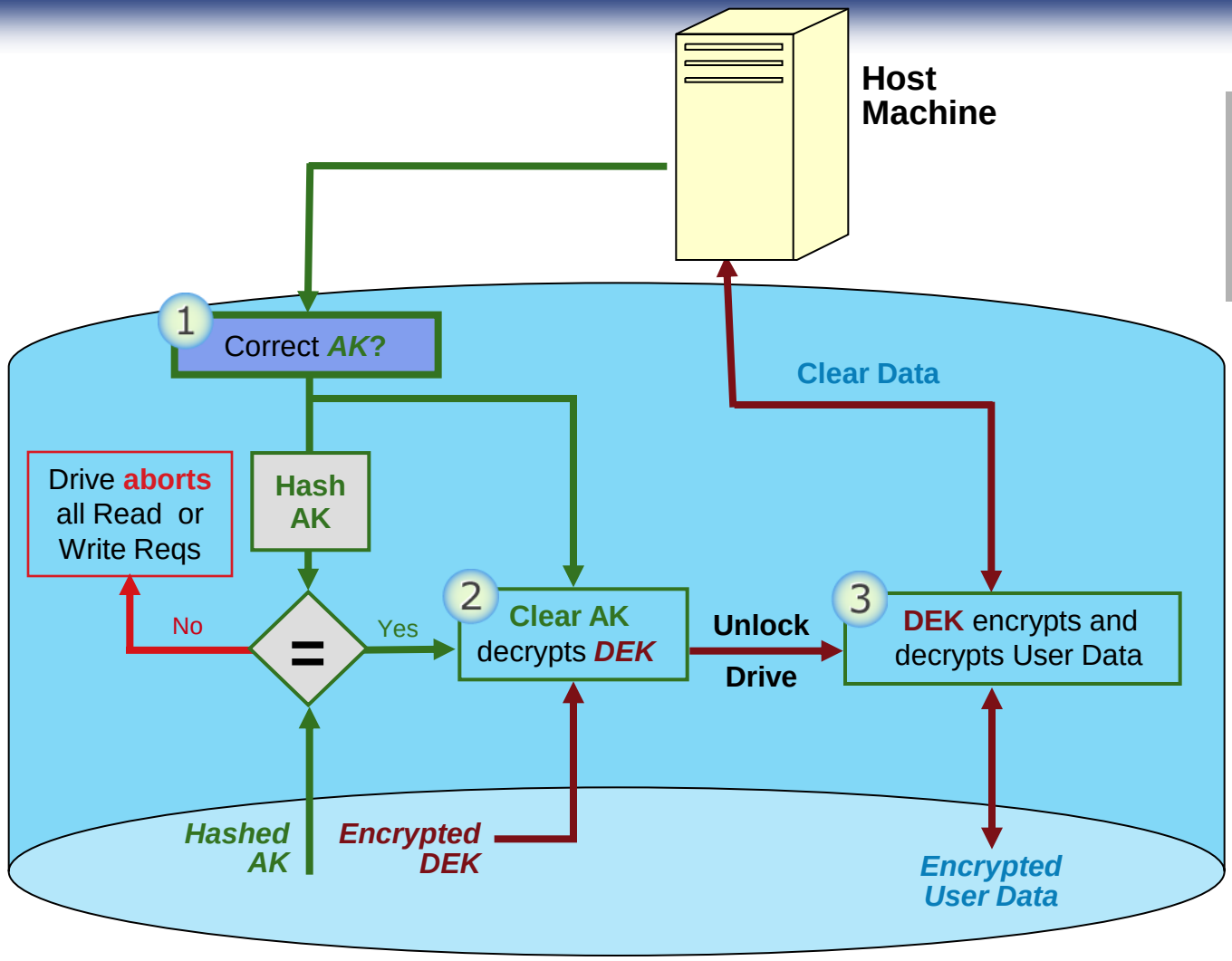
Write and Read data allowed



Encryption example



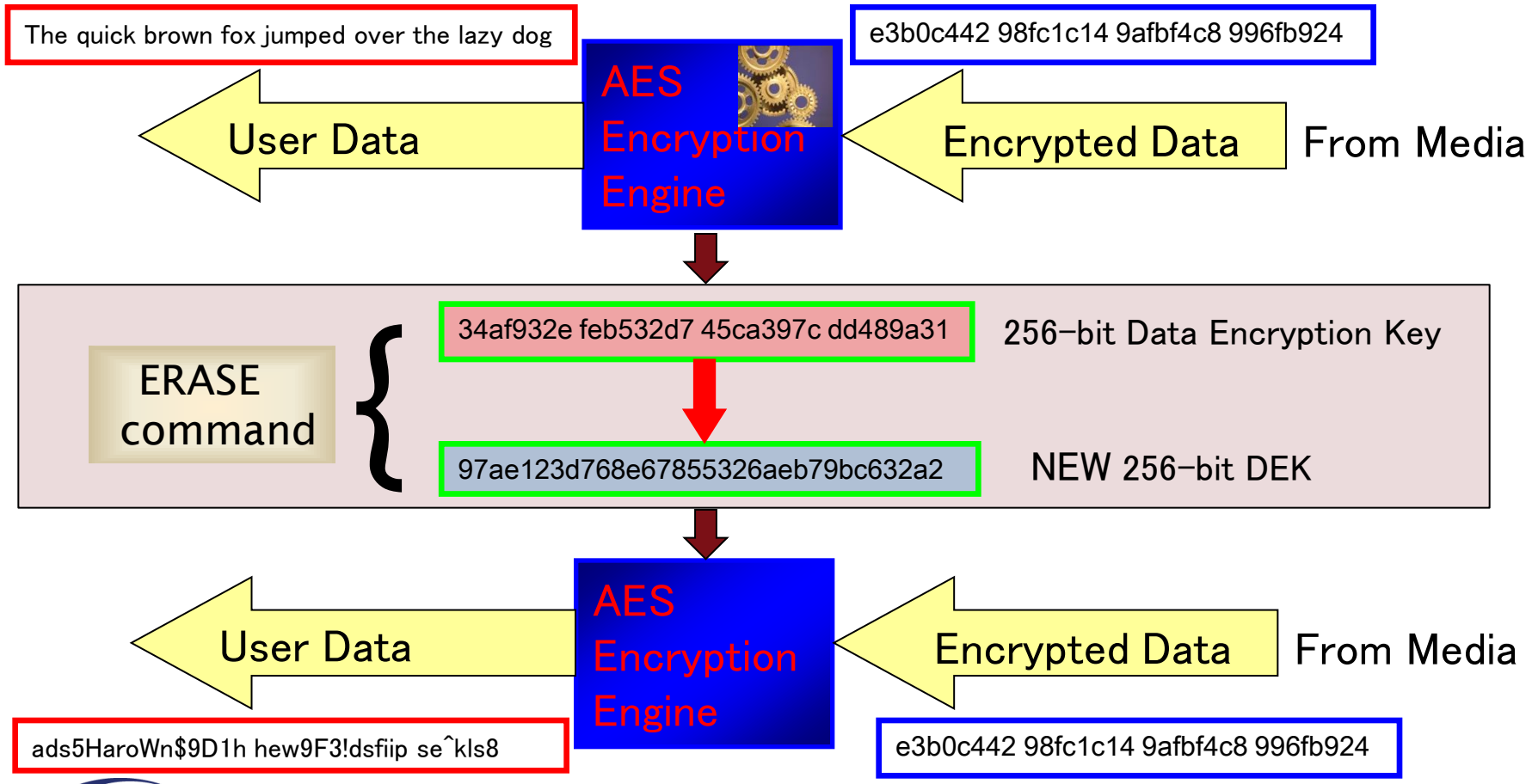
How the SED Protects the Data



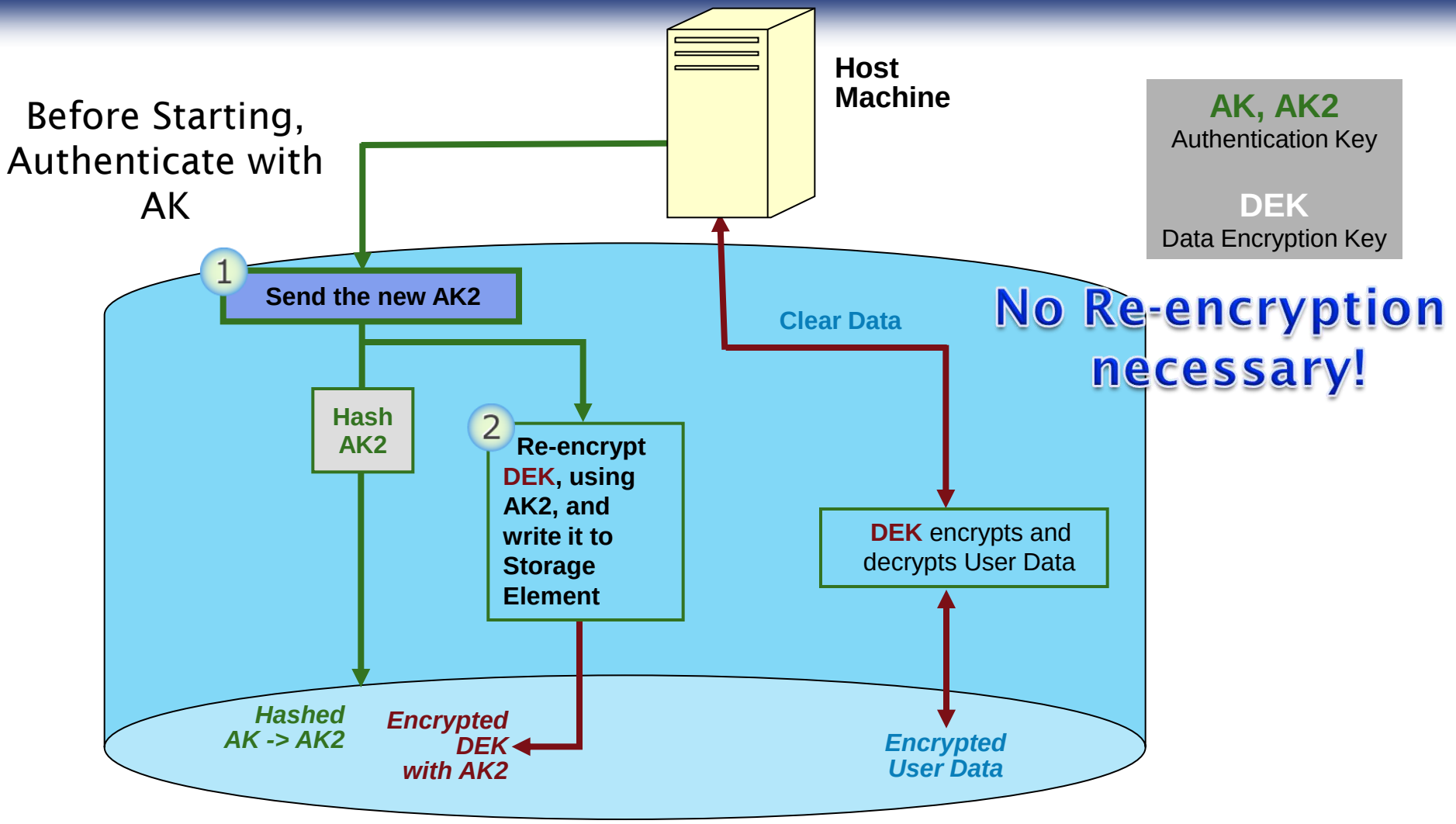
Note: This is not the only way to handle keys in a SED

Change DEK = Erase Data!

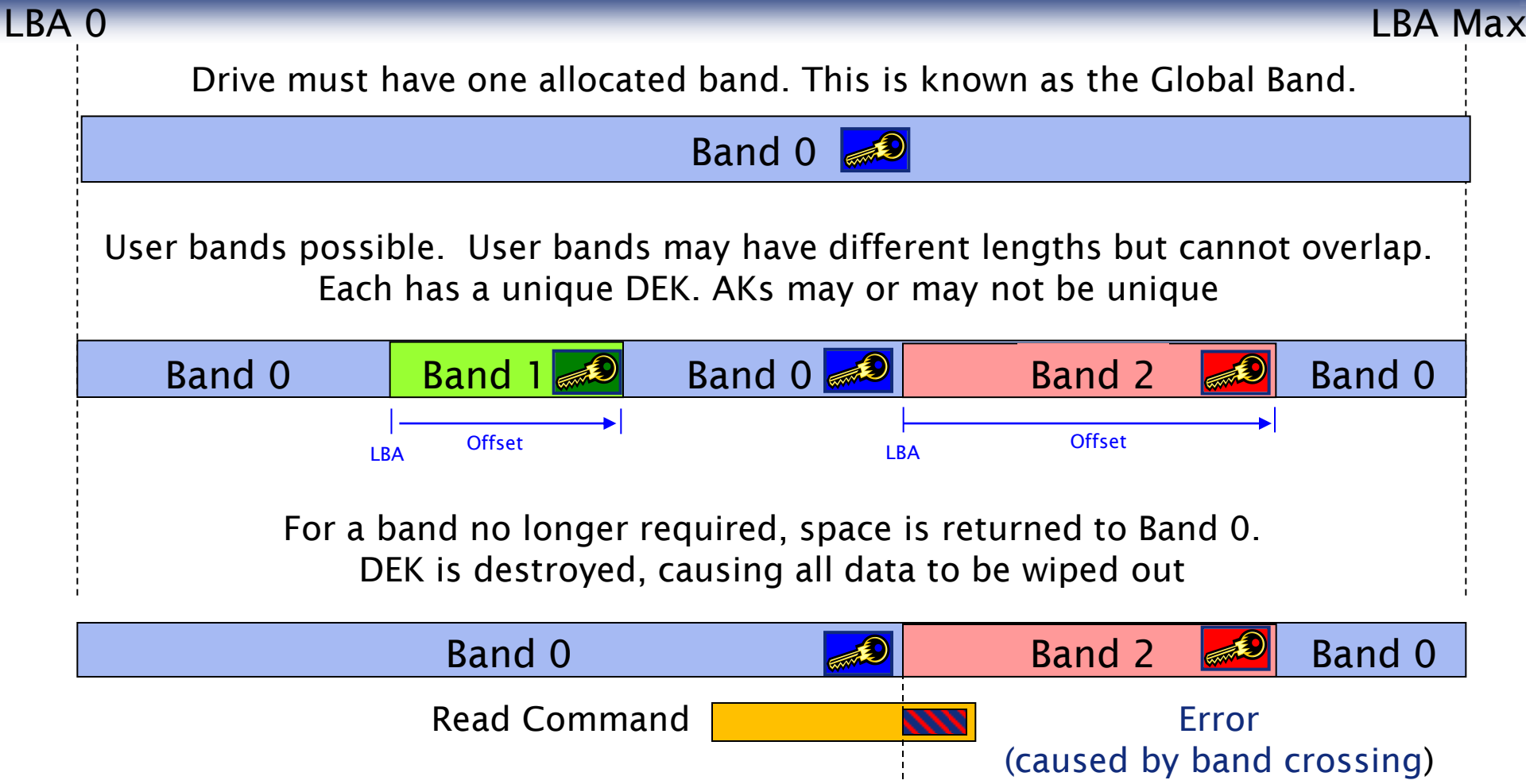
Replacing the DEK, in less than a second, makes original data impossible to retrieve!



Changing the Authentication Key

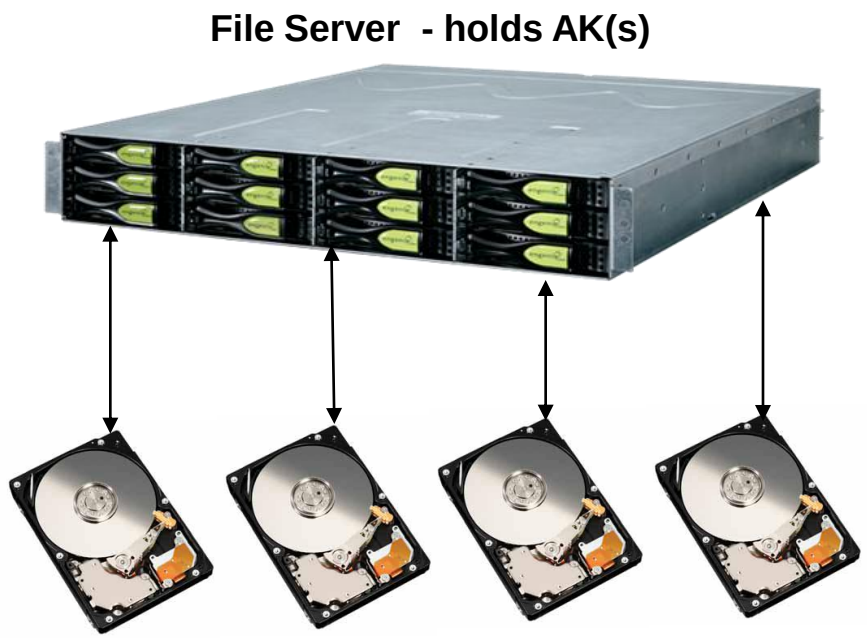


LBA Bands and Locking



Write Command crossing bands will terminate in a check condition

Local Key Management in a Single Server



- The Server has AK(s) used for all SEDs
- If a SED is removed from the rack, the SED will be powered down and forget all keys
- For Repurpose or Retirement, if the SED is functional, the ERASE command should be given to overwrite the DEK

KMIP: Addressing Enterprise Key Management*

OASIS

OASIS KMIP Technical Committee

- OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-profit consortium that drives the development, convergence and adoption of open standards for the global information society.

- KMIP Technical Committee chartered in March 2009
  - "The KMIP TC will develop specification(s) for the interoperability of Enterprise Key Management (EKM) services with EKM clients. The specifications will address anticipated customer requirements for key lifecycle management (generation, refresh, distribution, tracking of use, life-cycle policies including states, archive, and destruction), key sharing, and long-term availability of cryptographic objects of all types (public/private keys and certificates, symmetric keys, and other forms of "shared secrets") and related areas."

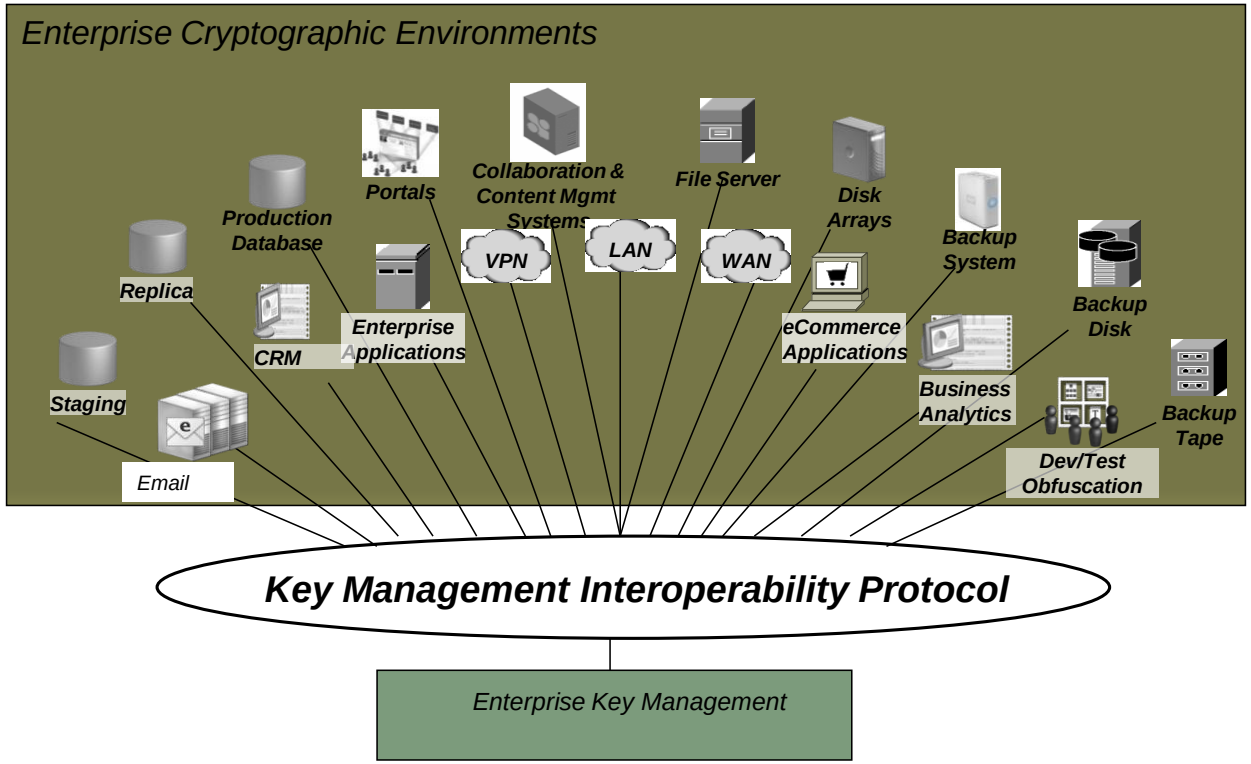
16

*This slide used with permission of OASIS KMIP WG

KMIP: For More than Just Storage*

OASIS

KMIP: Single Protocol Supporting Enterprise Cryptographic Environments

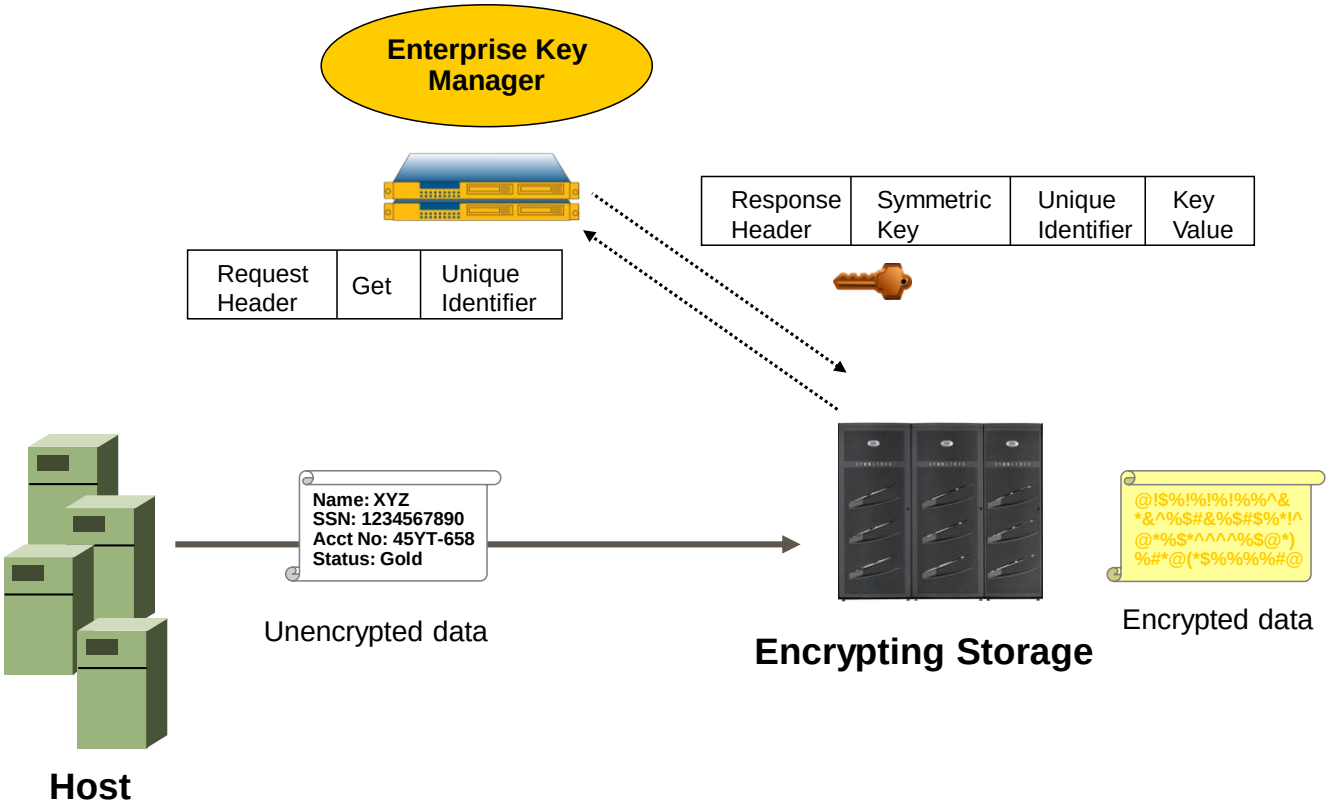


*This slide used with permission of OASIS KMIP WG

KMIP: Protocol for Managing Keys*

OASIS

KMIP Request / Response Model



*This slide used with permission of OASIS KMIP WG

SED Advantages - Performance

Each SED encrypts all data transferred to it transparently and FAST.

As SEDs are added, the encryption performance scales linearly.

No re-encryption necessary when external credentials (AKs) need changing

…

SED Advantages - Security

No Back Doors

No access without authentication – resistant to "evil maid" attack

All user data encrypted, always

Encryption cannot be turned off by user

Encryption not exposed outside drive

Rapid erase of data

SED Advantages - Manageability

User only manages Authentication Keys

No OS or Master Boot Record modification

Standard protocol, multiple sources

- All drive manufacturers support TCG standard

No interference with storage management functions:

- RAID, backup/restore, compression, PI, dedup, DLP

Lower cost disposal, no hazardous waste created

Summary

- SEDs encrypt and decrypt data at the endpoint
- Once authenticated, the encryption is completely transparent to the system
- All user data is encrypted, always
- OASIS/KMIP will be used in data center-wide key management tools
- Standardization and the promise of interoperability has led to support from multiple Storage Device Vendors, multiple File Server Vendors, and multiple Software Vendors
- Questions?

Thank You

Many thanks to the following individuals for their contributions to this presentation:

All Storage Manufacturers (contributors)

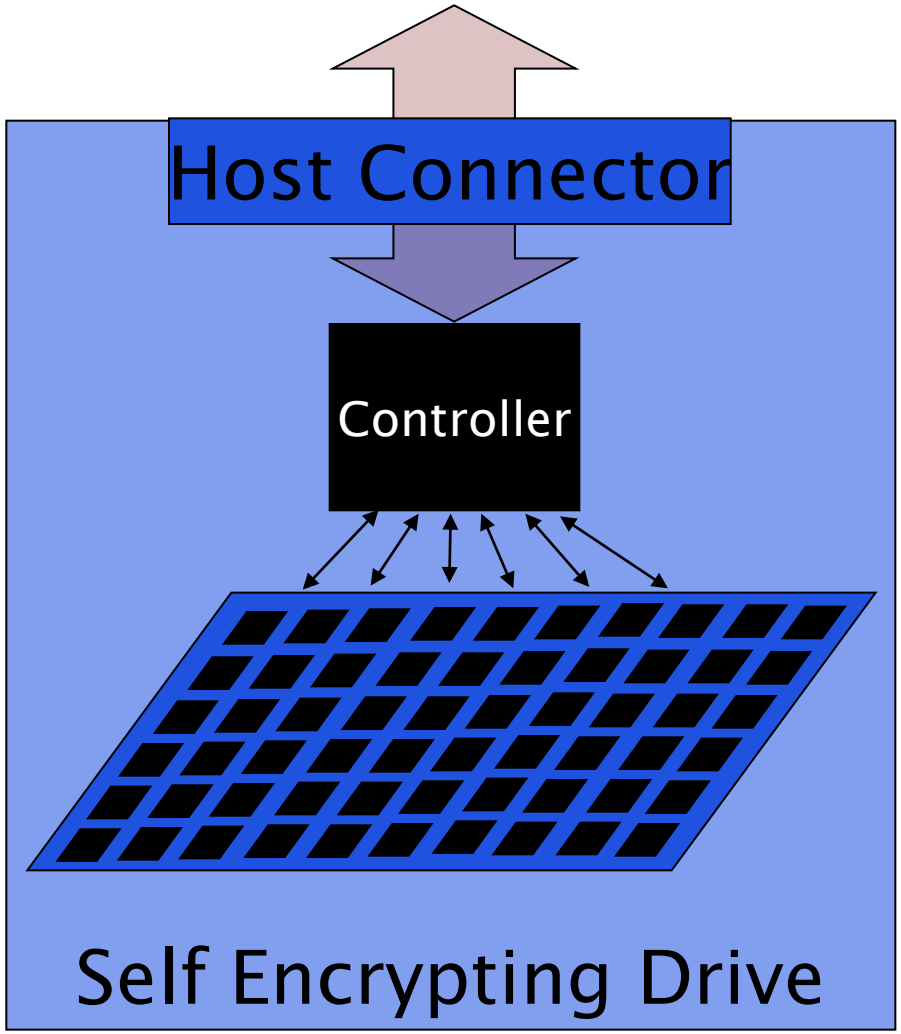
What is TCG SWG?

- The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, industry standards for trusted computing building blocks and software interfaces across multiple platforms.
- The Storage Work Group (SWG) builds upon existing TCG technologies and philosophy, and focuses on standards for security services on dedicated storage systems.
  - Storage Core Architecture Specification describes in detail how to implement and utilize trust and security services on storage devices.
  - Security Subsystem Class (SSC) Specifications describe the requirements for specific classes of devices
    - Enterprise SSC defines minimum requirements for Data Center and Server Class devices
    - Opal SSC defines minimum requirements for Client devices

How do we communicate with the SED?

- For configuring encryption and unlocking, container commands are used
  - T10 – SECURITY PROTOCOL IN and SECURITY PROTOCOL OUT
  - T13 – TRUSTED SEND and TRUSTED RECEIVE
  - The format of the payloads of the above commands are defined by TCG SWG
- Once the SED is unlocked, all read and write commands work as normal

Where is the crypto engine?



- Data at the host interface (SATA, SAS, FC, or USB) is clear text
- Data in the Storage Element is cipher text
- Encryption done in the Controller between the Host Connector and the Media
- Encryption happens on the fly in the write path
- Decryption happens on the fly in the read path