How To Use An Encryption Key Per I/O

Sponsored by NVM Express™ organization, the owner of NVMe® Family of Specifications

Speakers

Festus Hategekimana

SOLIDIGM

Frederick Knight

NetApp

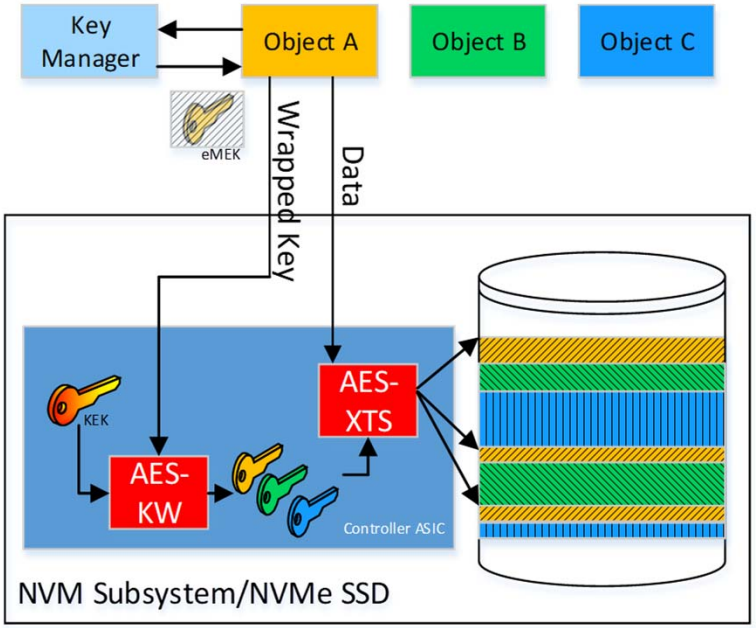
Flash Memory Summit

nvm EXPRESS®

Agenda

- Key Per I/O Technology Overview
- How to Use Key Per I/O
  - One-time Setup
    - Capabilities Discovery
    - Enabling and Configuring Key Per I/O
  - Host Management of a Storage Device's Key Cache
    - Loading of Encryption Keys into a Storage Device
    - Specifying Encryption Keys During I/O
    - Locking the Key Cache
  - Disabling Key Per I/O
- Industry Specifications Status
- Q & A

Key Per I/O Technology Overview



- Co-developed by NVM Express & TCG to enable Storage Devices(SDs)' support of Host-Managed (i.e., Customer-managed) Storage Encryption Use Cases.
- Hosts no longer need to encrypt-at-compute with customer supplied encryption keys. They can now parallelize encryption across SDs with host-supplied Media Encryption Keys (MEKs) to increase storage systems' performance & bandwidth.
- Encrypted MEKs are injected into Self Encrypting Drive (SED)'s key cache and assigned a "Key Tag" by host SW.
- Subsequent I/O can use the "Key Tag" to identify the MEK to encrypt/decrypt data to/from the SD in a non-contiguous fashion.
- MEKs are encrypted (wrapped) by a Key Encryption Key (KEK).
- KEKs may be supplied encrypted via RSA-based Key Wrapping.
- MEKs are not stored in the NVM of the drive and are lost on power loss.
- Crypto erase is done by deleting the MEK from the Key Manager and the SSD's key cache or by sanitizing entire SD.

Setting up Key Per I/O (one time setup): Capabilities Discovery

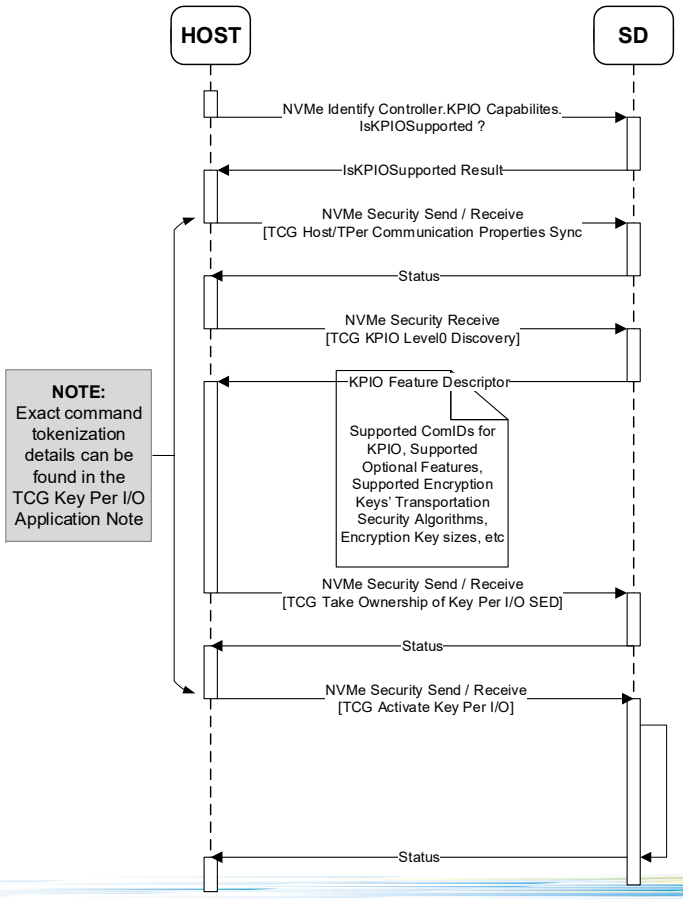
NVMe® Device Identify Discovery

- Identify Controller
  - Key Per I/O Capabilities field
    - Key Per I/O Supported (KPIOS) bit
    - Key Per I/O Scope (KPIOSC) bit
- Identify Namespace
  - Key Per I/O Status field
    - Key Per I/O Supported in Namespace(KPIONS) bit
    - Key Per I/O Enabled in Namespace (KPIOENS) bit
  - Maximum Key Tag (MAXKT) field
  - Key Per I/O Data Access Alignment and Granularity (KPIODAAG) field

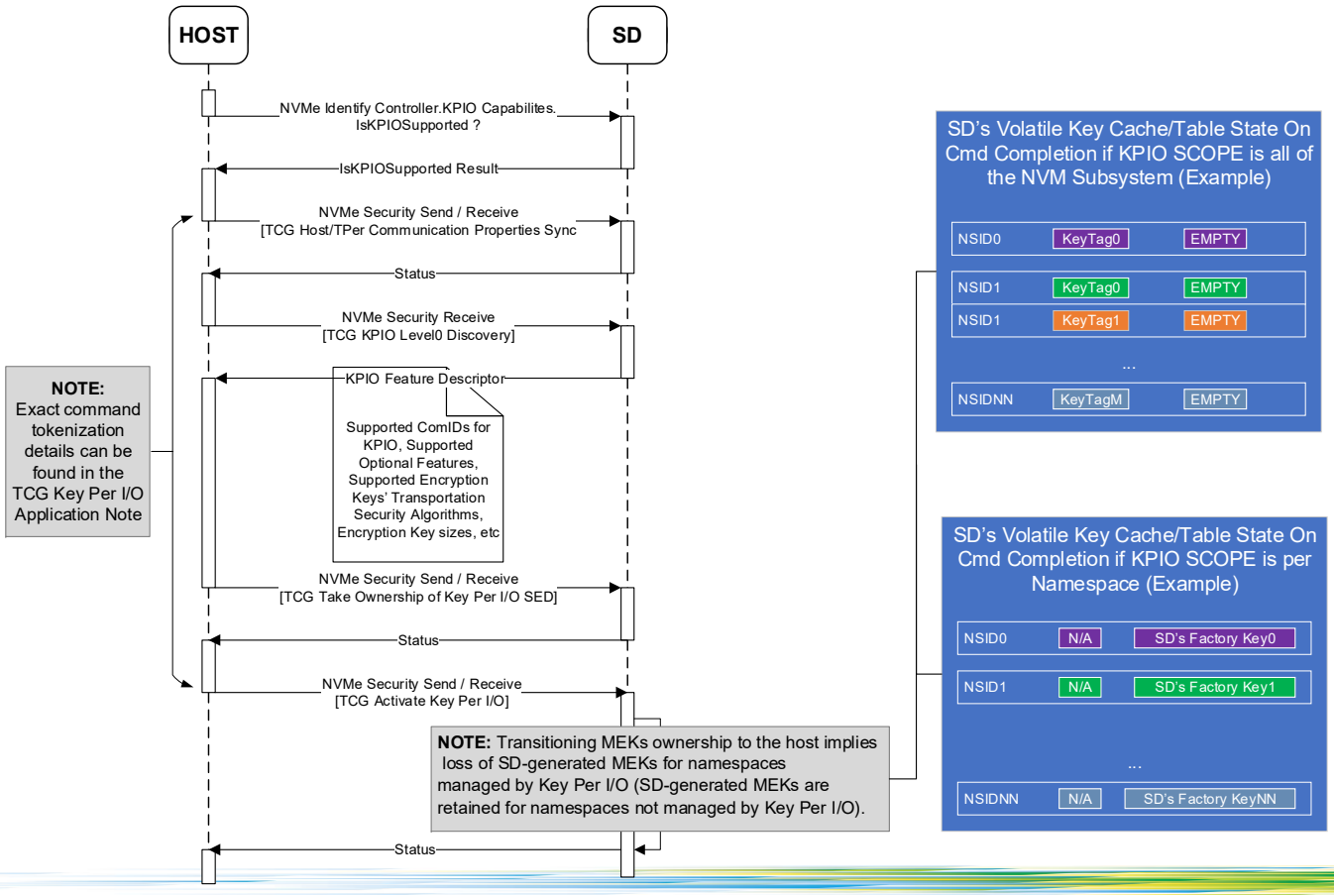
TCG Discovery (via NVMe Security Receive)

- Feature Level0 Discovery
  - Key Per I/O Security Protocols & ComIDs
  - Security properties for secure encryption key transport (RSA-OAEP wrapping, AES-GCM wrapping, etc..)
  - Number of Key Tags Supported (Globally vs Per-Namespace)
  - Maximum Supported Key Unique Identifier for Encryption Keys
  - Etc…
- Namespace Level0 Discovery
  - Managed By Key Per I/O bit
  - Number of Allocated Key Tags

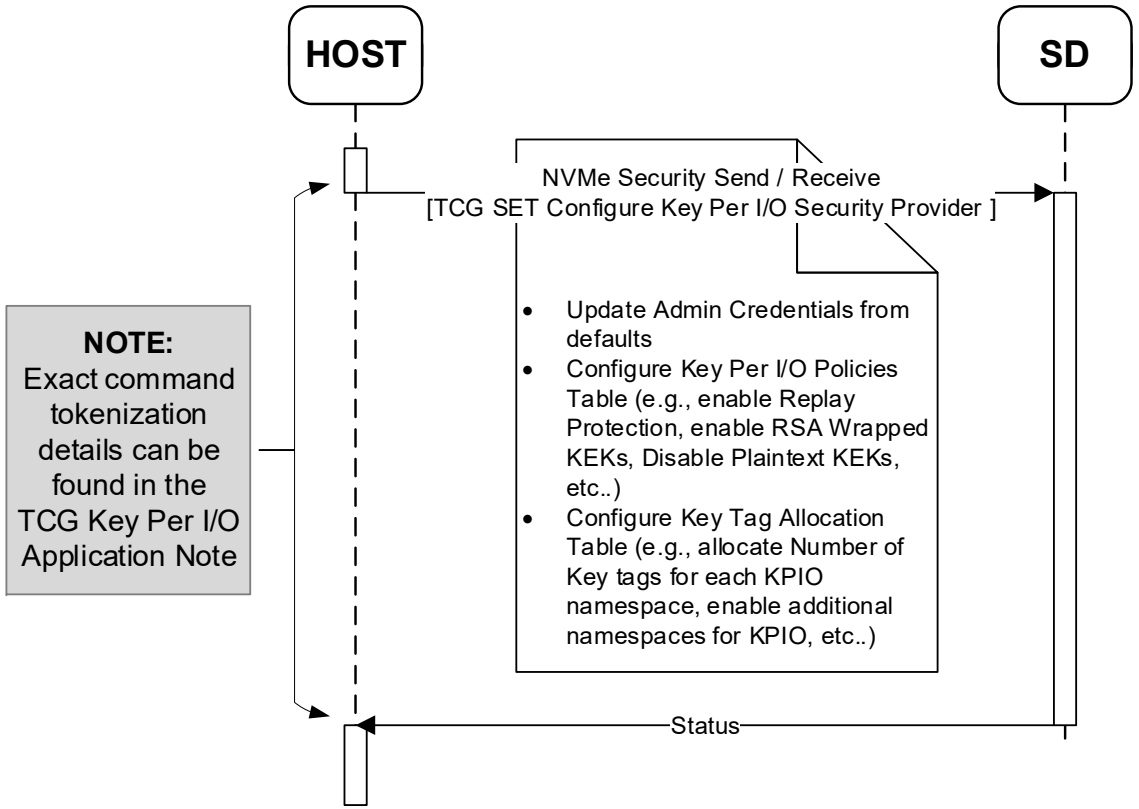
Setting up Key Per I/O (One Time Setup): Enabling Key Per I/O



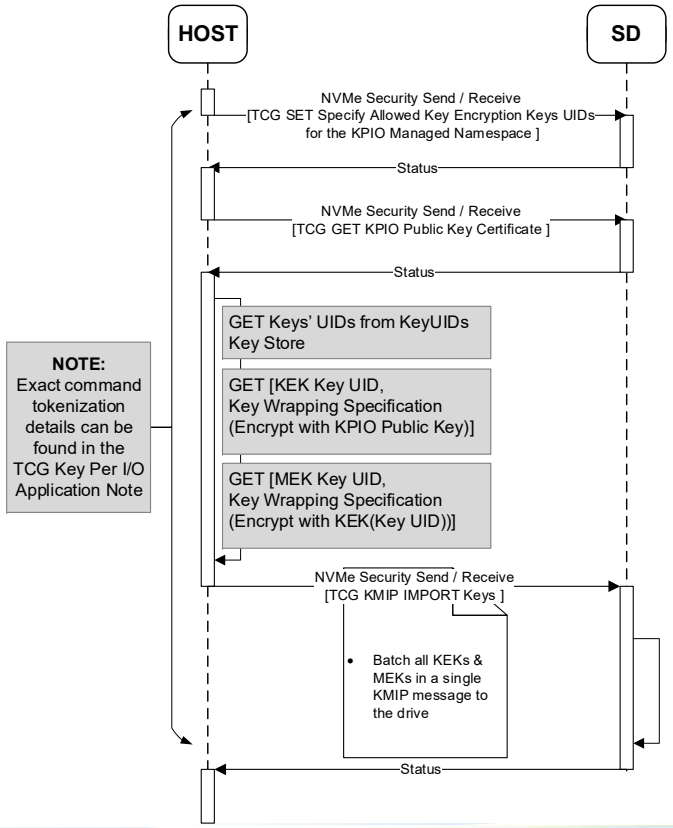
Setting up Key Per I/O (One Time Setup): Enabling Key Per I/O



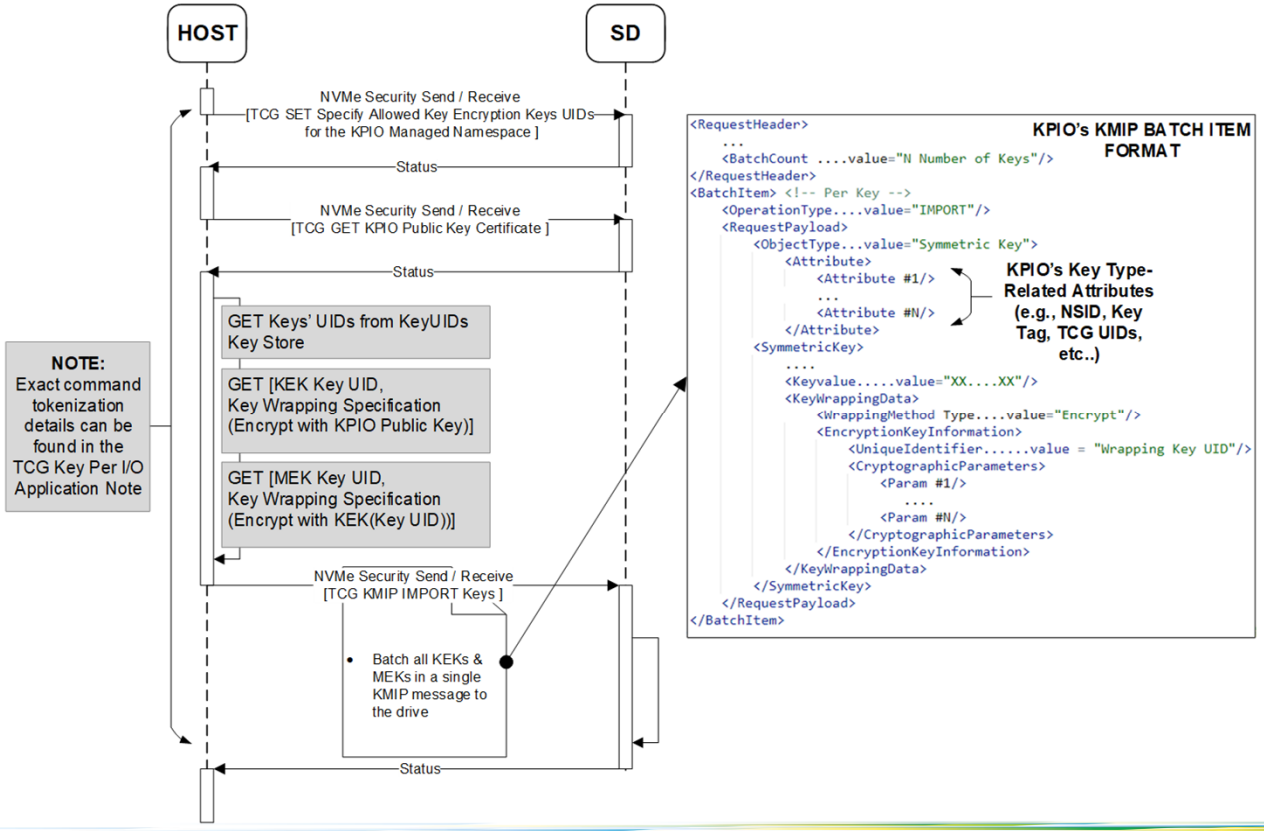
Setting up Key Per I/O (One Time Setup): Configuring Key Per I/O



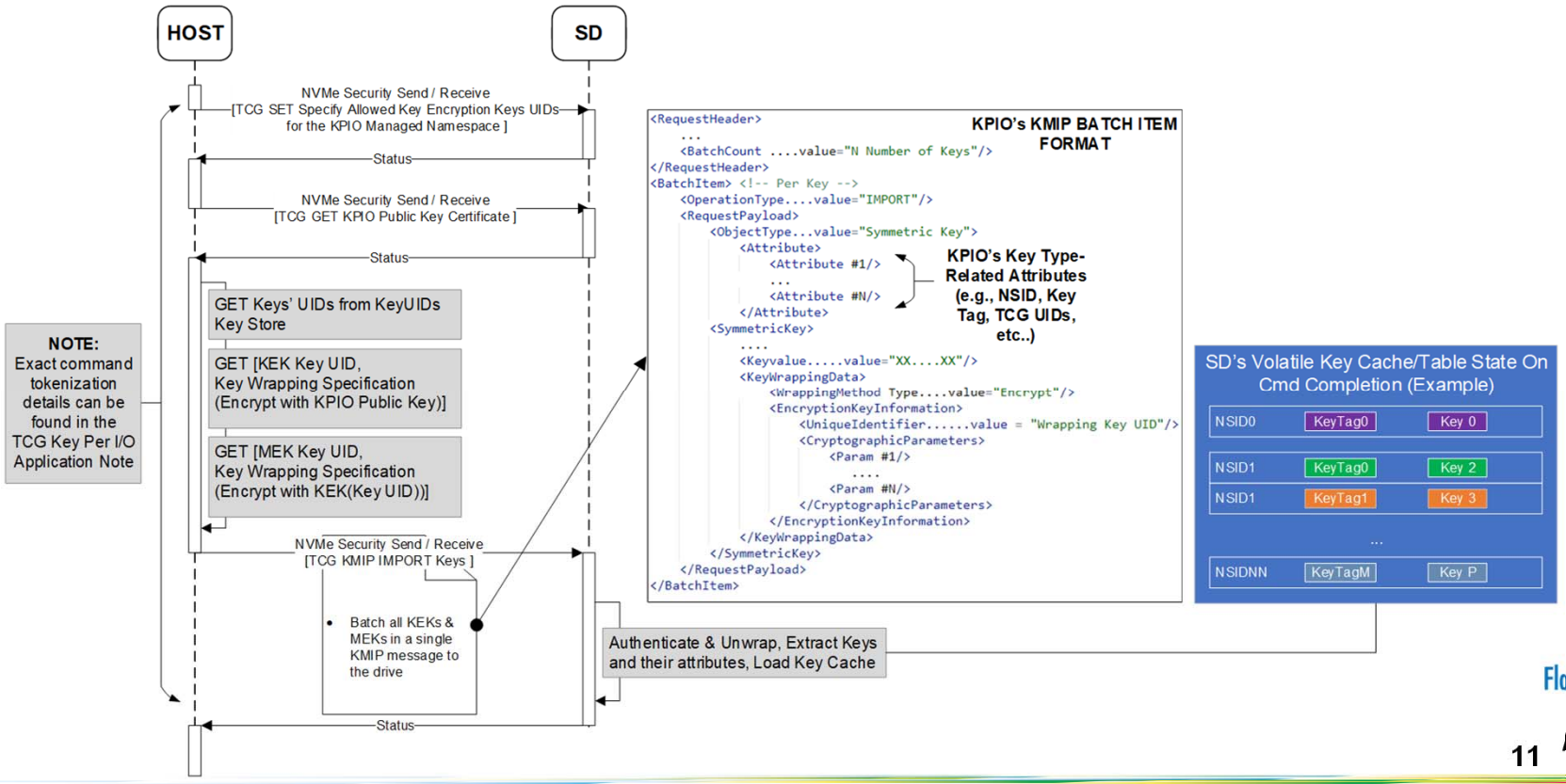
Host Management of the SD's Key Cache: Initial Loading of KEKs & MEKs



Host Management of the SD's Key Cache: Initial Loading of KEKs & MEKs



Host Management of the SD's Key Cache: Initial Loading of KEKs & MEKs

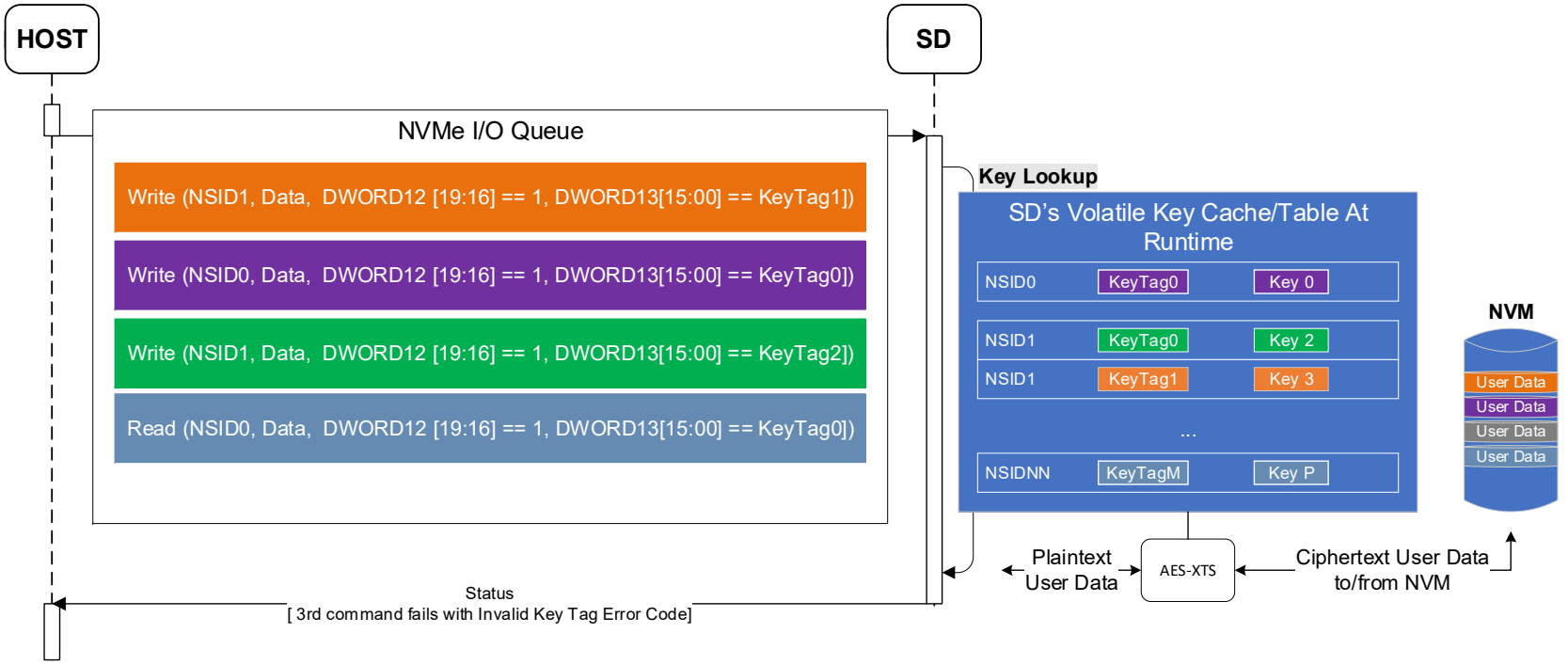


Host Management of the SD's Key Cache: Selecting MEKs to Use During I/O

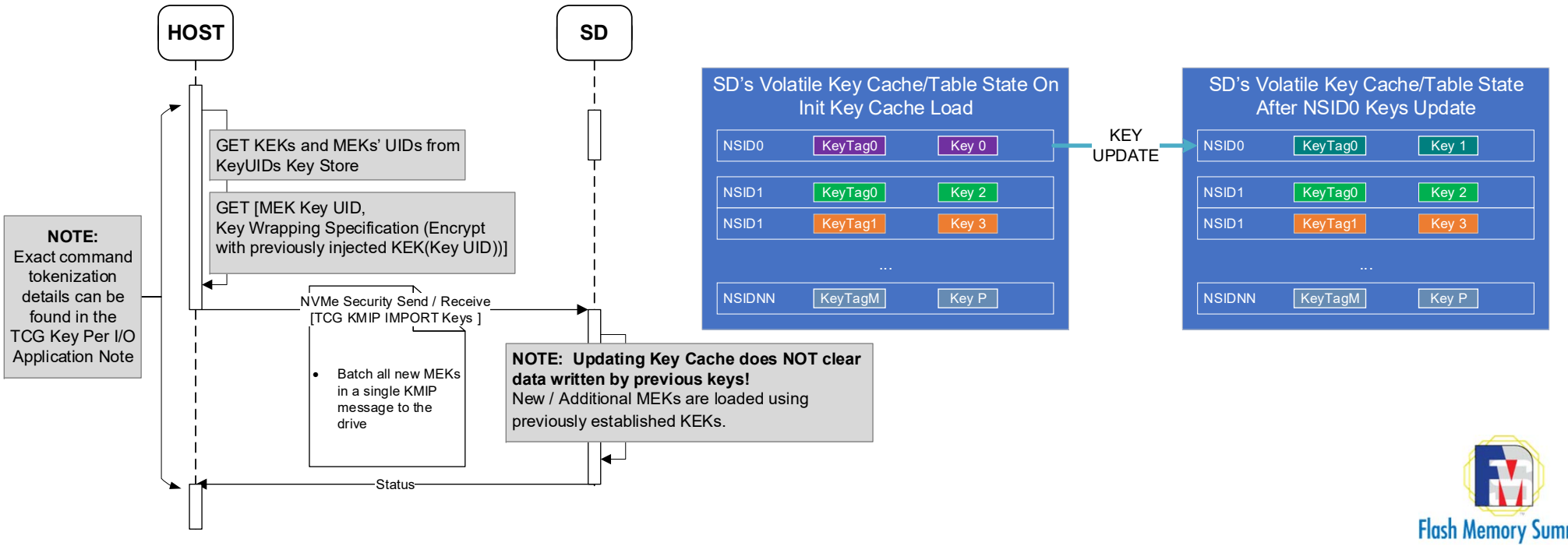
- NVM Express TP4055 defines new KPIO-related Command Extension Type (CETYPE) in DWORD12 and Command Extension Value (CEV) in DWORD13 fields for all read and write I/O commands to indicate to the Storage Device:
  - Key Tag Presence (CETYPE != 0).
  - Key Tag Value (CEV == KEYTAG) associated with MEK to be used for encryption or decryption of data in that I/O command.

Host Management of the SD's Key Cache: Selecting MEKs to Use During I/O

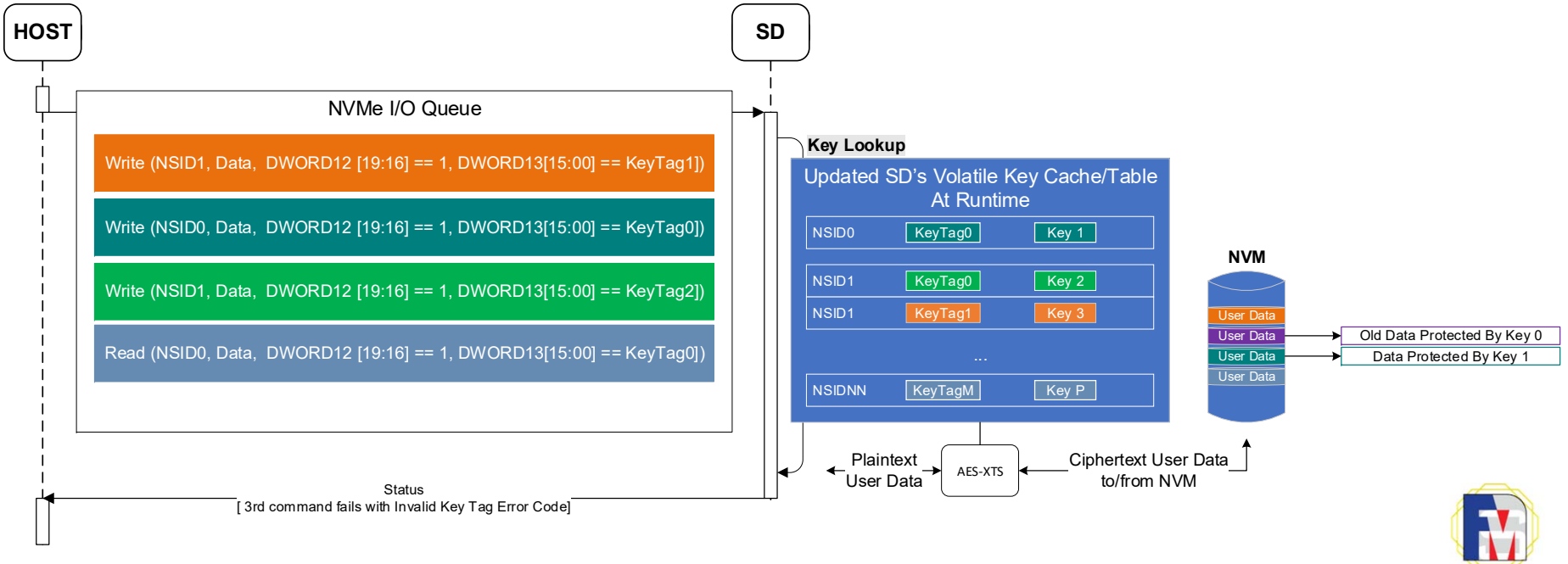
Read/Write IO Example:



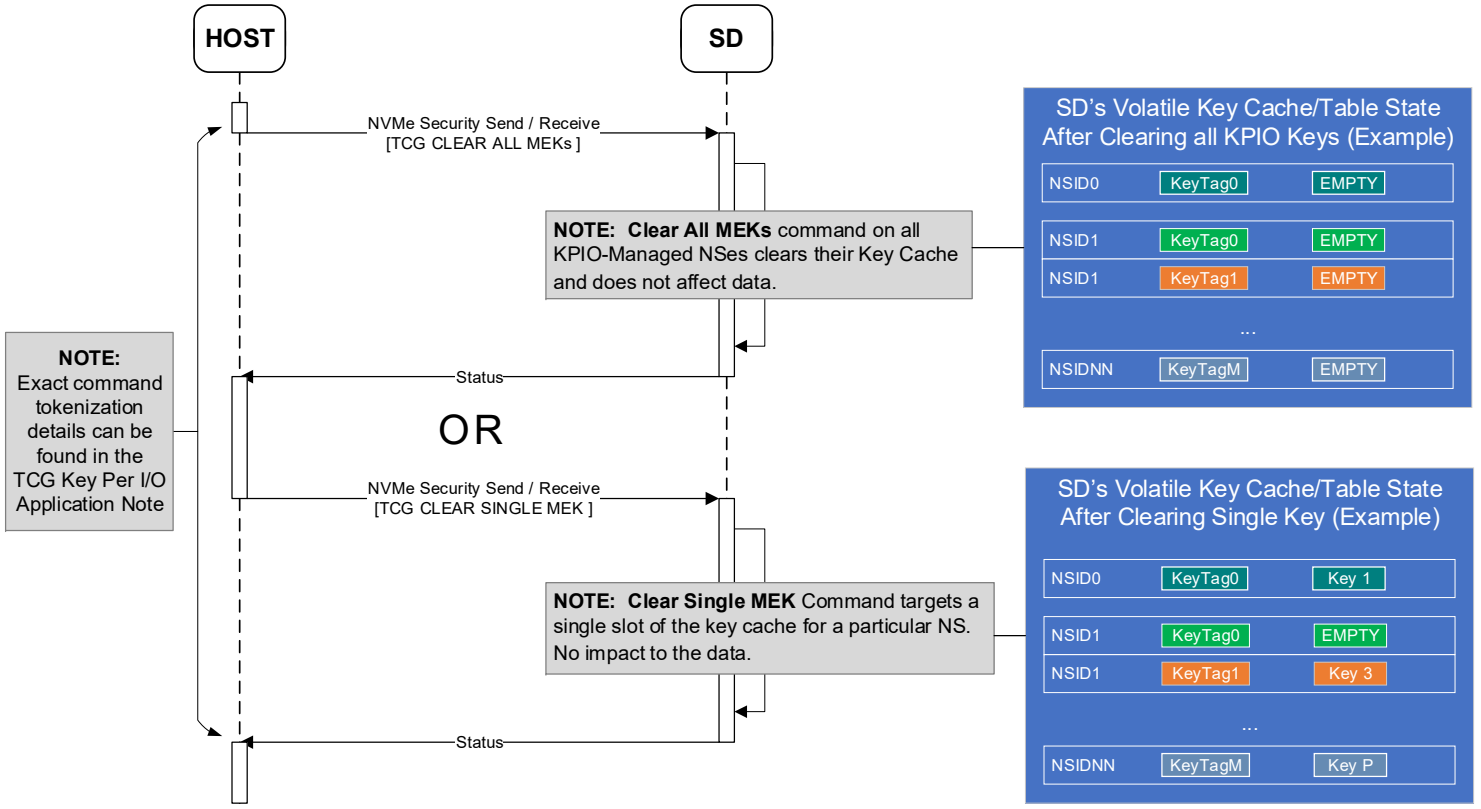
Host Management of the SD's Key Cache: Updating the Key Cache



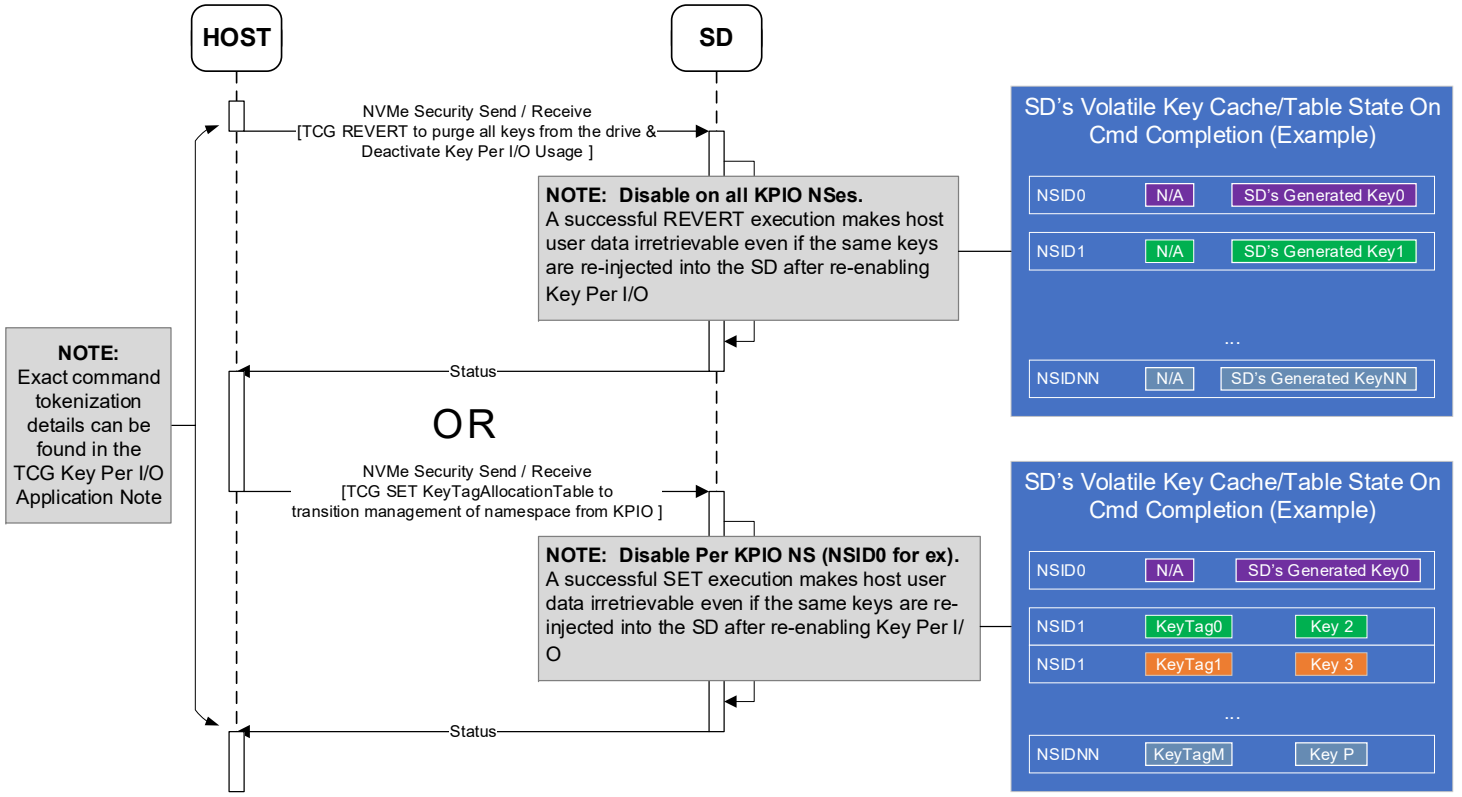
Host Management of the SD's Key Cache: Selecting new MEKs to Use During I/O



Host Management of the SD's Key Cache: Locking the Key Cache (All NSes vs. Per NS Locking)



Disabling Key Per I/O



Industry Specifications Status

Specification	Industry Standard Body	Status
NVMe® TP4055	NVM Express	Ratified
TCG Key Per I/O SSC v1.00	TCG	In Public Review
TCG Key Per I/O Application Note v1.00	TCG	In Public Review
TCG SIIS v1.11	TCG	Published

Questions?

Architected for Performance