SNIA COMPUTE + MEMORY + STORAGE SUMMIT

Architectures, Solutions, and Community
VIRTUAL EVENT, APRIL 11-12, 2023

Fine Grain Encryption Using Key Per I/O

Festus Hategekimana, TCG SWG

Fine Grain Encryption Using Key Per I/O

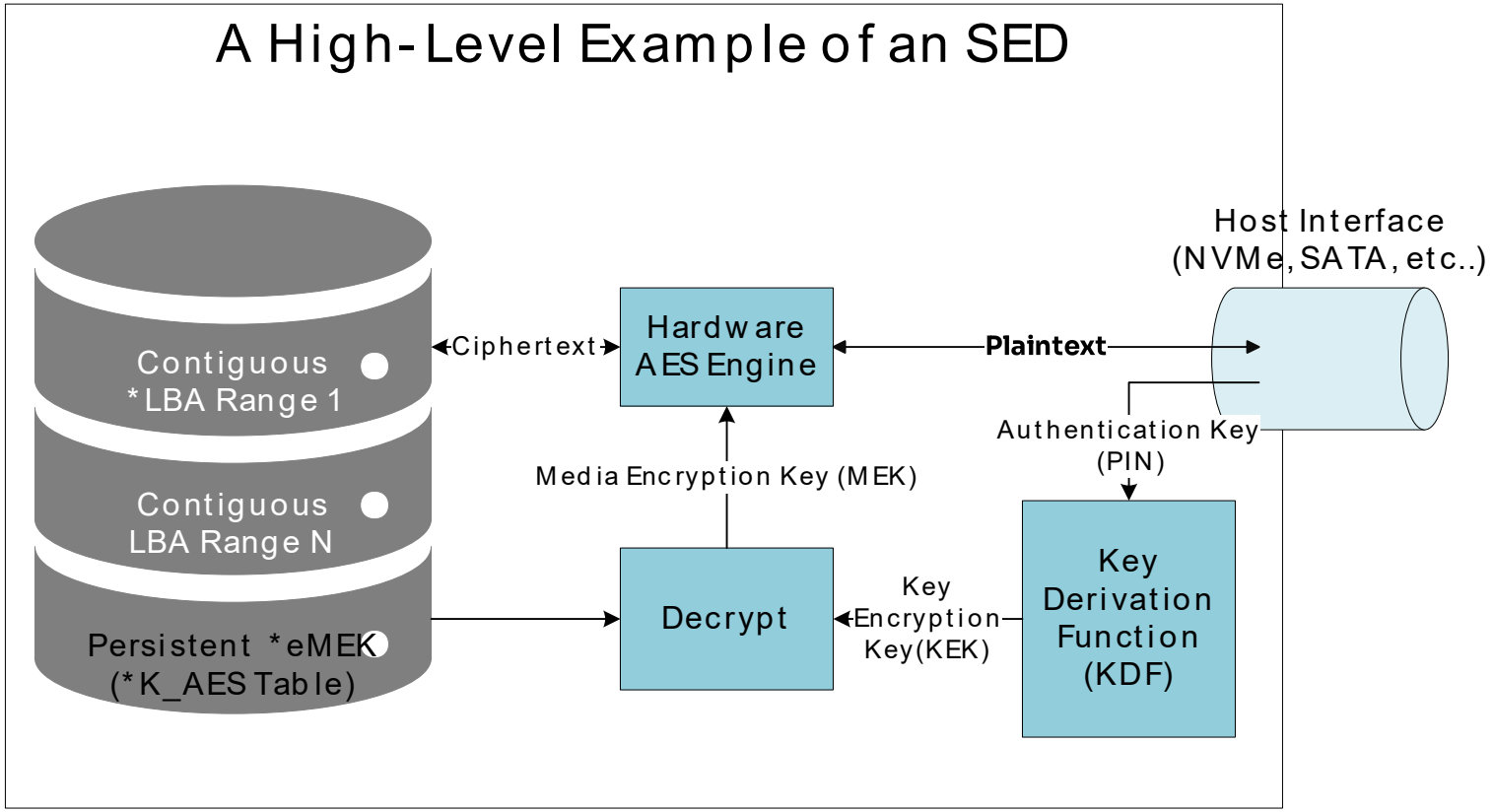
- Agenda
  - Evolution of Data At Rest (DAR) Protection
    - Today's Self Encrypting Drive (SED) Systems Review
    - Benefits & Challenges
  - Key Per I/O Overview
    - Architectural Elements, Theory of Operations, and I/O Interactions
    - Benefits & Challenges
    - Example Use Cases
  - Key Per I/O Specifications Status
  - Backup

SNIA COMPUTE + MEMORY + STORAGE SUMMIT

Architectures, Solutions, and Community
VIRTUAL EVENT, APRIL 11-12, 2023

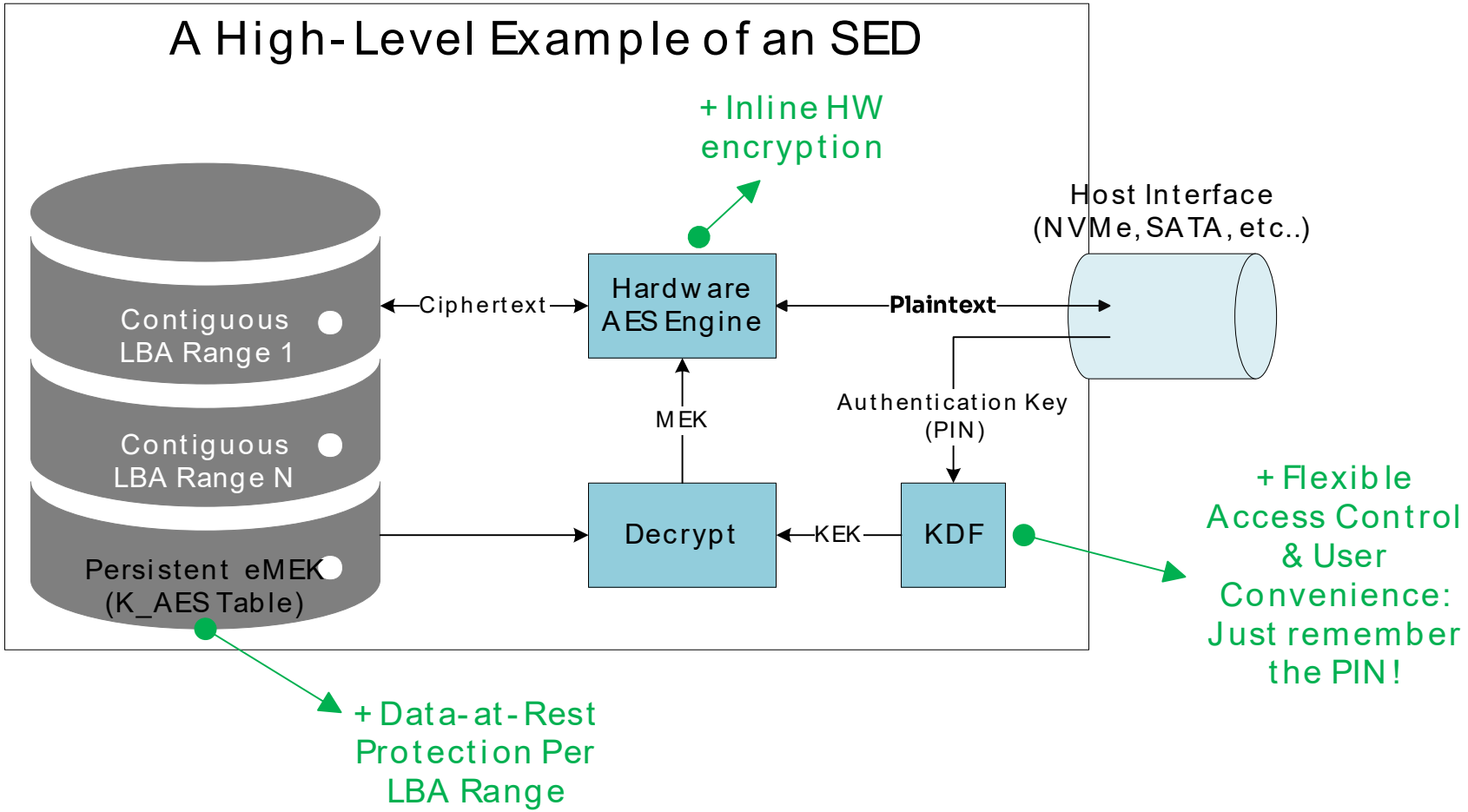
Evolution of Data At Rest (DAR) Protection

Today: SED Systems' Architecture

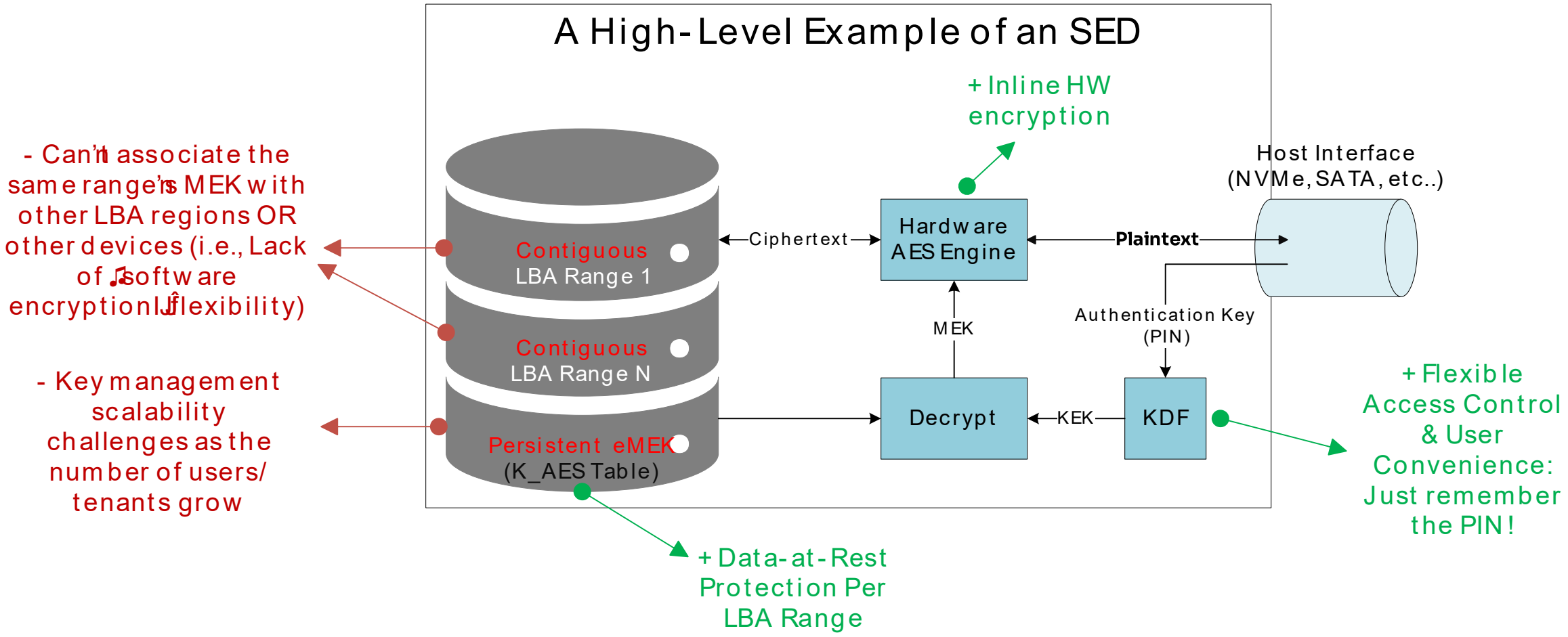


*See backup slides for acronyms definitions

Today: SED Systems' Benefits

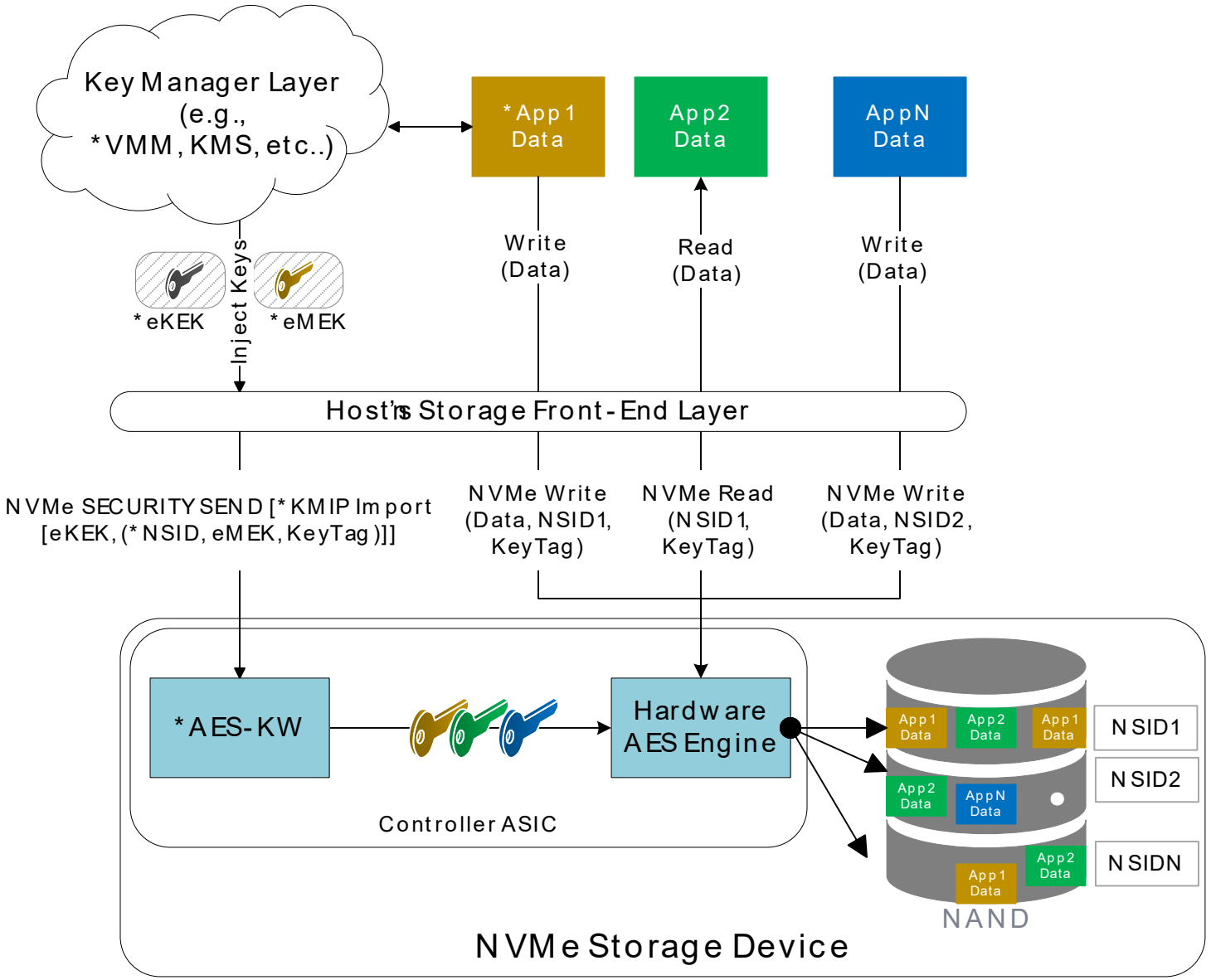


Today: SED Systems' Benefits & Challenges



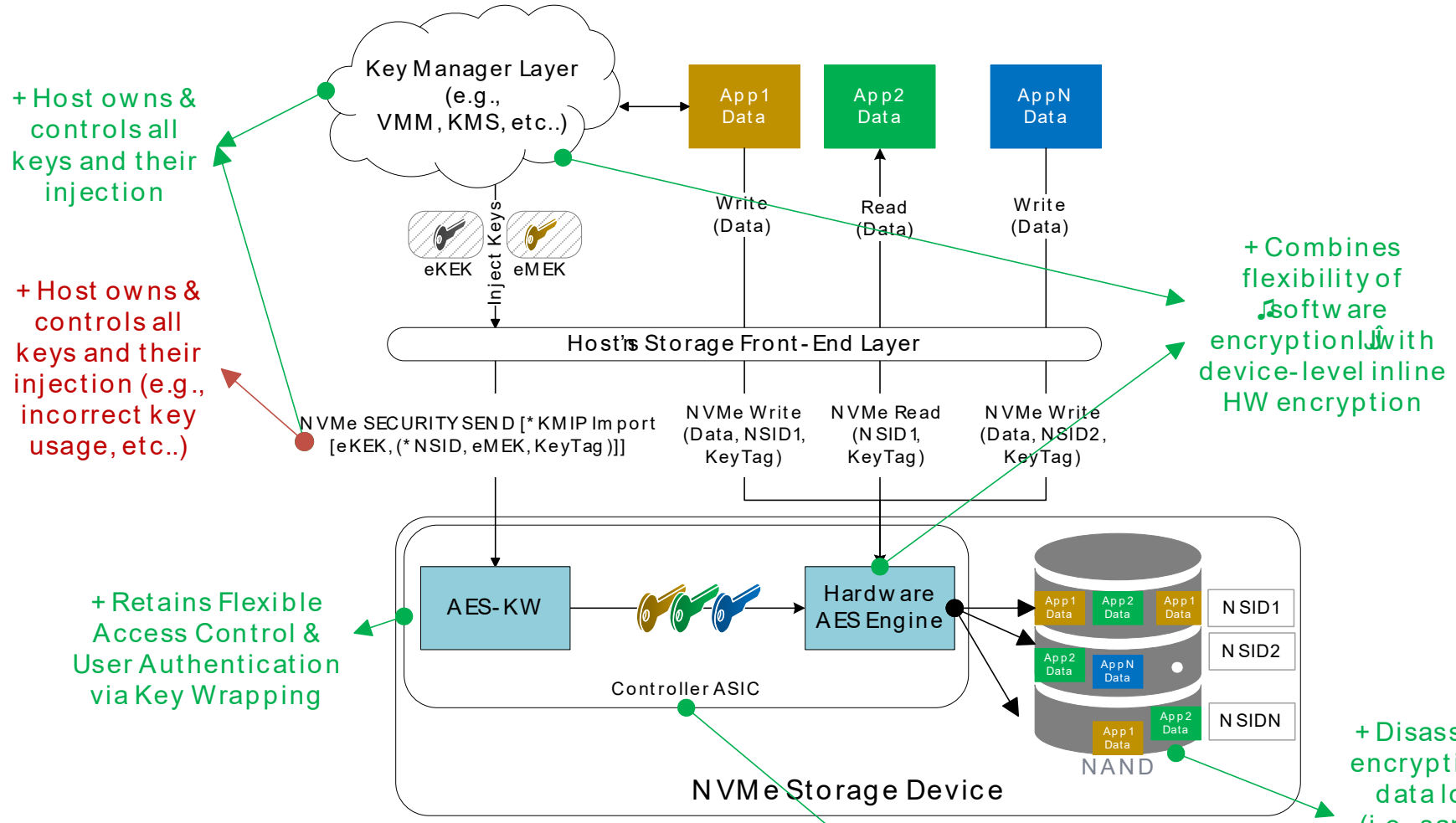
Key Per I/O Overview

Theory of Operation, Arch. Elements & I/O Interactions



*See backup slides for acronyms definitions

Benefits & Challenges

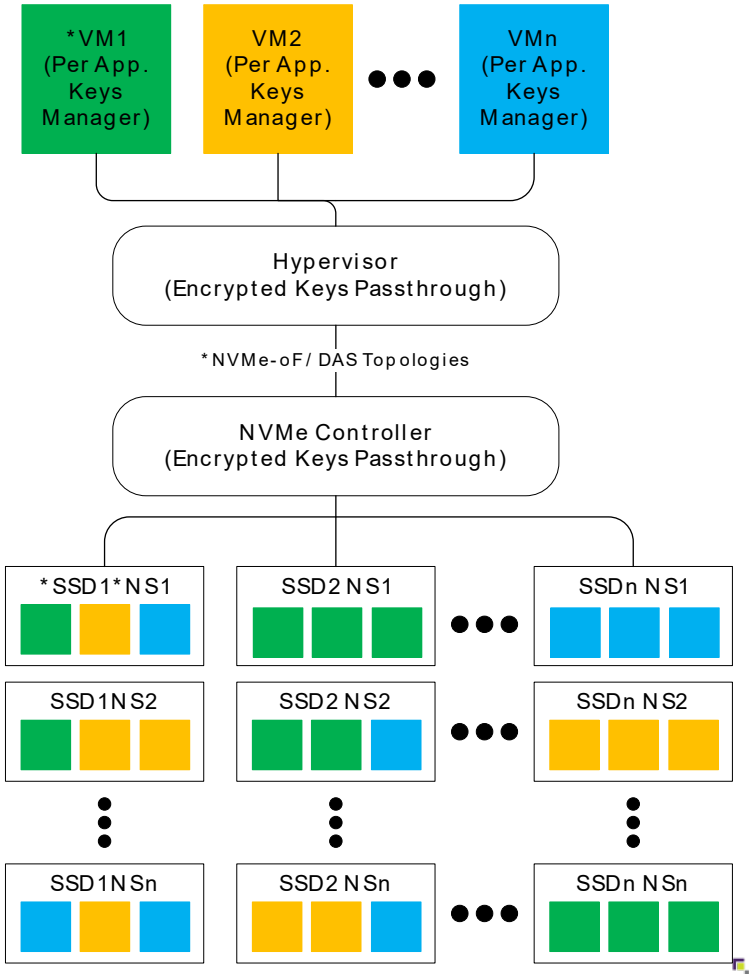


*See backup slides for acronyms definitions

Example Use Case:
Tenant Isolation & Encryption Keys Ownership Models

Option #1:
Users/tenants own & control the entire lifecycle of the keys across distributed storage systems.

- Secure key transport (KTS) is between the users/tenants and the SED.
  - Users control the entire lifecycle of encryption keys on the SED where they'll be used (i.e., key injection, key deletion, key update, etc..)
  - The SED automatically loses encryption keys on power cycles or clear keys requests.
- NVMe controllers only see encrypted keys when mapping them to SED/Namespace resources.

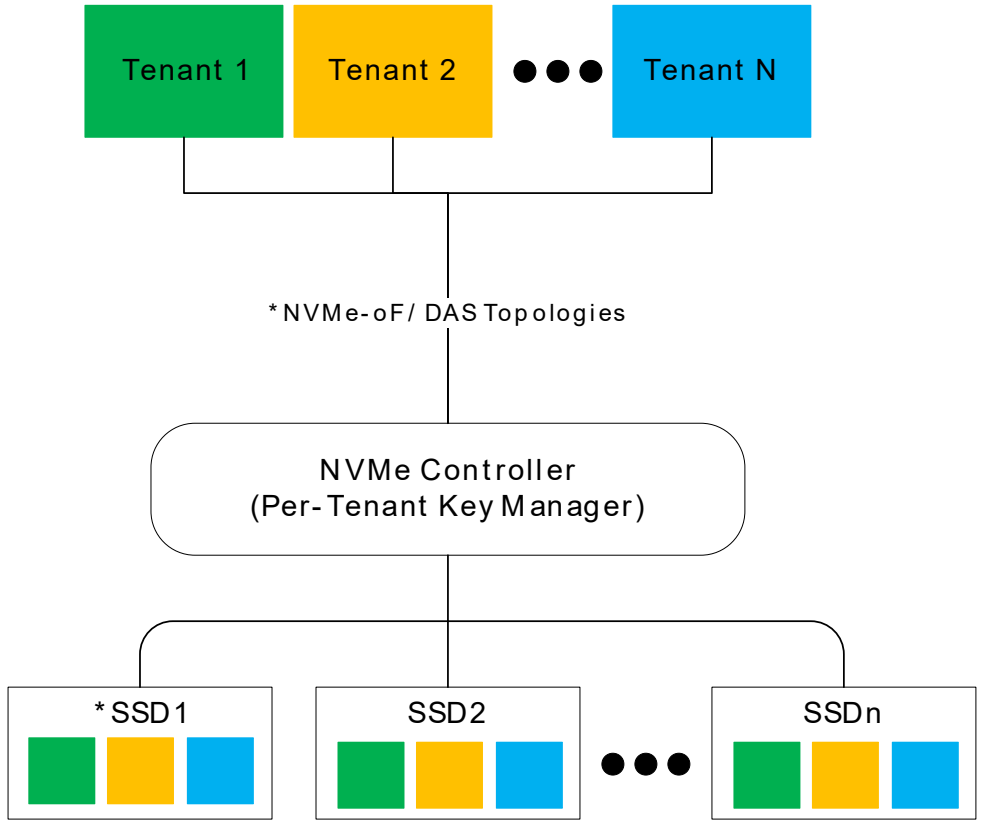


*See backup slides for acronyms definitions

Example Use Case:
Tenant Isolation & Encryption Keys Ownership Models

Option #2:
The storage platform controls the lifecycle of the keys.

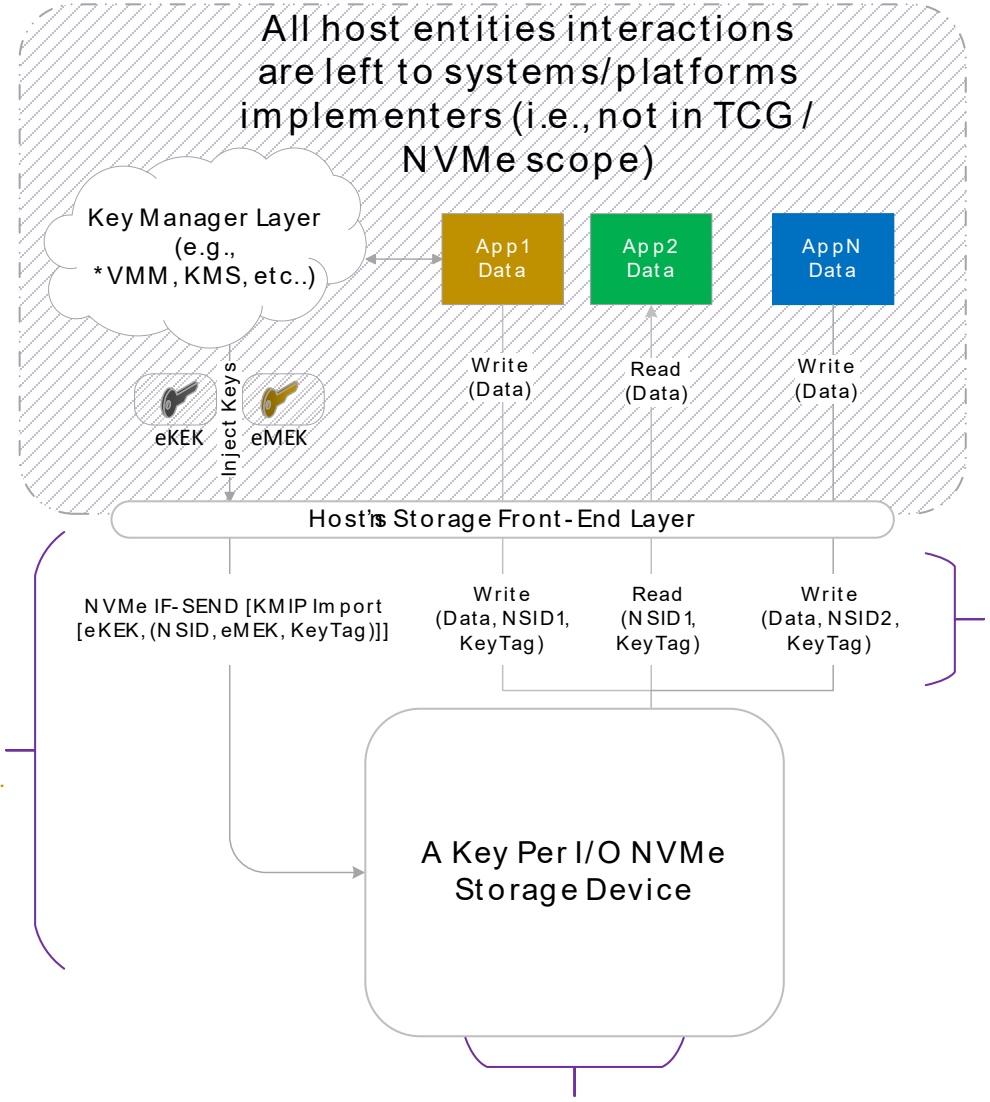
- Secure key transport (KTS) is between the storage platform and the SED.
  - The storage platform controls the entire lifecycle of encryption keys on the SED where they'll be used (i.e., key injection, key deletion, key update, etc..)
  - The SED automatically loses encryption keys on power cycles or clear keys requests.
- NVMe controllers may be designed to only see encrypted keys when mapping them to SED/Namespace resources.
  - Since, host keys would likely be managed by HSMs.



*See backup slides for acronyms definitions

Key Per I/O Industry Specifications Status

Industry Specifications Status



- Application Note Status:
- TCG Key Per I/O SSC v1.00 App Note soon to be public.

- Interface Specifications Status:
- NVMe TP4055 is public.
- TCG *SIIS 1.11is public.
- TCG Key Per I/O *SSC v1.00 soon to be public.

- SED Internal Processing Rules Specifications Status:
- TCG Key Per I/O SSC v1.00 soon to be public.
- TCG Key Per I/O Test Cases v1.00 is in development.

*See backup slides for acronyms definitions

Key Takeaways

- Key Per I/O:
  - Allows a fine-grained control of on-device SED capabilities to better support multi-tenancy usage models.
  - Provides stronger confidentiality of Data-At-Rest from unauthorized access once it leaves the owner's control.
  - Is an Industry Standard-based design for multi-vendor interoperability.
  - Is being specified by TCG Storage Work Group (SWG) such that existing host software TCG protocol infrastructures are compatible.

- Come join us at TCG SWG to continue the discussions!
  - Email: admin@trustedcomputtinggroup.org

Who are TCG and NVMe?

Trusted Computing Group (TCG) *is a not-for-profit organization formed to enable secure computing through open standards and specifications. Benefits of TCG technologies include protection of business-critical data and systems, secure authentication and strong protection of user identities, and the establishment of strong machine identity and network integrity. Trusted hardware and applications reduce enterprise total cost of ownership and support regulatory compliance. Through its member-driven work groups, TCG enables the benefits of trust in computing devices from mobile to embedded systems, as well as networks, storage, infrastructure, and cloud security. Almost all enterprise PCs, many servers, and embedded systems include the TPM; while networking equipment, drives, and other devices and systems deploy other TCG specifications, including self-encrypting drives and network security specifications.*

The original ***NVM Express*** *Work Group was incorporated as NVM Express in 2014 and is the consortium responsible for the development of the NVM Express specification. The organization currently has over 100 member companies.*

NVM Express is an open collection of standards and information to fully expose the benefits of non-volatile memory in all types of computing environments from mobile to data center.

NVMe is designed from the ground up to deliver high bandwidth and low latency storage access for current and future NVM technologies.

SNIA COMPUTE + MEMORY + STORAGE SUMMIT

Architectures, Solutions, and Community
VIRTUAL EVENT, APRIL 11-12, 2023

Backup

Definition of Acronyms

Term	Definition
App	Application
DAR	Data-At-Rest
DAS	Direct-Attach Storage
eKEK	Encrypted Key Encryption Key
eMEK	Encrypted Media Encryption Key
HSM	Hardware Security Module
LBA	A Logical Block Address
NS	Namespace
NSID	Namespace Identifier
NVMe-OF	NVMe-Over-Fabrics
K_AES Table	A table to store keys used in Advanced Encryption Standard algorithms
KMIP	OASIS Key Management Interoperability Protocol
KMS	Key Management System
KW	Key Wrap
SIIS	Storage Interface Interactions Specification
SSC	Security Subsystem Class
VM	Virtual Machine
VMM	Virtual Machine Monitor

SNIA COMPUTE + MEMORY + STORAGE SUMMIT

Architectures, Solutions, and Community
VIRTUAL EVENT, APRIL 11-12, 2023

Please take a moment to rate this session.

Your feedback is important to us.

