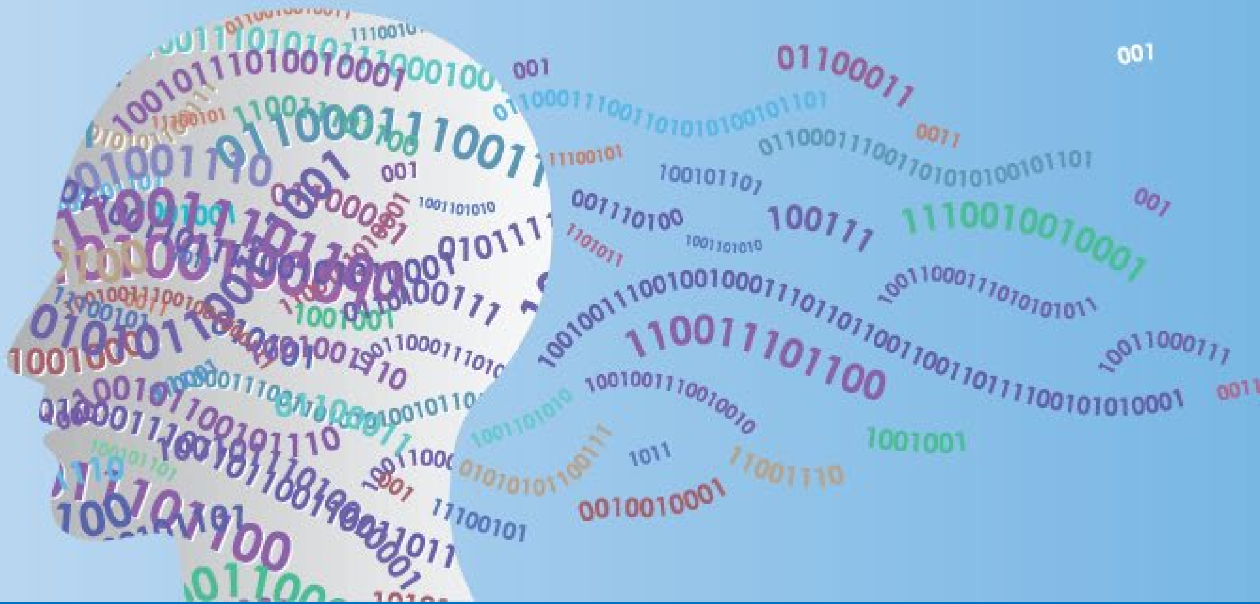
SNIA PERSISTENT MEMORY + COMPUTATIONAL STORAGE SUMMIT 2021

FROM DATACENTER TO EDGE : VIRTUAL EVENT
APRIL 21-22, 2021



Security with Computational Storage Drives

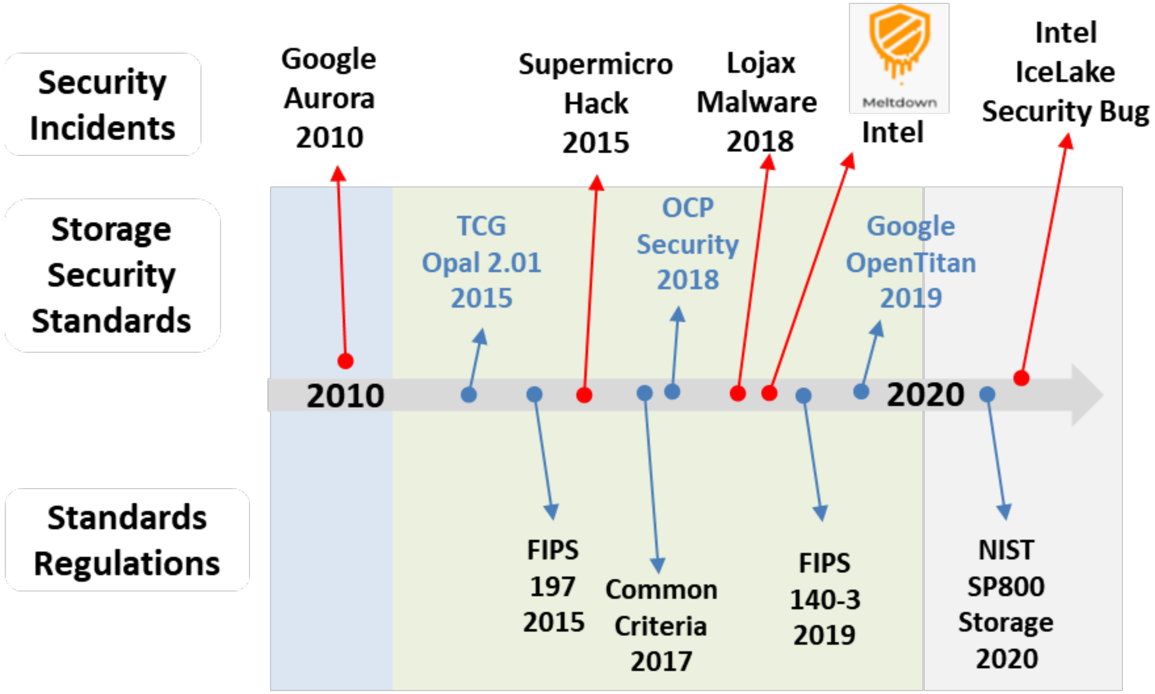
David McIntyre
Director, Product Planning and Business Enablement
Samsung Corporation

Agenda

- Introduction to Computational Storage Drives (CSDs)
- New security risks exposed by CSDs
- Security standards for Computational Storage
- Addressing risks
  - CSD security features
  - Other features: SW, HW, system-level
- Call to Action

Datacenter Security and Standards

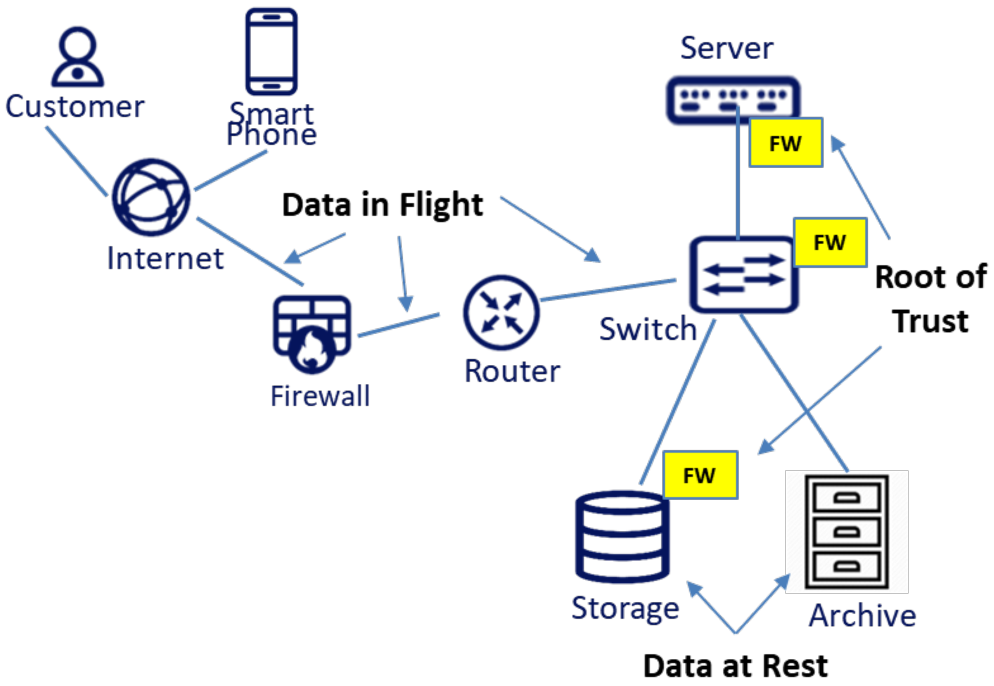
Rapid Changing Security Standards



- Standards, Security threats growing in past 10 yrs.
- New Security Standards organizations emerged
  - Open Compute Security Initiative
  - TCG Opal SSC (Enterprise, Device)
  - DMTF SPDM* (Enterprise, Manageability)

*SPDM: Security Protocol and Data Model

Data Center Security Considerations

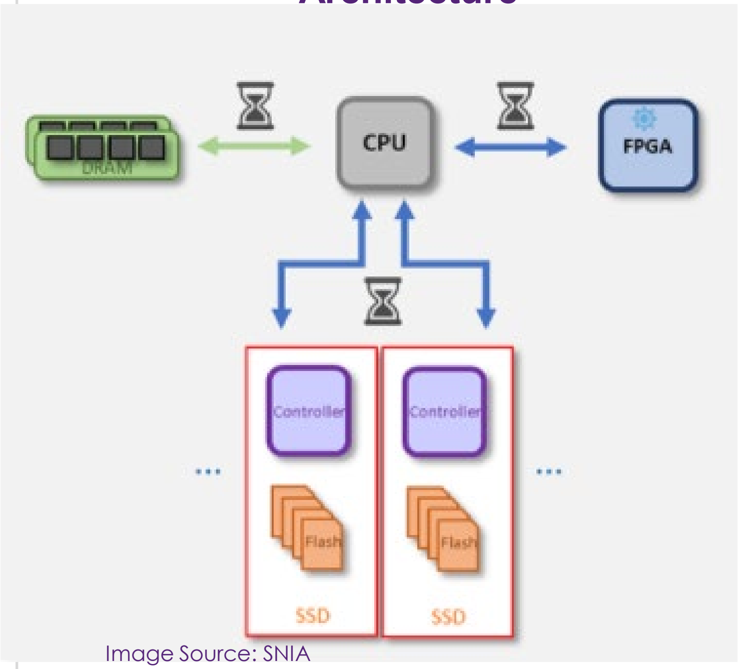


- **Data in Flight**: Network security
- **Data at Rest**: Against theft of data or keys, and ransomware (esp. SSD media and key encryption with SSDs
- **HW Root of Trust** : Dedicated security engine to ensure Secure Boot, Secure FW, and Key Management across all peripherals

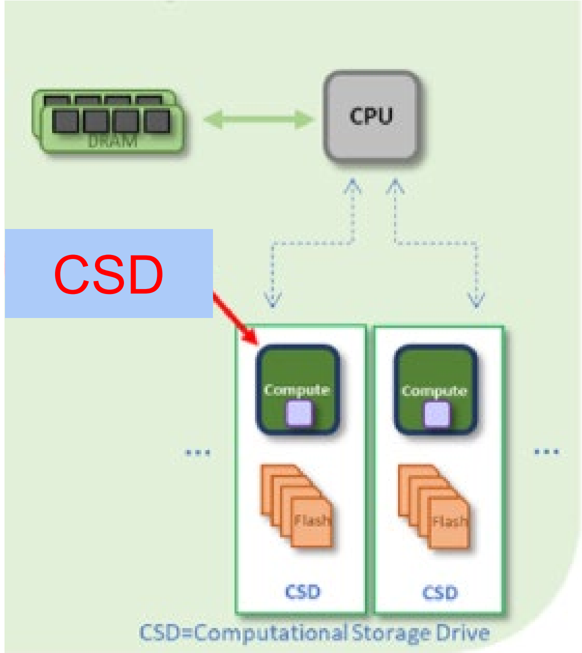
Computational Storage Drives (CSD) Overview

Move Compute Closer to Storage

Current Compute/Storage Architecture



Computational Storage Architecture

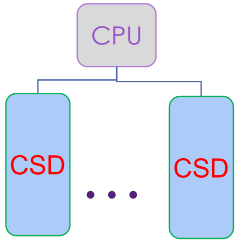


- Moving data between storage and host CPU creates performance bottlenecks for data-intensive applications

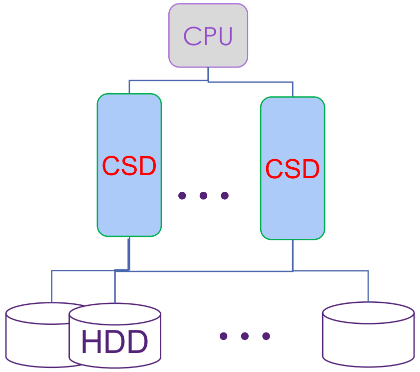
- Data processed directly on the CSD => no large data transfers, faster time-to-insight
- Adding CSDs adds processing power and internal bandwidth => scalable acceleration

Deployment Examples

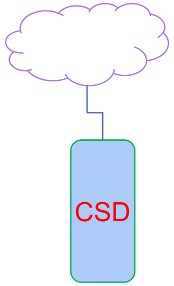
- Compute/Storage Server



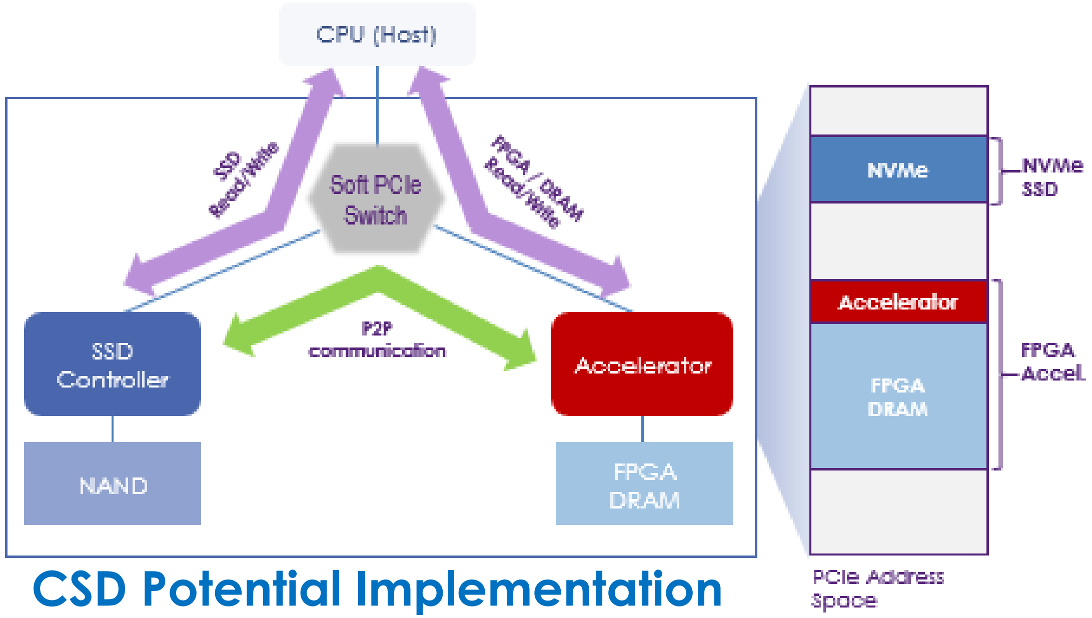
- Smart Cache Layer



- Cloud to Edge Compute



Potential Computational Storage Drive Implementation and Exposure



CSD Potential Implementation

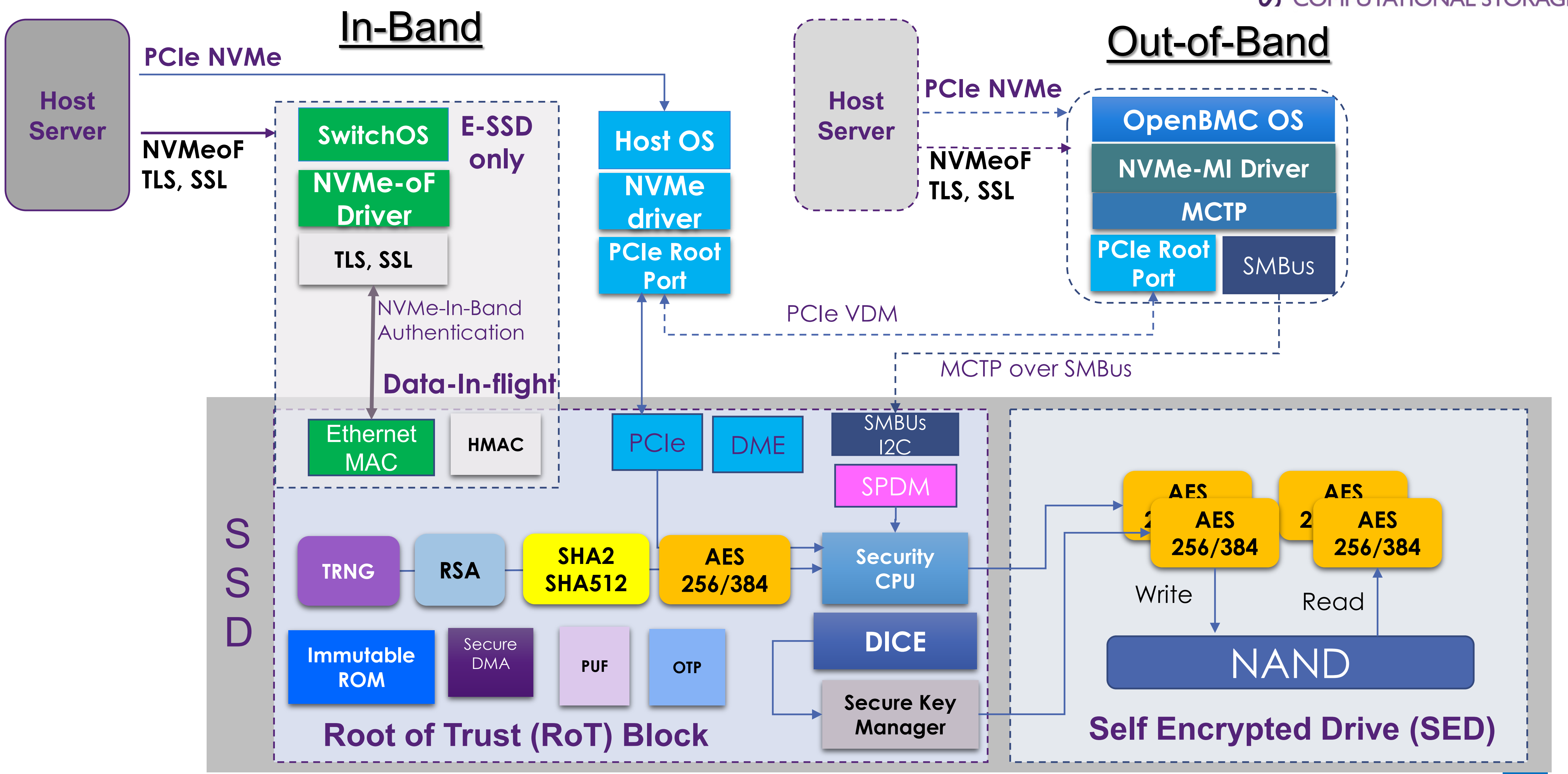
FPGA Accelerator, Flash Controller, DRAM, NAND

- Peer-to-peer (P2P) communication enables unlimited concurrency

SSD-to-Accelerator data transfers use internal data path

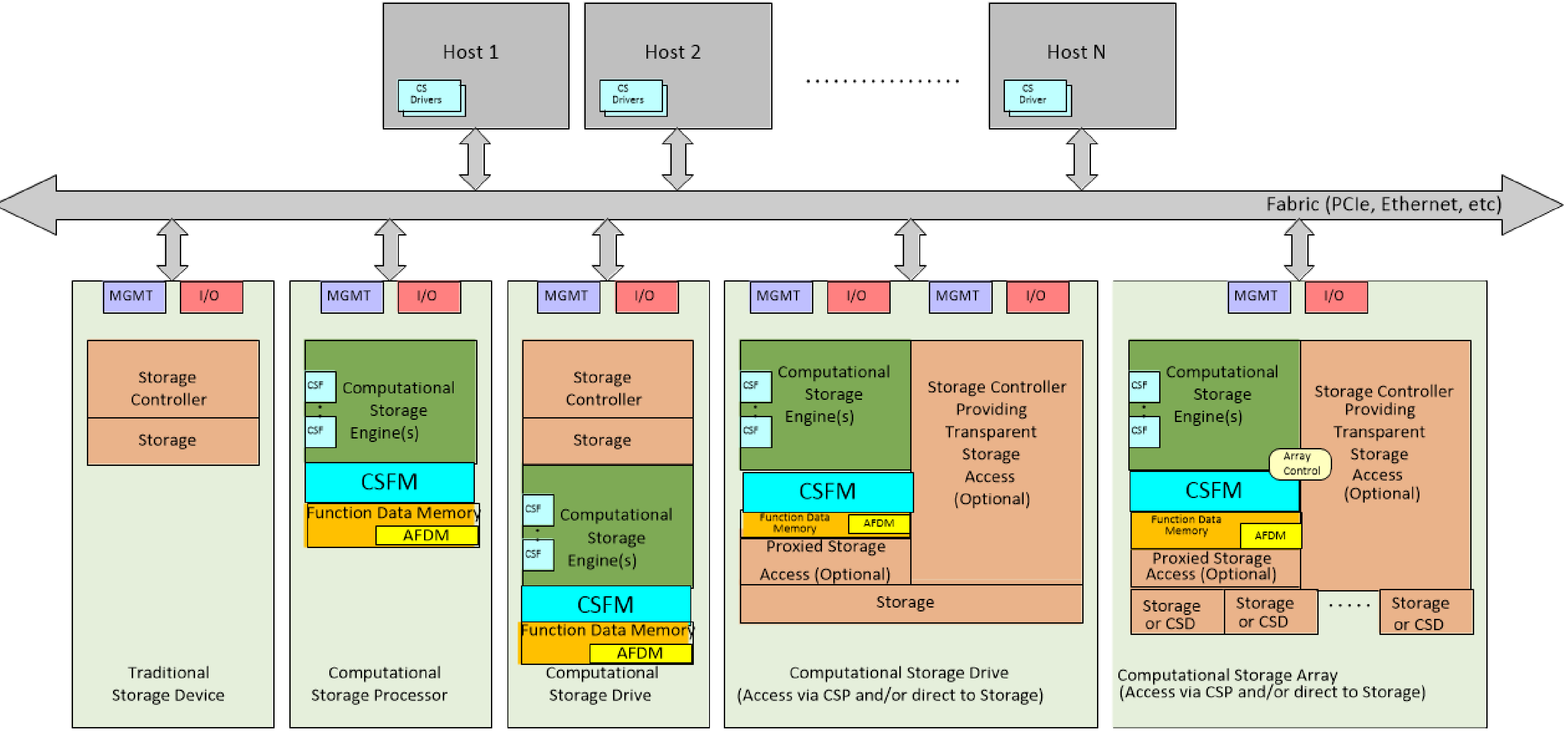
- Save precious L2:DRAM Bandwidth (Compute Nodes) / Scale without costly x86 frontend (Storage Nodes)
- Avoid the unnecessary funneling and data movement of standalone accelerators
- FPGA DRAM is exposed to Host PCIe address space
- NVMe commands can securely stream data from SSD to FPGA peer-to-peer

One View of Host-CSD Framework



re: Samsung SSI

New Risks Exposed by Computational Storage Drives



Security Functions:

- **Authentication.** Host agent to CSD
- **Authorization.** Secure data access & permissions
- **Encryption.** Encrypted data mechanisms
- **Auditing.** Generating/ retrieving secure logs

Risks vs standard storage:

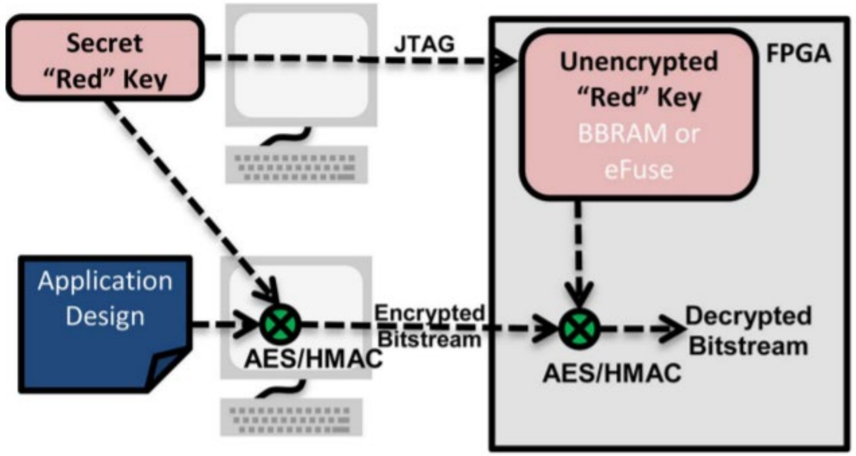
- The CSD may delete/add/modify data on the drive
- The CSD functionality may be programmed
- Virtualization

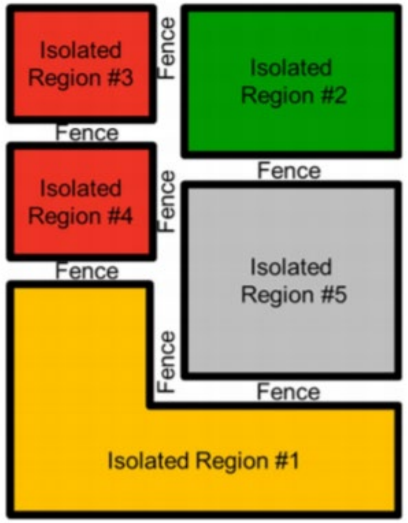
Risks vs external accelerator:

- Direct access to storage
- FPGA programming
- Access to network infrastructure (NVMe-oF)
- Decryption of data prior to processing

Ccomponent level considerations e.g. FPGA

- **FPGAs are SRAM based devices which are programmed by secure bit streams**
  - Key is programmed via JTAG port
  - Bitstream is encrypted with design tools
  - FPGA identifies encrypt/no encrypt for field testing
- **AES 256 secures bitstream programs**
- **Additional Security Measures**
  - Design Region Isolation
  - JIT Partial Reconfiguration
  - SOC and Bus Isolation
  - PUF files for device dependency
  - E-fusing





https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6849432

Developments in Security for Computational Storage

➢ Work in standards on security for CS

- SNIA – Computational Storage TWG
  - Host access and interfaces
  - API standardization in progress
  - *Q4’2021 – standard (expected)*
- **NEW:** SNIA Computational Storage Security Sub Group
- NVMe – Computational Storage Task Group
  - Device access, interfaces and implementation
  - *Q1’2022 – standard (expected)*

Threats
- Storage Infrastructure
- Bypass and Offload
- Computational Engines

Security Considerations by Cloud Service Providers

- Notable Cloud Service Provider Security Policy Categories
  - Data-in-flight
  - Processing requirements in data handling
  - Buffering, caching
  - Data-at-rest policies
  - Containers
  - Virtualization
  - Multi-tenant
  - Edge deployments for in-situ storage processing

Storage Security Pillars
and the standards that mandate them

1. Root of Trust
Microsoft Cerberus
Google OpenTitan
Intel TXT/TPM

2. Crypto
NIST SP800
*FIPS-140-2
*GDPR/ISO Requirements

3. Secure Enclaves
NIST *CSRC
OCP
Microsoft

4. Self-Encrypting Drive
TCG Opal
NIST SP 800

5. Key Management
*TCG DICE
NIST SP 800-57
*DMTF

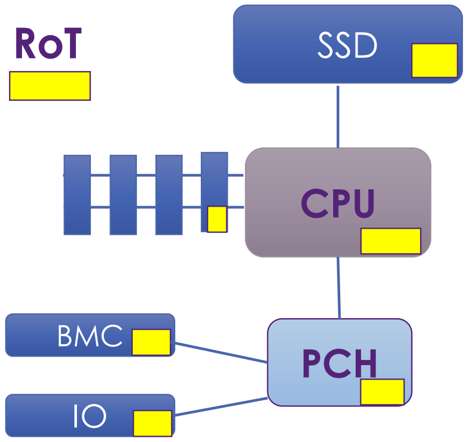
6. Security Lifecycle
Manufacturing/
Vendor Specific
*NIST SP 800

*NIST: National Institute of Standards and Technology
*TCG: Trusted Computing Group
*FIPS: US Federal Information Processing Standards
*GDPR: EU General Data Protection Regulation
*CSRC: US Federal Computer Security Resource Center
* DMTF: Distributed Management Task Force

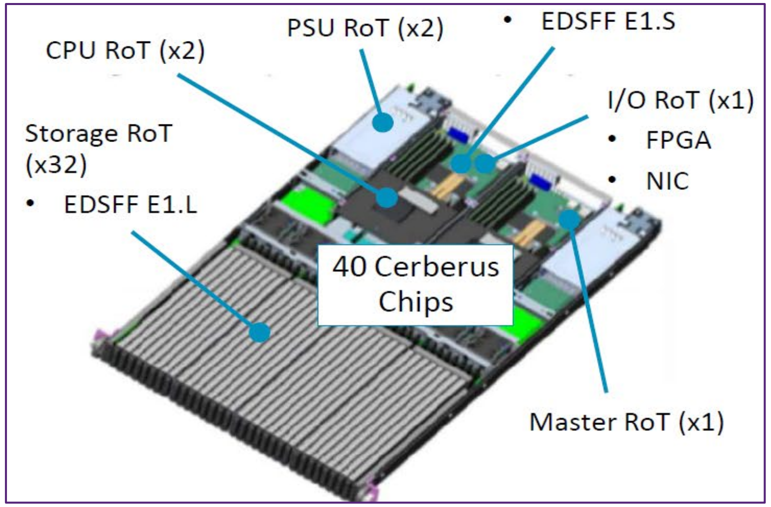
1. Roots of Trust

allow a system to trust its peripheral components

OCP Cerberus RoT

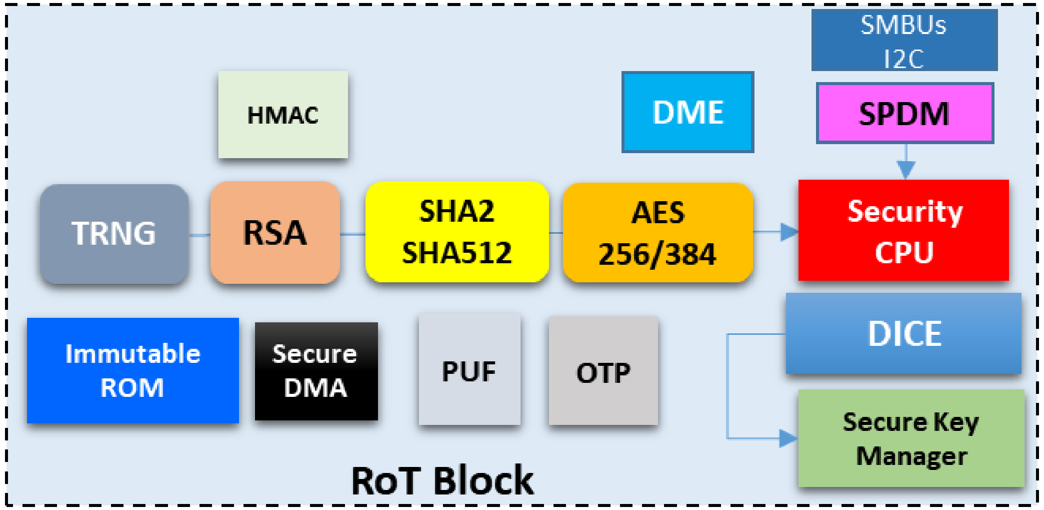


- Enables standard secure boot across all devices on the platform
- Prevents physical and side-channel attacks
- Automated and Secure Key Management



Microsoft Storage Server with 40 Cerberus chips

MSFT Cerberus Components



- **Microsoft has enhanced Cerberus RoT features**
- **Cerberus RoT enables:**
  - Secure Boot
  - Secure key storage and protocol for key management
  - Advanced security strength with AES 256, ECDSA 384
  - Host/Client secure communication via I2C/SMBus
  - Security through-out the Lifecycle of SSD Data and Keys

2. Crypto / 3. Secure Enclaves

allow a system to securely handle drive boot firmware and unencrypted keys

2. Crypto

- Cryptography standards are recommended by NIST and FIPS-140 for use in data processing
- FIPS-140 sets the standards for Security Strength Requirements for **CRYPTOGRAPHIC** Modules.

SSD Cryptographic Modules

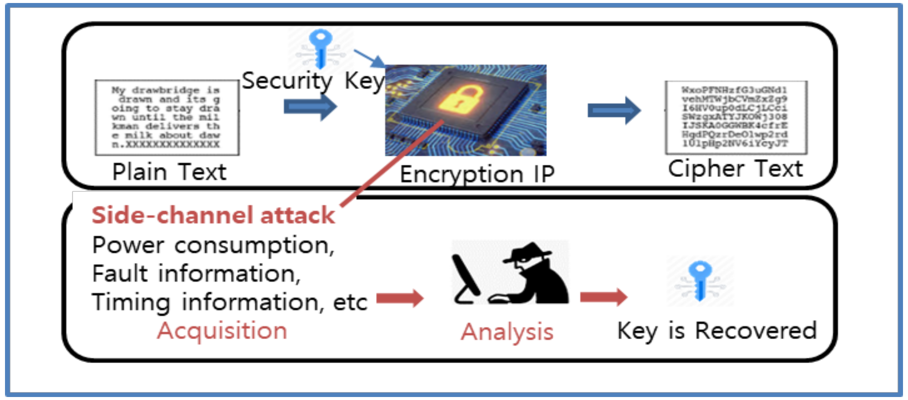
RSA | AES | ECDSA | HMAC

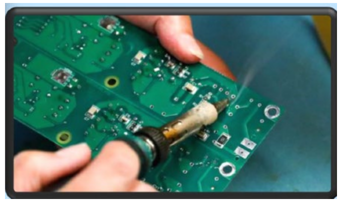
Security CPU

Security Strength	2030	2030+
AES	AES 128 →	AES 256
ECDSA	ECDSA 256 →	ECDSA 384
RSA	3072 →	4096

3. Secure Enclaves

- Protection against Physical & Side-Channel attacks are generated with Power monitoring, EMT, and Timing.
- Secure Enclaves are recommended for NIST and Common Criteria (EU) compliance and required by Cloud companies





SuperMicro hack

Hardware Tampering
Side-Channel Attack
with Differential
Power Consumption

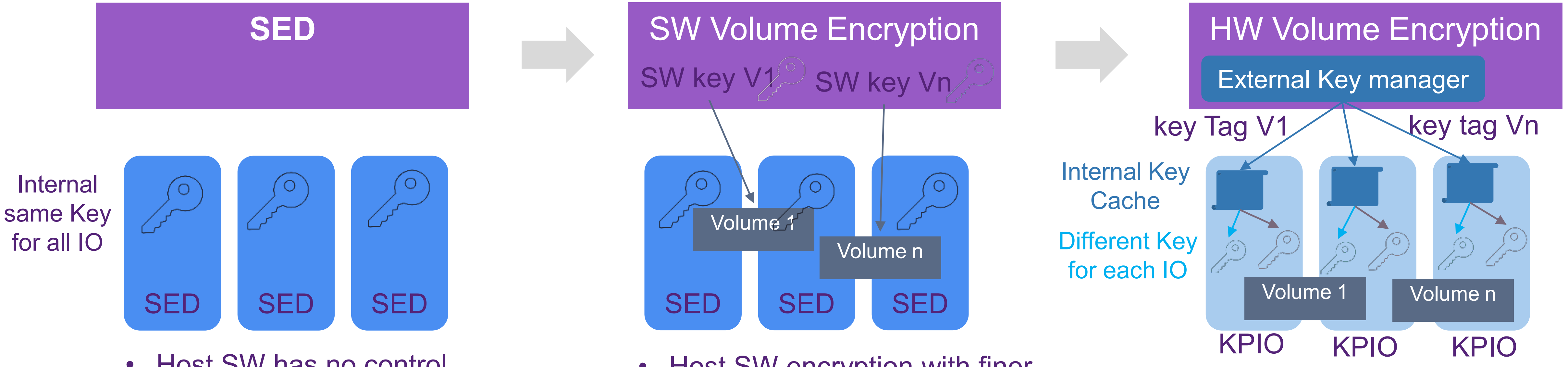
Security Subsystem
SSD Cont CPU / NAND

SSD w/o Enclaves

Security Subsystem
SSD Cont CPU / NAND

SSD with Enclaves

4. From SED today to Key per IO in the Future



- Host SW has no control
- SED drive encryption all IO blocks with same key.

Current	New 2019	2030
FIPS-140-2	FIPS-140-3	
✓ FIPS Level 2 Certification	✓ + FIPS-140-2	
✓ 128bit Security Strength	✓ TCG Opal 2.01 Compliance	
✓ HW Validation Only	✓ 256bit Security Strength	
	✗ FIPS Level 3 Certification*	

- Host SW encryption with finer granularity for volume
- SED drive encryption all IO blocks for volumes with same key
- FIPS-140-2

- Fine-grain HW encryption (new key per volume, per VM, or per IO)
- Offloads the CPU
- FIPS-140-3

- **<u>New SSD controller required</u>**

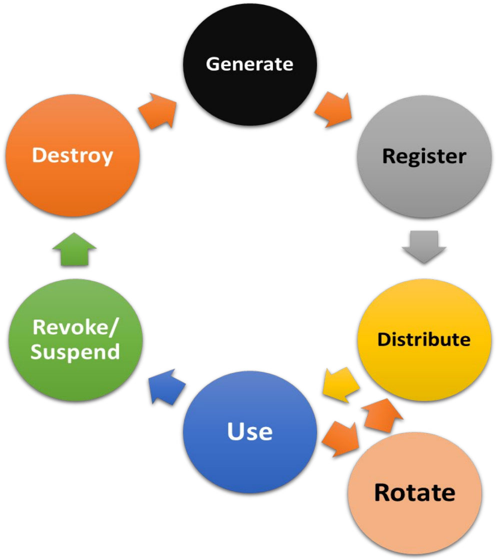
- Level 3 requires physical tamper circuitry inside SSD enclosure
- FIPS-140: US Government Security Requirements for Cryptographic Modules

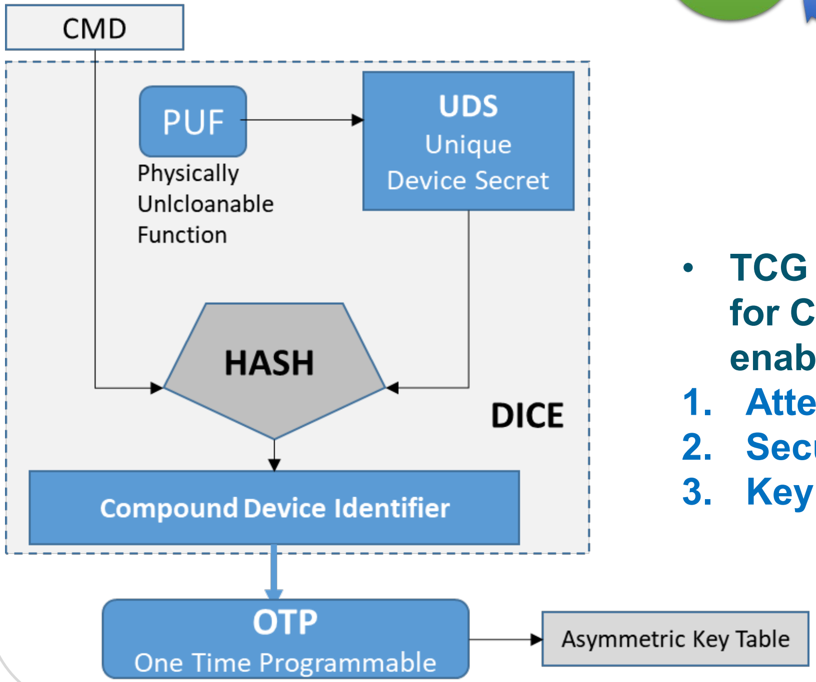
5. Key Management / 6. Security Lifecycle

allow peripherals to implement and interoperate with security best practices

5. Key Management

- Key management focuses on **protecting keys from threats**, and **ensuring** security of keys thru lifecycle of SSD.





- **TCG DICE is a requirement for Cerberus RoT and enables:**
1. **Attestation protocol**
2. **Secure boot**
3. **Key management**

6. Security Lifecycle

- **Security Lifecycle:** Customers have requirements covering every stage from Manufacturing to Cloud Deployment to Infrastructure Decommissioning.

- **NIST 800-88 and ISO** recommends how Keys generated, Crypto Erase and Media Sanitization. TCG Opal Spec recommends standards for Crypto Erase.

Manufacturing
- PUF
- UDS
- TRNG
- OTP

Vendor ID Inject
- DME
- Cerberus
- OTP

Decommission/Retire
- Crypto Erase
- Crypto Sanitize
- OTP

Microsoft Cerberus and Google OpenTitan

Cerberus spec is complex & several specifications including custom Azure lifecycle requirements

PERSISTENT MEMORY + SUMMIT 2021 COMPUTATIONAL STORAGE

Security Pillars	Microsoft facebook	Google
Root of Trust	Project Cerberus arm	opentitan RISC-V
Crypto Modules	✓ AES-256, ECDSA 384 ✓ SHA-512, RSA-4096,	✓ AES-128, ECDSA 256 ✓ RSA 3076, HMAC-SHA2
Secure Enclaves	✓ Isolated Power Domain ✓ Tamper shield, Temp	✓ Alert Responder
SED	✓ TCG Opal 2.01 ✓ PSID	✓ TCG Opal 2.01
Key Management	✓ TCG DICE ✓ 768-bits of OTP	✓ OTP
Security Lifecycle	✓ DME, PUF, UDS ✓ Crypto-Erase	✓ OTP fuses
Schedule	Microsoft Gen8 1H'21	2022+

✓ Meets highest requirements
✓ Meets minimum requirements

Call to Action: Put On Your Security Hat

- Participate in SNIA Computational Storage TWGs
- Contribute industry use cases that should be considered for security issues
- Attend SNIA compute, storage and networking events and think security
- Join the SNIA Computational Storage Security Sub Committee
  - ***Newly remodeled***: Addressing security threats and solutions for our industry!

Thank you

Please visit www.snia.org/pm-summit for presentations