sodacon
— Global 2021 — July 13-14

Computational Storage
Security Challenges and Solutions
for the Hybrid Cloud

David McIntyre
Director, Product Planning and Business Enablement
Samsung Corp.

July 14, 2021

soda
foundation

#sodacon2021

Common Threat Actors

- Cyber Terrorists
- Government-sponsored/State-sponsored Actors
- Organized Crime/Cybercriminals
- Hacktivists
- Insiders
- Script Kiddies
- Internal User Errors

Common Motivations

- Political, Economic, Technical, and Military Agendas
- Profit/Financial Gain
- Notoriety
- Revenge
- Multiple/Ov

Security is a People Problem!

Heavily Regulated

Privacy:
Collection Limitations, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, Accountability
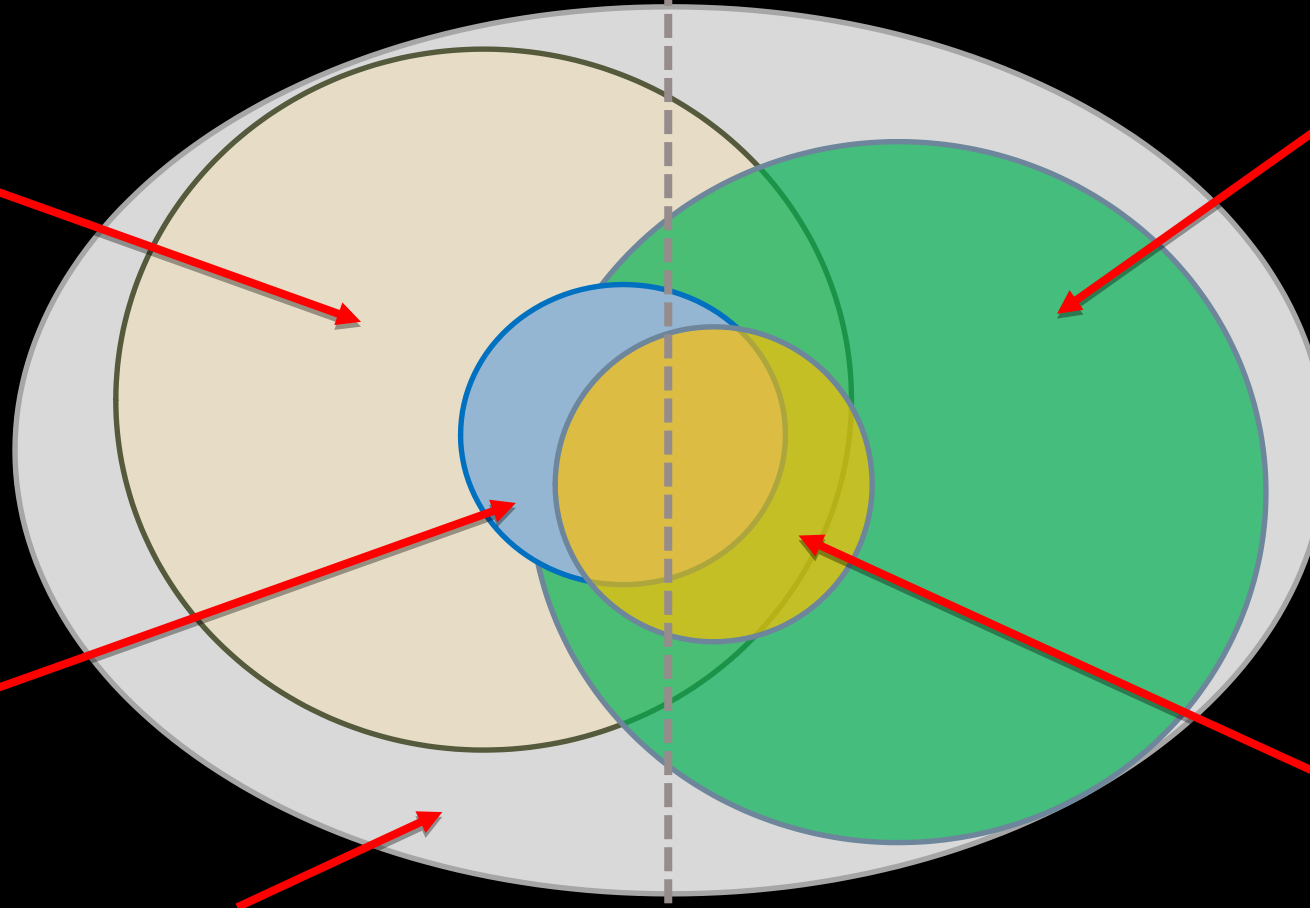
Information Security:
Ensures Confidentiality, Integrity, and Availability (CIA) of information

Personal Data Protection:
Safeguards applying under various laws and regulations to personal data (PII, PHI, etc.) about individuals that organizations collect, store, use and disclose

Ethics: Moral principles that govern Person's behavior or the conducting of an activity

Cybersecurity: Ensures Confidentiality, Integrity, and Availability of data; Identify, Protect, Detect, Respond, Recover

sodacon
— Global 2021 — July 13-14

#sodacon2021

4

Security and Data Resiliency at Par

Data Security

Data Protection

Information Assurance

Information Security

Information Dependability

Confidentiality, Integrity, Availability, Accountability…

Reliability, Availability, Fault Prevention, Avoidance & Tolerance, Performance…

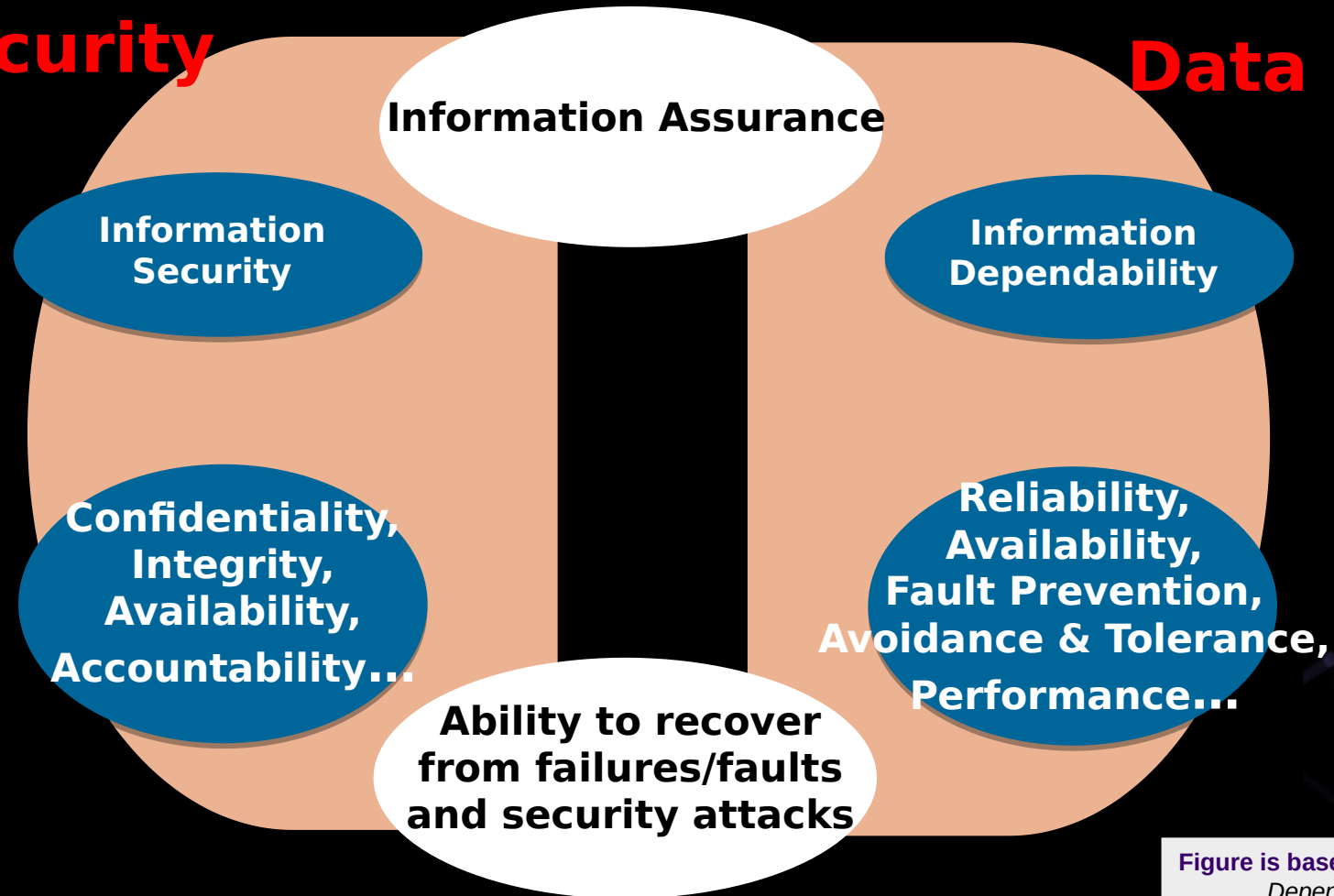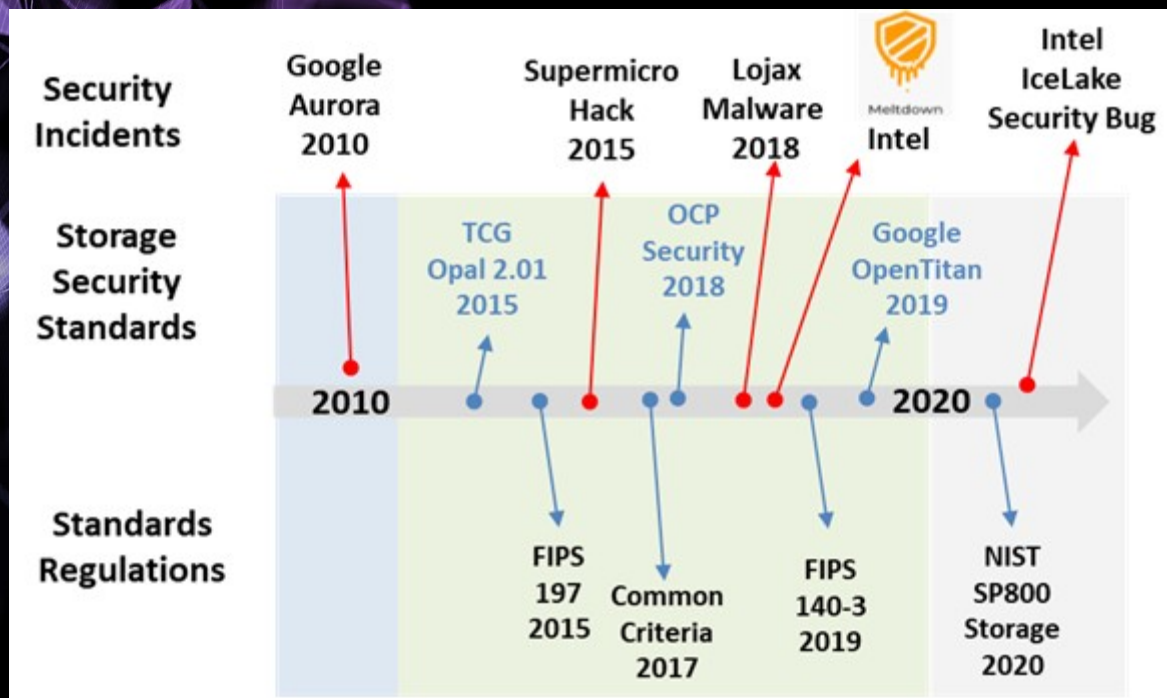Ability to recover from failures/faults and security attacks

Figure is based on the: *Information Assurance – Dependability and Security in Networked Systems*, Qian, Joshi, Tipper, Krishnamurthy, 2008, New York, ISBN: 978-0-12-373566-9.
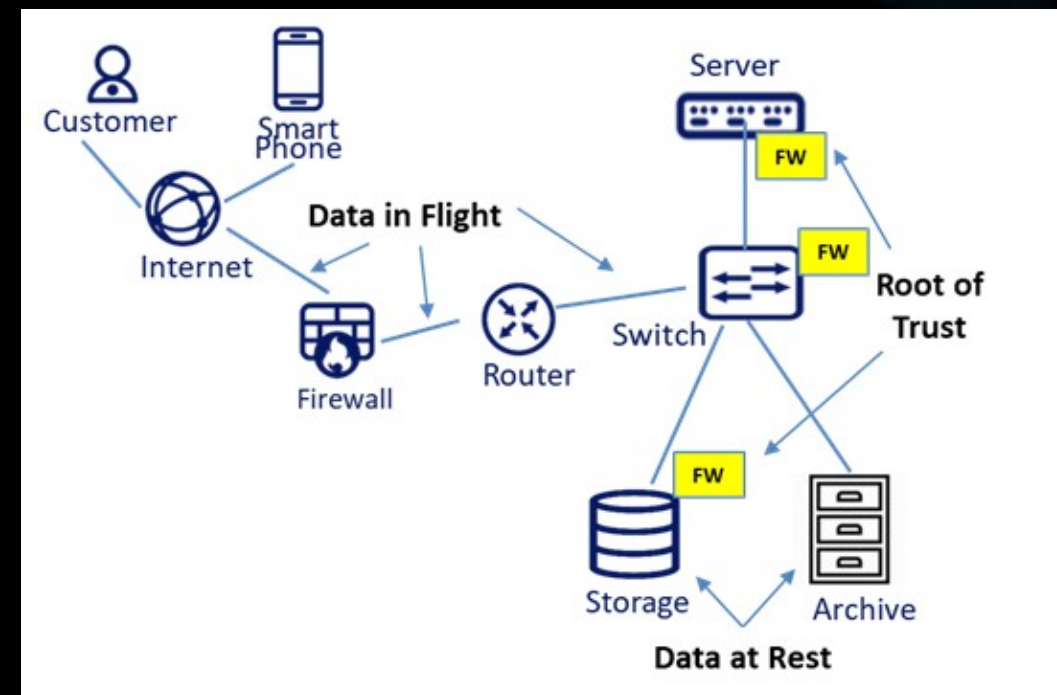
sodacon
— Global 2021 — July 13-14

#sodacon2021

Data Center 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)

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

sodacon
— Global 2021 — July 13-14

#sodacon2021

Computational Storage Security Risks

➢ **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**

#sodacon2021

Computational Storage Drives (CSD) Overview

Current Compute/Storage Architecture

Computational Storage Architecture

Image Source: SNIA

CSD

CSD=Computational Storage Drive
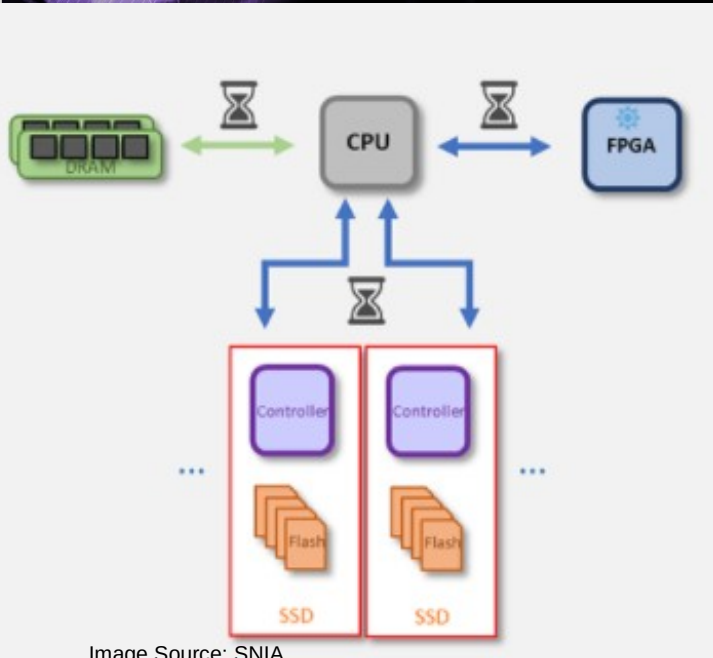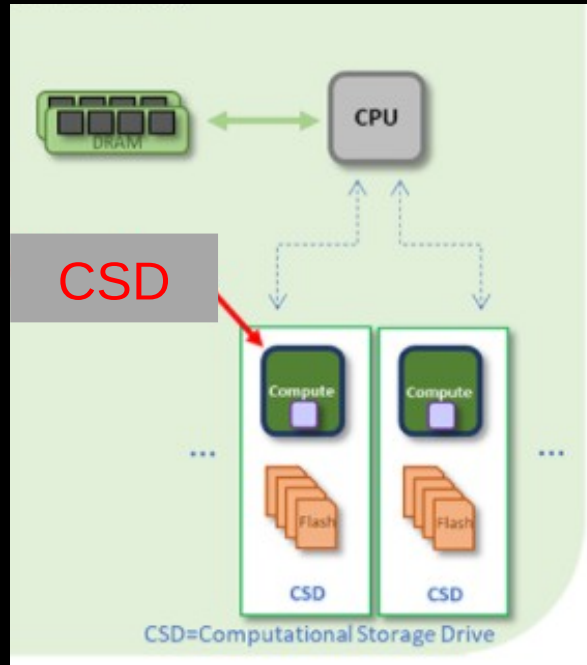
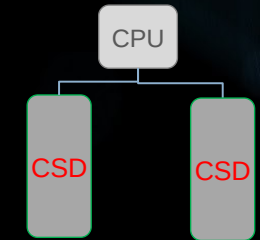Moving data between storage and host CPU creates performance bottlenecks for data-intensive applications

Data processed directly on the CSD => no large data transfers, Adding CSDs adds processing power and internal bandwidth => scalable acceleration
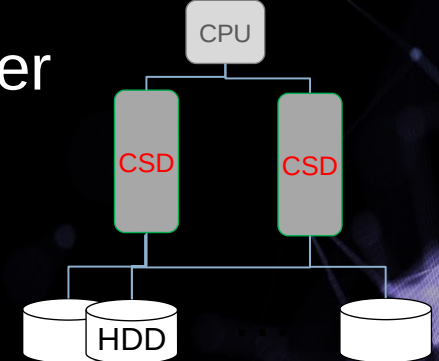
Compute/Storage Server

Smart Cache Layer

Cloud to Edge Compute

#sodacon2021

sodacon
— Global 2021 — July 13-14

Potential Computational Storage Drive Implementation and Exposure

CSD Potential Implementation
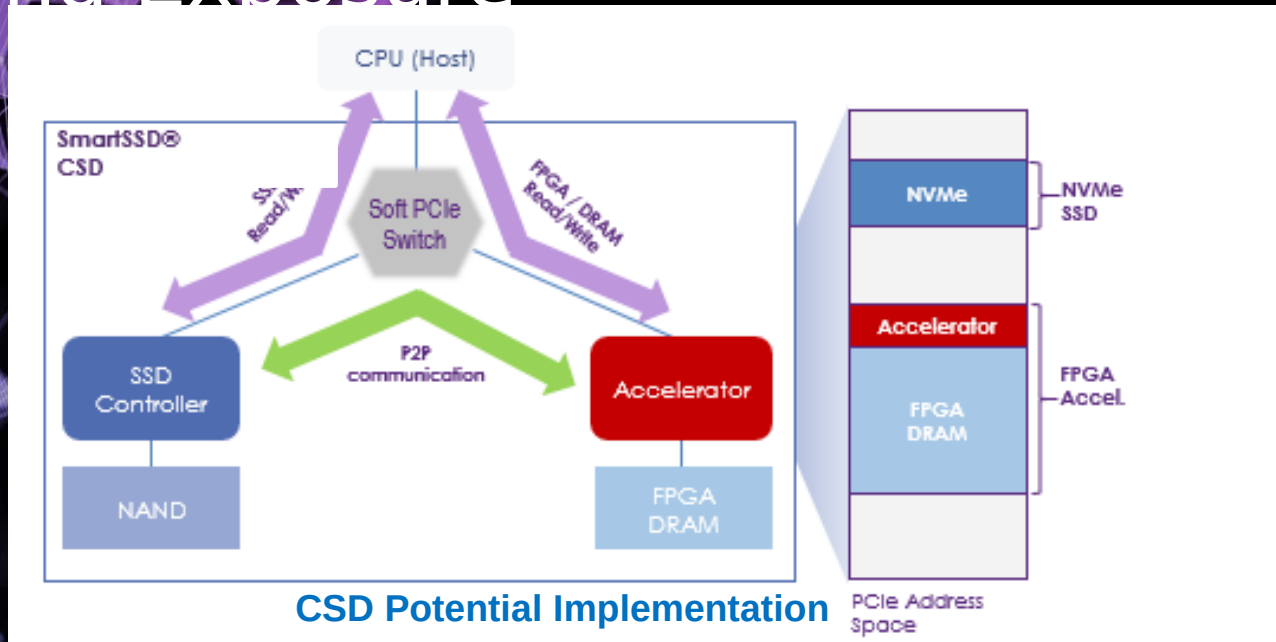
FPGA Accelerator, Flash Controller, DRAM, NAND
  Peer-to-peer (P2P) communication enables unlimited concurrency

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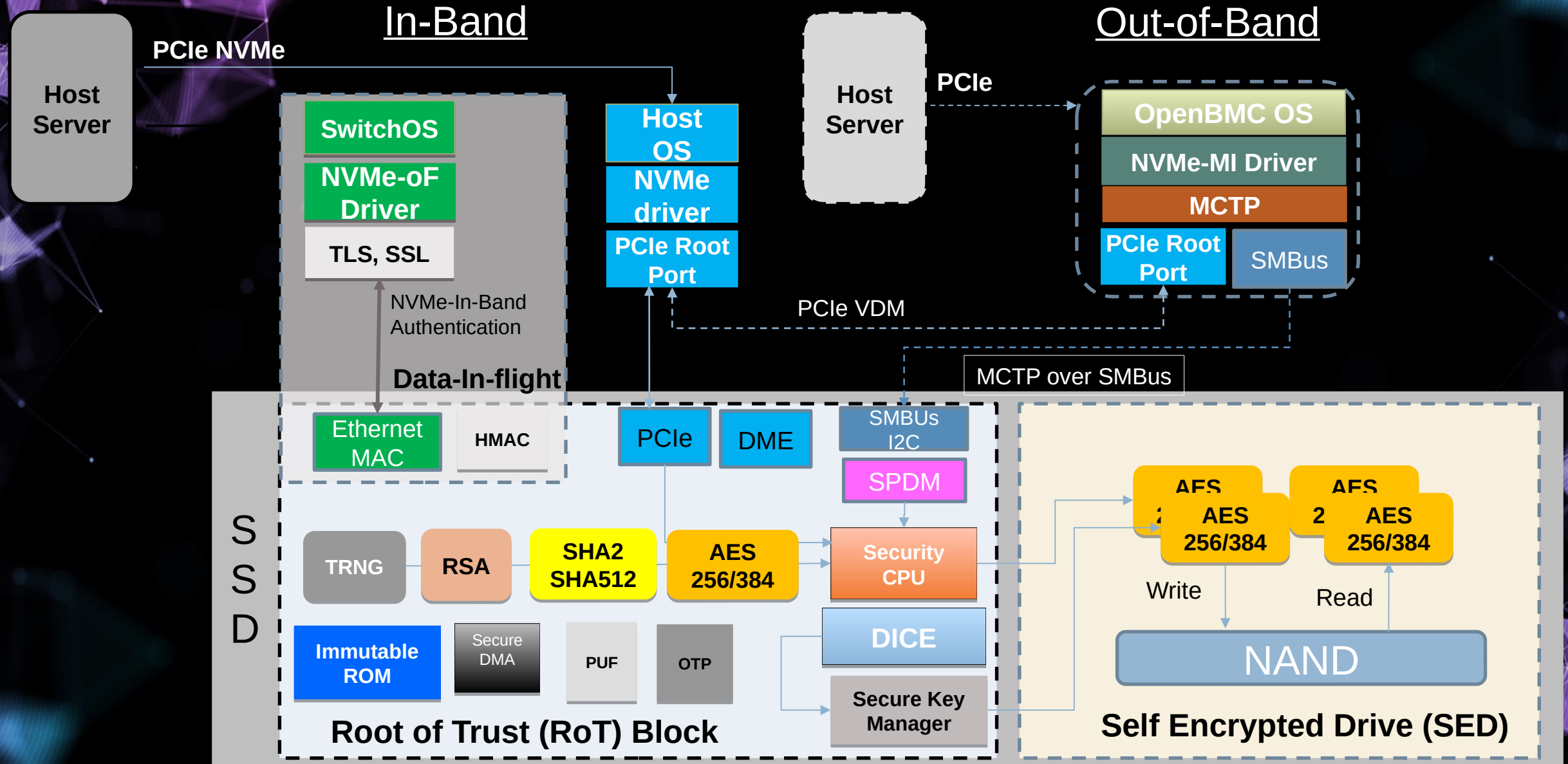 FPGA DRAM is exposed to Host PCIe address space
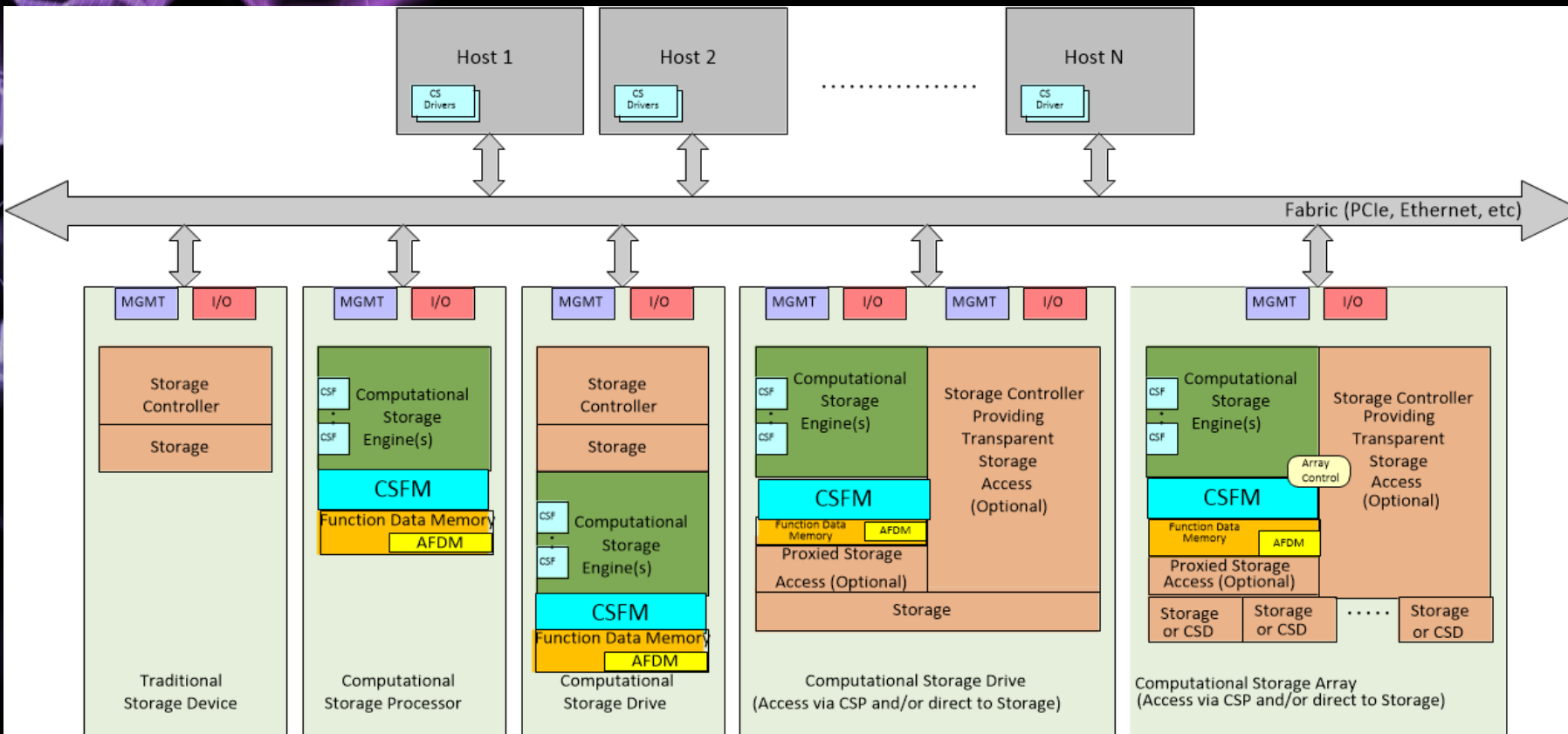 NVMe commands can securely stream data from SSD to FPGA peer-to-peer

One View of Host-CSD Framework

In-Band

Out-of-Band

Host Server

PCIe NVMe

SwitchOS

NVMe-oF Driver

TLS, SSL

NVMe-In-Band Authentication

Data-In-flight

Host OS

NVMe driver

PCIe Root Port

Host Server

PCIe

OpenBMC OS

NVMe-MI Driver

MCTP

PCIe Root Port

SMBus

PCIe VDM

MCTP over SMBus

Ethernet MAC

HMAC

PCIe

DME

SMBUs I2C

SPDM

AFS

AES 256/384

AFS

AES 256/384

S
S
D

TRNG

RSA

SHA2 SHA512

AES 256/384

Security CPU

Write

Read

Immutable ROM

Secure DMA

PUF

OTP

DICE

Secure Key Manager

NAND

Root of Trust (RoT) Block

Self Encrypted Drive (SED)

— Global 2021 — July 13-14

#SDDCon2021

Samsung SSD

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

sodacon
— Global 2021 — July 13-14

#sodacon2021

Component 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
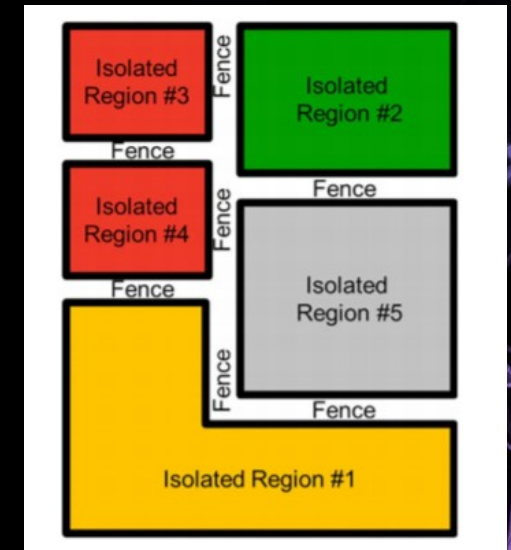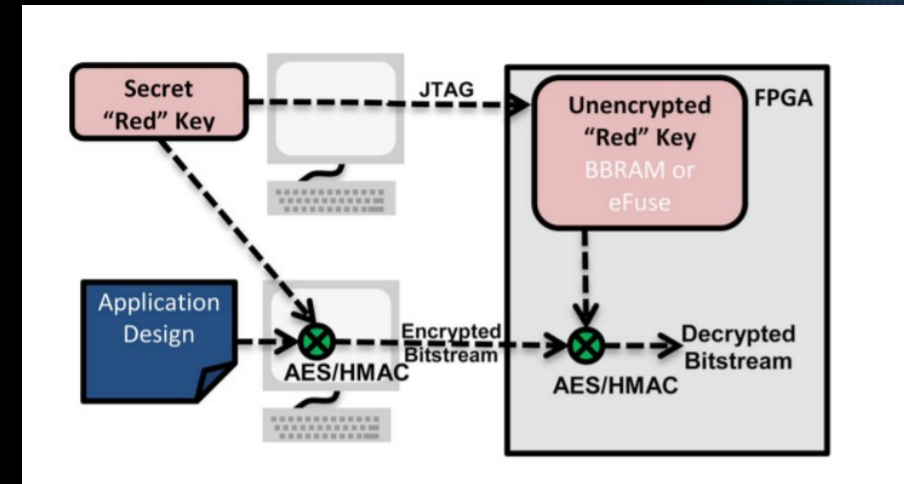
Developments in Standards Orgs for Computational Storage Security

➢ **SNIA – Computational Storage TWG**

- Host access and interfaces

- API standardization in progress

- *Q4'2021 – standard (expected)*
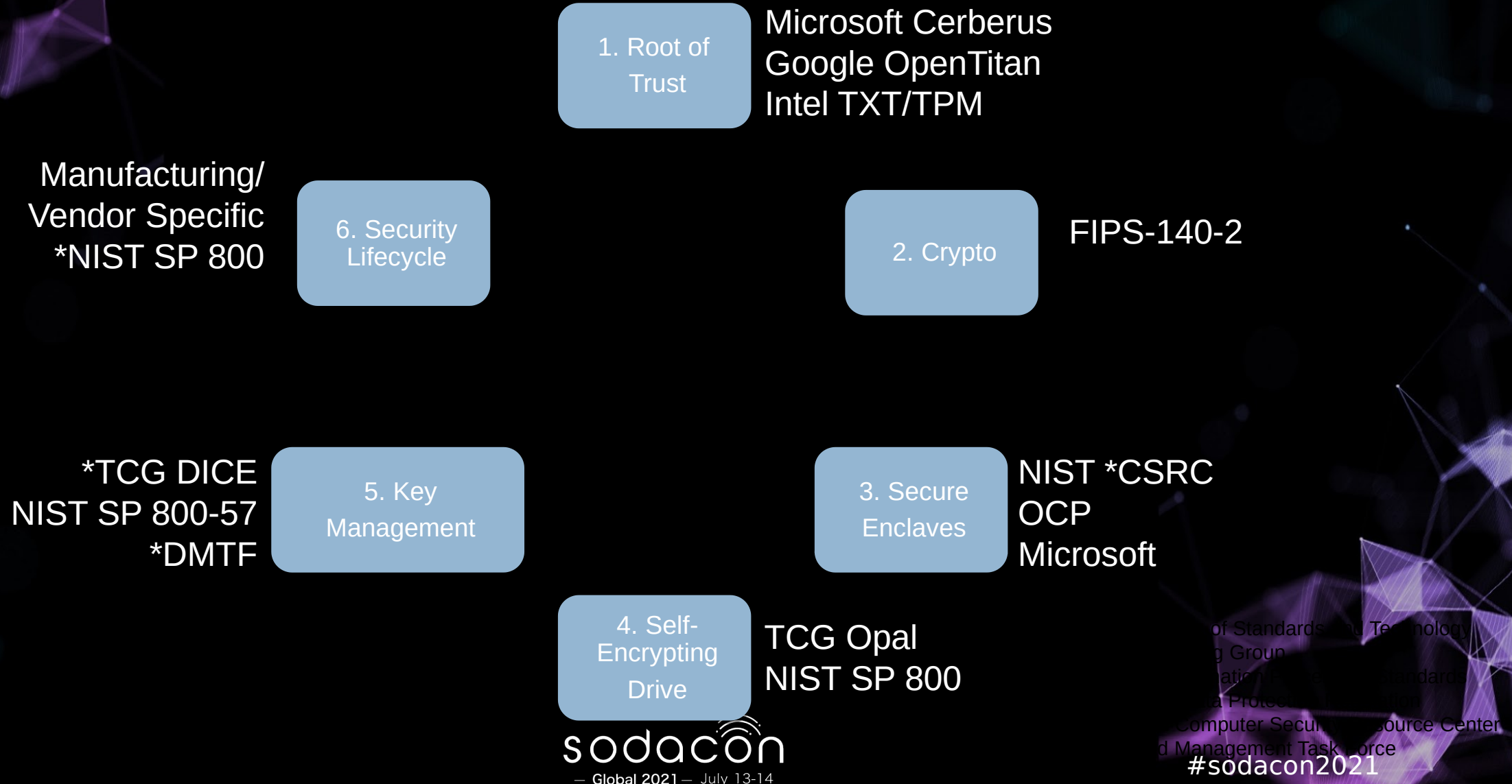
➢ **NVMe – Computational Storage Task Group**

- Device access, interfaces and implementation

- *Q1'2022 – standard (expected)*

sodacon
— Global **2021** — July 13-14

#sodacon2021

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

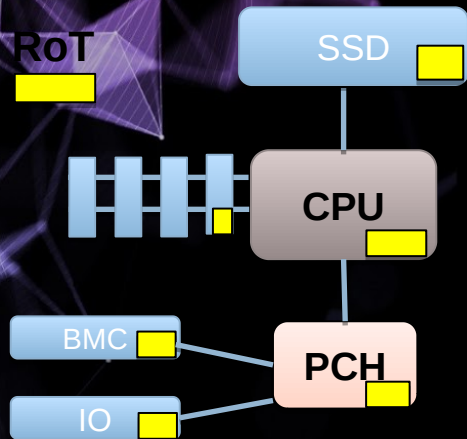- Edge deployments for in-situ storage processing

sodacon
— Global 2021 — July 13-14

#sodacon2021

Computational Storage Potential Security Considerations

1. Root of Trust

Microsoft Cerberus
Google OpenTitan
Intel TXT/TPM

6. Security Lifecycle

Manufacturing/
Vendor Specific
*NIST SP 800

2. Crypto

FIPS-140-2

5. Key Management

*TCG DICE
NIST SP 800-57
*DMTF

3. Secure Enclaves

NIST *CSRC
OCP
Microsoft

4. Self-Encrypting Drive

TCG Opal
NIST SP 800

sodacon
— Global 2021 — July 13-14
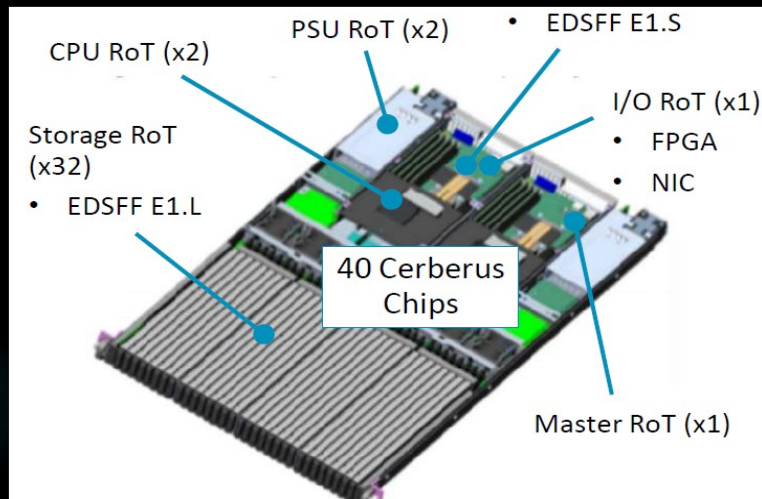
#sodacon2021

1. Roots of Trust
allow a system to trust its peripheral components
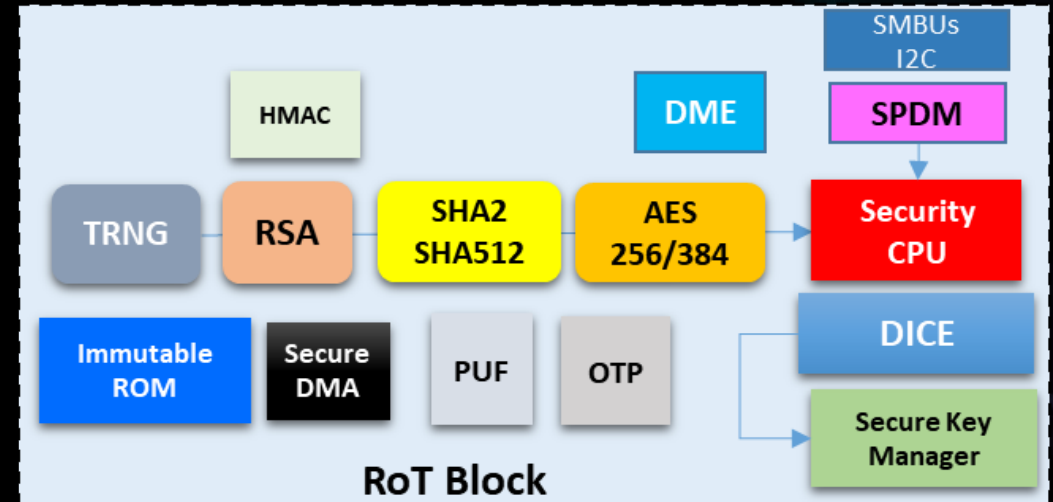
OCP Cerberus RoT

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

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

sodacon
— Global 2021 — July 13-14

#sodacon2021

2. Crypto / 3. Secure Enclaves
allow a system to securely handle drive boot firmware and unencrypted keys

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

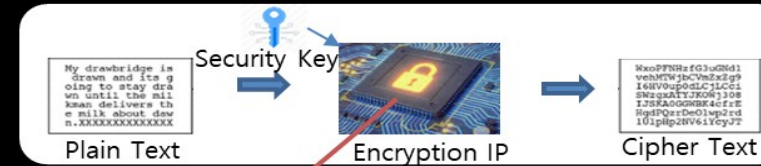| Security Strength	2030	2030+
AES	AES 128 →	AES 256
ECDSA	ECDSA 256 →	ECDSA 384
RSA	3072 →	4096

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

My drawbridge is drawn and its going to stay dra wn until the mil kman delivers th e milk about daw n.XXXXXXXXXXXXX

Plain Text   Security Key   Encryption IP   Cipher Text

WxoPFNHzfG3uGNdl
vehMTWjbCVmZxZg9
I6HV0up0dlC1LC6i
SWzgxATTJKON1jO8
IJSKAOGGNBK4cfrE
HgdPQzrDeO1wp2rd
lO1pHp2NV6iYCyJ7

Side-channel attack
Power consumption,
Fault information,
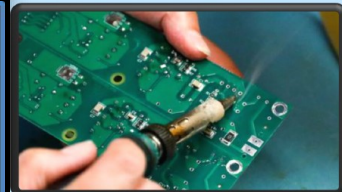Timing information, etc
Acquisition   Analysis   Key is Recovered

Hardware
hack Tampering
Side-Channel
Attack
with Differential
Power

Security Subsystem

| SSD Cont CPU | NAND |

→

Security Subsystem

| SSD Cont CPU | NAND |
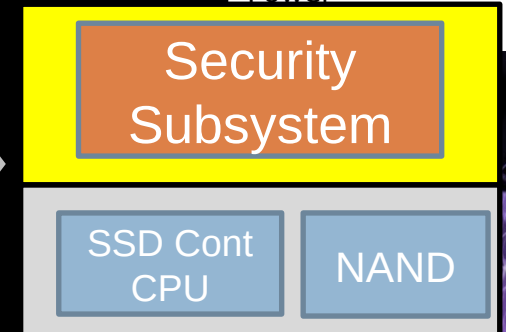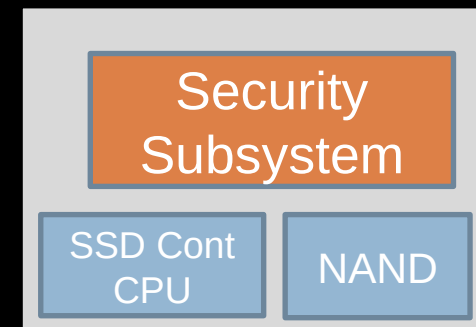
SSD with Enclaves

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

SED → SW Volume Encryption → HW Volume Encryption

SW Volume Encryption
SW key V1 🔑   SW key Vn 🔑

HW Volume Encryption
External Key manager

key Tag V1   key tag Vn

SED   SED   SED

🔑 🔑 🔑
Volume 1
Volume n

SED   SED   SED

Internal Key Cache
Different Key for each IO

Volume 1   Volume n

KPIO   KPIO   KPIO
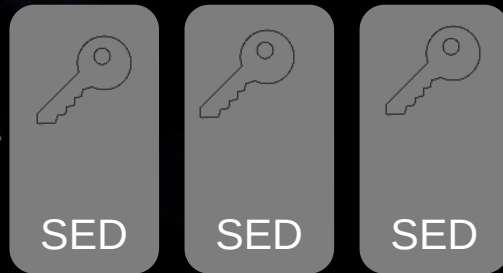
Host SW has no control SED drive encryption all IO blocks with same key.
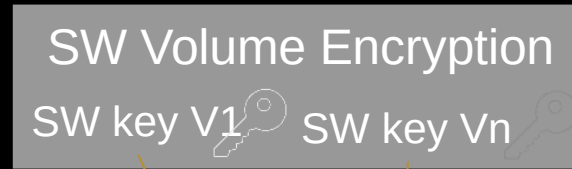
Host SW encryption with finer granularity for volume SED drive encryption all IO blocks for volumes with same key FIPS-140-2
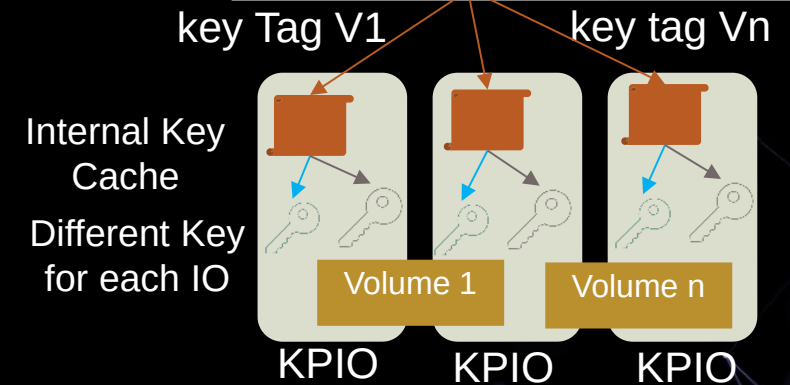
Fine-grain HW encryption (new key per volume, per VM, or per IO) Offloads the CPU FIPS-140-3

New SSD controller required

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*	

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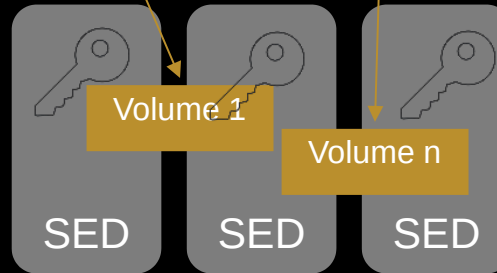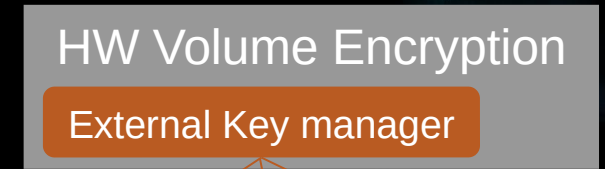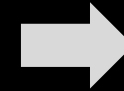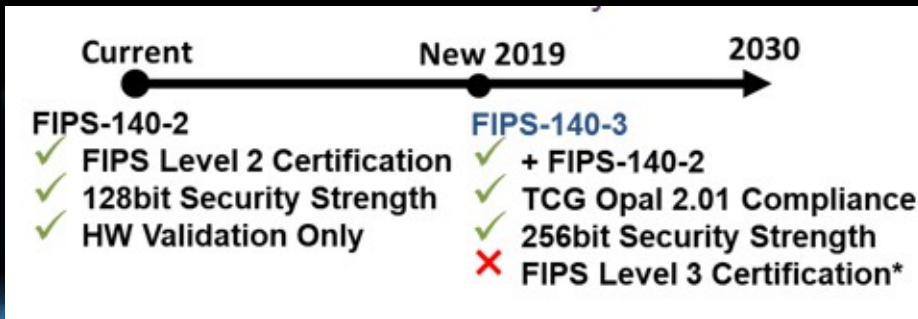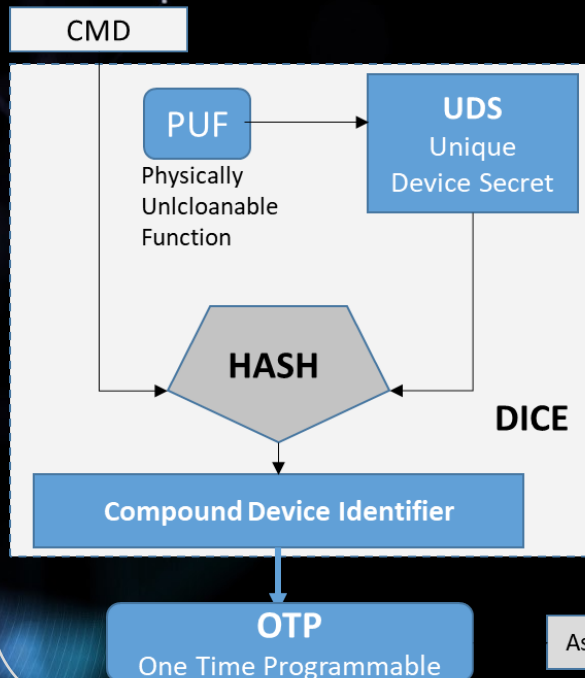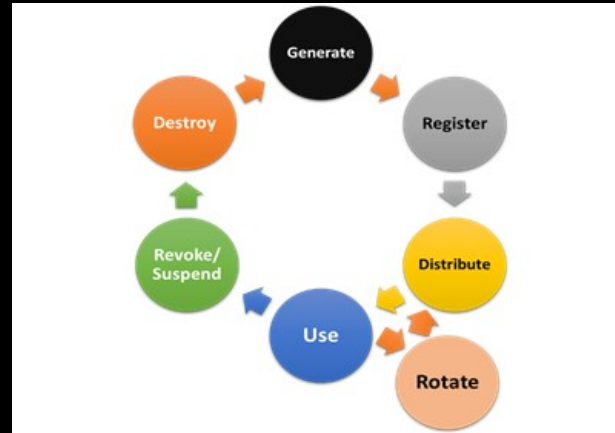- FIPS-140: US Government Security Requirements for Cryptographic Modules

sodacon
— Global 2021 — July 13-14

#sodacon2021

5. Key Management / 6. Security Lifecycle
allow peripherals to implement and interoperate with security best practices

5. Key Management

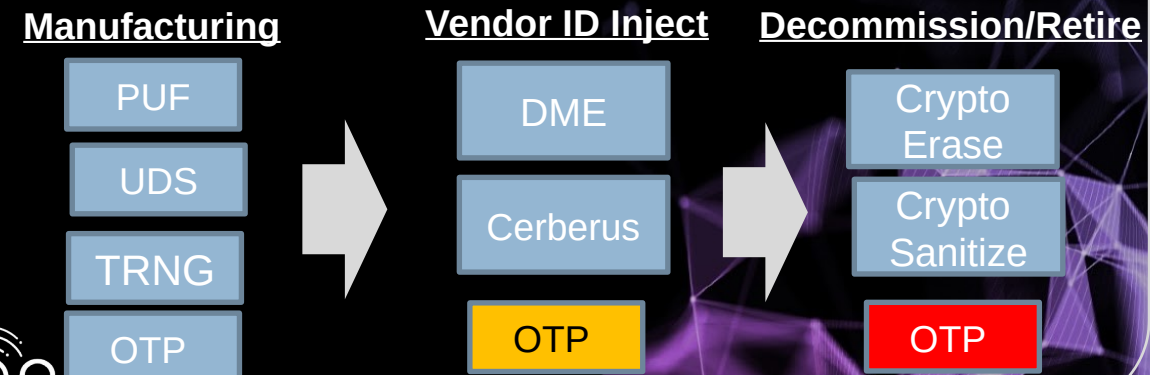Key management focuses on **protecting keys from threats**, and **ensuring** security of keys thru lifecycle of SSD.

CMD

PUF
Physically Unlcloanable Function

UDS
Unique Device Secret

HASH

DICE

Compound Device Identifier

OTP
One Time Programmable

Asymmetric Key Table

TCG DICE is a requirement for Cerberus RoT and enables:
 Attestation protocol
 Secure boot
 Key management

6. Security Lifecycle

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

| Design | Source | Mfg | Deliver | Deploy | Use | Retire |

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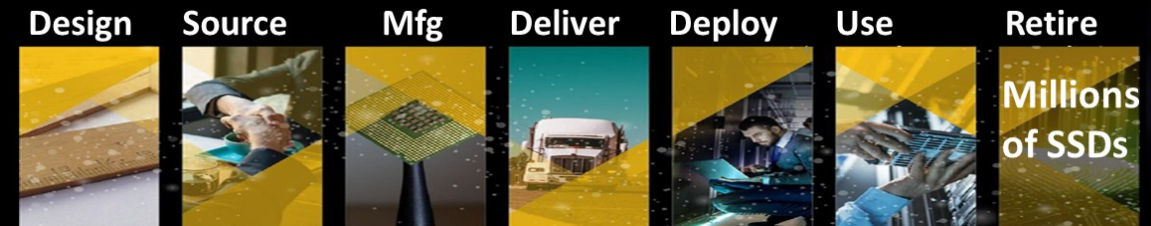
NIST 800-88 and ISO recommends how Keys generated, Crypto Erase and Media Sanitization. TCG Opal Spec recommends standards for Crypto Erase.

Manufacturing	**Vendor ID Inject**	**Decommission/Retire**
PUF	DME	Crypto Erase
UDS	Cerberus	Crypto Sanitize
TRNG		
OTP	OTP	OTP

sodacon
— Global 2021 — July 13-14

#sodacon2021

Microsoft Cerberus and Google OpenTitan

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

Security Pillars	Microsoft / facebook / Project Cerberus arm	Google / opentitan RISC-V
Root of Trust		
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

sodacon
— Global 2021 — July 13-14

#sodacon2021

Summary and Actions

➢ Computational Storage provides better application performance with new security challenges to solve.

- Data at rest

- Processed data

- CSD to host data

➢ Cloud Service Provider data security policies need to be su

➢ Hybrid cloud deployments need to address security concer

- On-premise or colocated

- Cloud

➢ Industry Standards working groups are defining computational storage architectures with security in mind.

➢ Participate in standards committees and contribute to a secure computational storage ecosystem!