September 16-18, 2024
Santa Clara, CA

Challenges and Opportunities in Storage Security

Seagate Technology

Arie van der Hoeven

Cloud Ecosystem Lead, Principal Project Manager

Agenda (Yes, broad in scope)

- Threats to Data Security
- Supply Chain Security
- OCP Implementations vs. Standards
  - OCP S.A.F.E.
  - OCP Caliptra
- PQC Security and CNSA 2.0
- IEEE 2883 Data Sanitization
  - Data Security
- Circularity and Sustainability Opportunities
- SPDM Attestation (See next talk!)

Threats to Data Security

- Storage Devices stay in the ecosystem for years
- We must think about the threat environment 10+ years out
- Advanced laboratory techniques, Government Grade Security, PQC, AI and increases in compute power are just some of the factors to consider
- Security is a must have for circularity and CO2e reductions
- Standards move slowly and lack of agility is a threat
- Implementations (i.e. OCP and Chips Alliance) are a legitimate way to move more quickly
- Too many implementations and requirements today
- Budgets and the health of the storage industry play a role

Supply Chain Security

Software Supply Chain

CISA, NSA, and Partners Release New Guidance on Securing the Software Supply Chain | CISA

- Risks in the software supply chain
  - A majority of organization will experience a software supply chain attack
  - Monocultural supply chains are more susceptible to these disruptions
    - SolarWinds
    - Log4j
    - Crowdstrike – not an attack, but example of impact
    - Linux attempted XZ Utils data-compression backdoor
    - Evaluation of these components becomes more critical
- Knowing what's in your product
  - Software composition
  - Vulnerability management
  - Importance of activity and contribution in open-source projects
  - Internal Policies and Guidelines

Challenges

Source Component Analysis

- CI/CD Scans
- Difficult to know what is in a release
- Shows the current state of development repos

Open source

- Different processes for managing open source
- Not easy to correlate to external versions
- Varying qualifications for each project

Vulnerability Management

- Mostly manual assessment
- No centralized tracking
- Perception vs. Reality

Software Supply Chain Security

Secure Coding

Static Analysis

Memory Access

Logic Errors

Error Handling

Dynamic Analysis

Runtime memory analysis

Input Sanitization

Fuzz Testing

Source Component Analysis

Vulnerability Management

CVE Monitoring

Product Assessment

Remediation

SBOMs

Release oversight

Software Inventory

Secure Builds

SLSA

(Supply-chain Levels for Software Artifacts)

Secure Builds

Controlled Environment

DevSecOps

Early detection

Fully integrated security monitoring

Software Composition Analysis (SCA)

SCA Tools (e.g. Mend)

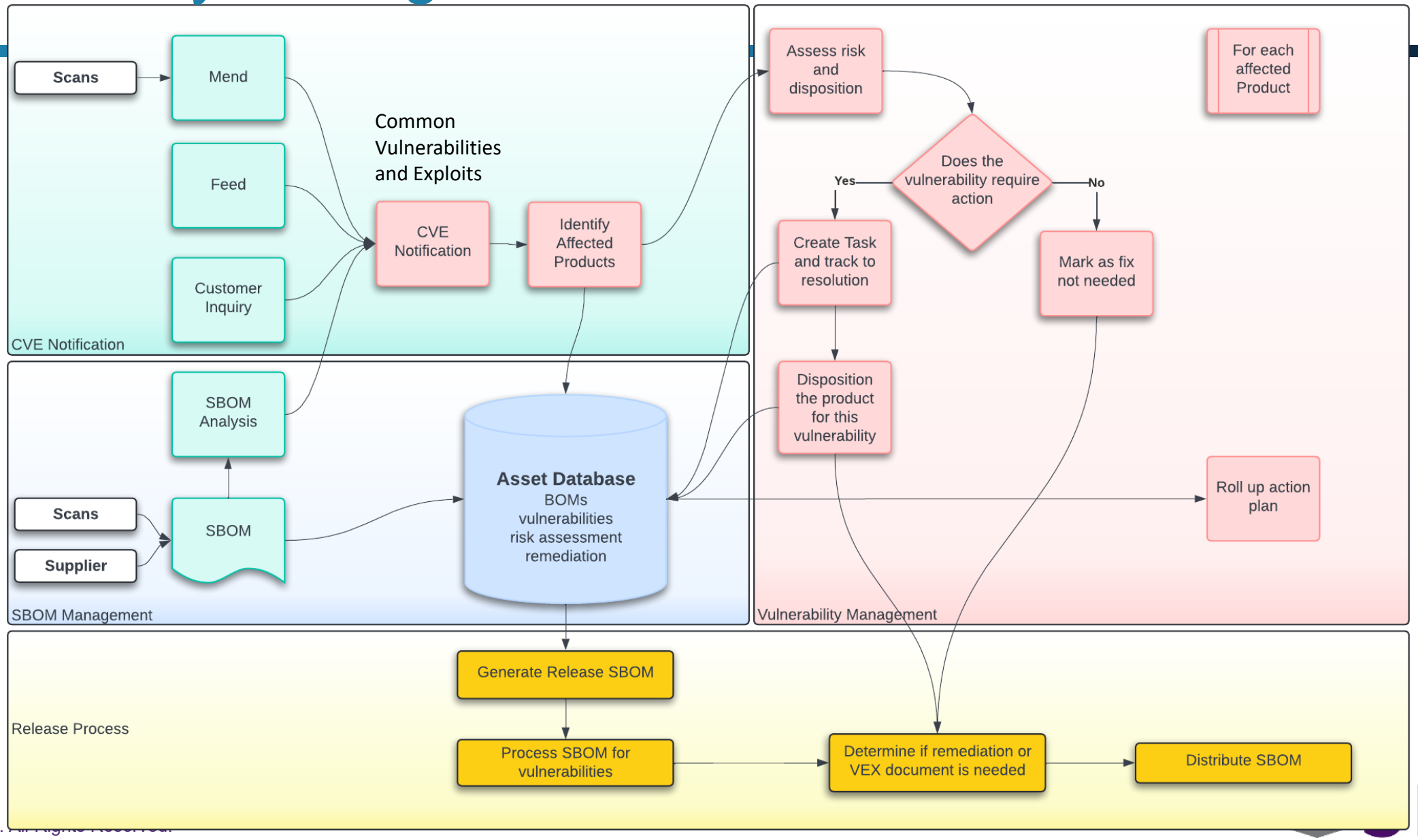
- Analyze packages and source to find third party code
- Mapped to vulnerabilities
- Understand license risks
- Mend SCA is one example of a third-party tool

SBOMs

- Complete software composition description
- Machine readable
- Ability to share with external parties

- Why do we need both?
  - SBOMs are release artifacts that document dependencies in a machine- readable form
  - SCA tools provide a continuous integration tool and ultimately can generate SBOMs

Vulnerability Management



SBOM Workflow

Product Team

3rd Party Code

Open Source

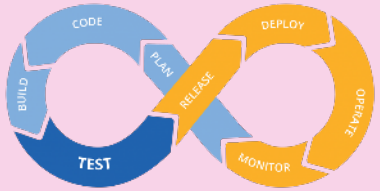
Package Manager

OSS Libs

Import

Ensuring complete SBOMs from supply chain and understanding that we identify all known vulnerabilities

CI CD



Evaluate

We need to understand what code we are consuming and how to assess the risk

We are responsible for the supply chain of the software we use

Corporate

SBOM Repository

SBOM

Analyze

Vulnerabilities

Licenses

SCA Tools

What level of SBOM analysis is needed vs what SCA tool already satisfies?

Release

Distribution for each release to allow customers to evaluate their supply chain

Release SBOM

SPDX

CycloneDX

SWID

SBOM Adoption Challenges

- Challenges
  - Source and binary analysis are not 100% accurate and yield different results
  - SBOMs still require manual editing
  - C/C++ still has many gaps
  - Open-Source tooling vs. Commercial
  - Assumption is that SBOM generation should be simple and straightforward

- SBOMs can vary
  - Quality
  - Caliber
  - Consistency
- Generate
- Augment
- Enrich
- Consolidate

- Practice needs to be broadly adopted and refined
- Challenges will not be overcome unless we implement the practice and work through the issues

Map the Supply Chain Ecosystem

Requirements

Market | Regulatory & Compliance | Security

Architecture

Threat Model | Security Architecture

Feeds

National Vulnerability Database | Threats

Software Providers

Internal | OSS | COTS | Services

Attacks

Intellectual Property | Counterfeit | Network | Data

Software Stack

Firmware | Containers | Operating Systems | Apps | APIs

SAST | DAST | Code Review | Unit Test

Scan | Assess | Review

SBOM

Products

HDD | Consumer | Systems | Cloud | Tools

Data Formats

CycloneDX | SPDX | VEX

Software Consumers

Customers | Compliance | Products

Stakeholders

IT | Product Security | Legal

Education

Security Champions | Developers

Open Source Management

- Checklists for evaluation
- Update management and testing
- Investigate scorecards for open source
  - Linux Foundation – CHAOSS
  - Open Source Software Foundation – OpenSSF Scorecard

Product Team Practices

- SCA tool used for every mainline build or CI/CD integration
- SBOMs are generated for every release and stored in an artifact repo
- Follow best practices for open-source acquisition and dependency management
- License compliance
- Security awareness

The OCP Security Appraisal Framework and Enablement (S.A.F.E.) Program for Storage

OCP SAFE

The OCP Security Appraisal Framework and Enablement (S.A.F.E.) Program

Review Areas

https://github.com/opencomputeproject/OCP-Security-SAFE/blob/main/Documentation/review_areas.md Re

Modern data centers are composed of a wide variety of processing devices (CPU, GPU, FPGA, etc.) and peripheral components (network controllers, accelerators, storage devices, etc.). These devices typically run updatable software, firmware or microcode, which can reside internally or externally to the device.

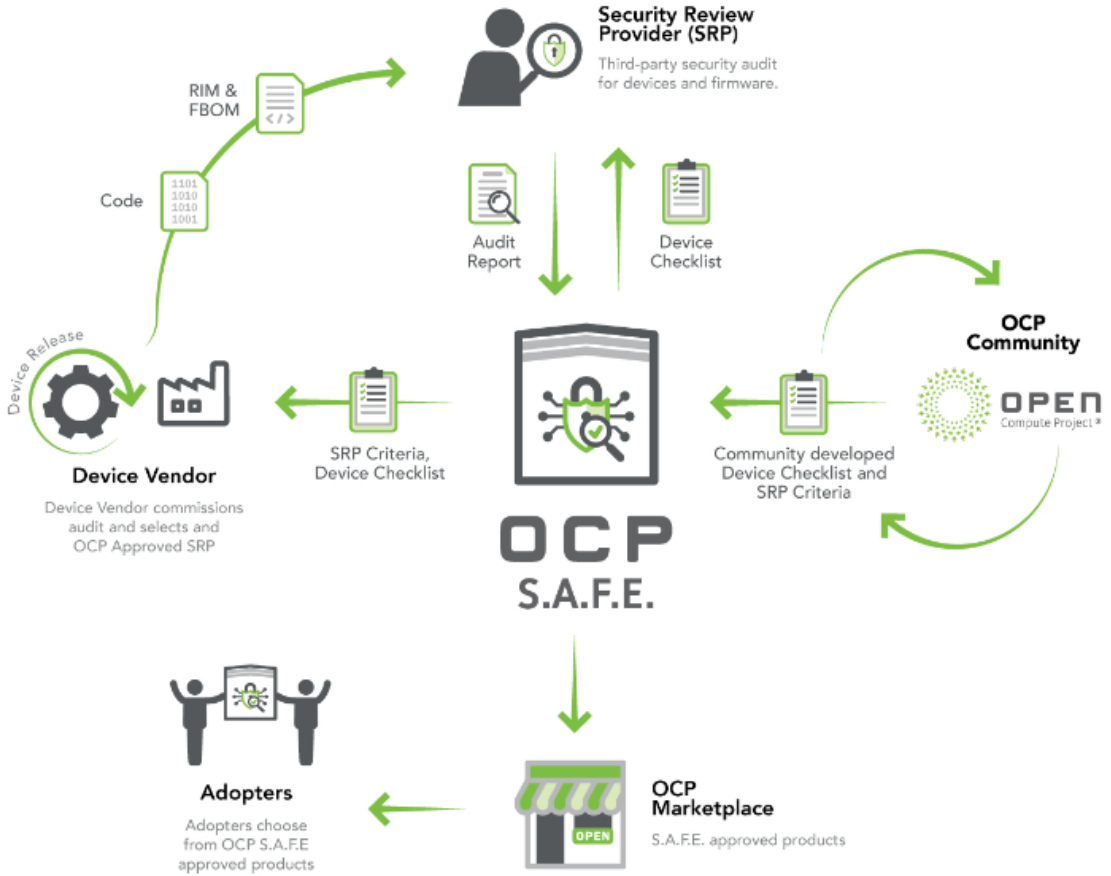
The provenance, code quality and software supply chain for firmware releases and patches that run on these devices requires a strong degree of security assurance.

Goals: The OCP S.A.F.E. Recognition Program is designed to address the challenges of currently faced by device vendors, end users and third party security review providers including:

- Reduce overhead and redundancy of security audits.
- Provide security conformance assurance to device consumers.
- Decrease competitive objections that prevent source code sharing for the purpose of robust independent security testing and the dissemination of findings and reports.
- Increase the number of devices whose firmware and associated updates are reviewed on a continuous basis.
- Through iterative refinement of review areas, testing scopes and reporting requirements, progressively advance the security posture of hardware and firmware components across the supply chain.

OCP SAFE

How to Participate



OCP SAFE | Assessment Scope & SRP Assessment Strategy

Documentation	Build Standards
	SDL
	Security Implementation Details (HDL and LDL)
	Security Compliance
	Evidence
	Security Information Details (both documented and DV internal)
Code Review	Booting and general
	Attestation
	Update
	End of Life / De-provisioning / Ability to securely re-provision
	Cryptography
	Auditing & Telemetry
	Debug
	Secure management
	Dependencies
	Hardening
	Trusted Execution Environment
	Root of Trust
	Identity
	Volatile and non-volatile storage

- **Align on Threat Model**
- **Establish Scope of Applicable Line Items**
- **Documentation: Review & Interview**
- **Code Review: Cooperative HW Penetration of Test Target Device**
- **Formal Report**
- **Remediation Phase**
- **Remediation Validation**
- **Public “Short Form” Report**

OCP SAFE | Gap Analysis

N% of Line Items Will Be Identified as Having Gaps
Not a Full List, 112 Line Items Total and Growing

Telemetry design and specific configuration
Full memory map for volatile and non-volatile memory
Certifications and methods linking to dependencies (e.g. ACME Crypto library v1.2 is certified on public register to FIPS 140-3)
Fuzzing results
Debugging implementation
All API's implemented on DUT
Attestation support for persistent storage
Attestation enforcement for security configuration
Cryptographic tamper detectable logs
HW ROT support/enforce quoting attestation claims at boot
Enforcement of measurements for security configuration loaded into DUT
HW ROT key store must support secure erasure
Unsecured persistent event/log storage sanitization
Secure support for re-provisioning of all cryptographic material
Secure logging and telemetry
Configurable logging to support security events

Cryptographic tamper detectable logs
Debug and test code should not be present in production DUT
If debugging functionality can be re-enabled, it must not provide any sensitive information
Third party software/firmware components including version specifics recorded in SBOM
Configuration specifics for third party dependencies recorded in SBOM
Third party dependencies up to date
Third party dependencies version pinned and in change control
DV implemented TEE's must generally conform to standards evolving in the Confidential Computing Consortium.
Trusted execution environment has physical and logical safeguards to provide isolation from other processing entities
IO from the TEE follows industry standards such as IDE or TDISP. If a proprietary protocol is used, e.g. XGMI, NVLINK, it must provide similar authentication, integrity, and isolation guarantees
The HW ROT shall implement cryptographically secure tamper resistant logs

Caliptra and L.O.C.K.
(**L**ayered **O**pen-Source **C**ryptographic **K**ey-management)

Caliptra – Use Case Overview

- The goal of Caliptra is to satisfy the Root of Trust for Measurement (RTM)
  - Other capabilities are out of scope (e.g., FW update and recovery)

- Use cases
  - Mutable Code Integrity
    - Allow the device owner to prove the device is running genuine FW
    - All the device manufacturer to vouch for the authenticity and integrity of the FW
    - Allow the device owner to ensure only authorized FW updates are applied to the device.
  - Configuration and Lifecycle Management
    - Allow the platform owner to securely configure the RoT capabilities
    - Allow the platform owner to enable/authorize lifecycle state transitions of the SoC
  - "DICE-as-a-Service" API
    - Allow Caliptra to use a DICE identity on behalf of other elements within the SoC

1 https://www.opencompute.org/documents/caliptra-silicon-rot-services-09012022-pdf

Caliptra – Feature Comparison Summary

Feature	Caliptra	STX HDD
Root of Trust for Measurement (RTM)	Yes	Yes
Rollback	Yes	Yes
DICE	Yes	Yes
DICE-as-a-Service	Yes	PoR
DICE Ownership Transfer	Yes	PoR

(*)Architecture is capable, currently only attestation uses DICE capabilities because of potential performance impact during TTR.
(^)Progress in OCP. For storage a dual-signing model is most appropriate.

1 https://www.opencompute.org/documents/caliptra-silicon-rot-services-09012022-pdf

https://www.opencompute.org/blog/open-compute-project-and-cloud-security-integrating-trust-into-every-chip

Caliptra Feature Worksheet

Features/Areas	Caliptra	Compare to your RoT here/ Caliptra 2.0.
Root of trust	Yes	
External Chip/Within SoC	Both	
Isolated Execution	Yes	
Digital Signature for Attestation	ECDSA P384	
Digital Signature for FW Signing	ECDSA P384 or LMS	
SHA Size	384	
Integration Modes	AP or PP mode	
OCP Compliance (Secure Boot)	Yes	
OCP Compliance (Caliptra)	Yes	
PQC support	Yes, LMS	
ROM Size	32K (meant only for RoT)	
SRAM Size	256K	
OTP Size	~34K	
Cost	Free (effort / time needed to bring it into shape)	
Development Model	Open Source	
Maturity age	Initiated in 10/2022, still new.	

(Cont'd..)

Features/Areas	Caliptra	Compare to your RoT here/ Caliptra 2.0.
IPs	Open Source	
Longevity	TBC, other standards being developed.	
Flexibility/Customization	Moderate	
Support	Low, nobody is obliged to help	
Maintenance	Same	
Change Inertia	High	
Quality of Development	Generally high	
Unused Code / Features	High	
Vulnerability Disclosure	High	

OCP L.O.C.K.

- **L**ayered **O**pen-source **C**ryptographic **K**ey-management
  - Risk:
    - Data exposure through poor data sanitization, drive theft, supplier infiltration, exploits in crypto-graphic erase and sanitize overwrite implementations
  - Problem:
    - Storage key management is critical to get right
    - Implementations vary in quality
    - Auditing implementations is resource intensive
    - Post deployment fixes are a nightmare Introducing: OCP L.O.C.K.
  - Introducing **L.O.C.K.**
    - A project to deliver an open implementation at CHIPS Alliance, leveraging and following Caliptra
    - Scoped specifically to storage devices
    - Provides key management services to the driveand host, utilizing services from Caliptra

NIST PQC Security and CNSA 2.0

Firmware Signing is Highest Priority to Protect From Quantum Threat

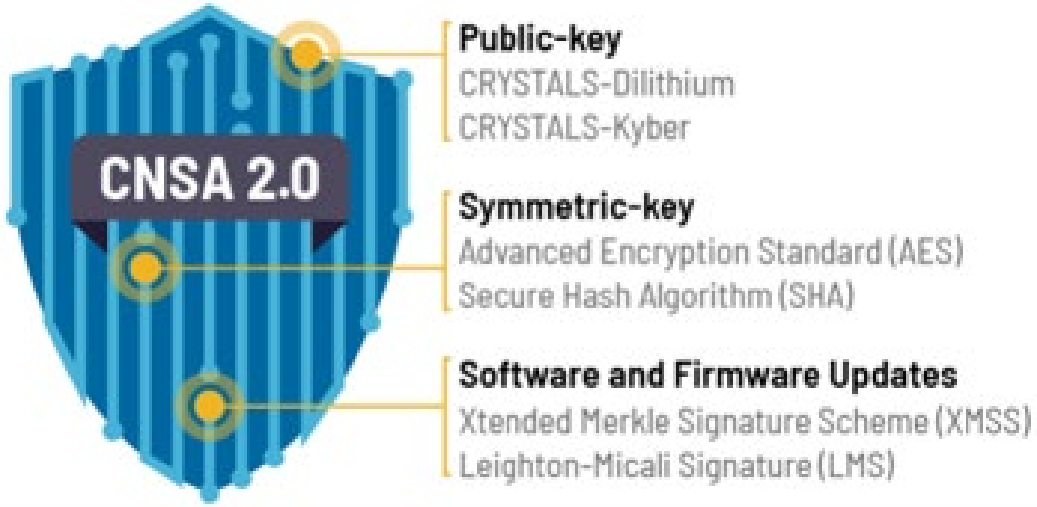


Table I: CNSA 2.0 algorithms for software and firmware updates

Algorithm	Function	Specification	Parameters
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels. SHA-256/192 recommended.
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels.

- Published by National Security Agency on 7-Sep-2022 (Finalized in August 2024)
- A suite of “post-quantum algorithms” that will eventually be requirements for NSS
- CNSA 2.0 establishes software and firmware signing as NSA’s highest priority; it says these applications should “begin transitioning immediately, support and prefer CNSA 2.0 by 2025, and exclusively use CNSA 2.0 by 2030

NIST 800-208 | Key Generation & Signature Generation Rqmts

Recommendation for Stateful Hash-Based Signature Schemes

8 Conformance

8.1 Key Generation and Signature Generation

Key Generation in HSM
Signature Generation in HSM
FIPS 140-3 Level 3 HSM
Operational Environment is Non-modifiable or limited
Approved Mode of Operation
Bypass Mode Not Allowed
Entropy Source from Approved Random Bit Generator w/in HSM

Hardware Security Module – Private Key Security | PSIS

FIPS 140-3 Validated Hardware Security Modules

Luna HSMs are the first in the industry to receive the FIPS 140-3 Level 3 validation and provide a hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption and more.

FIPS 140-3 will allow the certification of Post-Quantum Cryptography (PQC) algorithms, as it will ensure cryptographic modules are prepared to address the challenges and threats posed by quantum attacks. Implementing FIPS 140-3 validated security solutions is an essential part of building a quantum-safe crypto agile security posture, ensuring organizations stay data protected today, and into the future.

IEEE 2883 Data Sanitication and Circularity

Convergence of Security and Sustainability

Data Sanitization Research

- IEEE Compute Magazine article
- Storage market, intro to circular economy
- History of media sanitization specs
  - Show that DoD and NIST are old
- Highlight new IEEE 2883-2022 spec
- Review purge techniques

MEMORY AND STORAGE

EDITOR TOM COUGHLIN
Coughlin Associates; tom@tomcoughlin.com

New IEEE Media Sanitization Specification Enables Circular Economy for Storage

Jonmichael Hands, Chia Network
Tom Coughlin, Coughlin Associates

Modern media sanitization techniques can securely eliminate data on digital storage devices. This enables more effective efforts to reuse and recycle these devices, enabling a circular economy for data storage.

Digital Object Identifier 10.1109/MC.2022.3218364
Date of current version: 9 January 2023

Data growth has exploded, creating amazing opportunities and enabling quality of life improvements. The amount of data being created has far outpaced the amount of data being stored, with the International Data Corporation (IDC) forecasting that, in 2026, the massive 20.5 ZB of data being stored in the world will make up only about 10% of the total data generated that year (see Figure 1). This growth of stored data needs to be sustainable, with more companies than ever involved in the storage of digital data setting net-zero emission goals by 2030.

RAPID DATA GROWTH DEMANDS SUSTAINABLE PRACTICES

A modern high-capacity 3.5-in hard drive has an environmental footprint of 2.55 kg CO_2 emitted per terabyte per year.[2] One study estimated the embedded carbon from manufacturing solid-state drives (SSDs) to be as high as 0.16 kg CO_2 emitted

COMPUTER 0018-9162/23©2023IEEE

PUBLISHED BY THE IEEE COMPUTER SOCIETY JANUARY 2023

IEEE 2883.1: Recommended Practice for Use of Storage Sanitization Methods

- Storage Lifecycle, Risk and Management, Cryptography
- Choosing the Appropriate Sanitization Method: (clear, purge, or destruct) based on the intended use of the storage media, considering factors like risk and the sensitivity of the information
- Verification of Sanitization: Knowing that the data is gone

Example of Likelihood of Data Recovery after Sanitization

Sanitization Method	Adversary Capability		
	Novice	Expert	Virtuoso
None	Almost Certain	Almost Certain	Almost Certain
Clear	Unlikely	Likely	Almost Certain
Purge	Almost Impossible	Almost Impossible	Unlikely
Destruct	Almost Impossible	Almost Impossible	Almost Impossible

SPDM over MCTP Attestation Opportunities and Challenges

- STX completed a POC with SPDM 1.2 in June 2023
- Looking to productize
- SDC presentation from 2022: https://www.snia.org/educational-library/spdm-protocol-overview-component-integrity-security-standard-2022
- HDDs do not have a sideband bus like I3C
  - NVME HDDs may be an opportunity in the future
- Stay for the next talk! **SPDM: Updates for Storage & PQC (Post Quantum Cryptography)**
  - Jeff Hilland Distinguished Technologist / President HPE / DMTF
  - Brett Henning Security Architect, Broadcom

Questions?

Please take a moment to rate this session.

Your feedback is important to us.

