The evolving landscape of secure boot and device attestation

Sakul Gupta

Sr. Principal, MTS Firmware Security Engineering,
Micron Technology Inc.

August 5th 2025

micron Intelligence Accelerated™

FMS

Secure boot – What it is!

- Mechanism to ensure only trusted firmware from the OEM is loaded during the boot process.

- Ensuring Integrity and authenticity of the signed Firmware.

- Secure Boot can optionally implement device unique encryption for confidentiality protection of firmware images.

- Anti-Rollback feature – using security version number from the fuse. Avoids release / update of known vulnerability firmware into the field.

- Optionally uses a certificate-based trust hierarchy to validate firmware and OS loaders.

Secure boot – Establishing the Chain Of Trust

- *Root Of Trust* – Immutable ROM
  - Provides a mechanism for securely anchoring a root of trust public key, to verify the next stage.
  - One option using a digest of the root key as an immutable anchor in hardware fuses.

- *Chain of Trust*
  - Verify the device mutable firmware layers, digital signature using the anchored public key.
  - Each stage uses **digital signatures** and **hashes** to verify the integrity and authenticity of the next stage:
    - ✓ **Hashing** ensures the data hasn't been altered.
    - ✓ **Digital signatures** confirm the data comes from a trusted source.
  - Measured boot, as per the OCP_attestation spec and using SPDM protocol for device attestation.

- Provide a mechanism for revoking previously signed firmware / certificates, CRLs, DBX in UEFI Secure Boot, Online Certificate Status Protocol (OCSP) .

Secure boot – Guardrails against Glitching attacks

- Code execution path shall be designed to resist hardware glitching attacks.
  - Voltage Glitch detectors
  - Clock Frequency Glitch detectors
  - Electro Magnetic Pulse Glitch detectors

  - Identify threat vectors and mitigate them, via counter-measures, so that, secure-boot does NOT get compromised via a glitch attack.

- Active defenses against side-channel and differential power analysis, such as EM shielding, independent clocks, firmware measures.

- Mechanisms for transfer of ownership of the device. OCP Document being updated on it. Come attend the OCP Global summit-2025 to listen to the latest on it!

Secure boot – Fault Management & Recovery

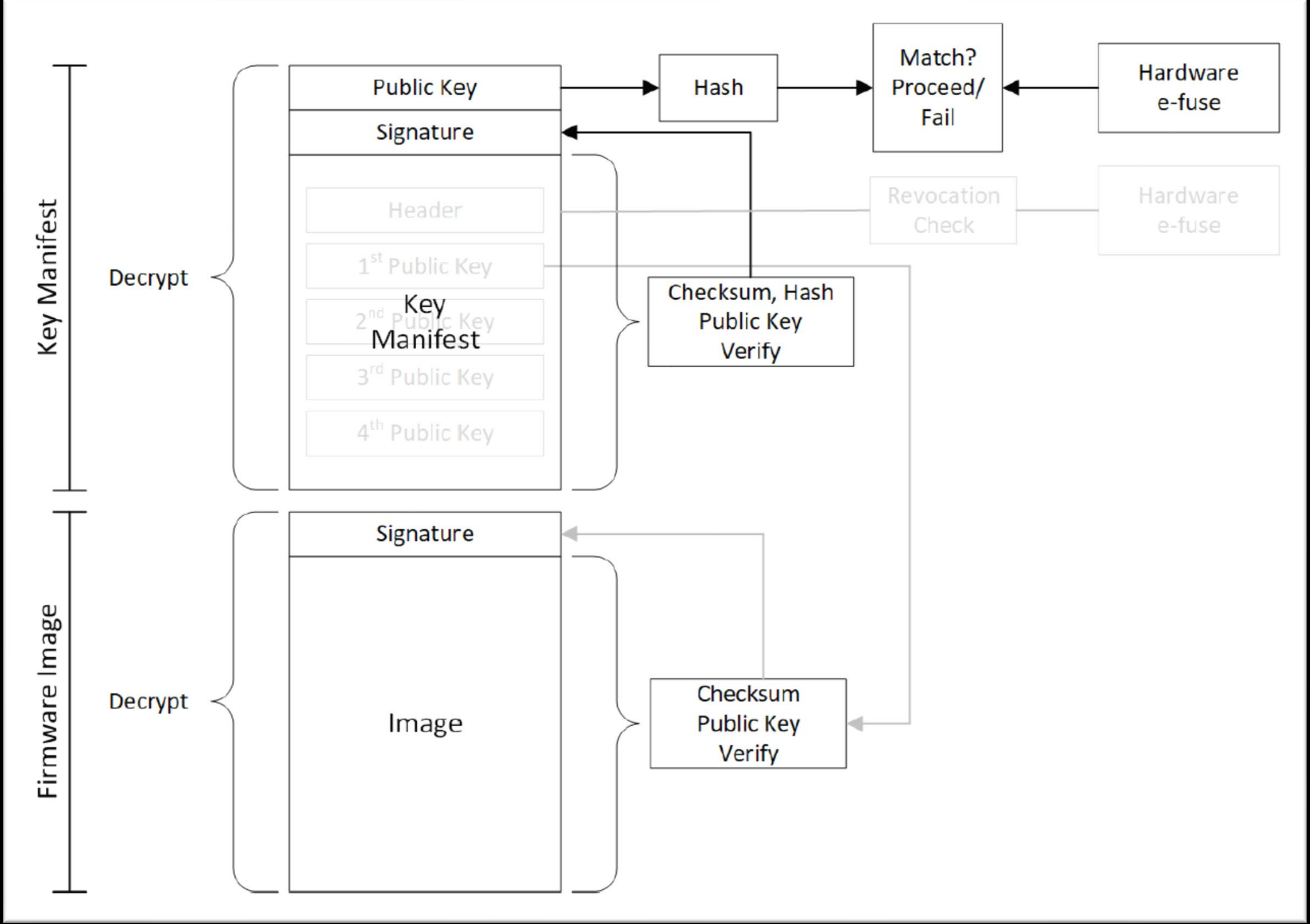
- Secure boot authentication failures need not render the device in-operable, nor should they permit the device to load mutable code without verifying integrity and signature.

- All failed boot attempt events should be signaled or logged in tamper evident log and made available as part of recovery.

- NIST SP800-193 NIST Special Publication 800-193 Platform Firmware Resiliency Guidelines
- OCP Recovery Document

- We have been working on OCP Fault Management Infrastructure Requirements, am a proud co-author and working on rolling them out in OCP Global Summit – 2025. Look forward to it!!

OCP Secure boot - Flow



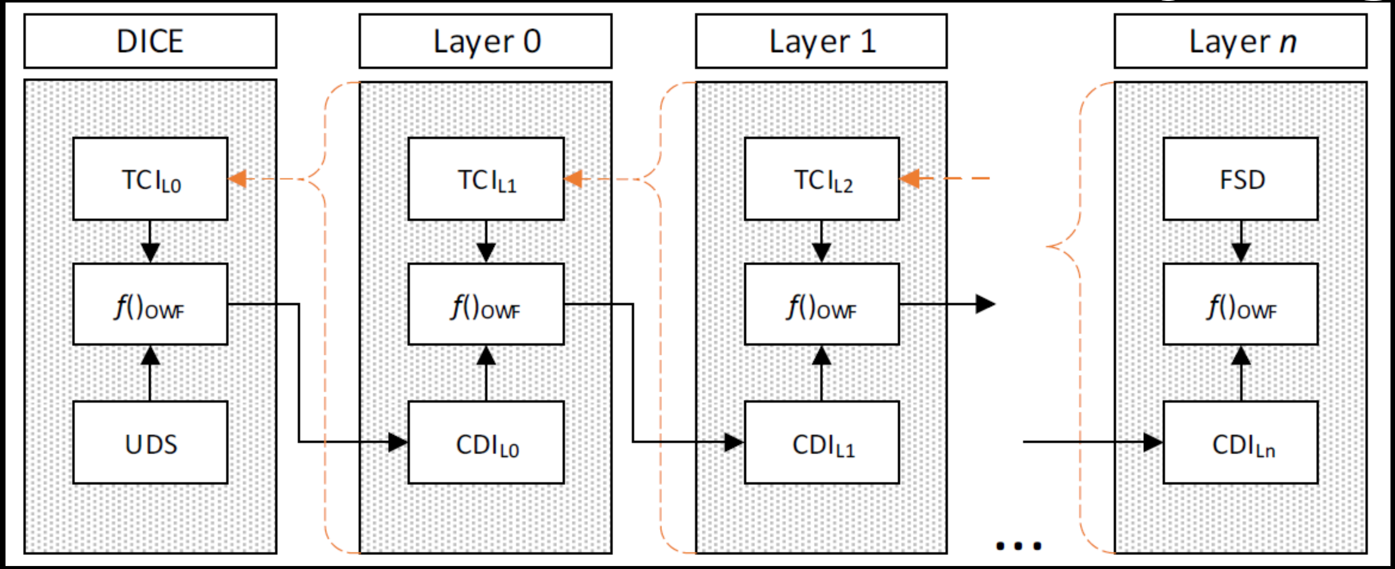
Device / OCP Attestation

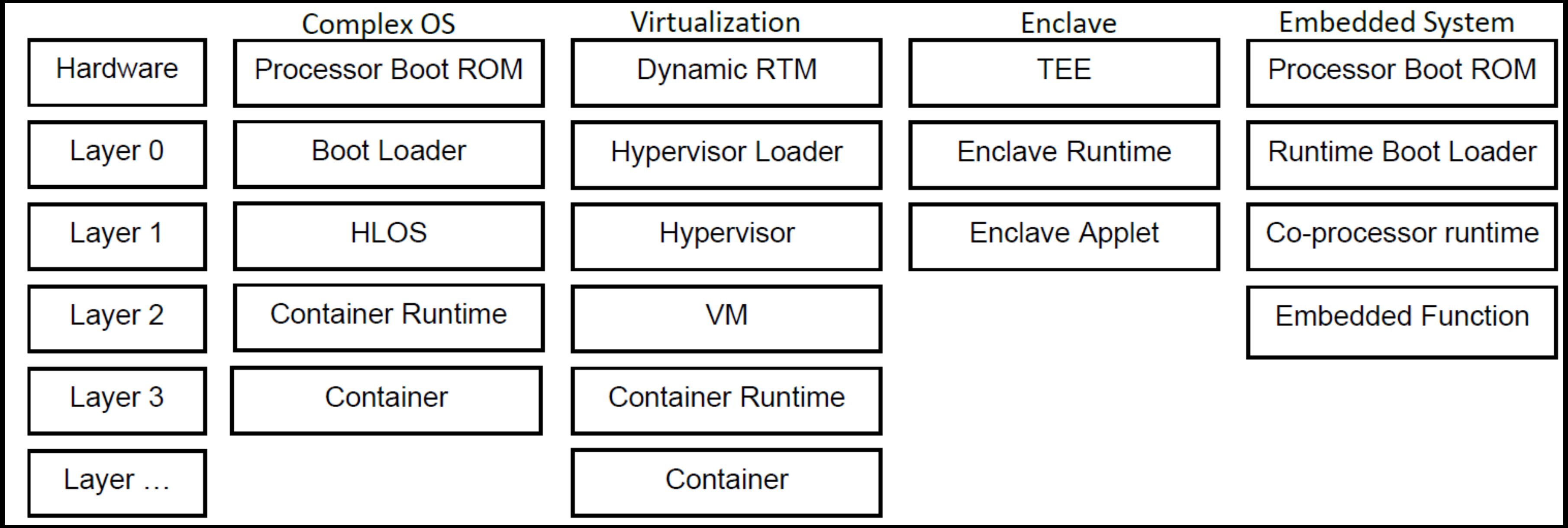
- The process of verifying the integrity and identity of a device using cryptographic proofs, often leveraging Trusted Platform Modules (TPMs) or hardware-backed Secure enclaves.

- Collect measurements (e.g., firmware version and cryptographic functions) from each attached device at cold-boot or after a FW update.

- Verify each device's certificate(s) and the certificate chain back to a trusted root, using DMTF's SPDM (DSP274).

TCG DICE Layering architecture





	Complex OS	Virtualization	Enclave	Embedded System
Hardware	Processor Boot ROM	Dynamic RTM	TEE	Processor Boot ROM
Layer 0	Boot Loader	Hypervisor Loader	Enclave Runtime	Runtime Boot Loader
Layer 1	HLOS	Hypervisor	Enclave Applet	Co-processor runtime
Layer 2	Container Runtime	VM		Embedded Function
Layer 3	Container	Container Runtime		
Layer …		Container		

Remote ATtestation procedureS

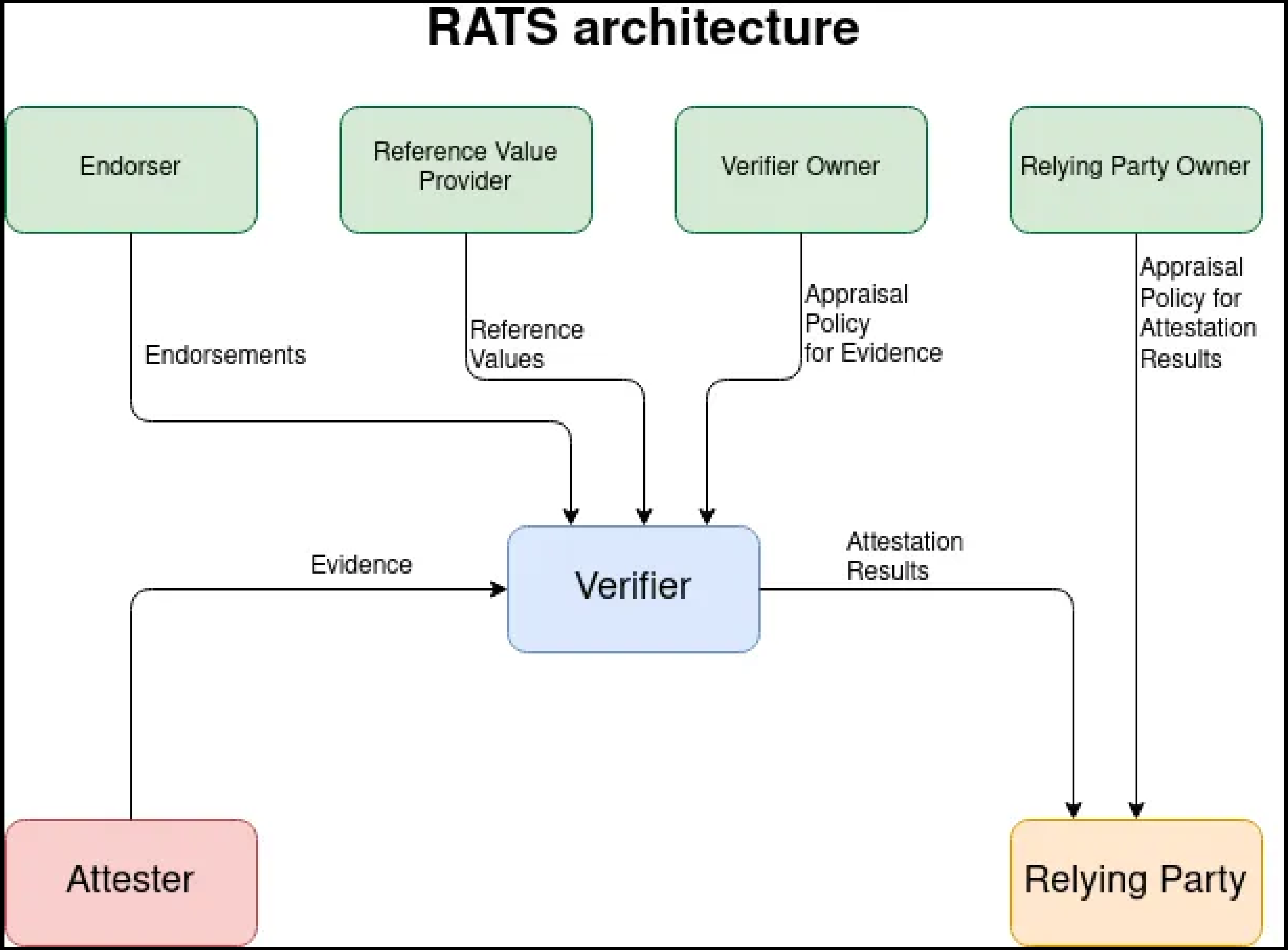
- The process of generating, conveying, and evaluating evidentiary claims.

- Verify the digital signature over device signed measurements, using DMTF's SPDM.

- Accept the verified device or decide on a remedial action.

- Increasing adoption of remote attestation in enterprise environments for Zero Trust architectures.

- The Internet Engineering Task Force (IETF) Remote Attestation Procedures (RATS) architecture



Recent Discussions on Attestation – via SPDM

- SPDM – Device certs, Alias certs, generic certs
  - The generic certificate model offers the greatest flexibility to the device manufacturer, a manufacturer in the supply chain, and the users of the SPDM endpoint.

- SPDM 1.3 multi-asymmetric key support, allowing different keys assigned to different purposes.
  - Enables cryptographic isolation between different use cases which potentially increases the security posture of the SPDM endpoint and its corresponding SPDM connections.
  - An SPDM Responder can choose which key-pairs to use in a CHALLENGE request and which key pairs to use in a GET_MEASUREMENTS request.
  - DMTF/libspdm now, has a user guide for multi-key support!

Tributes and Call to Action

- Let’s foster a Security-first culture, that spawns defense-in-depth.
- Security is Every-body’s responsibility and Let’s cohesively contribute to it more!

- Micron Technology Inc. Working towards offering the best of Secure boot and Attestation in its memory and storage products! Tributes to all our leadership, Security Architects, Security Firmware & Validation Engineers, Business Unit leads.

- Much appreciate the security related work we are doing as part of the enterprise data-center industry open specs, and weekly forums, which are referred to here,
  - OCP_Recovery_spec, OCP_Secure_boot , OCP_attestation
  - DMTF SPDM (DSP0274) spec, DMTF Authorization Specification (DSP0289)
  - (NIST Platform Firmware Resiliency 800-193 Platform Firmware Resiliency Guidelines
  - CSI_CNSA_2.0_FAQ_.PDF

Additional slides

PQC & CNSA 2.0

- Fast approaching deadlines for Post Quantum Cryptography (PQC), as spelt out in CSI_CNSA_2.0_FAQ_.PDF
- See government mandated algorithms and transition rules (CNSA 2.0)

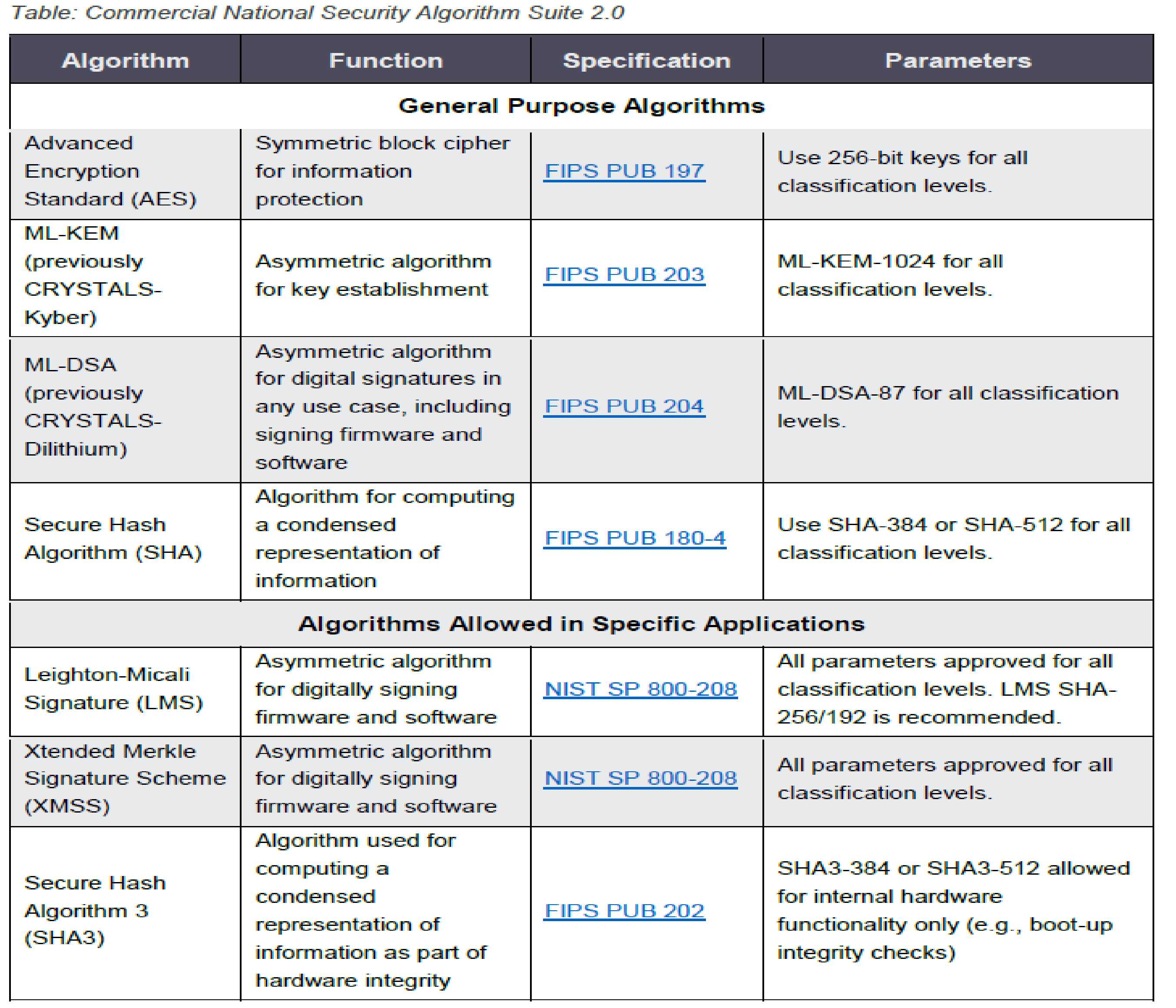


Table: Commercial National Security Algorithm Suite 2.0

Algorithm	Function	Specification	Parameters
General Purpose Algorithms			
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels.
ML-KEM (previously CRYSTALS-Kyber)	Asymmetric algorithm for key establishment	FIPS PUB 203	ML-KEM-1024 for all classification levels.
ML-DSA (previously CRYSTALS-Dilithium)	Asymmetric algorithm for digital signatures in any use case, including signing firmware and software	FIPS PUB 204	ML-DSA-87 for all classification levels.
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels.
Algorithms Allowed in Specific Applications			
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels. LMS SHA-256/192 is 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.
Secure Hash Algorithm 3 (SHA3)	Algorithm used for computing a condensed representation of information as part of hardware integrity	FIPS PUB 202	SHA3-384 or SHA3-512 allowed for internal hardware functionality only (e.g., boot-up integrity checks)

Recent Discussions on Attestation in Standard Bodies

- Remote ATtestation procedureS (RATS) **EAT** profile for SPDM binding
- SPDM EAT Profile for Device Attestation
  - In confidential computing, device assignment (DA) is the method by which a device (e.g., network adapter, GPU), whether on-chip or behind a PCIe Root Port, is assigned to a Trusted Virtual Machine (TVM).
  - For the TVM to trust the device, the device must provide the TVM with attestation Evidence confirming its identity and the state of its firmware and configuration. SPDM compliant devices are expected to present attestation Evidence that is within the boundaries of the SPDM protocol,
  - Out of concern for interoperability and to leverage existing attestation standards, this common representation is expressed as an EAT (**Entity Attestation Token**) profile.
- Chips Alliance's Caliptra 2.0 defines a design standard for a Silicon internal RoT baseline. This standard satisfies a Root of Trust for Measurement (RTM) and cryptographic services for the SoC. The SoC must measure the code and configuration it boots into Caliptra in this configuration. Caliptra must store these measurements and report them with signed attestations rooted in unique per-asset cryptographic entropy. Caliptra serves as a Root of Trust for Identity for the SoC
- chipsalliance/Caliptra: Caliptra IP and firmware for integrated Root of Trust block