Flash Memory Summit

Evolution from Secure Boot to Real Time Platform Resiliency

Richard Wahler

Eileen Marando

35 YEARS OF NAND FLASH MEMORY INNOVATION

Evolution from Secure Boot to Real Time Platform Resiliency

Attendees will understand the basics secure boot, how to extend secure boot from a Root-of-Trust (RoT) to a non-secure processor and the basics of attestation, why it is important, and how to implement it in their secure systems

Trust and Attestation

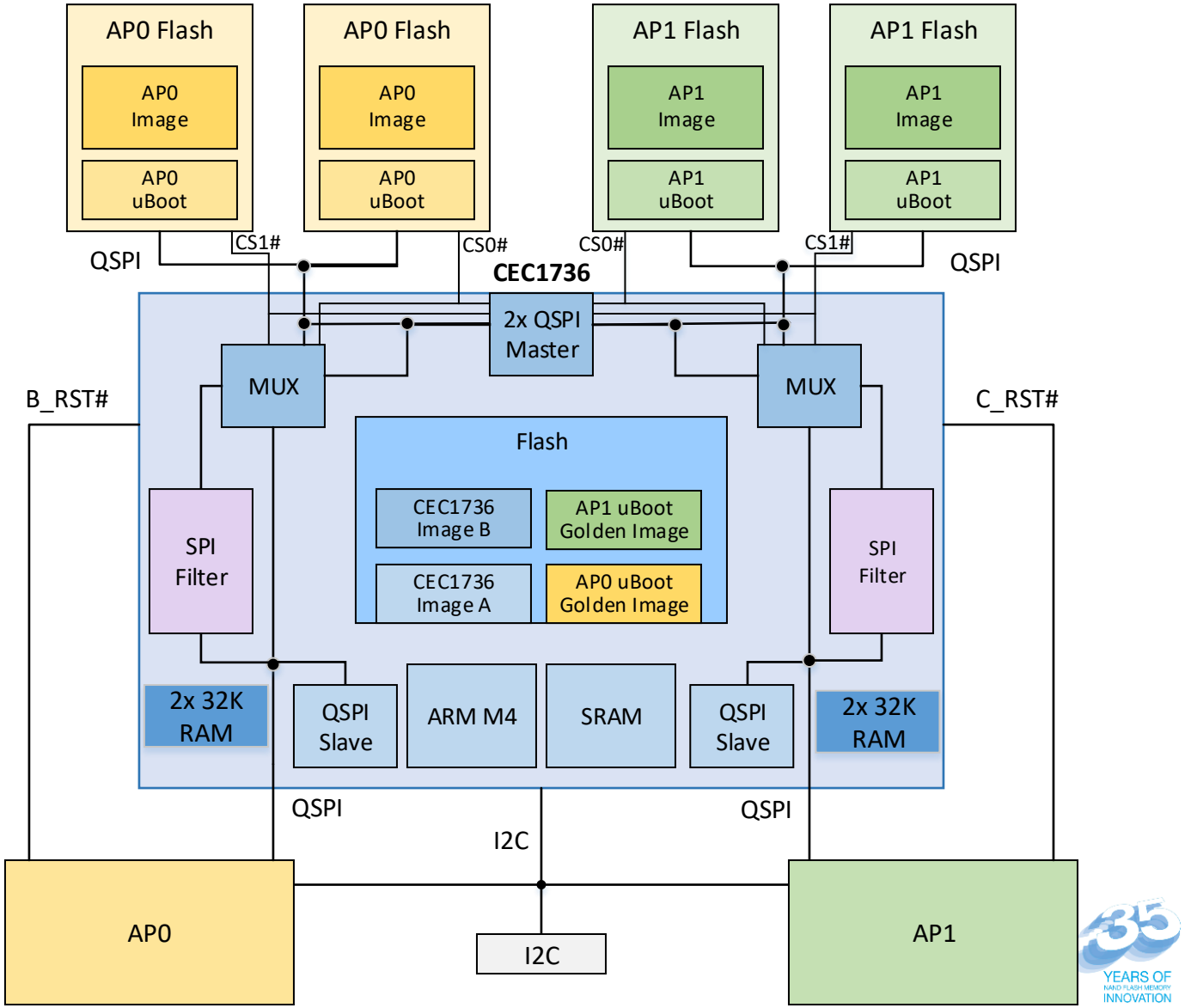
Flash Memory Summit

- Root-of-Trust
  - Secure boot
- Resiliency
  - Protect, detect, recover
  - Real time monitoring
  - NIST 800-193
- What is Attestation?
  - Why is it important?
  - How does attestation work?
    - Dice/RIoT
    - OCP

35 YEARS OF NAND FLASH MEMORY INNOVATION

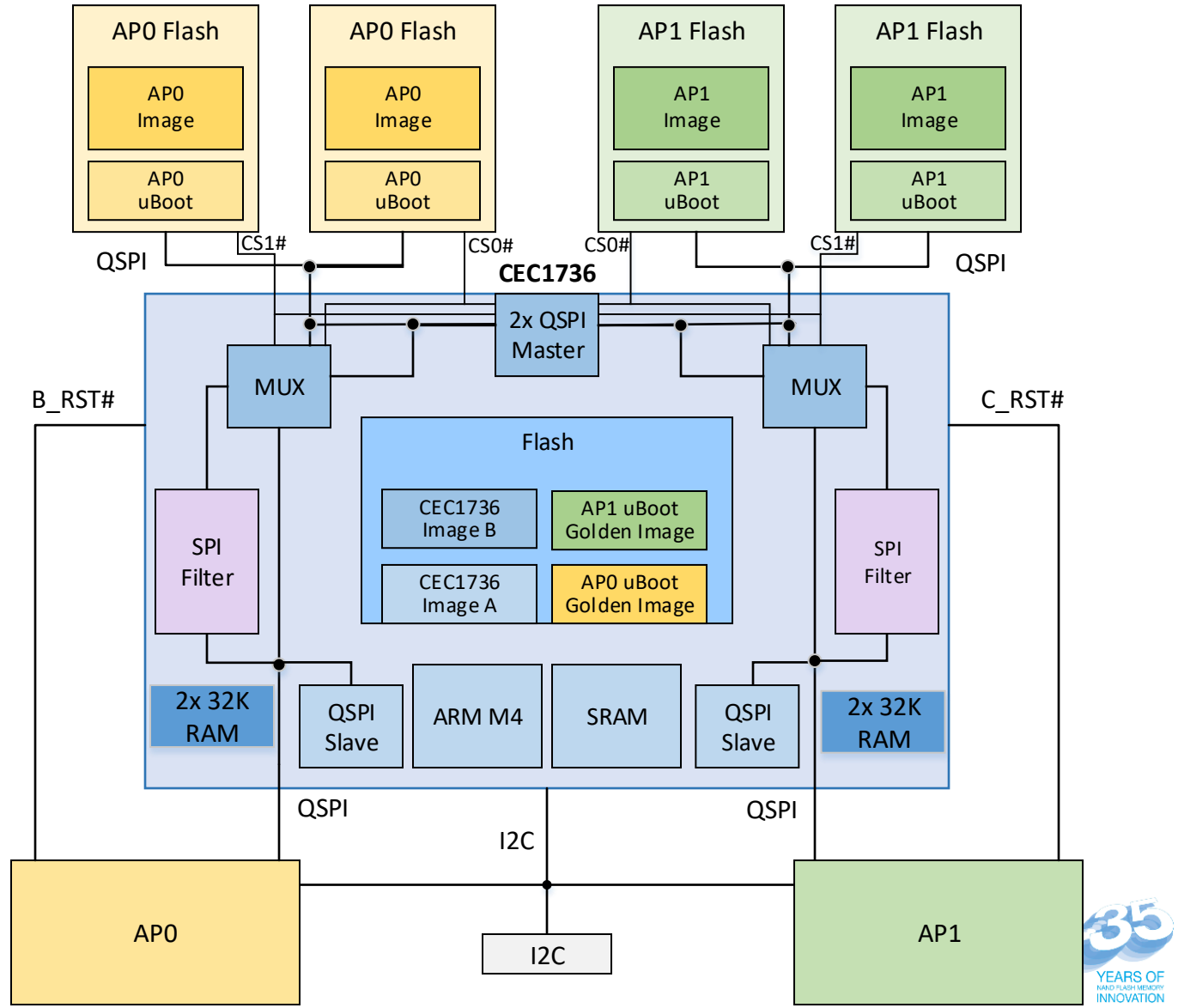
Root-of-Trust

- Secure Boot
  - Secure immutable code
  - All mutable code authenticated before use
  - Strong authentication (CNSA)
    - SHA2 – 384 minimum
    - ECC384 minimum
- Resiliency
  - Protect, detect, recover
  - Authenticate before use
  - Use backup image



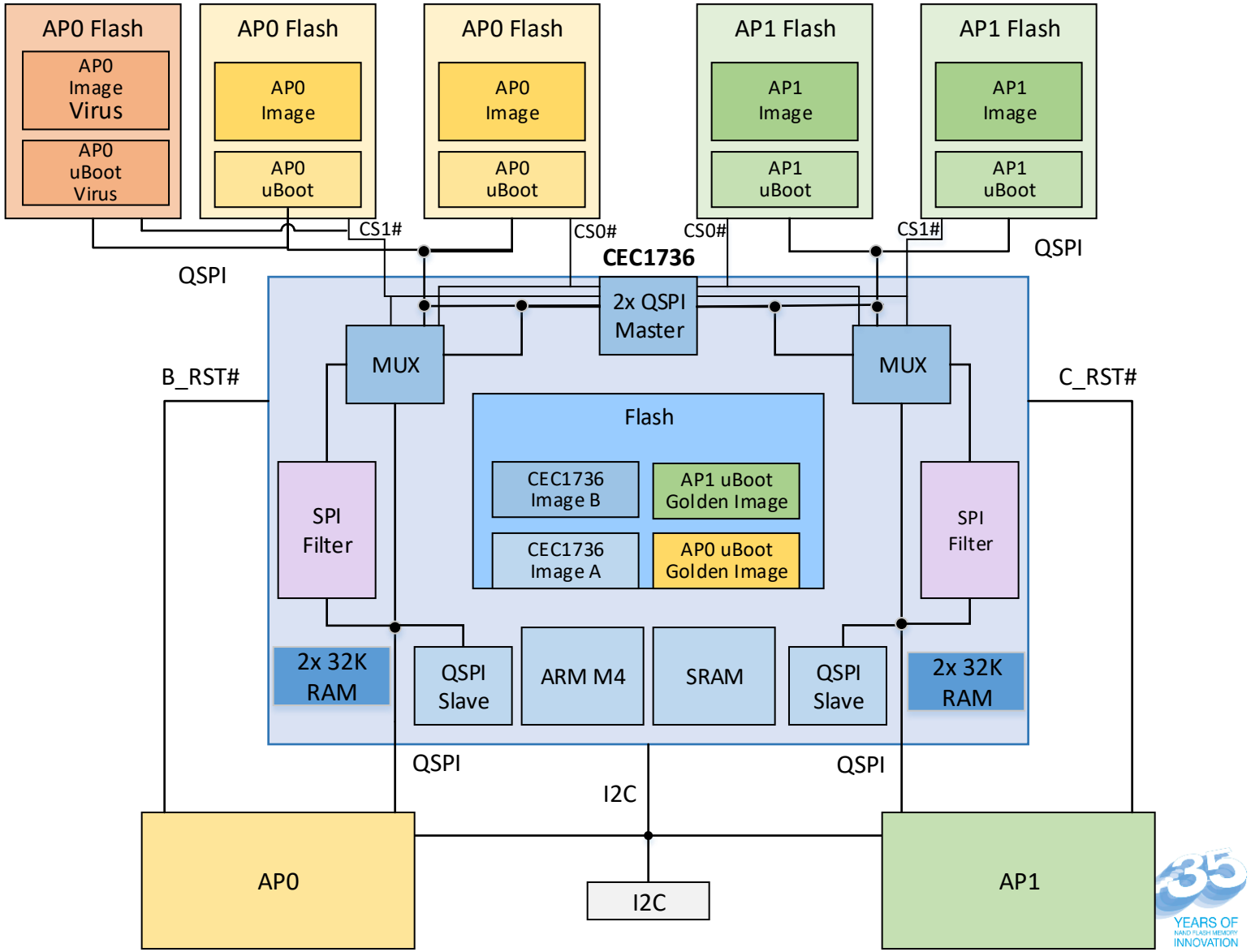
Extend Root-of-Trust

- Protect Application Processor (AP)
- Resiliency
  - Protect, detect, recover
  - Protect the APx code images
  - Authenticate before use
  - Time-of-Check (TOC)
  - Authenticate all images in APx FLASH
  - Generate hash tables



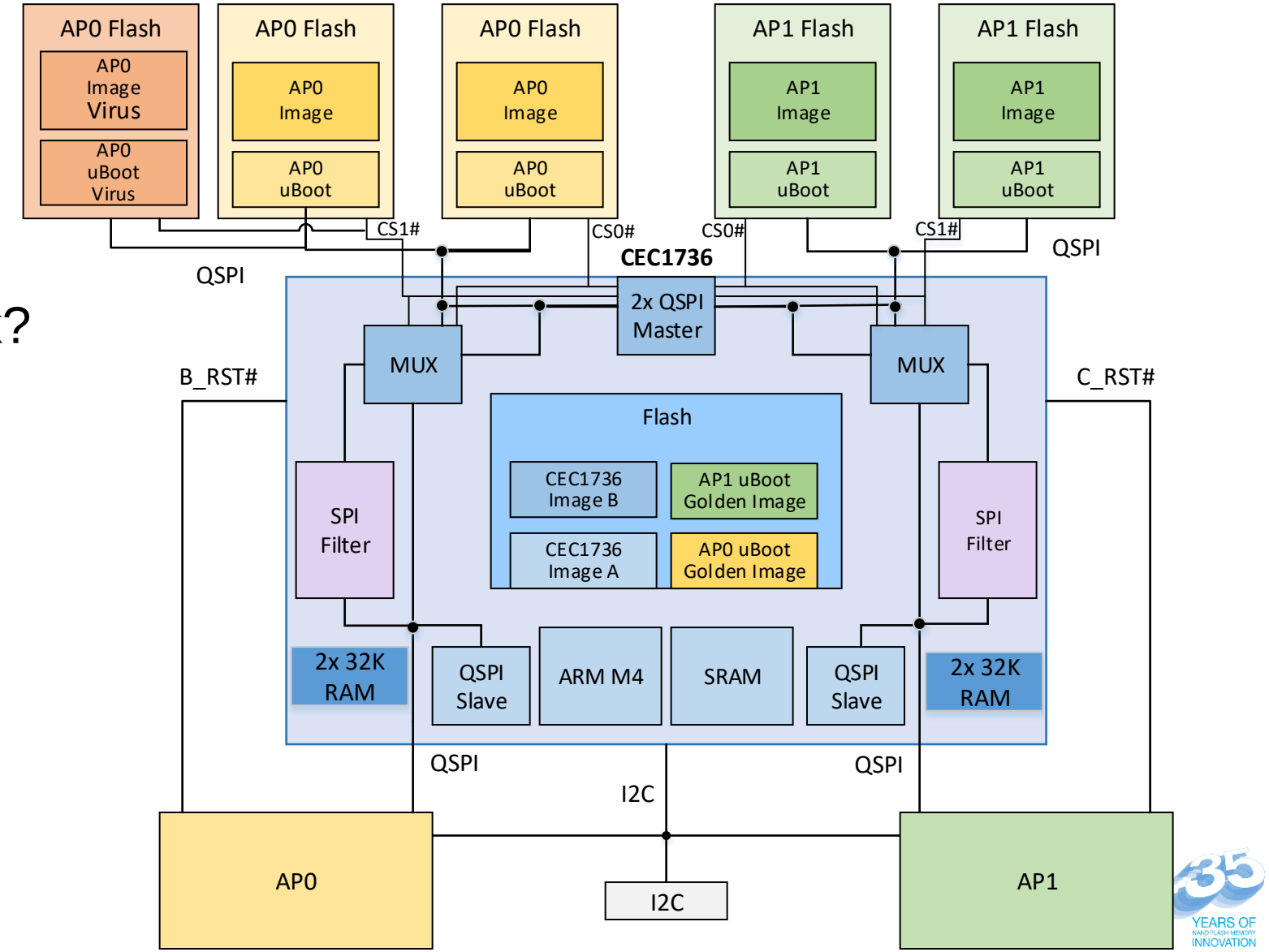
Real Time Monitoring

- Real Time Monitoring
  - Reauthenticate when loaded by the application processor (AP0/AP1)
  - Time-of-Use (TOU)
  - Monitor traffic to/from SPI
    - Read only
    - Read/write
    - No access



Trust and Attestation

- What is Attestation?
  - Why is it important?
  - How does Attestation work?
    - TCG - Dice/RIoT
    - OCP

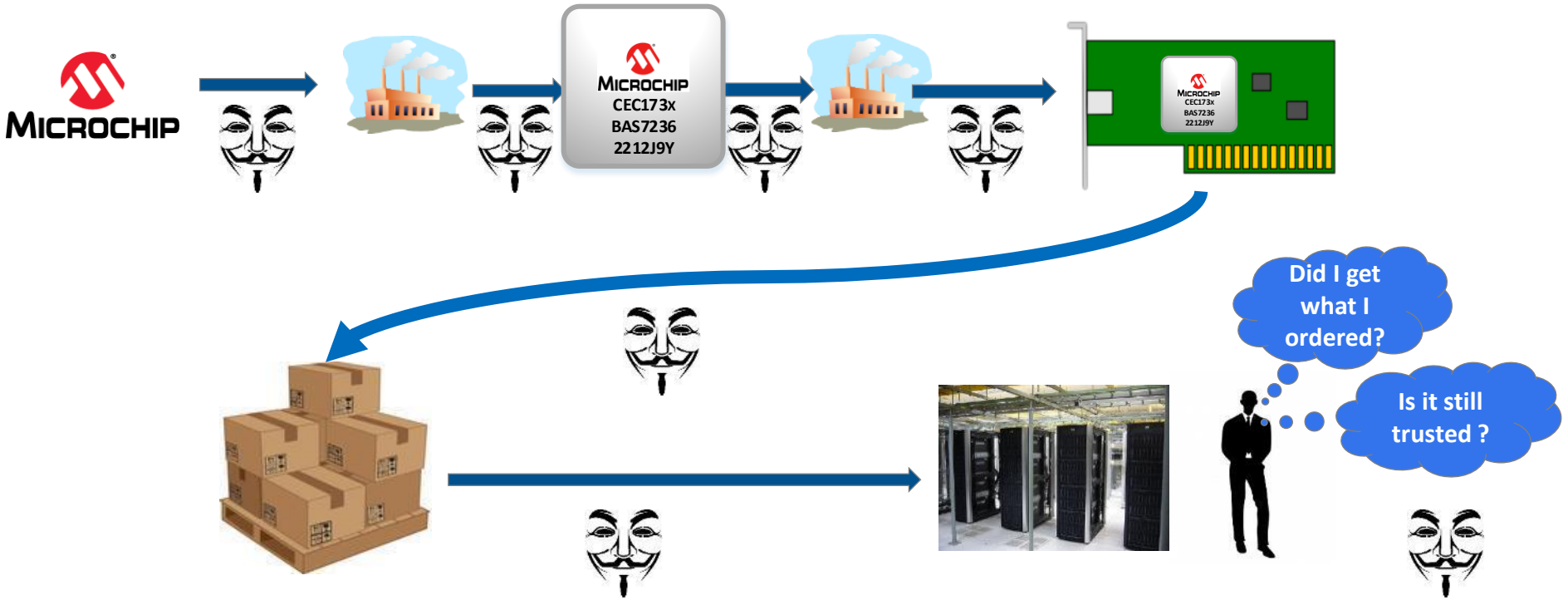


What is Device Attestation?

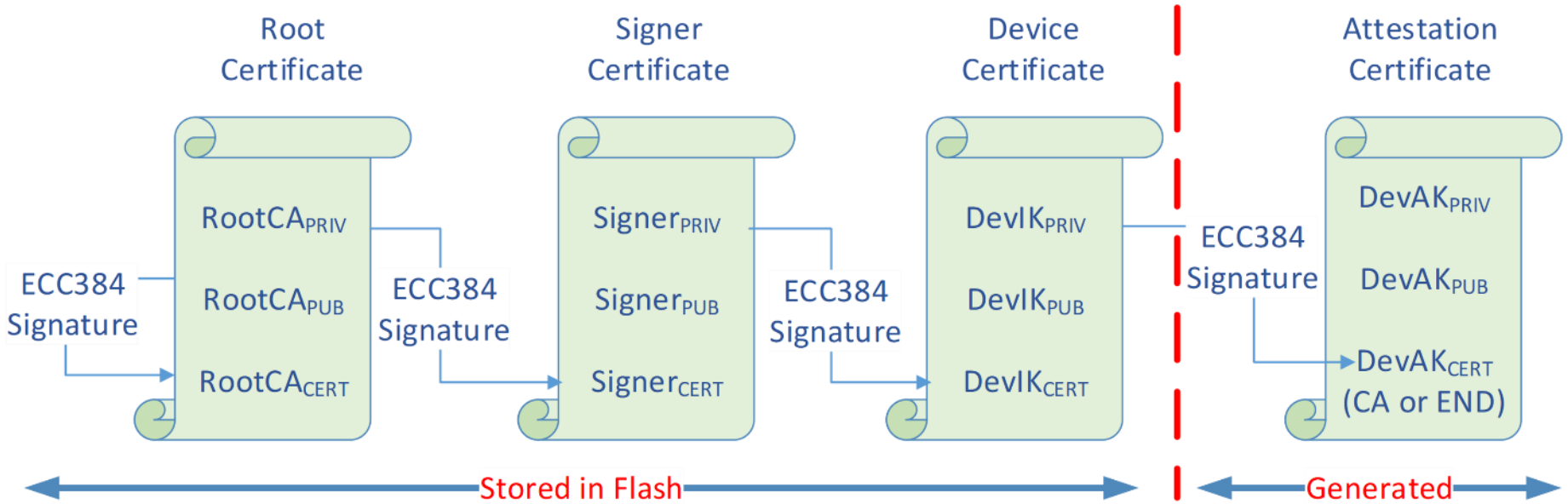
Upon request, a device must be able to provide credentials that provide clear evidence of the device's identity and the device's state of operation

Why Do We Need Attestation?

- Supply Chain Integrity
- Runtime System Integrity
- Owner Integrity



Manufacturing Certificate Chain



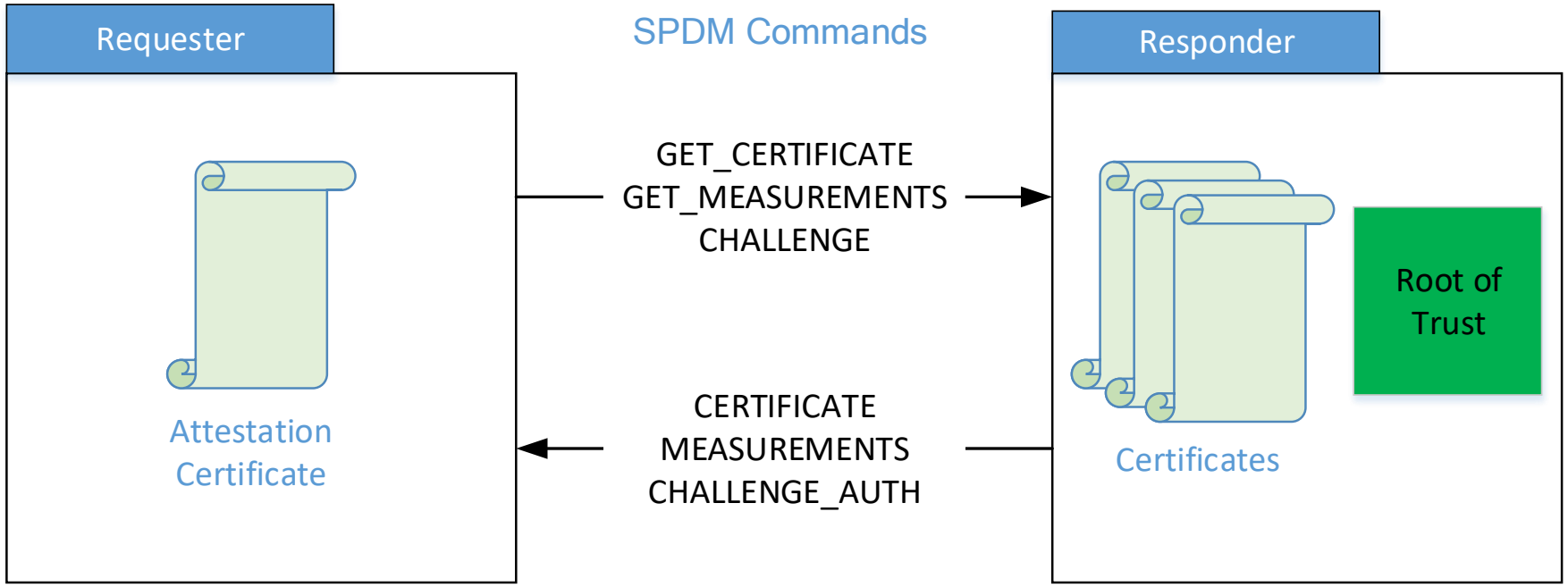
- Root certificate is unique per manufacturer or Certificate of Authority (CA)
- Signer Private Key (Signer$_{PRIV}$) is unique per customer (e.g., OEM)
  - Customer submits a Certificate Signing Request (CSR)
- Device Identity Key (DevIK$_{PRIV}$) is unique per device
- Manufacturer provisions the root, signer and DevIK certificates during manufacturing
- Device code (e.g., Boot ROM) generates and signs Device Attestation (DevAK) certificate
- Customer verifies certificate chain when product is received

Attestation Standards

Exchanging Device Attestation Information

- DMTF - Distributed Management Task Force
  - Security Protocol and Data Model (SPDM)
  - SPDM defines message formats and sequences for exchanging device identity and attestation certificates, measurements and challenge response commands

Security Protocol Data Model (SPDM)



- SPDM defines message formats and sequences for exchanging attestation information between devices

Attestation Standards

Generating Device Identity and Attestation Information

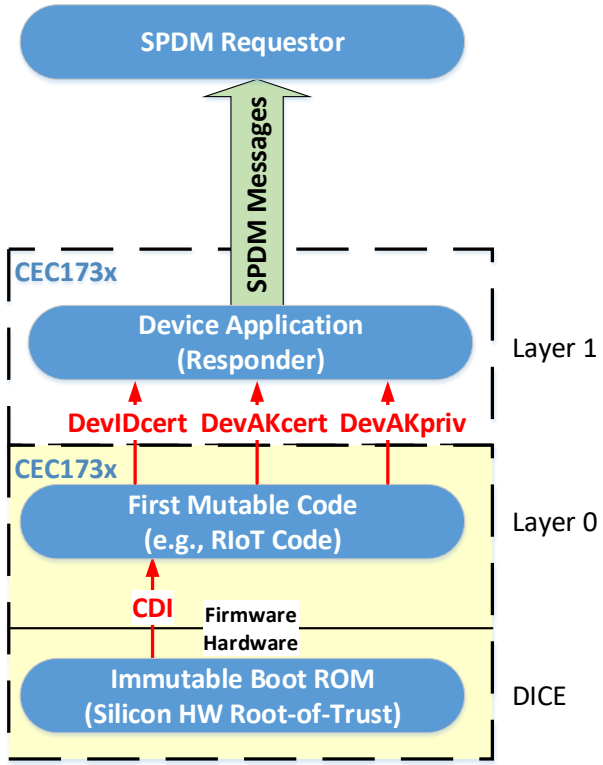
- TCG – Trusted Computing Group
  - Implicit Identity Based Device Attestation v1.0 specification
  - Describes the Device Identifier Composition Engine (DICE) use case that provides hardware-based Device Identity and Device Attestation
- OCP - Open Compute Project
  - Attestation of System Components v1.0 Requirements and Recommendations white paper
  - Describes attestation operations that produce information about ownership, system configuration and system components

TCG and OCP Attestation Options

Flash Memory Summit

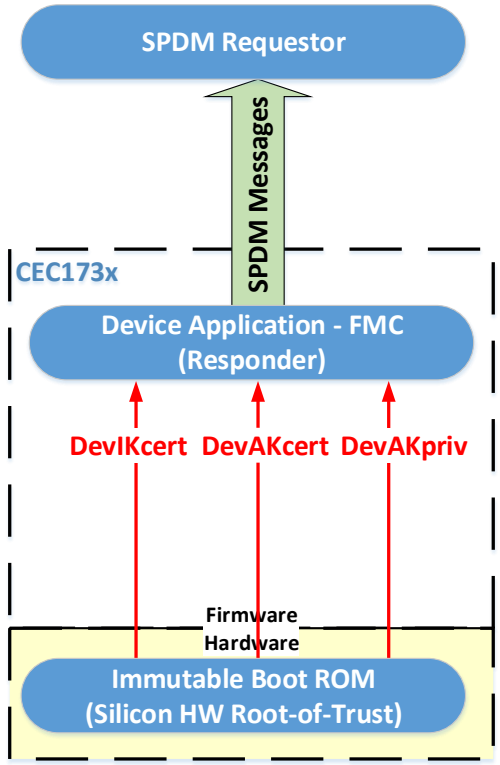
Device Identity

TCG DICE



- DICE Compound Device Identifier (CDI) is generated as a fx{UDS, Hash(FMC)}
- DeviceID key and alias key are generated as a fx{CDI}

OCP



- DevIK is generated on board by KDF or injected during provisioning - E.g., fx{UDS}
- DevAK is generated on board by KDF or by DevIK private key (optionally DICE compliant) – E.g., fx{UDS, Hash(FMC), hardware state, and owner}

35 YEARS OF NAND FLASH MEMORY INNOVATION

References

- National Institute of Standards and Technology, “Platform Firmware Resiliency Guidelines”, NIST SP 800-193, May 2018
- DMTF Security Protocol and Data Model (SPDM), DSP0274, Version 1.1.0
  - https://www.dmtf.org/sites/default/files/standards/documents/DSP0274_1.1.0.pdf
- OCP Attestation of System Components v1.0 Requirements and Recommendations
  - https://www.opencompute.org/documents/attestation-v1-0-20201104-pdf
- TCG: “Implicit Identity Based Device Attestation,” Version 1.0, Revision 0.93. March 5, 2018
  - https://trustedcomputinggroup.org/wp-content/uploads/TCG-DICE-Arch-Implicit-Identity-Based-Device-Attestation-v1-rev93.pdf

Questions?

- Come see our demo in Booth #613
- www.microchip.com/cec1736

Thank You

