Caliptra: A silicon root of trust

Making Silicon more Secure through Open Collaborative Design

SPONSORED BY

Caliptra Core

What is Caliptra?

- Silicon RoT block for integration into SoCs
- Targets datacenter devices (CPU, GPU, SSD, etc…)
- Goals: implementation consistency, transparency, standards compliance
- Output: Public specification, open-source RTL & firmware

How does Caliptra work?

- Anyone can contribute
  - Must sign CHIPS Alliance CLA
  - Free, no obligation – a licensing of contributions to the open-source project
- Anyone can integrate
- Anyone can attend meetings & discussion channels <caliptra.io>
- TAC decided by ¾ vote on major technical issues
  - TAC = Founding companies (AMD, Google, Microsoft, Nvidia)
  - TAC also decides project governance & trademark licensing

Caliptra

Caliptra Design Principles

- Open and Extensible
  - Developed in open on Github
  - Provided as SDK to build RoT Applications
  - Extensible and customizable by integrators
- Secure & Safe
  - Follows established security & isolation best practices
  - Memory Safe – Developed in Rust
- Consistent
  - Consistent implementation of Secure Boot, Measured Boot, Attestation, Recovery, Streaming Boot etc.
  - Standards Based - TCG, DMTF, OCP, NIST
- Compliant
  - OCP SAFE Audited
  - FIPS 140-3 Ready
  - Caliptra Trademark

Caliptra Roadmap

- Identity & Measurement
- Attestation
- Owner Authorization
- NIST CAVP, FIPS L1-Capable
- PQC Resilient FW-Based LMS Support
- ECC Signature Verify Primitive
- TCG DPE Support (iROT Profile)
- Bus User Identity (enabling higher priv/lower priv users)

- 1.0 bug fixes
- ECC & LMS acceleration
- LMS Signature Verify Primitive
- Measurement Manifest Verification (FW Only – v 1.2)
  - Vendor Secure Boot
  - Owner Authorization

- NIST PQC (CNSA 2.0 Compliant)
  - Dilithium/ML-DSA-87
- VeeR Updated with Privileged Mode
- OCP Recovery / Streaming Boot
- MCU for SoC Specific FW
- Fuse Controller (extensible for SoC Use)
- Crypto Algorithm Mailbox

- NIST PQC (CNSA 2.0 Compliant)
  - Kyber/ML-KEM-1024
- VeeR (RISC-V) Security Counter Measures / features
  - TBD based on Feedback
- OCP L.O.C.K

Benefits of Caliptra

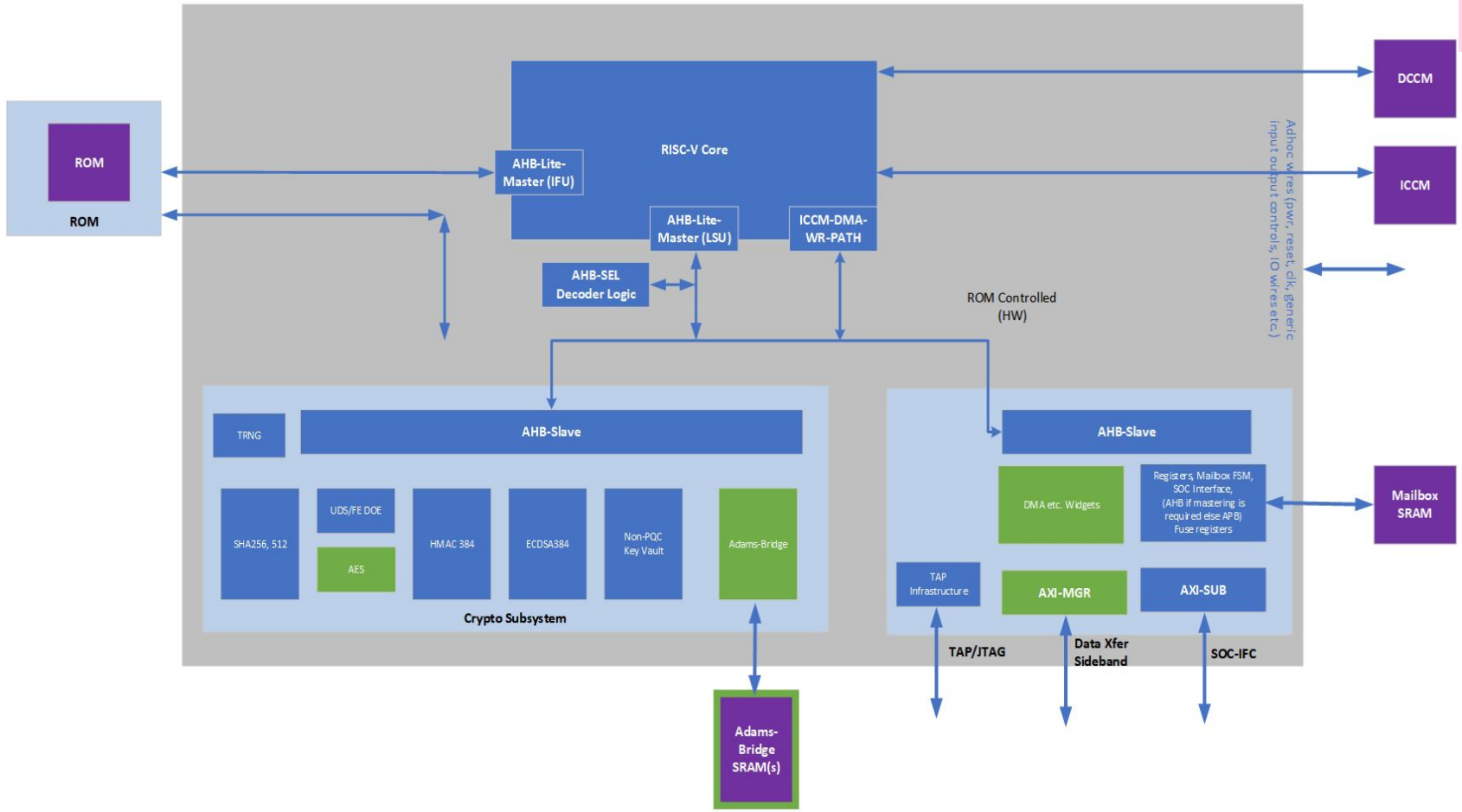
- Built on community contributions to OCP
- Fully open-source with ASL 2.0 license
- OCP S.A.F.E audited (RTL, ROM, FW)
- Caliptra is its own CNA: Ease of PSIRT integration
- NIST CAVP ready and CMVP capable
- PQC ready!

Caliptra 2.0

- Caliptra 2.0 comprises of consortium governed ROM, FMC and Runtime
- Caliptra 2.0 provides foundational security features for MCU
  - Quantum Resilient DICE
  - OCP Recovery Boot
  - Classical and Post Quantum Cryptography API support
  - Debug Unlock support
  - Quantum Resilient DPE

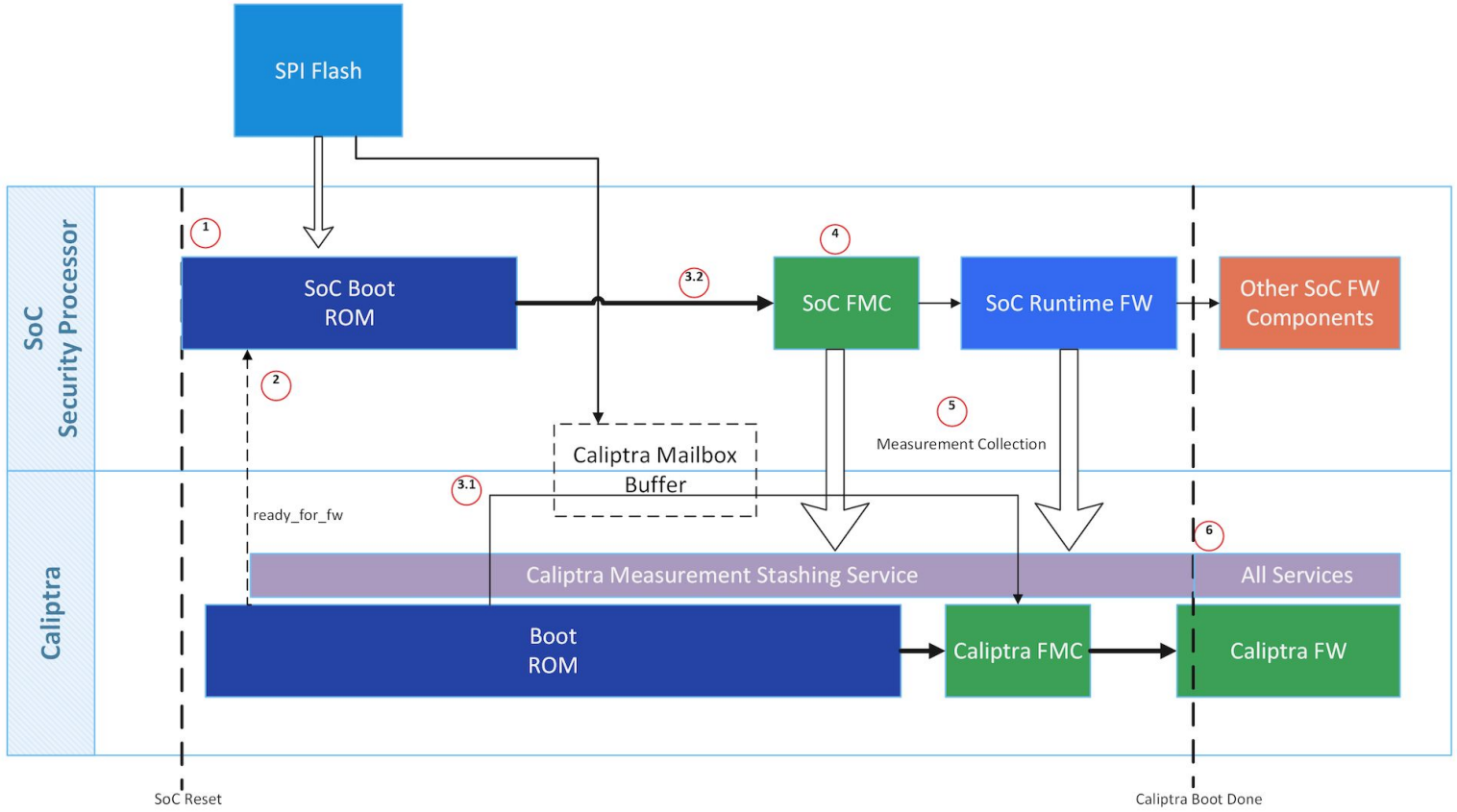
Caliptra Core

- Caliptra HW IP
  - Large gray box
- Caliptra Wrapper
  - Purple SRAM/ROM
  - Fuses
  - Noise Source
- New in Caliptra 2.X
  - Green



Caliptra Core Bootflow

- SOC Root of Trust and Caliptra Boot at the Same Time
- Caliptra creates identity and DICE/DPE Profile on boot
- SOC RoT sends Measurements to Caliptra (Stash Cmd)



Caliptra Subsystem

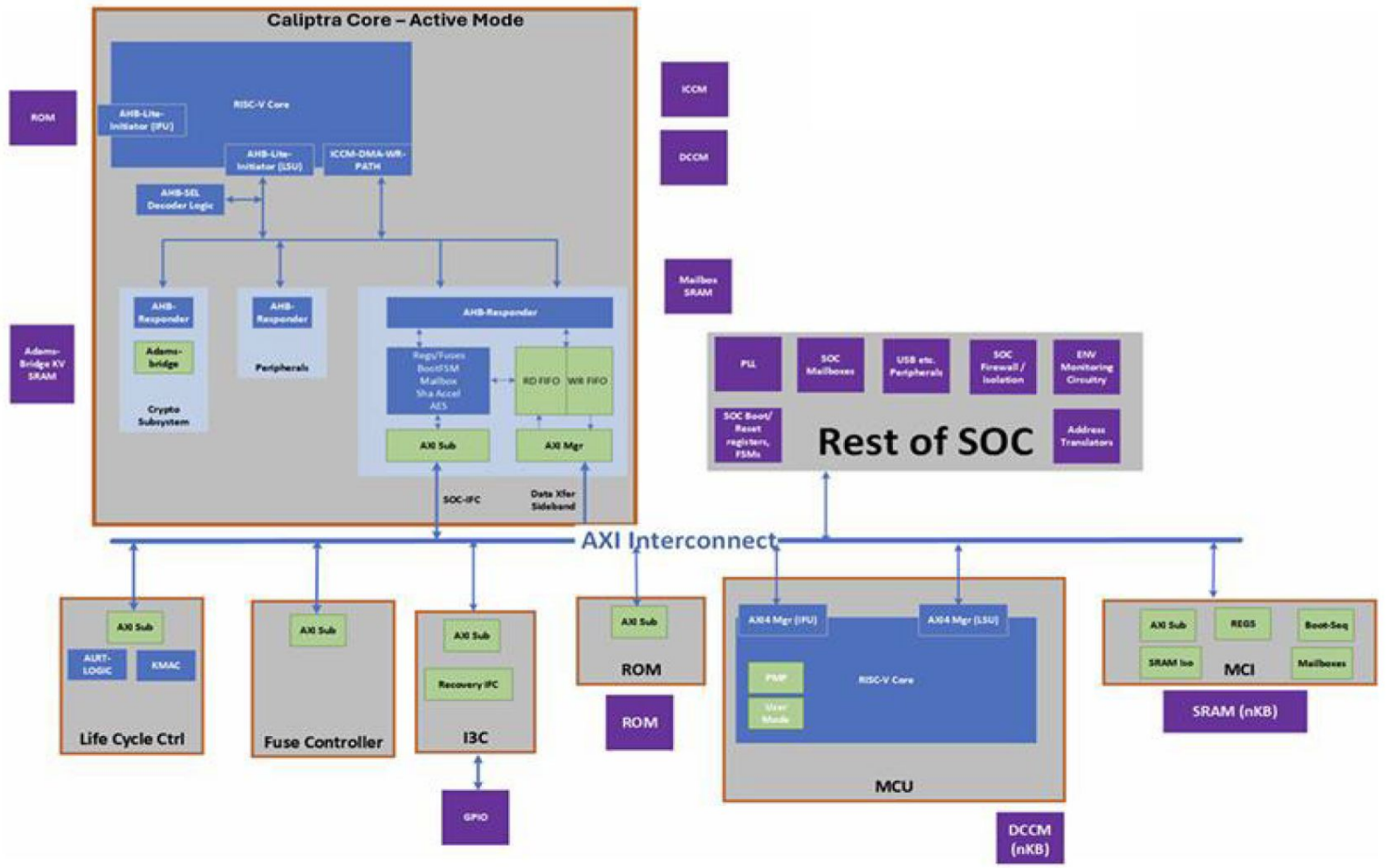
Enables Caliptra Integrators to build fully featured RoT

Caliptra Subsystem Features

- Caliptra 2.0 - Security Features
  - ML-DSA (with Adams bridge integration), DICE extension w/ PQC, AES, Key Vault Extensions for PQC, PCR Signing with PQC
  - Subsystem Mode Support: AXI DMA Assist, Manufacturing & Product Debug Unlock, UDS programming, Streaming boot support in Caliptra
  - Integration of Life cycle controller & Fuse controller
  - OCP Streaming boot support over I3C
  - MCU & corresponding HW support for running SOC specific FW (whose FW is loaded/bootstrapped by Caliptra)

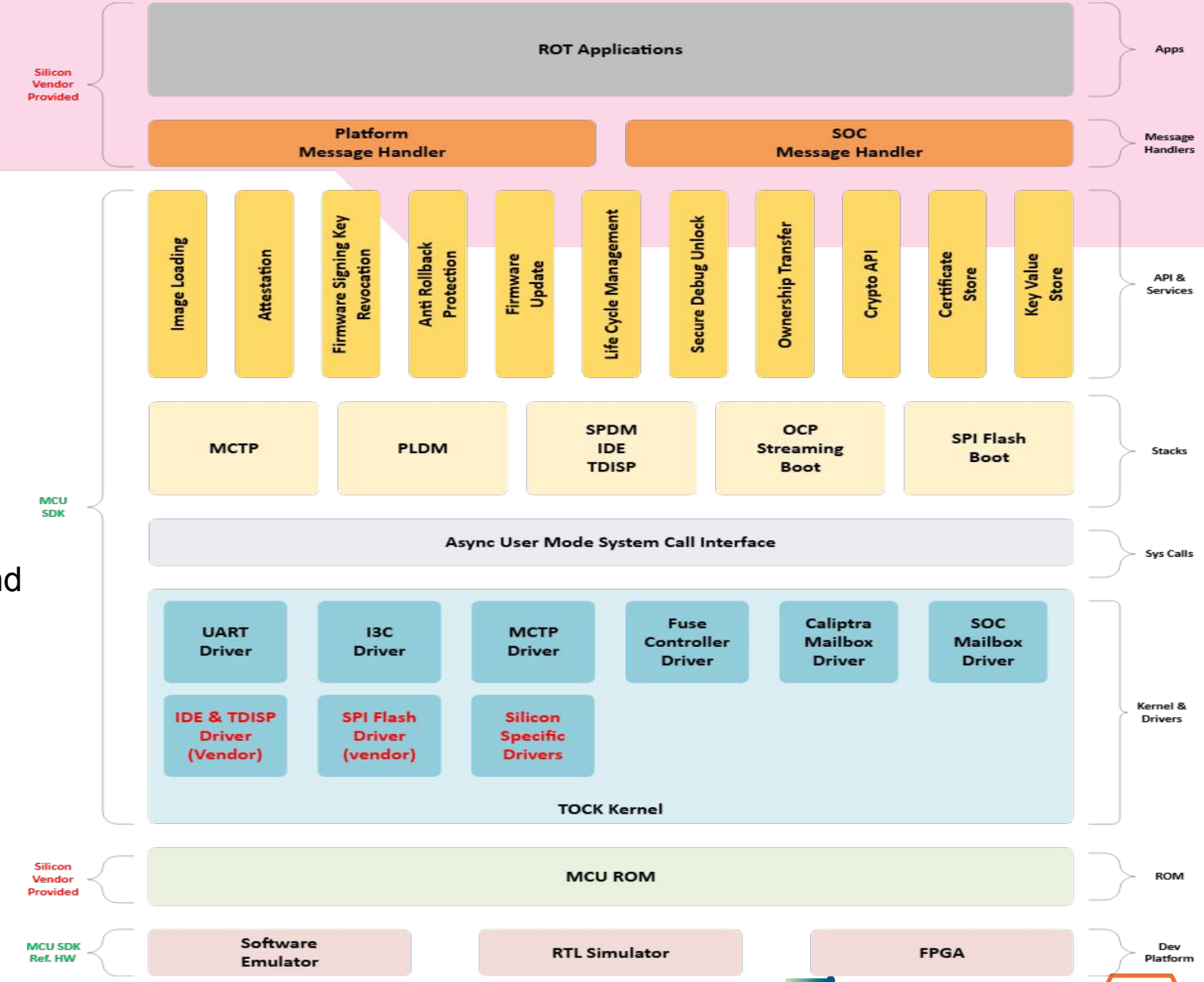
Caliptra Subsystem

- Caliptra HW IP
  - Large gray box
- Caliptra Wrapper
  - Purple SRAM/ROM
  - Fuses
  - Noise Source
- New in Caliptra 2.X
  - Green



MCU SDK

- Development Tools
  - Emulators, RTL Simulators & FPGA
- Reference MCU ROM
  - Reference MCU ROM implemented in Rust
  - Illustrates integration b/w Caliptra 2.x and MCU
- TOCK Kernel
  - Provides user/kernel mode isolation via RISCV MPU
  - Driver Model for extensibility



Caliptra Compliance and Trademark

- MCU SDK will be reviewed, audited and compliant to various standards

- Current Plan is to support compliance with:
  - Caliptra Trademark
  - OCP SAFE
  - FIPS 140-3