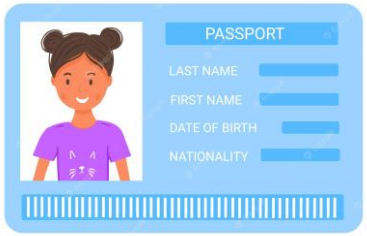
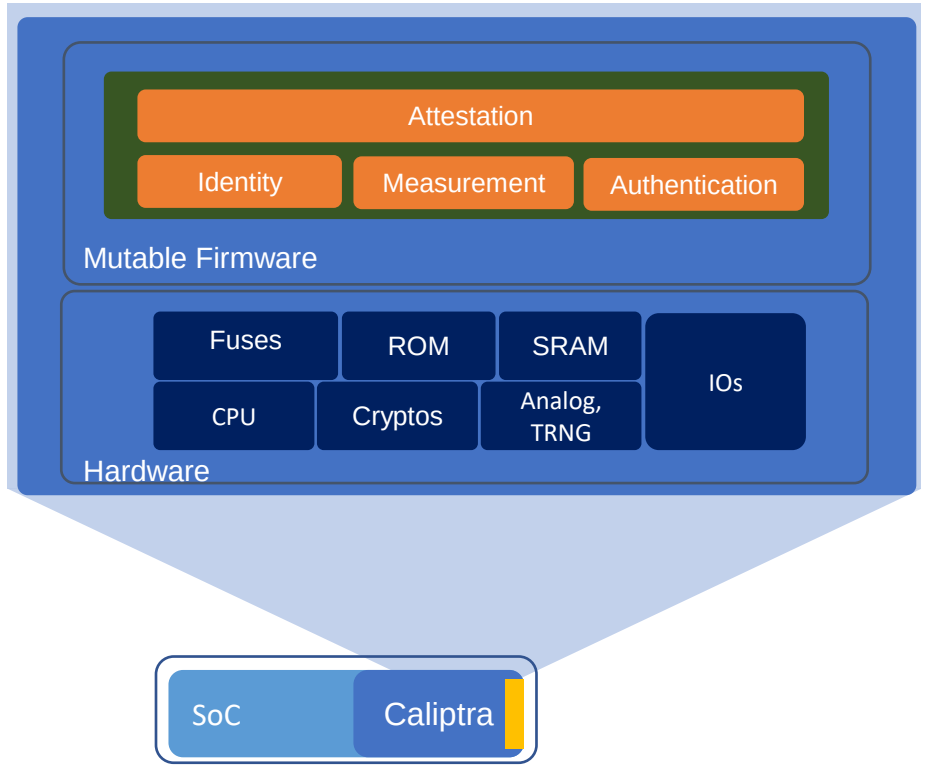

Caliptra

What is Root of Trust

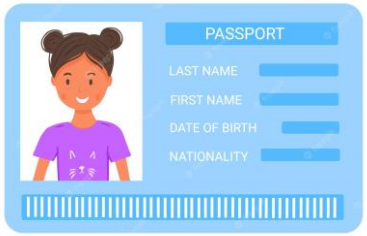


Identity	Manufacturer Identity aligned to TCG DICE
Measurement	Code & configuration posture of the device.
Lifecycle	Debug mode (ON/OFF), modes of operation
Ownership	Vendor authored firmware only, with stateless Owner Authorization
Attestation	Identity & Measurement reporting



Set of security primitives that form the foundation for building more advance security features

Root of Trust – State of the Industry

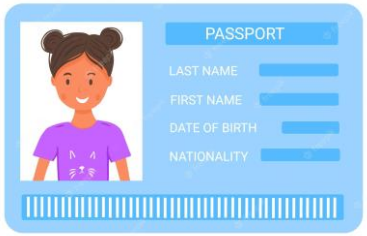


There are many solutions…

Industry fragmentation…

Many deficiencies…

What is Caliptra

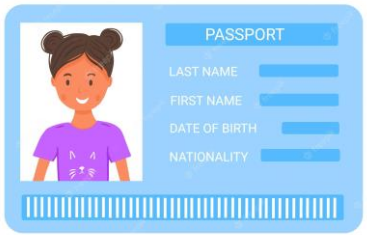


Caliptra (*Spanish,* 'root tip') an open-source silicon Root of Trust

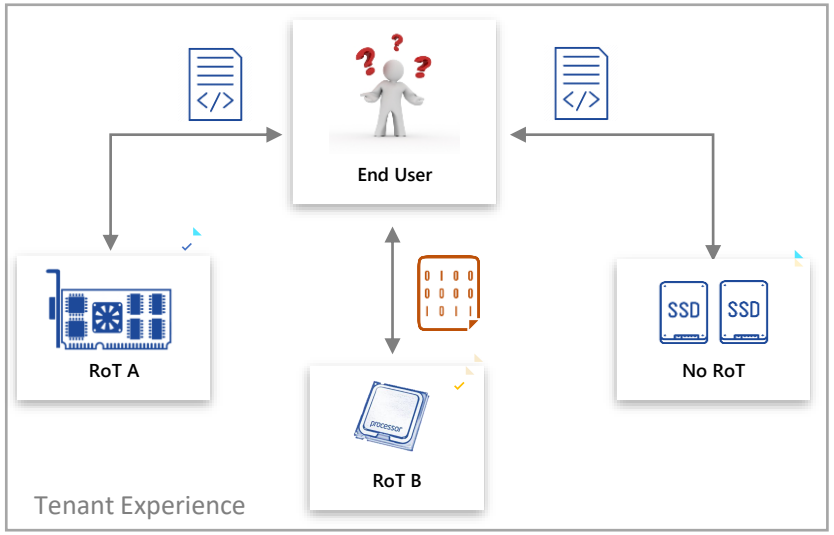
Consistency of security primitives that underpin higher-level capabilities and operational behaviors.

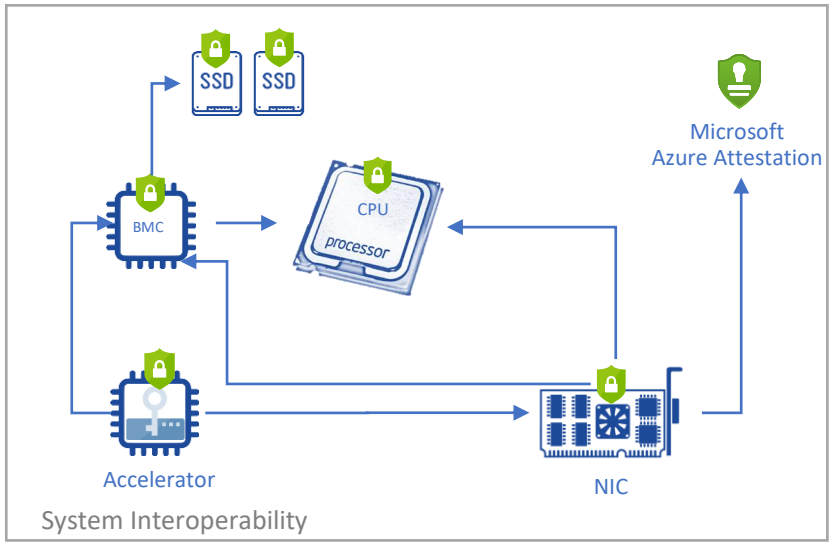
Transparency of security mechanisms of confidential cloud devices.

Why Consistency is Important

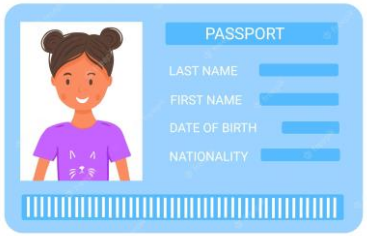


- Heterogeneity of RoT implementations is massive drain on our: operations; customer experience
- Confidential device measurements are tenant visible
- Interoperability, components intercommunicate and report to measurement
- Functional consistency across operational flows, tightly coupled to life-cycle and live-site





Why Transparency is important



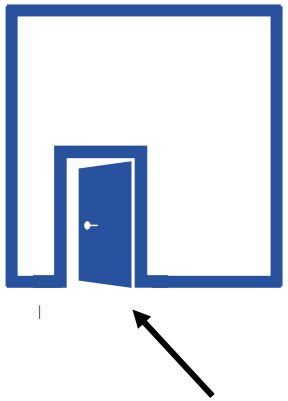
Root-of-Trust is a foundational hardware security primitive that bootstraps higher-level security capabilities

Transparency builds trust… provides assurance of the hardware mechanics for measurement

Caliptra akin to a door that records entry into a room, don't care about décor, just security at entry and exit

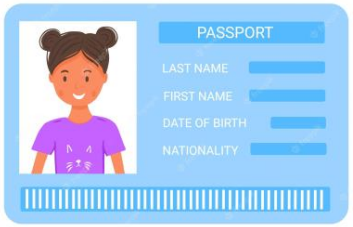
Lower silicon burden of proof through transparency of RoT, narrows verification and audit.

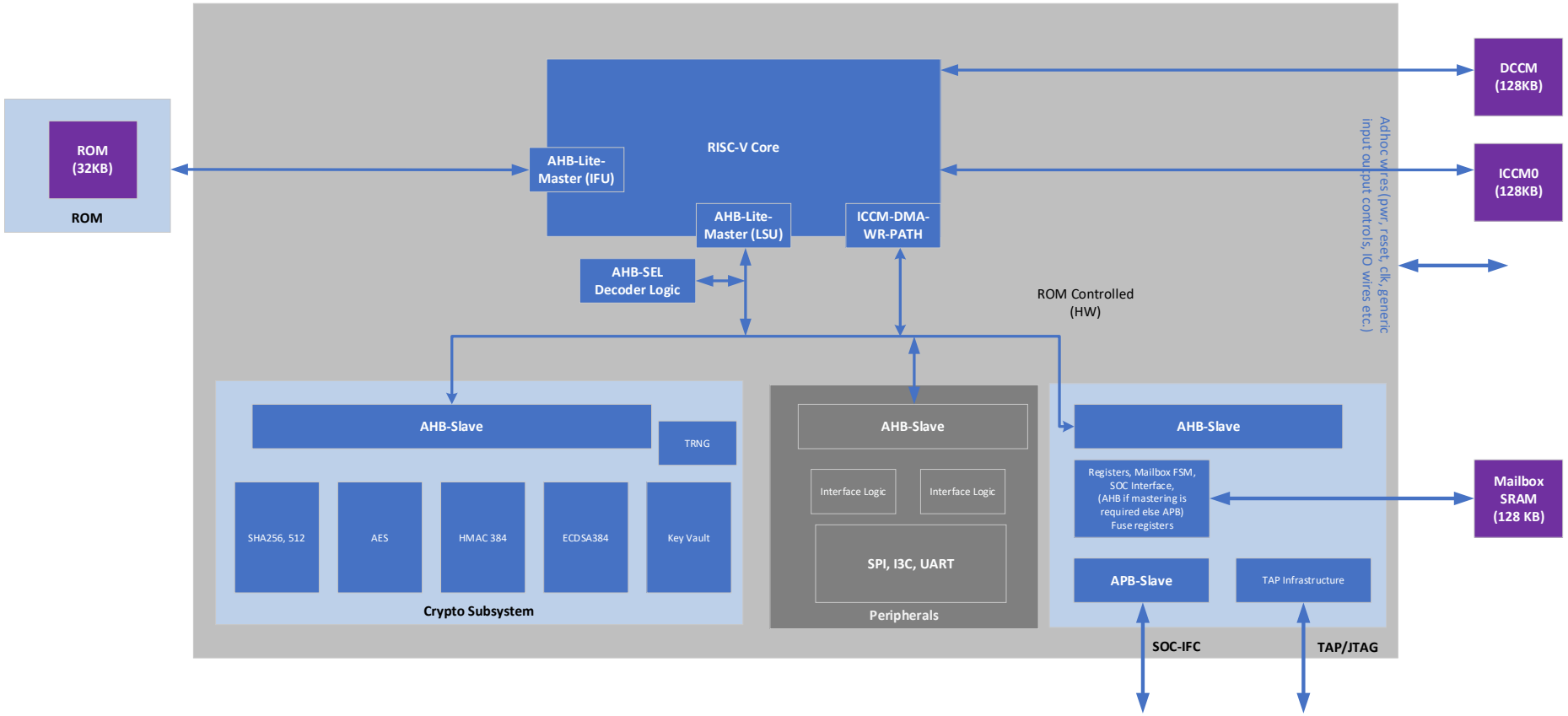
Caliptra, focuses on monitoring ingestion points



Transparency on what enters and leaves, not explicitly what's inside.

Caliptra – HW View

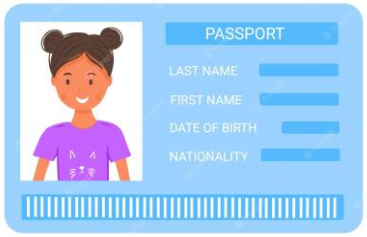




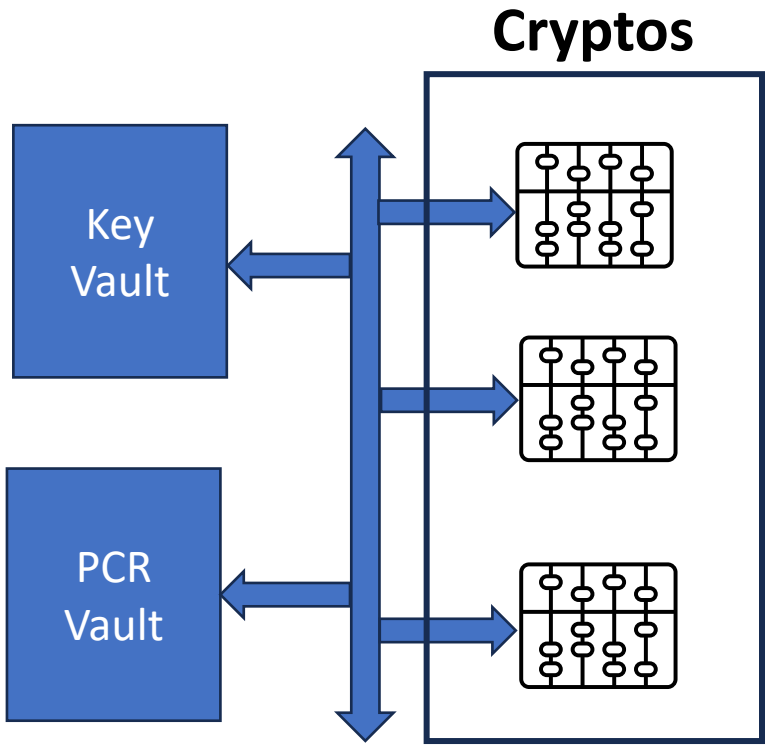
- Open-source VeeR core, Instruction RAM (ICCM) & Data RAM (DCCM) physical separation, No DMA access from any peripherals/external SOC into ICCM/DCCM, No writes into ICCM on ROM-exit
- Side-channel protected Crypto HW & No FW access to security keys/assets (more on this later)

- Caliptra as-a-whole is an APB-device (can only speak when spoken to!)
  - Cannot ‘master’ random transactions to rest of the SOC
- No integrated peripherals required

Caliptra – Cryptos & Operations



- DICE (Device Identity Composite Engine) is implemented in HW
- Fuses are external but security critical fuses itself are decrypted with Caliptra internal class keys (by HW)
- **Cryptos:** ECC384, HMAC-DRBG, SHA256, SHA384/SHA512, HMAC-384, Integ-TRNG, DICE-obfuscation-Engine (DOE)
  - Refer to Caliptra spec on the RFC references and side channel mitigation information.
- Key Vault & PCR Vault are implemented in HW
  - FW (ROM or run-time) cannot access keys; only key-handles are available
  - PCRs can only be 'extended'
  - Key vault also implements various key protection mechanisms (ex: a key can only used 'ECC signing')
  - PCR signing is also fully implemented in HW (FW can only 'request' for PCR signing – cannot specify the key or change PCRs that are being signed)
- Assets are cleared and Cryptos are zeroized in debug/scan modes



Caliptra - Status

Caliptra was open sourced on October 18th, 2022 with multiple partners planning products.

Built supporting industry standards; TCG DICE, DMTF SPDM, OCP Secure-boot, Attestation, Recovery.

Microsoft, Google, AMD, Nvidia are founding project partners.

Design (RTL & ROM) release in August'23. Run-time FW will follow that immediately

Project Caliptra Next Steps

Development & Discussions in the open – no more NDA requirements (CLA is still required)

CHIPSALLIANACE Caliptra Public WG meeting – Every Friday 9am PST

Call for Action

- ❑ Best technologies blossom with “brain share” & collaboration
- ❑ Security is the critical pillar to protect all “our” data and RoT technologies is the “Caliptra” of it