



**OPEN**  
Compute  
Project®

# Caliptra

**An open source, reusable silicon IP block for  
a Root of Trust for Measurement (RTM)**

Andrés Lagar-Cavilla (Google)

Prabhu Jayanna (AMD)

Bryan Kelly (Microsoft)



# What is Caliptra

- An OCP specification for a **silicon Root of Trust** internal block
- Targeting **SoCs** and ASICs in the **hyperscaler**/datacenter space
- **Goals:**
  - implementation consistency, transparency, openness, reusability
- A **multi-party collaboration** including (today):
  - Google, AMD, Microsoft
- An **open source** implementation of the specification
- The first Security project specification proposing a technology block
- Work in progress!





# Targets

- Datacenter devices use by CSPs, hyperscalers
- Not for phones
- Not a discrete or platform RoT
- Key priority are devices handling plaintext user data
  - SoC, GPU, NIC/IPU/DPU
  - Provide a transparency substrate to root confidential compute
  - For example, could fulfill the HES role in Arm RME spec
- Follow on: devices handling cipher text
  - Storage, [NV] DIMMs, switches

# Architectural Role



“Composable Security Architectures” in 2021 OCP summit

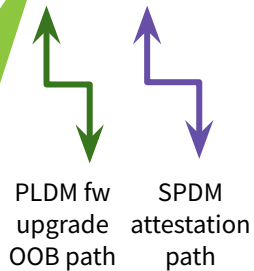
Let's define this today



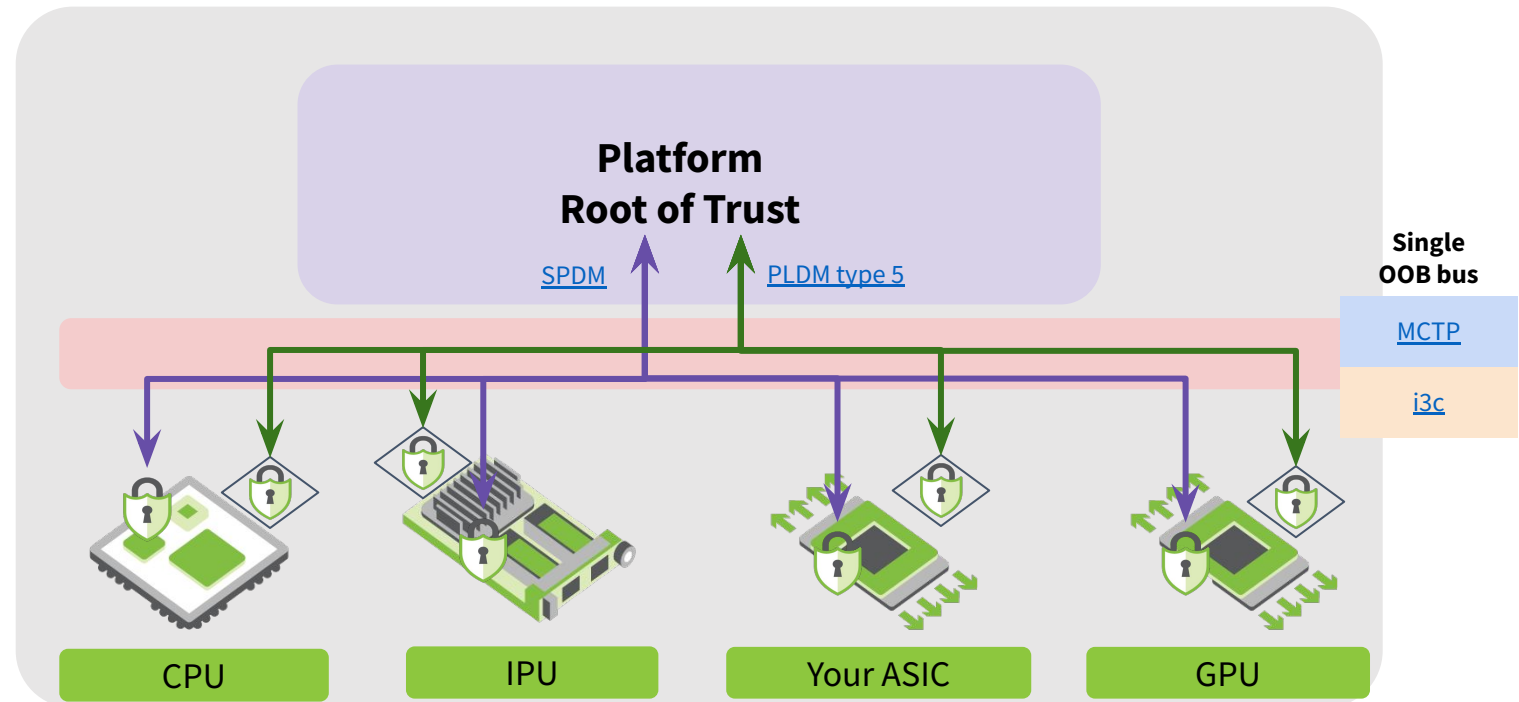
Internal RTM



Discrete RTU  
+ RTRec





Examples:  
BMC,  
iLO,  
iDRAC,  
Titan,  
Cerberus,  
PFR,  
CEC1712



# What is an RTM?


## [NIST 800-193, Platform Firmware Resiliency Guidelines](#)

<b>Detection</b>	<b>RTM</b> : RoT for Measurement (a.k.a. RTD)	<b>Integrated Silicon RoT</b> <ul style="list-style-type: none"> <li>• Well and narrowly defined job</li> <li>• Measure, verify and attest</li> <li>• In package – best bet against physical attacks on integrity</li> <li>• Limited fuses</li> </ul>	
<b>Protection</b>	<b>RTU</b> : RoT for Update	<b>Discrete RoT Chip</b> <ul style="list-style-type: none"> <li>• Mitigate DoS at scale</li> <li>• RTU: reject random blobs pushed at scale</li> </ul>	
<b>Recovery</b>	<b>RTRec</b>	<ul style="list-style-type: none"> <li>• RTRec: automated recovery against buggy updates</li> <li>• Ok to be a separate discrete element <ul style="list-style-type: none"> <li>• Physical attacks irrelevant to scalable DoS mitigation</li> </ul> </li> <li>• Integrated flash for unlimited renewability <ul style="list-style-type: none"> <li>• Enforce versions, owners, rotations</li> </ul> </li> </ul>	



# Value of Decoupling

## [NIST 800-193, Platform Firmware Resiliency Guidelines](#)

<b>Detection</b>	<b>RTM</b> : RoT for Measurement (a.k.a. RTD)	<b>Integrated Silicon RoT</b> <ul style="list-style-type: none"><li>• Well and narrowly defined job</li><li>• Measure, verify and attest</li><li>• In package – best bet against physical attacks on integrity</li><li>• Limited fuses</li><li>• Not concerned with update or ownership</li></ul>	
<b>Protection</b>	<b>RTU</b> : RoT for	<b>Discrete RoT Chip</b>	
<b>Recovery</b>	Decoupling Update and Recovery DoS mitigations usefully simplifies the SoC RTM <ul style="list-style-type: none"><li>• No need for persistent flash</li><li>• No need for update, fallback, A/B schemes</li><li>• No need for TPM behaviors, or persistent ownership</li></ul>		

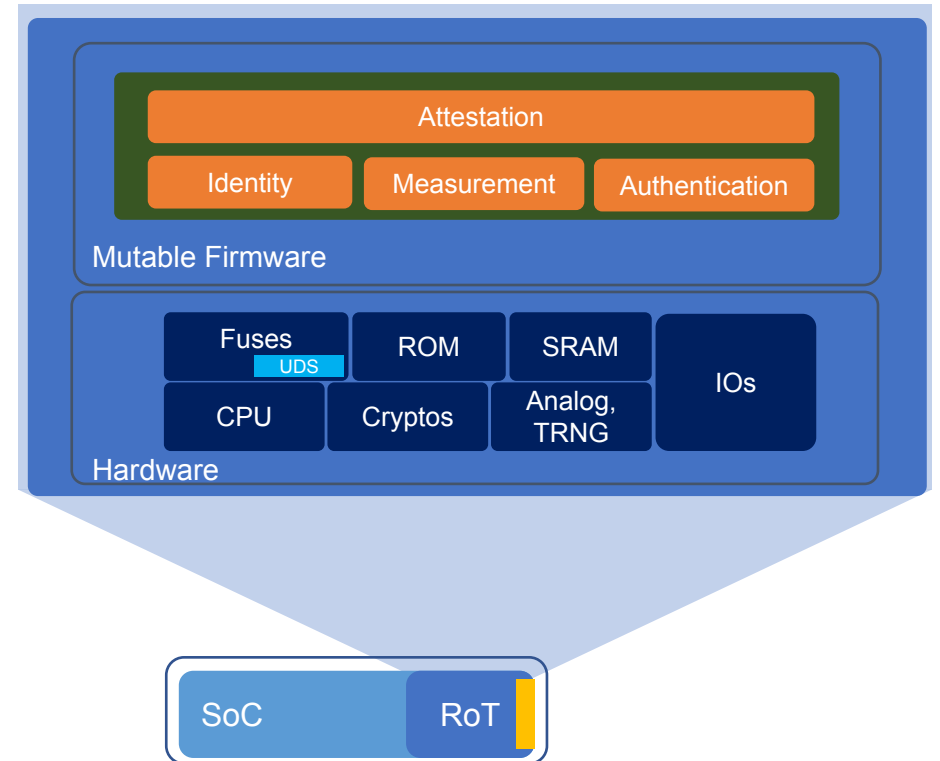


# Our Goals

- RTMs have a well and narrowly defined job
  - Measure, verify and attest
  - No need for update, fallback, A/B recovery, TPM, ownership flows
- Useful simplification leads to easier path for **convergence**
  - Aligned/converged specification
  - Open Sourcing
  - Transparency
  - Reusability
  - Implementation Consistency
  - **These are our goals**

# Caliptra: Behavioral Elements

Identity	Manufacturer Identity aligned to TCG DICE
Measurement	Code & configuration posture of the device.
Lifecycle	Debug mode (ON/OFF), established at reset.
Ownership	No stateful transfer. Vendor authored firmware only, with stateless Owner Authorization
Attestation	Identity & Measurement reporting using DMTF SPDM v1.2+





# Summary of Key Behaviors

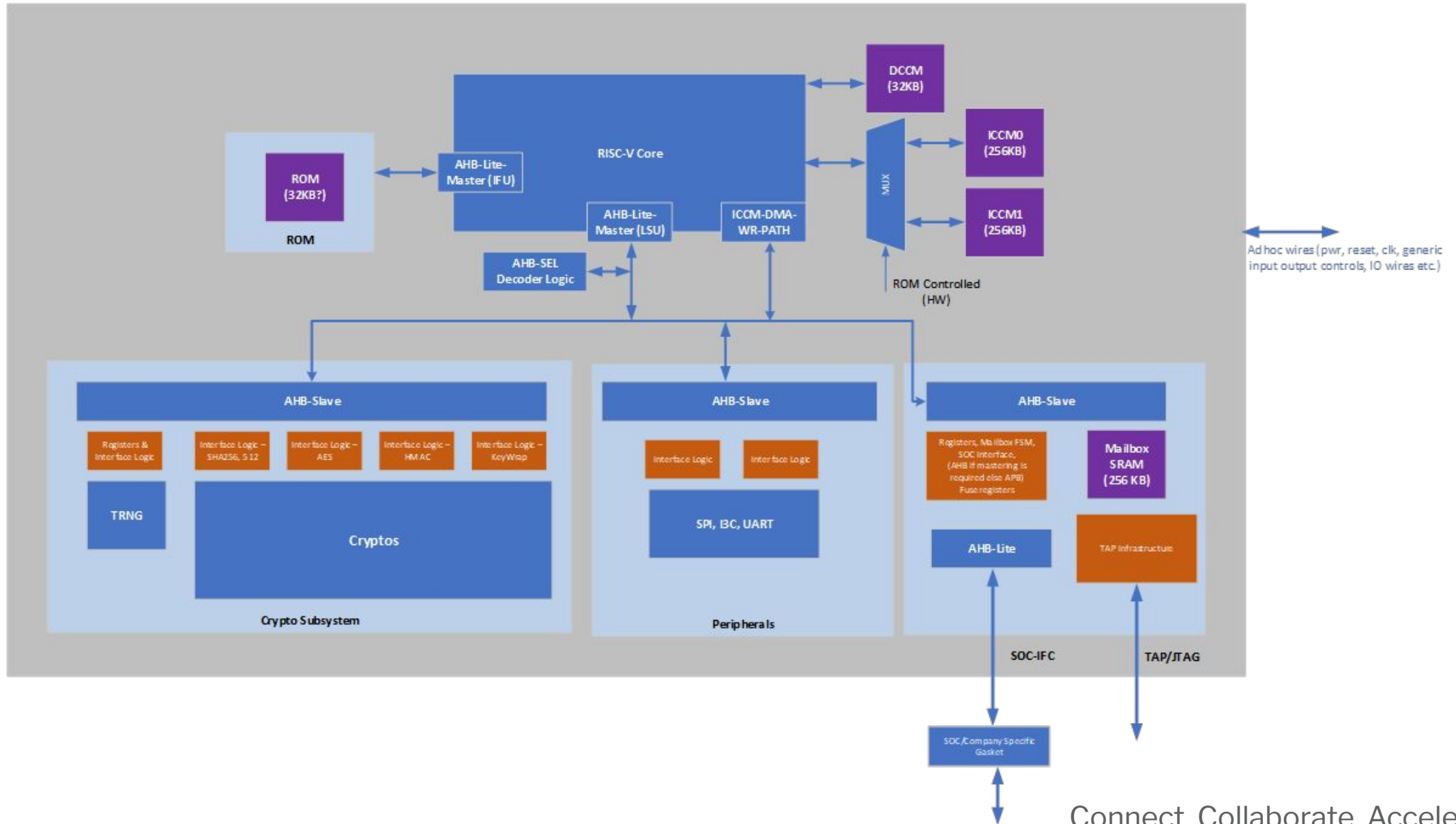
- **Measurement**
  - Load fw, measure fw, and release fw target from reset
- **Configuration**
  - Measure relevant security configuration state
  - JTAG enablement, GPIO/straps/fuses
- **Attestation**
  - Form an attestation and sign it with unforgeable entropy
- **Identity**
  - Provide and protect unique asset entropy (DICE UDS)
- **Identity Service**
  - For example provide derived keys from UDS to core



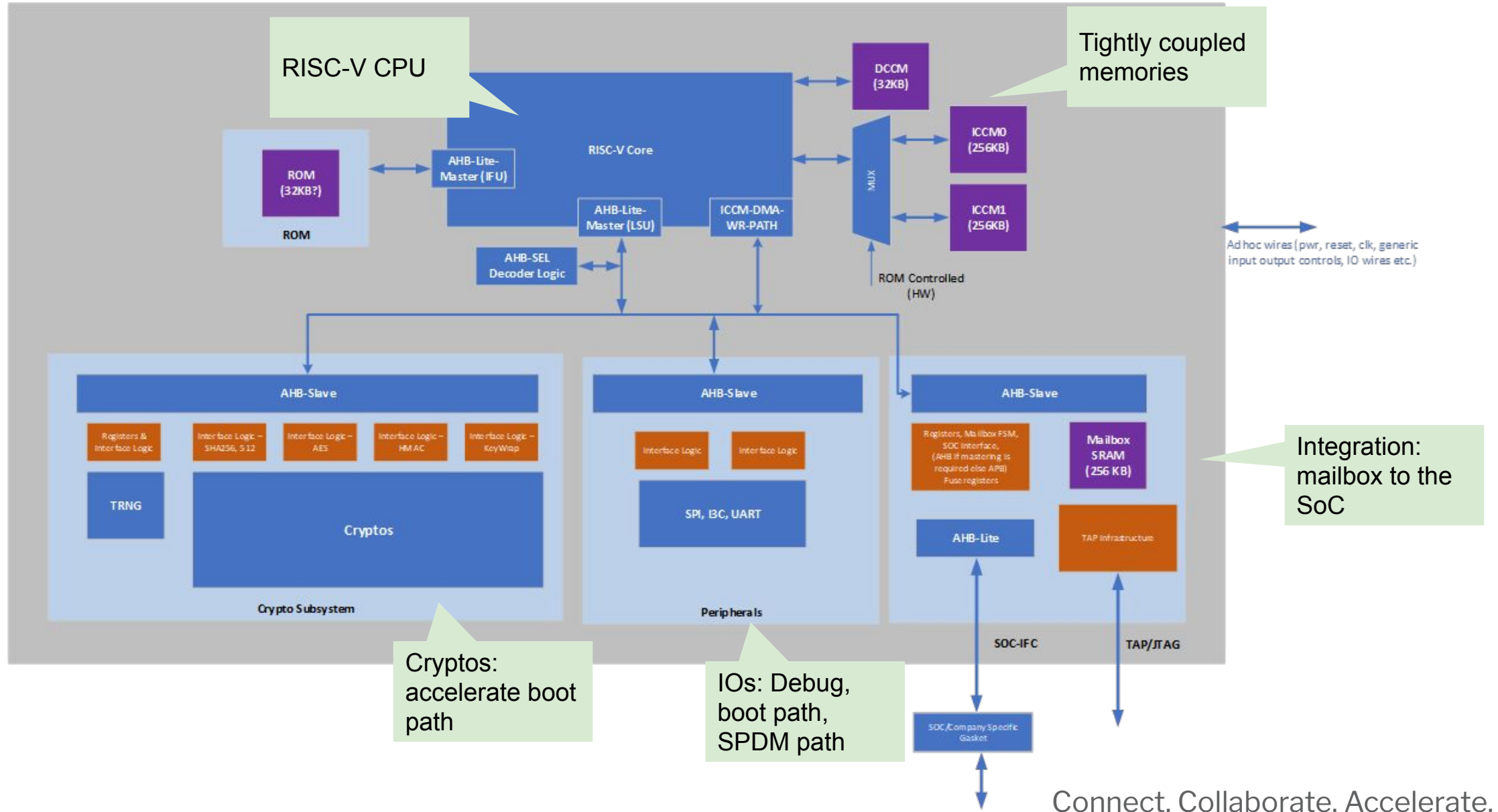
# Critical Decisions

- Not interested in differentiation
  - Caliptra is not a landing pad for vendor “value adds”
- Support only manufacturer signed RTM code
  - Code roots back to open source fw development
- Leans on DICE
  - FMC mixed into UDS to generate an Alias keypair
  - Derived Alias key signs attestation
- Stateless ownership enforcement
  - A silicon owner can additionally sign code with their key
  - The public signing key is reported in attestation
  - Until next power-on, owner key enforces runtime upgrades
- SPDm responder
  - GET\_CERTIFICATES 1.2 (or 1.3) responder for attestation
- Facilitate SoC integration

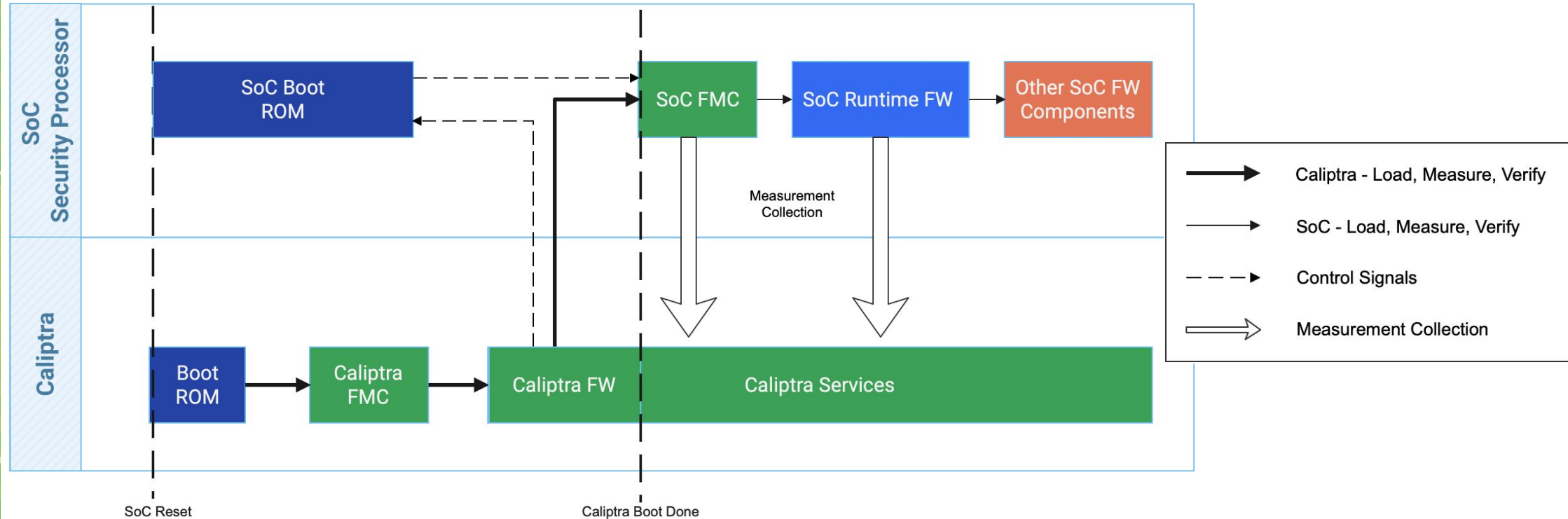
# High Level Block Structure



# High Level Block Structure

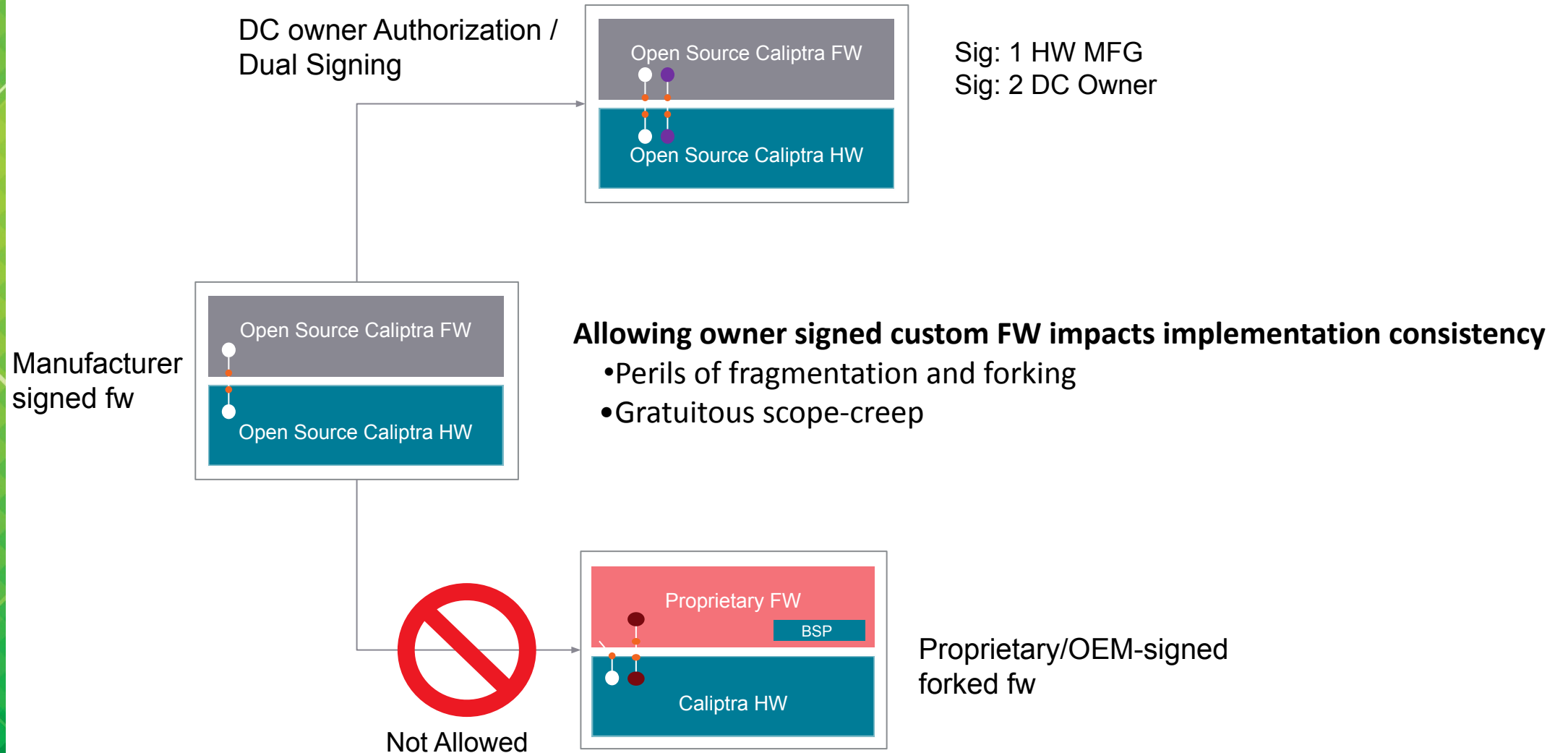


# Making It SOC Independent



- Caliptra boots first, reads its fw, creates identity
- Copies and measures SOC FMC firmware into SRAM buffer
- Releases SOC ROM from reset to boot
- SOC ROM loads FW using current flows and authentication
- Simplifies integration, preserves existing security flows.
- Attestation is always done through, and rooted to, Caliptra

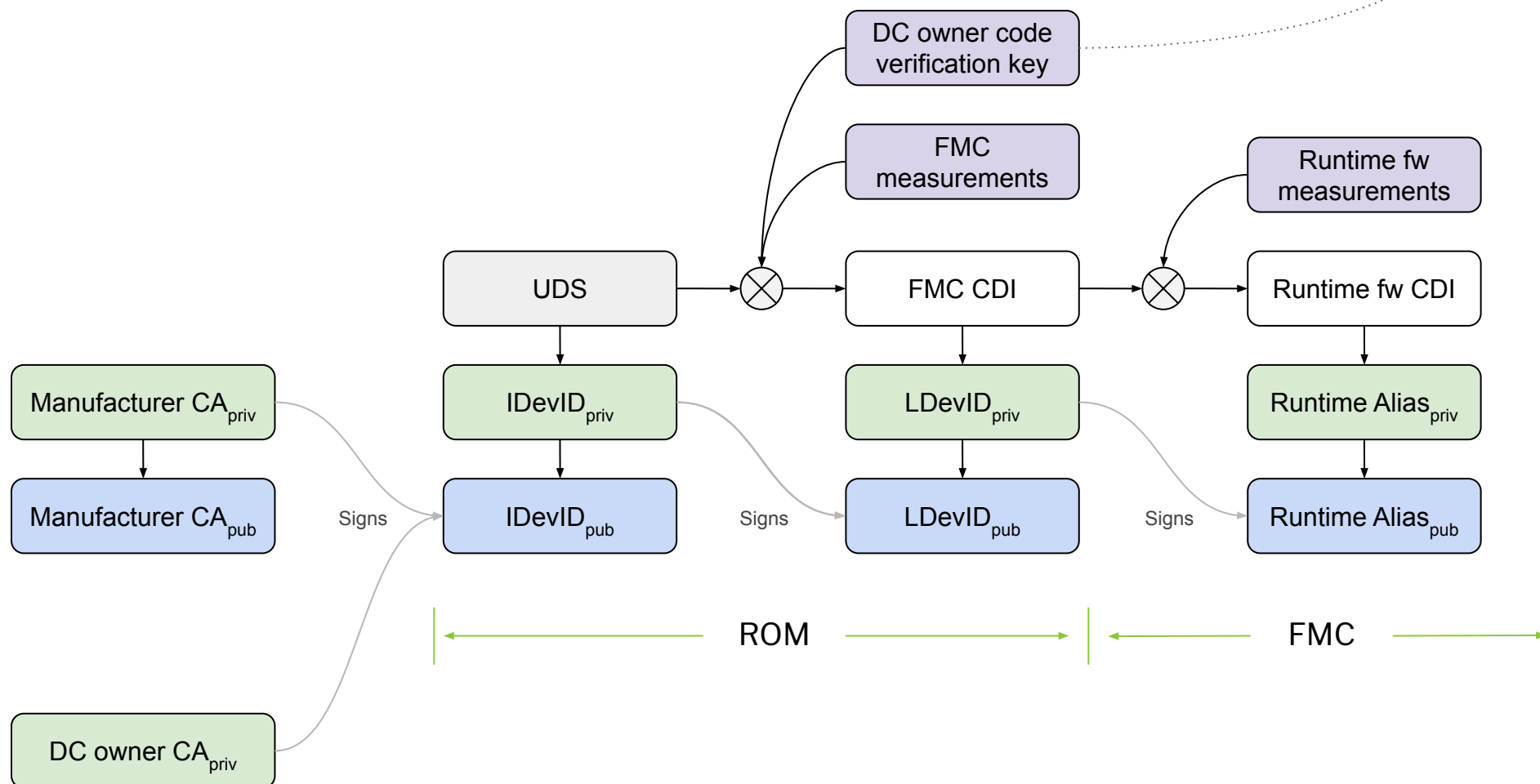
# Ownership & Implementation Consistency



# DICE Identity

BK

- Co-signs Caliptra firmware
- Latched into Caliptra RAM on cold-boot
- Authorizes runtime Caliptra updates





# Commitments

- Google silicon target 2024
- AMD silicon target 2026+
- Microsoft silicon since 2024



# Work In Progress

- Three parties in CLA
- v0.5 spec by end of May, then publish to community
- **Partners welcome**
  - **Must commit to integrate and contribute!**
- RTL in progress
  - fw to follow on
- Committed to open sourcing RTL, FW and Specifications

# FAQ (don't panic)

ALC



- Not a whole chip! It's an IP block
- Not intending to over-specify how you should build your SoC
  - Not mandating backend IP synthesis methods
  - Not mandating certification criteria
  - Not mandating analog IPs, or counter-measures
  - Not mandating a fuse technology or a process node
  - Not mandating manufacturing operational security processes
- Not a datapath element or general purpose crypto accelerator!



# Caliptra: Take Home

- Silicon IP block for integration into SoC
- Hyperscaler/datacenter device targets
- Public specification, open source logic and fw
- RTM: Measurement, attestation, identity
- Goals are implementation consistency, portability, transparency, openness
- Explicitly decoupled other security functions to achieve goals
- Google, AMD, Microsoft
  - Contributors who will integrate are welcome!

# Caliptra

**An open source, reusable silicon IP block for a Root of Trust for Measurement (RTM)**

Andrés Lagar-Cavilla (Google)

Prabhu Jayanna (AMD)

Bryan Kelly (Microsoft)

# Thanks! Q&A

Connect. Collaborate. Accelerate.



**OPEN**  
Compute  
Project®