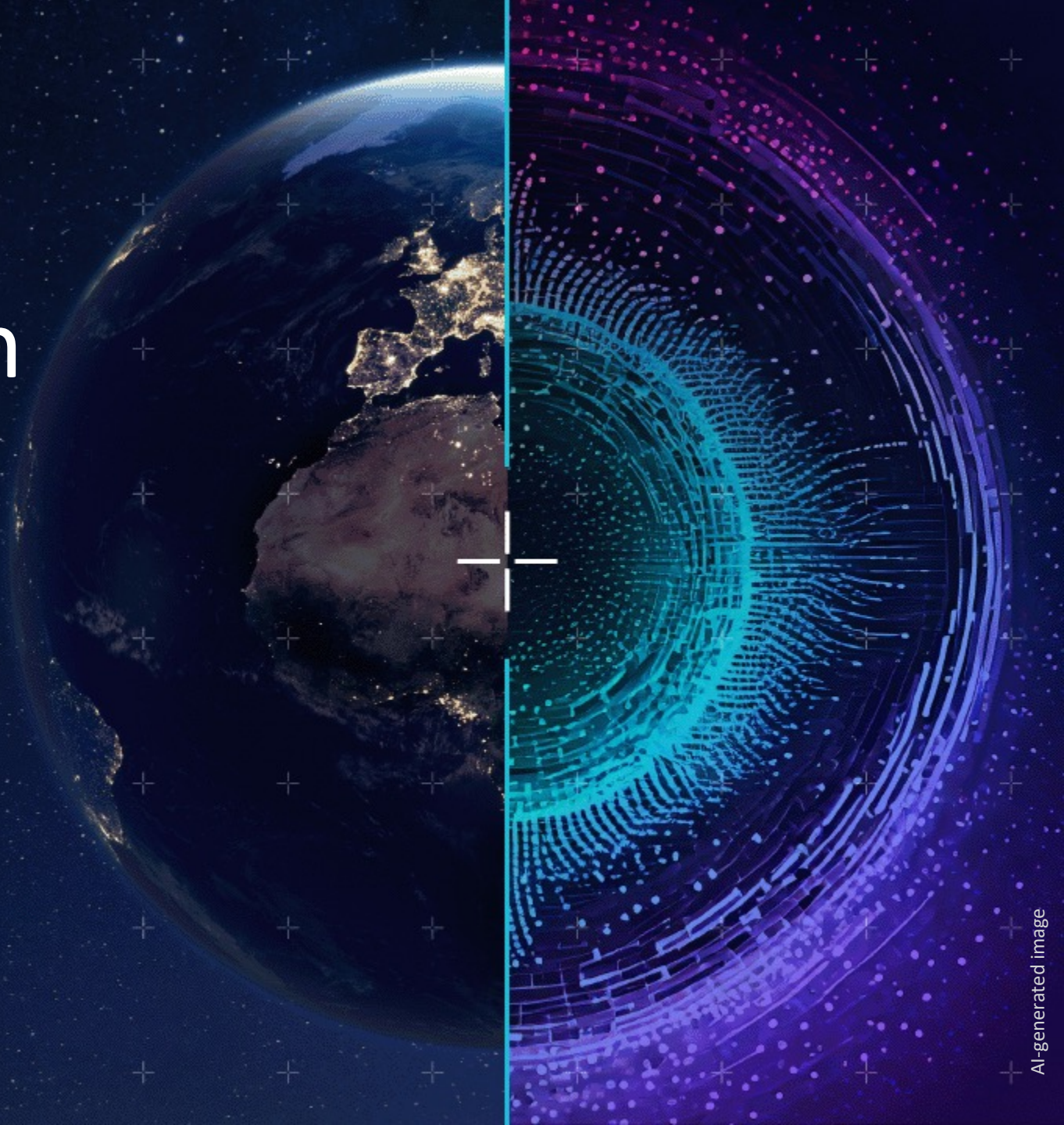
arm

# Device Assignment in Arm CCA



Derek D. Miller

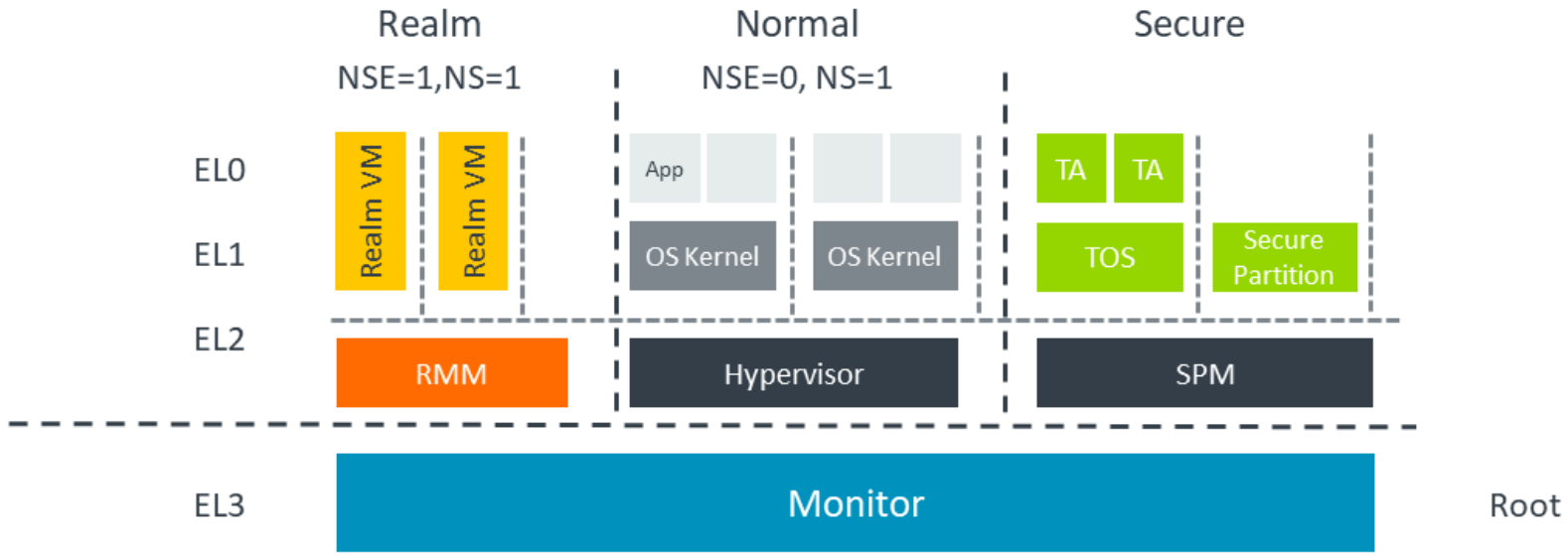
4 September 2024



AI-generated image

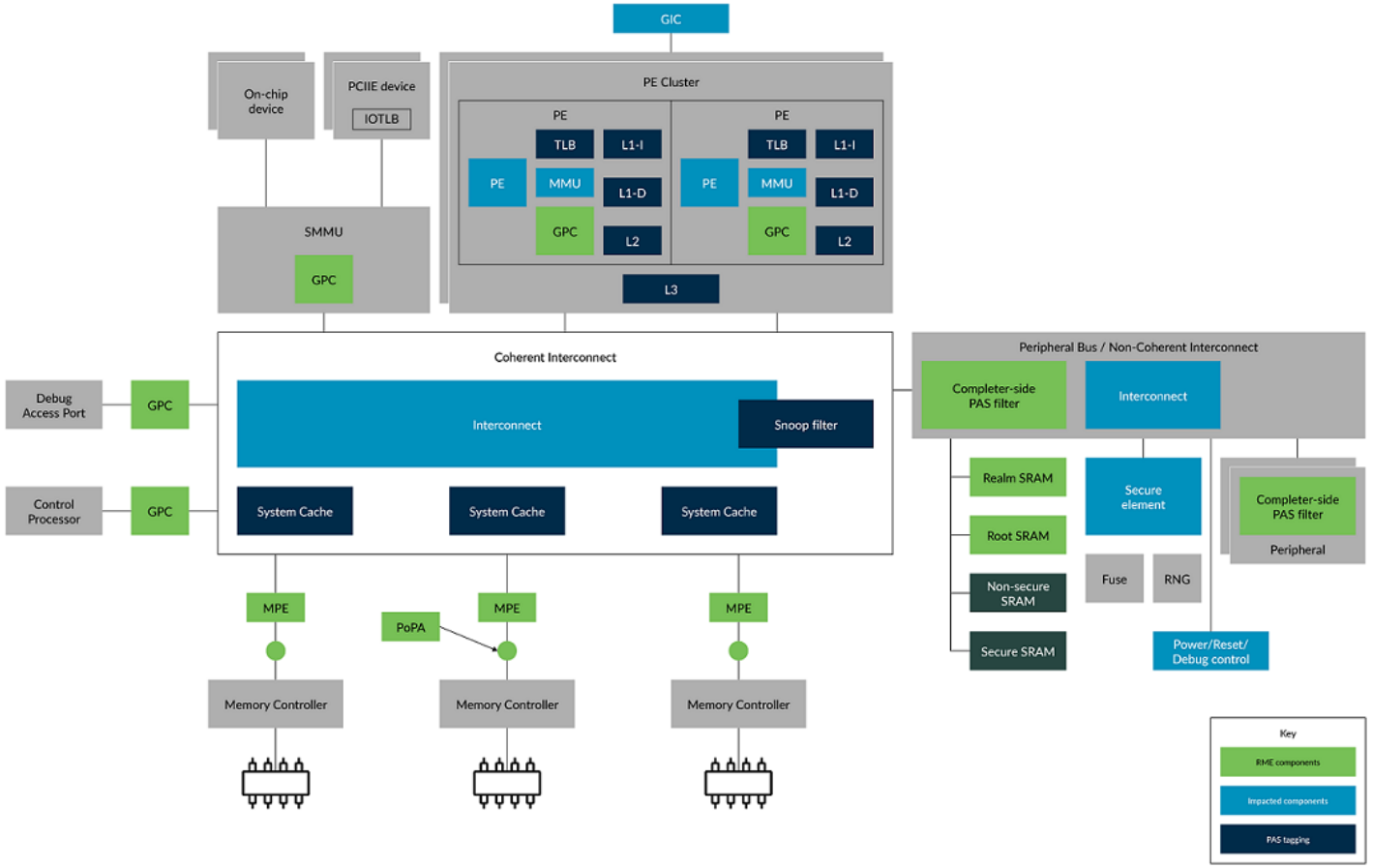
# Introduction to Arm CCA

- Arm Confidential Compute Architecture (CCA) is designed to protect data and code in use by creating isolated execution environments called Realms.
- **Key Features**:
  - Full software stack Isolation from the host OS and hypervisor
  - Hardware-based security mechanisms
  - Blind hypervisor – Realm can contain a full OS stack
  - Support for attestation

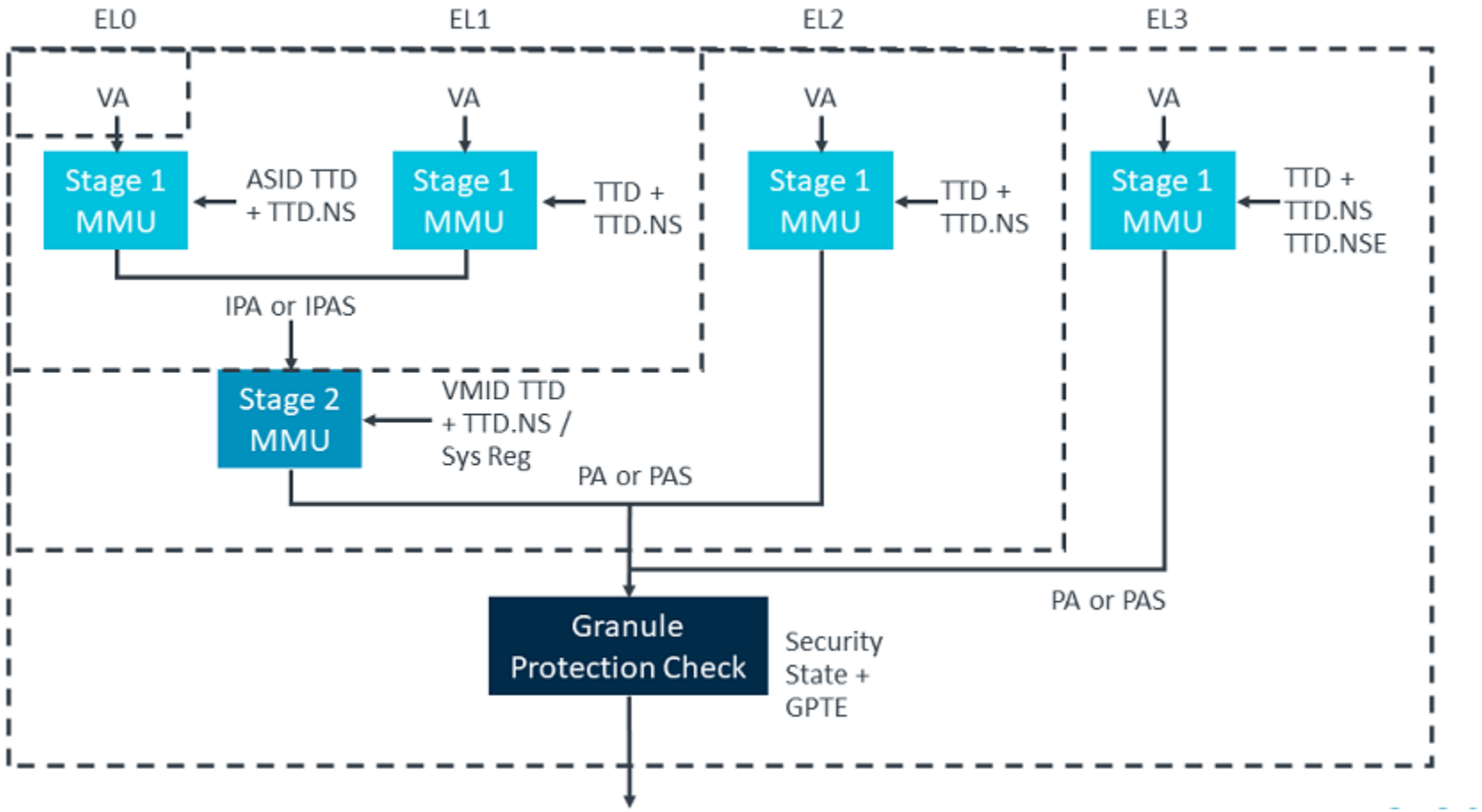


# Architecture Components

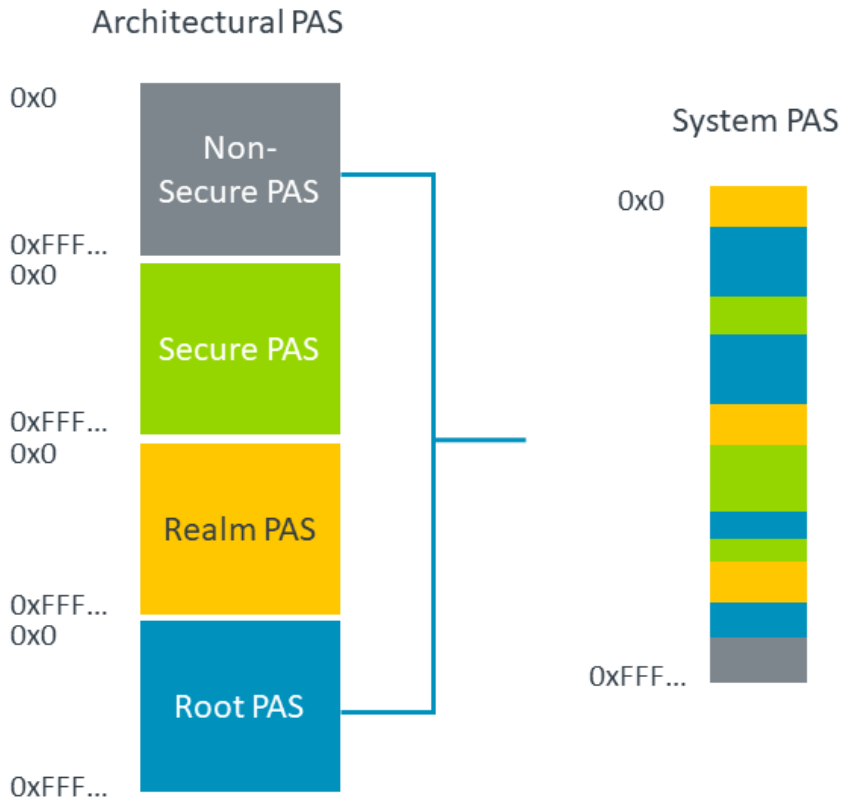
- RME extension in the CPU
  - MMU
    - Add GPC
- SMMU
  - Add GPC
- MPE – Memory Protection Engine
  - Provide encryption and optionally integrity
- Completer-side PAS Filter on simple on-chip, memory mapped peripherals
- Granule Protection Checks (GPC) between peripherals that can independently access memory and the system bus
  - For some of these, this will be provided by the SMMU



# Granule Protection Check



# Granule Protection Check




| Security state | Non-secure PAS | Secure PAS | Realm PAS | Root PAS |
|---|---|---|---|---|
| Non-secure | Yes | No | No | No |
| Secure | Yes | Yes | No | No |
| Realm | Yes | No | Yes | No |
| Root | Yes | Yes | Yes | Yes |

# What is Device Assignment?

- **Definition**: Device assignment allows hardware devices to be securely mapped to Realms, ensuring that only authorized Realms can access assigned devices.
- **Importance**: Allow CCA realms' Roots of Trust (RoT) to be extended to devices outside of the CPU
  - Enabling them to use GPUs, ML Accelerators, cryptographic accelerators, even DPUs
- Three broad categories of devices
  - On-SoC peripherals that are not DMA-capable
    - These do not need device assignment – RMM/VMM managed page tables are sufficient
  - On-SoC peripherals that are DMA-capable (Root Complex Integrated Endpoints – RCiEP)
  - Off-SoC peripherals
- For devices with multiple interfaces, the realm must trust the device to isolate the device context appropriately

# On-SoC peripherals that are not DMA-capable

- Attestation is provided via the platform attestation token
- Trust in the peripheral is presumed by trust in the platform
- But the presence of the device is not explicit
  - It’s implicit in the platform’s memory map

# On-SoC peripherals that are DMA-capable (Root Complex Integrated Endpoints – RCiEP)

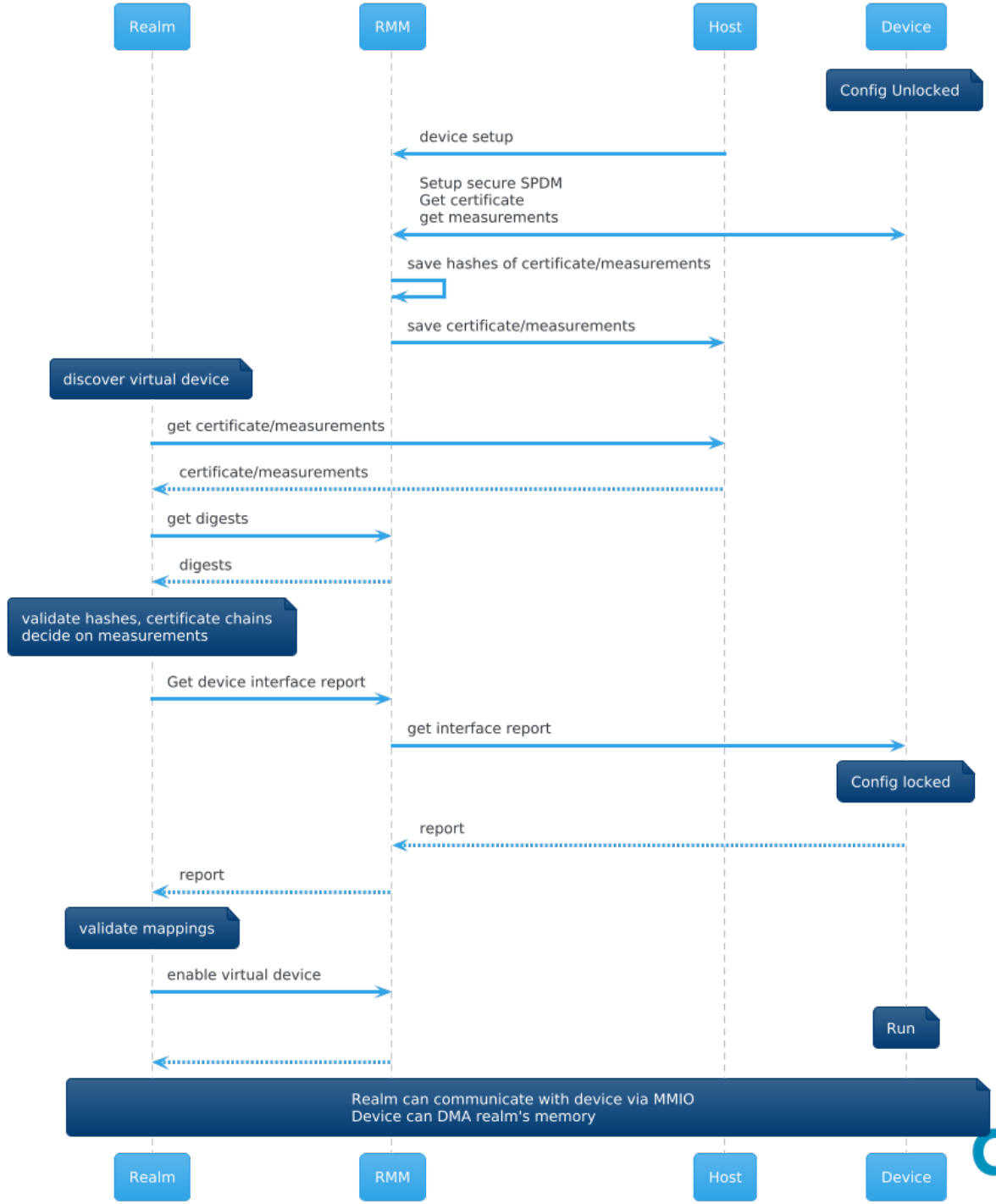
- Attestation is provided via the platform attestation token
  - But additional GET_MEASUREMENTS calls may be supported to establish trust in the device firmware
- Realm must approve it being added to its root of trust
- Each device needs an EL3 driver
  - The specifics of interface report retrieval is device-specific
- Realm can get details on the device through the RSI_RDEV_GET_INFO call
- To ensure that non-secure cannot intercede, the device should be placed behind a Realm Physical Address Space filter (by the SoC vendor)
  - Limit access to Root/Realm security state

# Off-SoC peripherals

- Device Assignment does apply
- physical link must be protected against physical attacks
  - By IDE or similar
- Attestation is provided via TDISP/SPDM
- But the realm must approve it being added
  - After checking the GET_CERTIFICATES and GET_MEASUREMENTS results
- Interface between the RMM and device is generic
  - So the RMM does not need device drivers
  - This was a requirement to keep the RMM as simple as possible

# Software Flow

- SPDM/IDE session is setup by the RMM before the device is trusted
  - Necessary to ensure integrity of certificate and measurements
- Storage of certificate and measurements is done by the host
  - To avoid allocations in the RMM
  - RMM maintains hashes of them
- Realm enters the picture relatively late



# Attestation challenges

- Unification of Attestation “ground truth of trust”
  - It is desirable to have one entity responsible for determining acceptability of a TCB
  - Often, this is an external service (such as Veraison) – but essentially, attestation is establishing the suitability of an environment to a relying party
  - However, RME-DA requires the Realm software to determine if it trusts the device
    - It can do this autonomously (without going to an external service)
      - But this separates the “ground truth of trust” between the service and the Realm software – management of this can be error prone (or, more likely, not done)
    - It can do this by going to the external service
      - But this adds another round trip to the external service – or the relying party
  - More work needs to be done here
- Inclusion of on-SOC devices in the address map means they ”appear” on the platform attestation token
  - But this is not as explicit as I’d like

arm

Thank You
Danke
Gracias
Grazie
谢谢
ありがとう
Asante
Merci
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה
ధన్యవాదములు