Attestation in Arm's Reference Firmware

Establishing Trust and What's Next

Agenda

- Intro
- PSA Attestation
- Arm CCA Attestation
- PoC: DICE Protection Environment (DPE)
- Planned: enhance TPM support
- Planned: adding SPDM support

PSA: Platform Security Architecture

CCA: Confidential Compute Architecture

DICE: Device Identifier Composition Engine

TPM: Trusted Platform Module

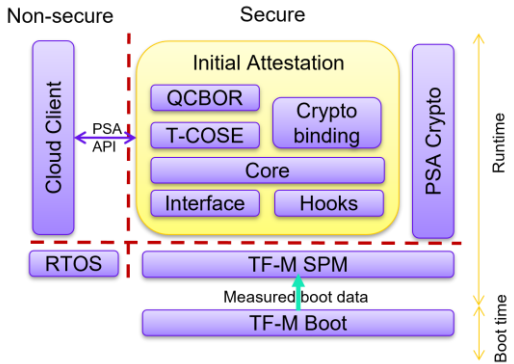
SPDM: Security Protocol and Data Model

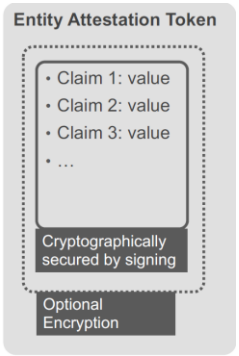
Overview

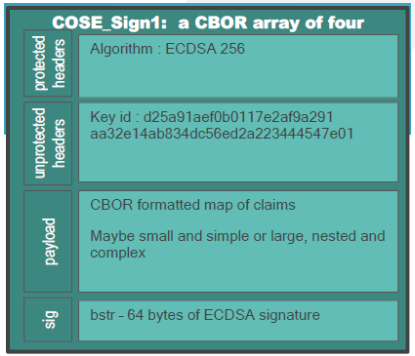
- Trusted/Secure Boot
  - Bootloader verifies signatures of code or config at boot time, on-device
  - Halts boot on failure, but recovery is possible
- Measured Boot
  - Bootloader hashes code, config, or HW state and stores it securely
  - No validation; just measurement
  - Functionality is shared between bootloader and storage backend
  - Examples storage backend: RSE Measured Boot, TPM PCR, DPE backend
- Attestation
  - Runtime-signed report of measured system state
  - Verified off-device; errors may restrict service
  - Examples: PSA/CCA (by RSE/RMM), TPM2_Quote + Event Log (by TPM), SPDM or DPE (by an Internal RoT)

PSA Attestation

- Designed by Arm to be a lightweight attestation solution primarily targating the IoT market but applicable for high end SoC as well.
- Simple API to retrive attestation token and size info. Supports replay protection.
- Implementation defined hooks to get boot measurements and platform data when generating the report.
- The token has CBOR/COSE encoding; It consists of claims, which are key-value pairs.
- The RoT generates and signs the report by the Initial Attestation Key (ECDSA or HMAC)
- Trusted Services project exposes the API to the Linux user space: link
- Resources: psa-token spec, API, implementation in TF-M

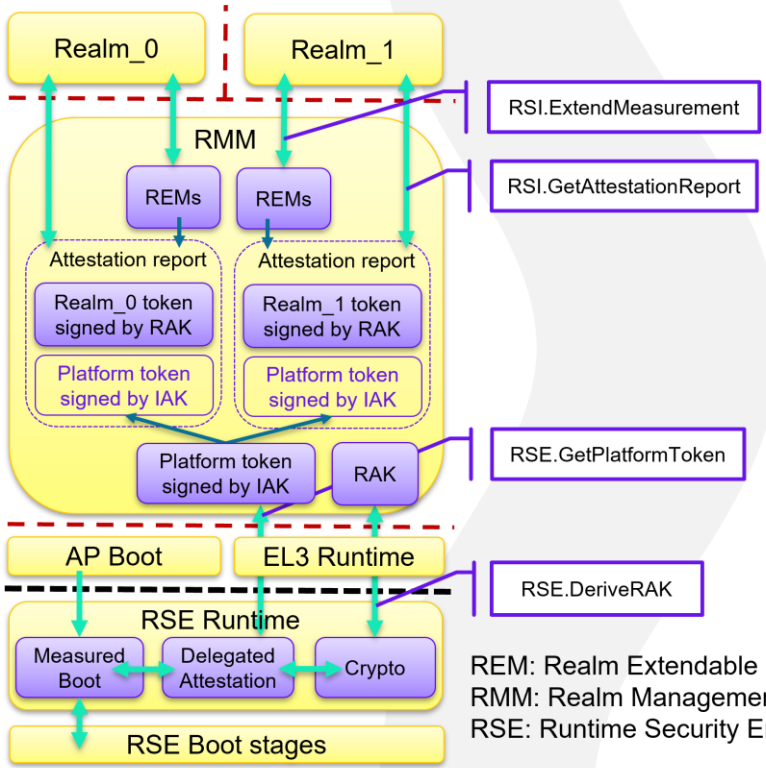






CCA Attestation

- Built on PSA Attestation; tailored for Confidential Compute Architecture
- Attestation report = CCA platform token + Realm token
- RSE Responsibilities
  - Act as RoT: secure boot + stores measurements
  - Provides measured boot backend
  - Derives Realm Attestation Key (RAK)
  - Sign CCA Platform token with Initial Attestation Key (IAK)
- RMM Responsibilities
  - Interfaces with Realm Runtime to record REMs
  - Stores runtime + initial content measurement
  - Signs Realm Token with RAK
  - Binds tokens via H(RAKpub)
- Resources: cca-token spec, RMM spec for ABI
- Planned: Align the PSA and CCA token specs



DPE

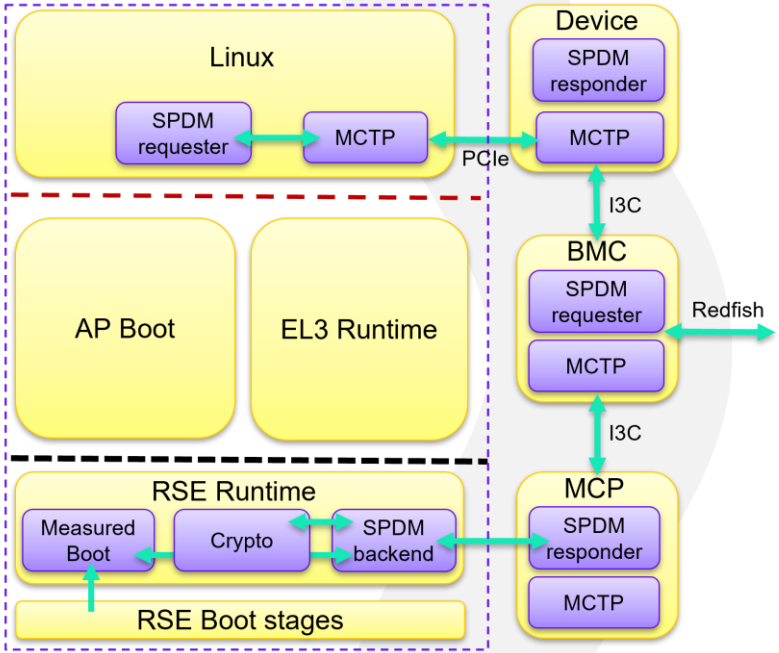
- DICE Protection Environment (DPE) is a TCG specification for an isolated enclave used to store and manage DICE secrets, perform DICE derivations and sign attestation certificates.
- It defines the HW and the SW requirements to make DICE computation in a secure, isolated environment.
- Server-client architecture, where all bootloader components are a client of the entity that executes the DPE service.
- There are many implementation defined details in the spec, which can be specifed by profiles:
  - Andorid profile / Open DICE for client market
  - IRoT profile for server market
- Google has a SW-only implementation of the Open DICE; It is used in Android
- Arm has implemented a Proof of Concept (PoC) of the DPE, based on the Open DICE profile, which is available on the Total Compute platform.
- It is a hybrid implementation which mixes HW-backed and SW-only solutions to produce a single DICE certificate chain.
- Early boot stages are integrated with DPE. NS botloader gets the certificate chain from DPE, which is handed off to Linux and to the pVMs.
- Linaro Connect Madrid 2024: Enabling mobile trust thanks to DICE/DPE in Android

TPM

- Trusted Platform Module by TCG; Broadly used in the PC and server market
- Rich security features: key derivation, key storage, data sealing, X.509 certificate support
- Boot measurements are extended to PCR registers in the TPM and recorded in an Event Log by the SoC
- The attestation report is combination of the Event Log + Signed report which contains the PCRs values
- Discrete TPM (dTPM): an external device connected via SPI/I2C to the SoC
  - Certifiable
  - TF-A bootloaders support it as a measured boot backend: link
- Firmware TPM (fTPM): SW runs in a TEE within the SoC
  - HW dependencies: secure storage, RND generation, etc.
  - Trusted Services integrated ms-tpm to a secure partition: link
- Upcoming activities
  - Add TPM client support to RSE to replay measurements to a dTPM
  - CRB over FF-A support in Linux and edk2

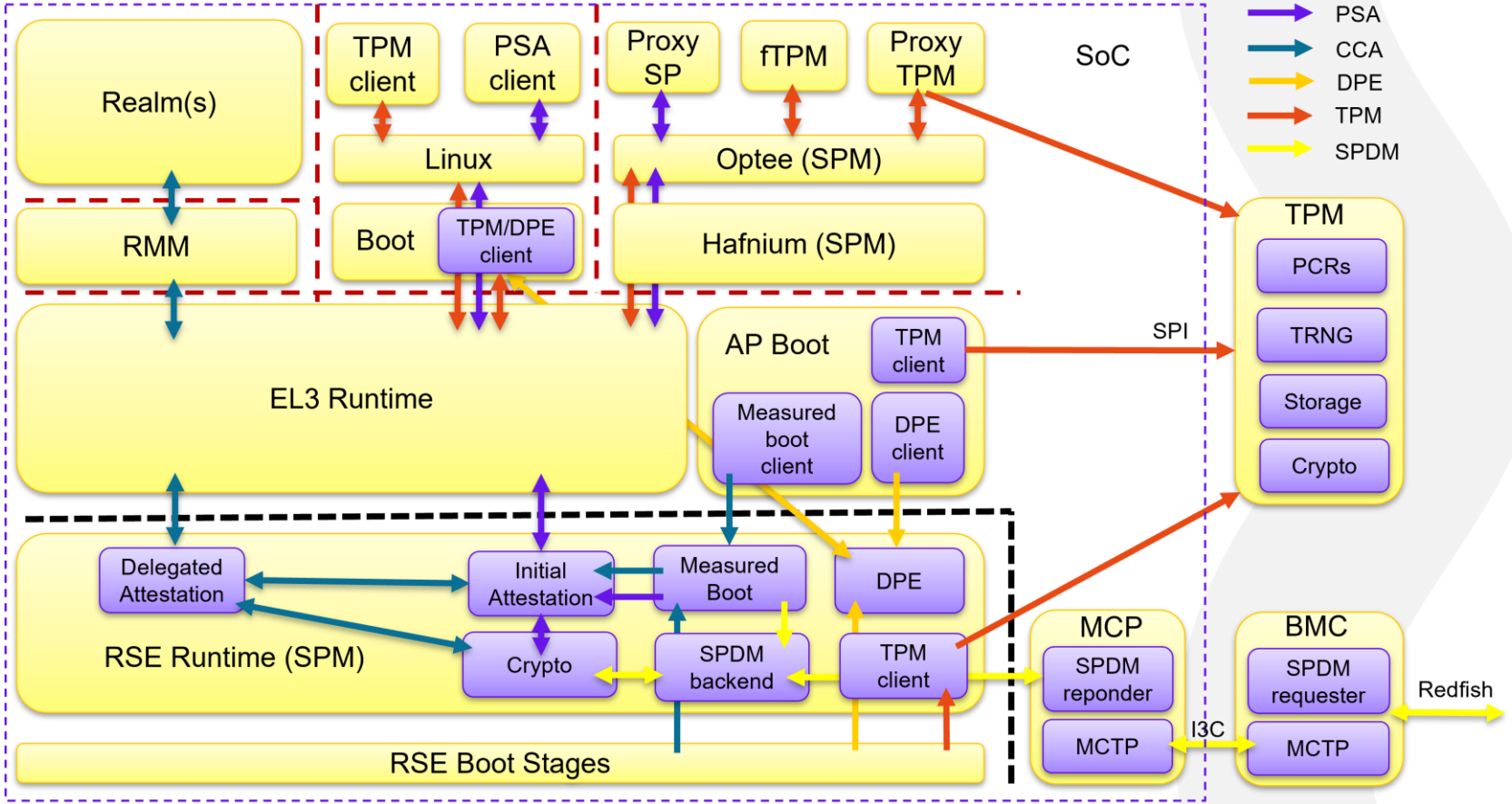
SPDM

- Security Protocol and Data Model by DMTF
- Device authentication, attestation and secure channel establishment
- Used on the server market to attest the SoCs and PCIe devices
- Data path:
  - In-band over PCIe between SoC and device
  - Out-of-band over I3C via MCP and BMC
- Request – Response based protocol
- Use X.509 certificates for authentication
- Attested endpoint has an internal RoT, which signs the messages and provide certificates
- Upcoming activities:
  - Investigation to add support



BMC: Baseboard Management Controler
MCP: Managebility Control Processor
MCTP: Management Component Transport Protocol

Attestation architecture



Thank You!