Linaro Connect

MADRID 2024 | MAY 14-17 2024

Deploying and managing Confidential Virtual Machines on Arm platforms

Leonardo Garcia
Thomas Fossati
Mathieu Poirier
Kevin Zhao

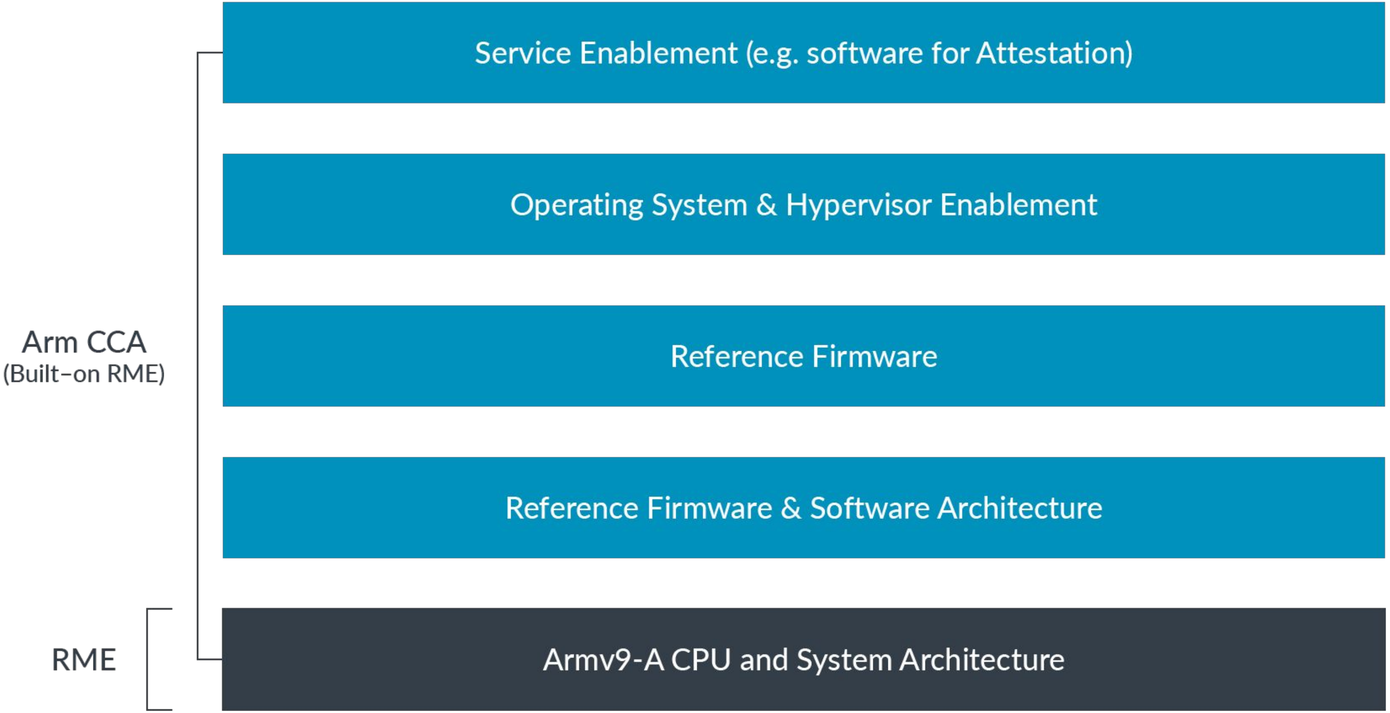
Confidential Computing

data at rest

data in transit

data in use

Confidential Computing stack on Arm



Service Enablement (e.g. software for Attestation)

Operating System & Hypervisor Enablement

Reference Firmware

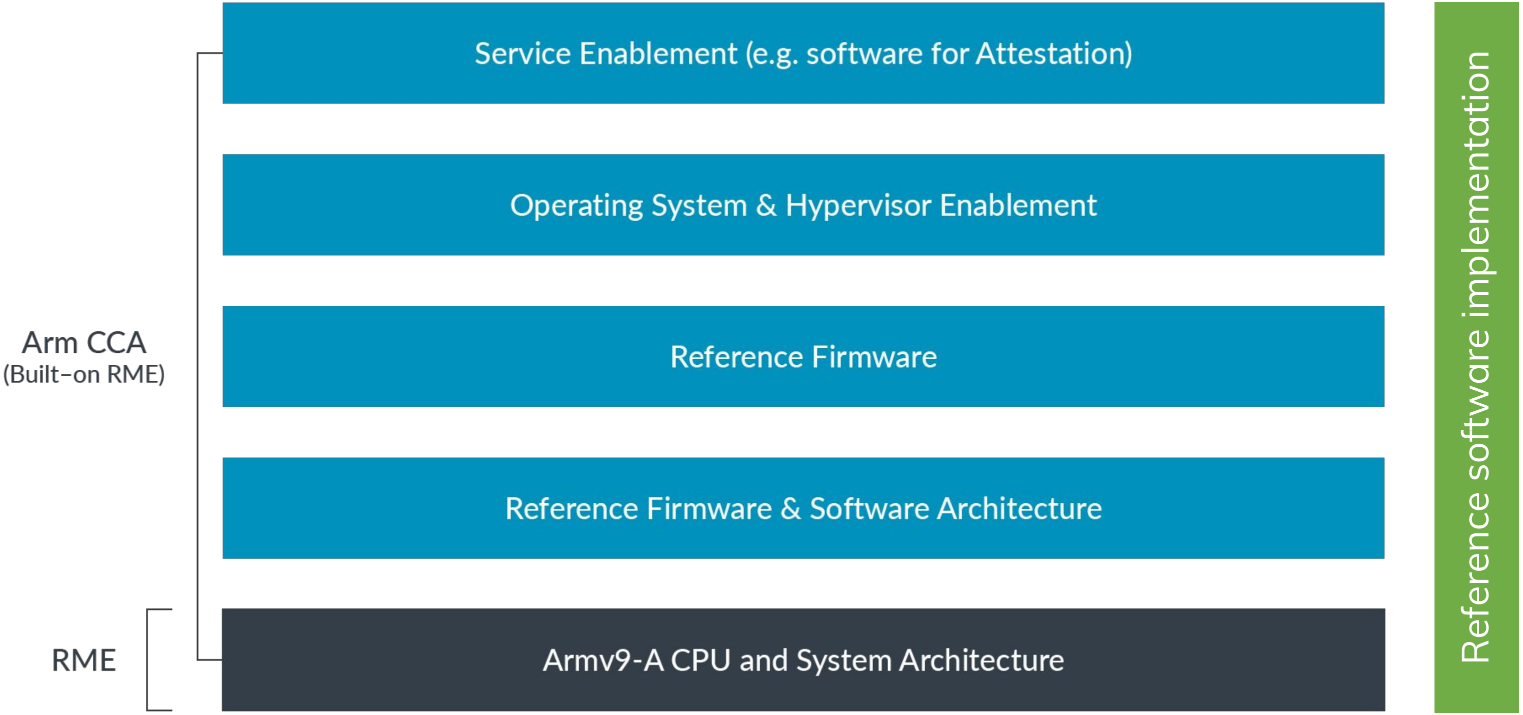
Reference Firmware & Software Architecture

Armv9-A CPU and System Architecture

Arm CCA
(Built-on RME)

RME

Confidential Computing stack on Arm



Service Enablement (e.g. software for Attestation)

Operating System & Hypervisor Enablement

Reference Firmware

Reference Firmware & Software Architecture

Armv9-A CPU and System Architecture

Arm CCA
(Built-on RME)

RME

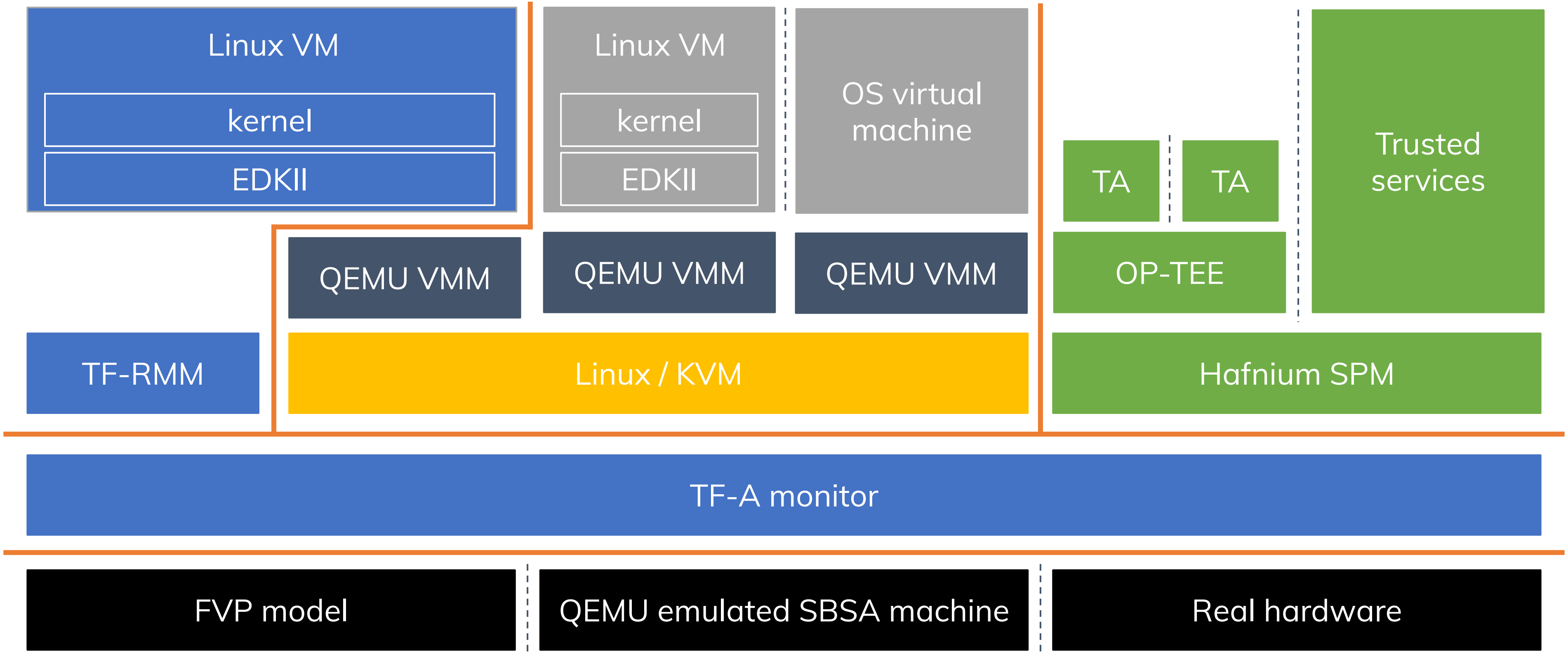
Reference software implementation

Project objectives

Provide a comprehensive set of software and emulated hardware that supports Confidential Computing on Arm:

- QEMU support for Arm’s Realm Management Extension (RME).
- Provide a low level stack (TF-A, TF-RMM, EDK2) that conforms to the Arm's Confidential Compute Architecture (CCA) specification.
- Provide user space components that can start and support a Realm Virtual Machine.
- Provide a user space environment capable of attesting the platform.

Low level reference software stack



CCA low level software reference stack

Arm developed a CCA stack that runs on their FVP model.

With the release of QEMU 8.1, Linaro ported that stack to QEMU:

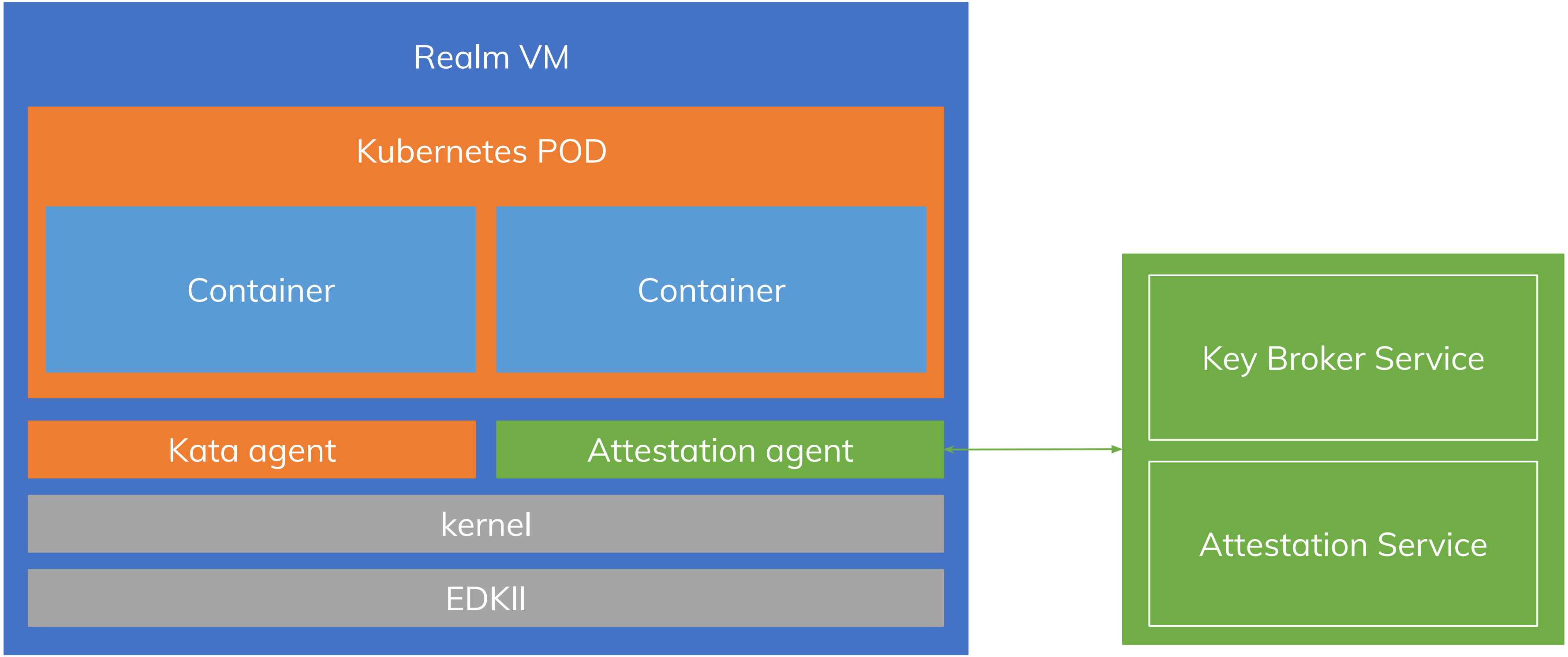
- Patches for TF-A, TF-RMM and EDK2 are available on CodeLinaro (cca/v2 branch).
- Patches for the Linux kernel and kvmtool are hosted by Arm (cca/v2 branch).
- The solution is currently for the QEMU virt machine type with buildroot.
  - QEMU as a system emulator with RME support and as a VMM launching Realms.

Work to support QEMU SBSA reference machine type is ongoing.

Support for RME in Linaro's Trusted Reference Stack (TRS) is ongoing. Plans for a CI.

Documentation is available to compile and run the stack, from base system to Realm.

High level reference software stack



CCA high level software reference stack

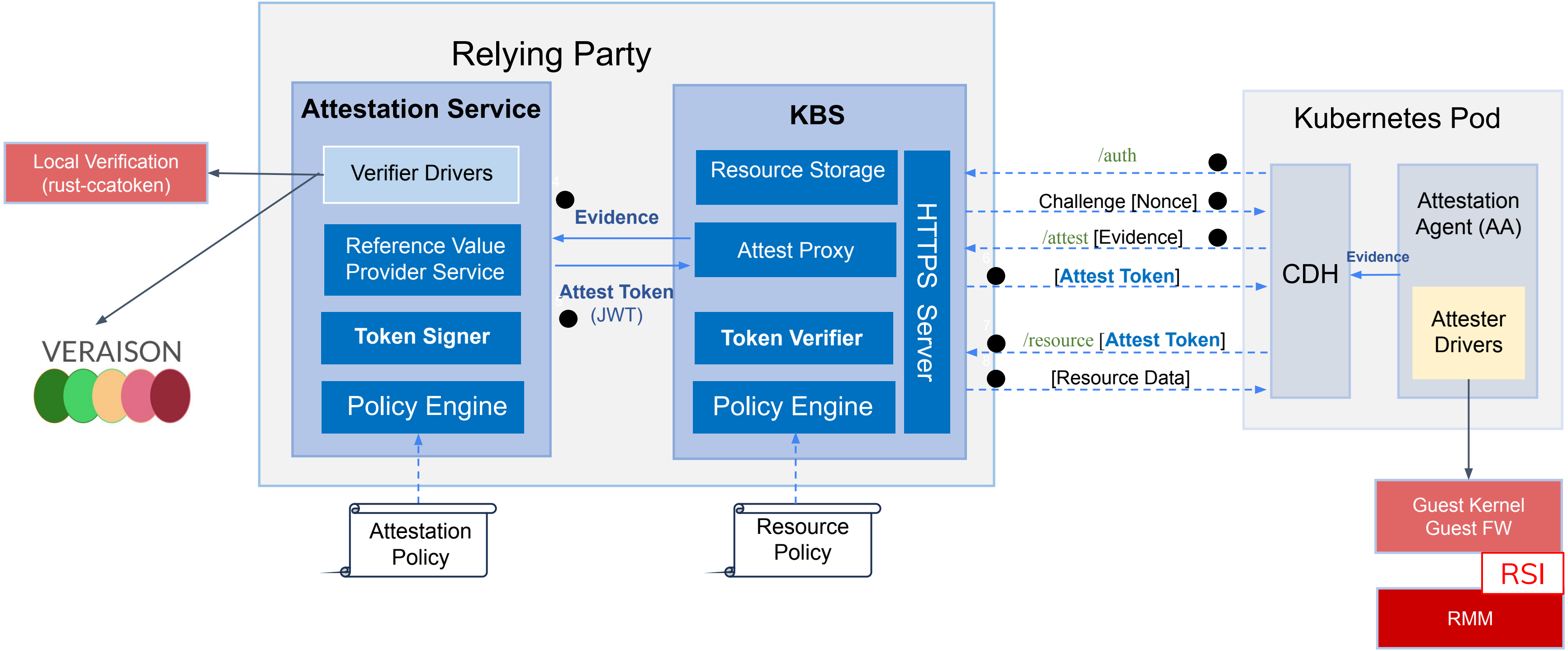
Kata container support: code repo.

- Current features:
  - Only supports Kata v2.
  - Only supports QEMU back end.
  - Only supports direct kernel boot with Kata. The UEFI boot disk image has been validated.
  - Only supports ACPI=off in QEMU.

Confidential Containers (CoCo):

- Framework adoption
  - Kubernetes Confidential Computing operator
  - Container image service (service offload, encryption verification).
- Trustee support: code repo.

CoCo and Veraison - Remote Attestation



Attestation tools

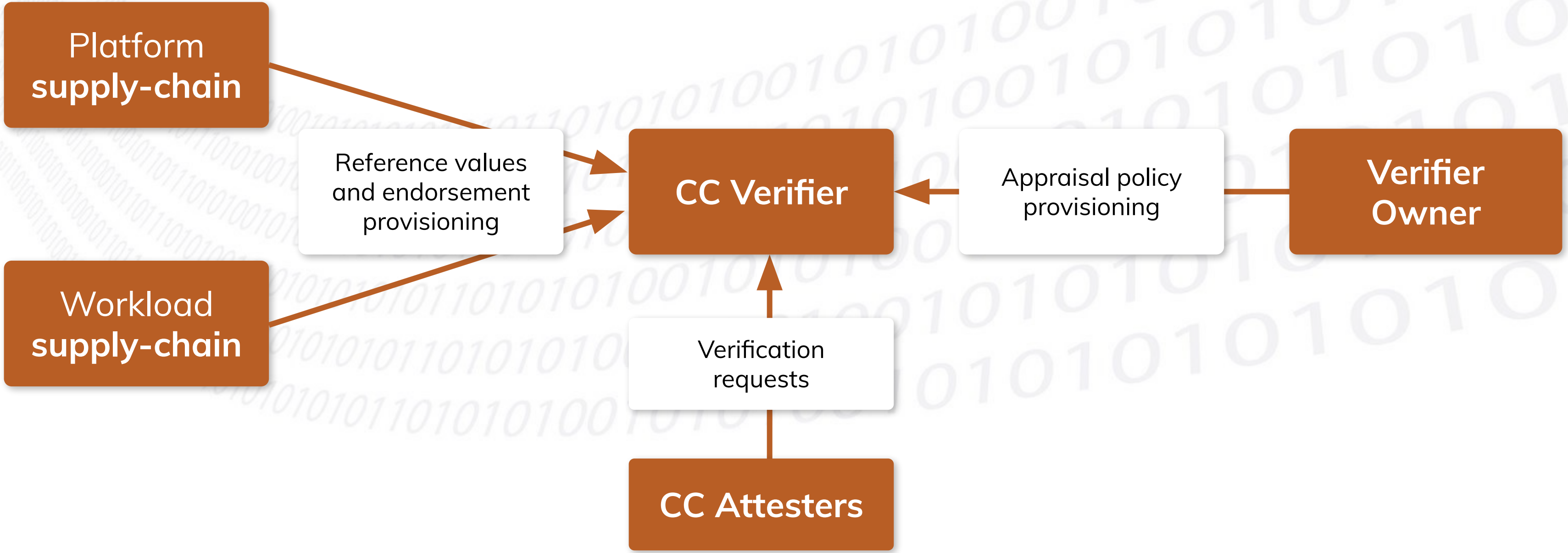
ccatoken crate

- Provides command line tools and APIs to decode and verify CCA attestation tokens.
- Published at https://crates.io/crates/ccatoken.
- Sources at https://github.com/veraison/rust-ccatoken.

realm-token crate

- Tool that calculates the Realm initial and extended measurements, needed for CCA attestation.
  - Sources at https://git.codelinaro.org/linaro/dcap/realm-token.

Remote attestation verification



Platform **supply-chain**

Workload **supply-chain**

Reference values and endorsement provisioning

CC Verifier

Appraisal policy provisioning

Verifier Owner

Verification requests

CC Attesters

Future steps

QEMU support for memory encryption.

QEMU support for SMMU. This is a requirement for device assignment.

Cloud Hypervisor support.

Lightweight firmware support for Arm CCA.

End-to-end demo for CoCo on Arm CCA with Qemu backend.

Integration of Veraison and CoCo Attestation Service (AS) to provide a holistic end to end reference solution for confidential containers on Arm platforms.

Linaro Connect
MADRID 2024 | MAY 12-17 2024

Thank you