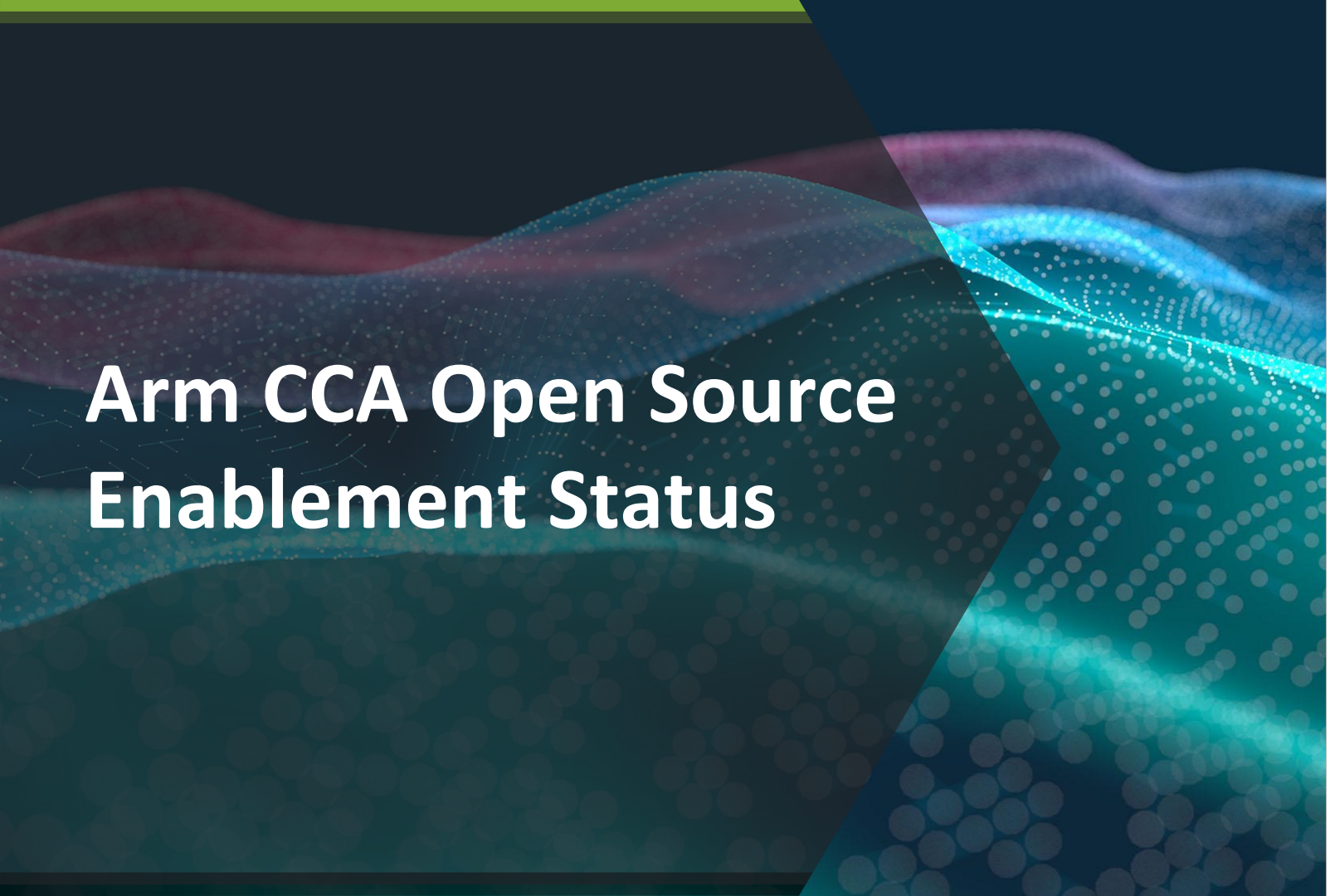
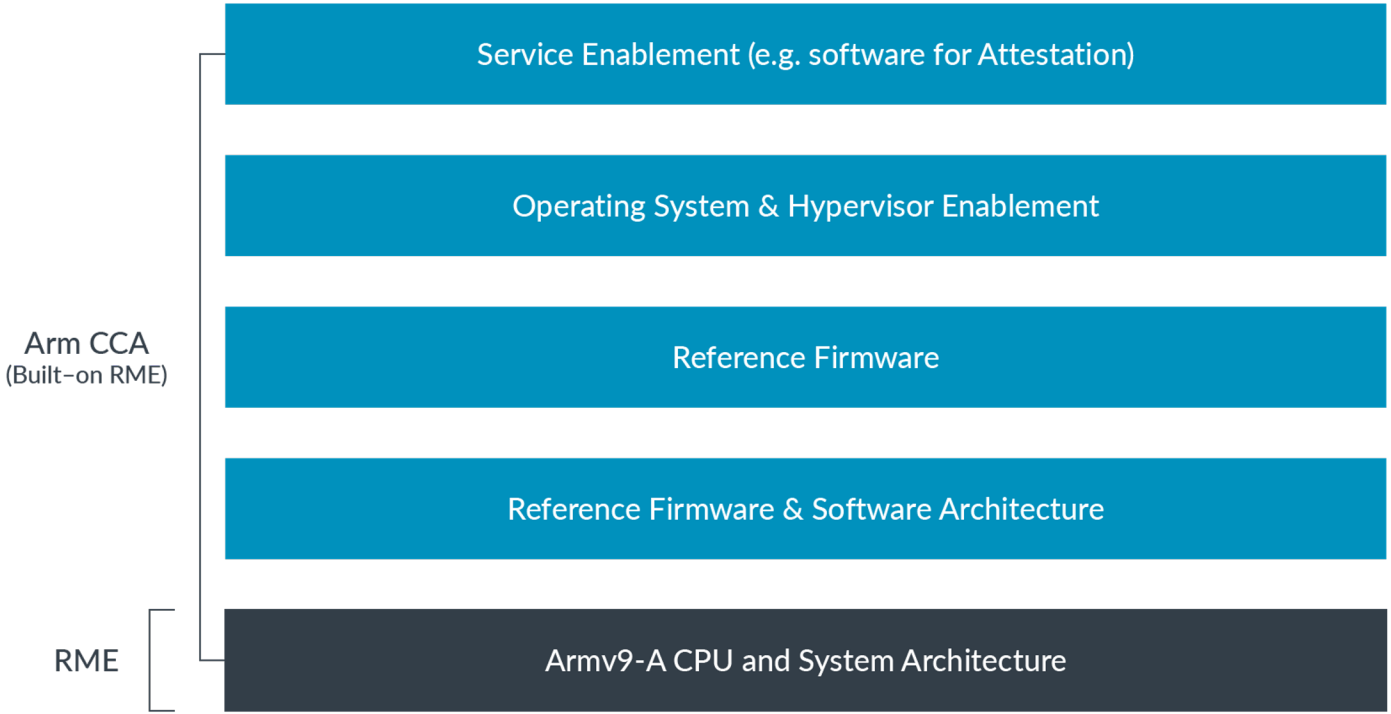
Arm CCA Open Source Enablement Status



Arm Confidential Compute Architecture SW Stack



Linaro

GPT: TF-A运行在Root状态，作为EL3的firmware。
CCA 在一个名为Realm新隔离 环境中进行计算. RMM运行在异常级别 EL2 也使用现有的虚拟机管理技术，如阶段-2转换表来隔离realm.

RME是CCA的硬件组件，扩展了TrustZone 中引入的隔离模型. 与 TrustZone相比，RME将CCA引入了两个新的状态，Root和Realm。监控器运行在Root. 根世界防止从任何其他世界访问EL3内存.

当进行地址转换时，MMU会根据转换表（包括页表和Granule Protection Tables）将虚拟地址映射到物理地址。MMU会通过Granule Protection Check来验证所请求的内存页面是否可以被访问。它会检查相应的Granule Protection Table项，以确定当前安全状态下是否允许对该页面进行读取、写入或执行操作。RME阻止非法访问，并返回一个访问 故障（granule protection fault，GPF）. CCA 维护一个granule protection table，GPT，作为内存中的结构，它规定了每个细粒度的物理内存（例如 4KB）所属的安全世界,支持通过更新GPT动态地将一块物理内存转换为一个新的安全地址空间secure, normal, realm

RMI
RMM和normal world的接口。RMI可以让hypervisor在normal world通过接口给RMM来create/destroy RMM.
RSI 是realm vm和RMM的接口。提供service管理分配给realm的资源以及请求attestation report。

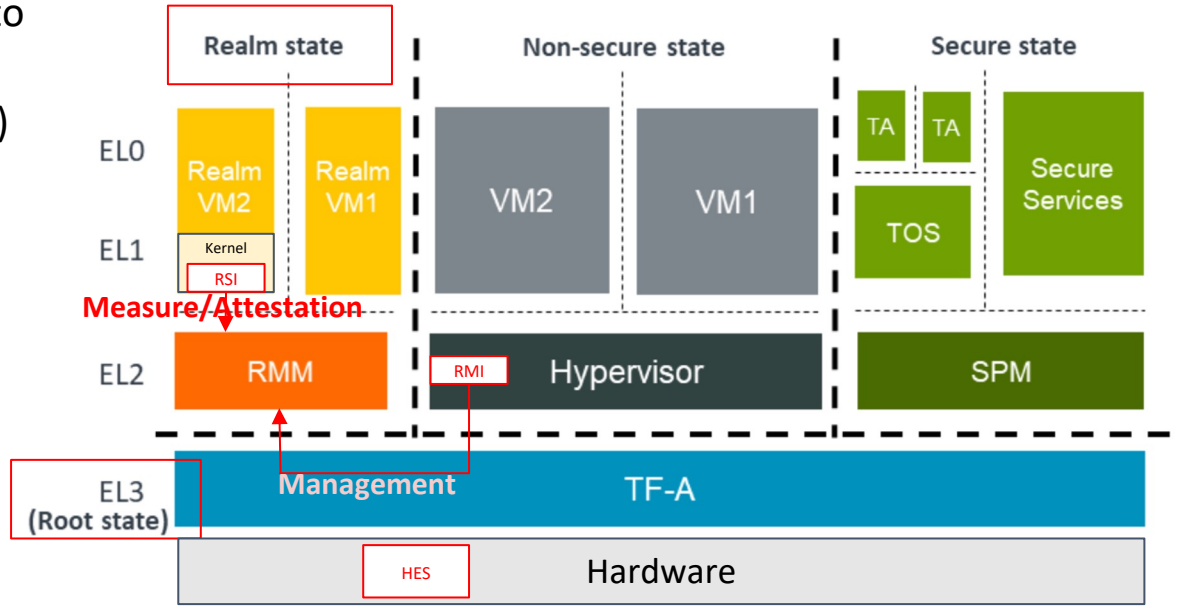
Arm CCA Stack

Realm VM

- Guest Kernel enlightenment to support RSI
- In-realm FW (Guest firmware) enlightenment to support RSI
- Sharing memory with host
- Measurement & attestation

Host

- Host Kernel/KVM support for RMI
- No impact to host FW



Linaro

TF-A 2.9

2023 Q2:

Spec 1.1 release.

RMM 完全follow Spec 1.0，开始Spec1.1

Current Status

- TF-A 2.9 is released alongside with TF-RMM 0.3.0
  - PMU Support for Realm/SVE Support for Realm
  - Refactor the Stage 1 translation table library lib/xlat API to better fit RMM usage.
  - Upcoming Features:
    - RMM EAC Specification alignment.
- Kernel
  - Both host and guest need extra patches.
  - Status: Re: [RFC] Support for Arm CCA VMs on Linux - Suzuki K Poulose
  - https://gitlab.arm.com/linux-arm/linux-cca cca-full/rmm-v1.0-eac2
- EDK2
  - Out-of-box for host EDK2
  - WIP for Guest EDK2, Only the ArmVirtQemu firwmare supports booting in a Realm at the moment, not ArmVirtQemuKernel
- Qemu
  - TCG (Tiny Code Generator), interpreter/emulator component allowing QEMU to be used as an abstract platform model → QEMU 8.1
  - VMM (Virtual Machine Manager) support for launching KVM realm guests → patches on-list

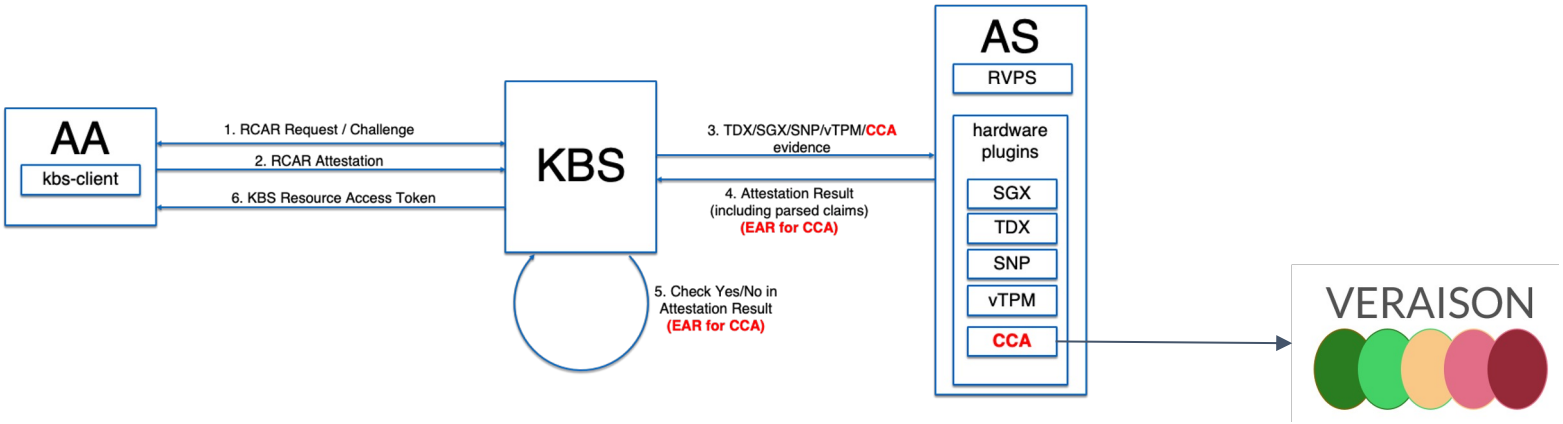
Current Status

- Run the full CCA stack on Arm FVP
  - Reference Arm CCA integration stack Software User Guide
  - AEMFVP Release Note AEMFVP-A-RME-2023.06.30
  - Include all the corresponding components needed to launch the Realm on FVP.
- Run full CCA stack on Qemu(Realm launched by Qemu in a Qemu environment)
  - Linaro has successfully entering into the Qemu Realm guest shell.
  - Currently there are some WIP patches in Qemu/Guest EDK2/TF-A/TF-RMM
  - More info will coming in the next several months.

- Linux
  - Source : https://gitlab.arm.com/linux-arm/linux-cca
  - Tag : cca-full-rfc-v1
- Kvmtool-CCA
  - Source : https://gitlab.arm.com/linux-arm/kvmtool-cca
  - Tag : cca-rfc-v1
- Trusted Firmware-A
  - Source : https://git.trustedfirmware.org/TF-A/trusted-firmware-a.git/
  - Tag/Hash : e87102f32bbdf0fa4b2892394cb4f2766321b9d4
- Hafnium
  - Source : https://git.trustedfirmware.org/hafnium/hafnium.git
  - Tag/Hash : ef0627686b4965274eb646914f244497daa5b86c
- TF-RMM
  - Source : https://git.trustedfirmware.org/TF-RMM/tf-rmm.git
  - Tag/Hash : 2e06f0dc7113c1e4e858f75c5070bdbf290fc63c
- Buildroot
  - Source : https://github.com/buildroot/buildroot.git
  - Tag/Hash : 2020.05
- KVM Unit Test
  - Source : https://gitlab.arm.com/linux-arm/kvm-unit-tests-cca
  - Tag/Hash : cca-rfc-v1
- TF-A Test
  - Source : https://git.trustedfirmware.org/TF-A/tf-a-tests.git
  - Tag/Hash : 47b2cb2f314a4d1e0d43c90f65edb66a4b4f9475

Confidential Container(CoCo) CCA Support

- When Confidential Container Meets CCA



- Existing Implementation:
  - CCA Verifier in AS leverages Veraison for attestation token verification and appraisal)
  - Other TEE like TDX/SGX operates the token verification/appraisal locally
- Proposed new implementation: CCA native verifier

Arm CCA Attestation Primitives Library

Rust-ccatoken project: https://github.com/veraison/rust-ccatoken

- Decode a CBOR-encoded CCA token
- Verify the CCA token (Platform, Realm and their binding)
- Appraise CCA evidence using user-supplied reference values and endorsements
- The basic Library of the attestation primitives for Arm confidential computing architecture.

Thanks

Linaro