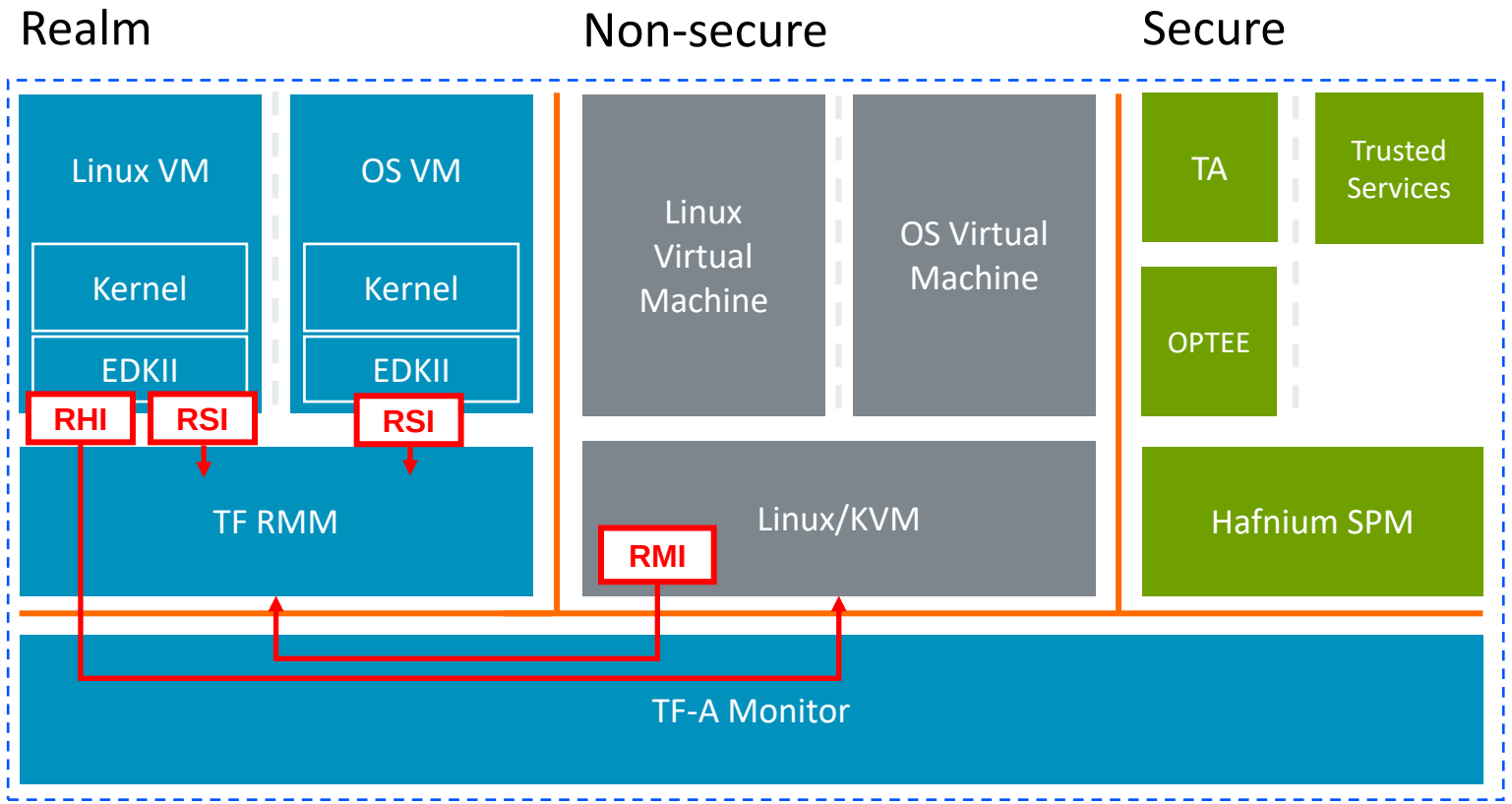
arm

Arm CCA TrustedFirmware.org TSC update

Dan Handley
March 2025

Arm CCA reference open source components



RSI: Realm Service Interface

RMI: Realm Management Interface

RHI: Realm Host Interface

RSI & RMI defined in Arm RMM spec (DEN0137)

RHI defined in Arm RHI spec (DEN0148)

RSE (Runtime Security Engine)

arm

Arm CCA 1.0 (stack for RMM spec 1.0)

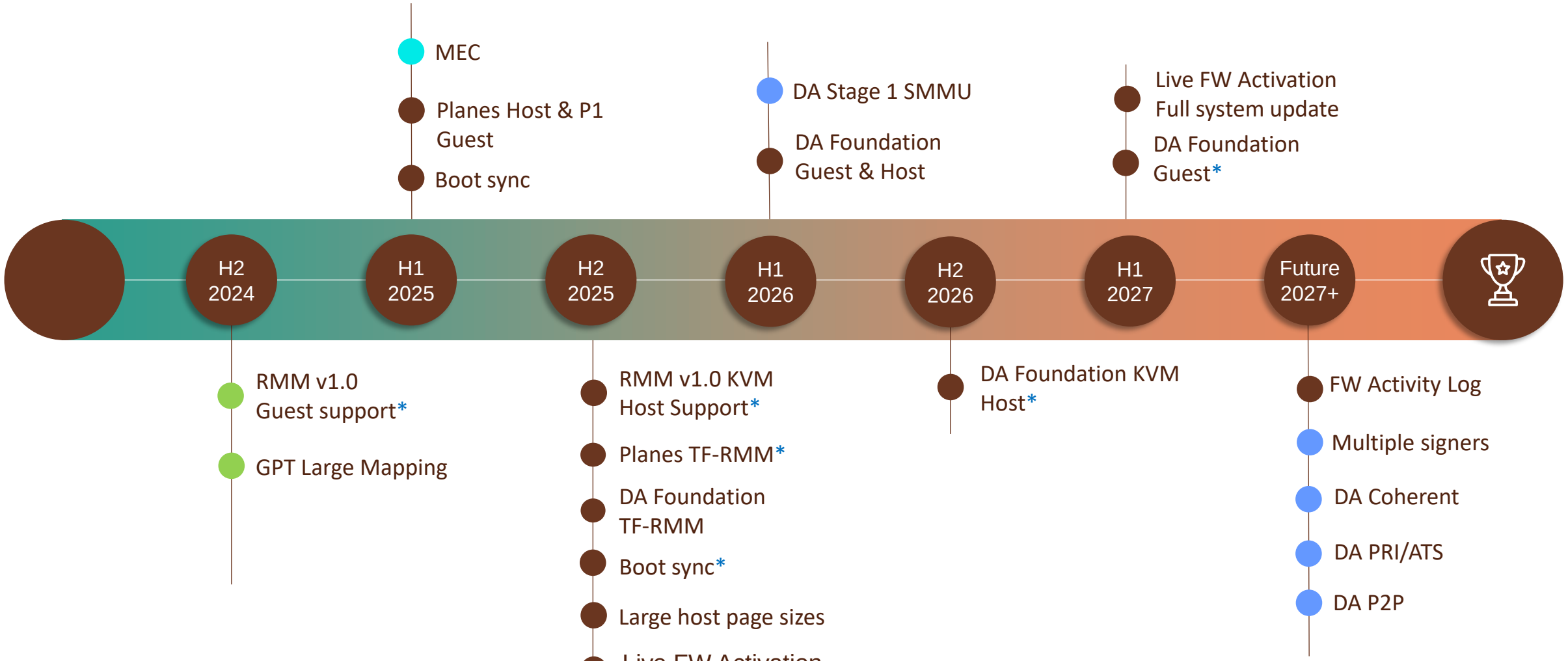
- Enables protection of CPU state and memory contents owned by a realm
  - Minimum Viable Product
- Final RMM 1.0 spec (REL0) released in Sept 2024
- TF-A / TF-RMM (tag rmm-spec-v1.0-rel0) support upstream since Oct 2024
- v7 Guest Linux patches merged to v6.13 in Jan 2025
  - Latest v7 Host KVM patches on list since Feb 2025
  - Combined Guest/Host branch available here and kvmtool patches here
- Latest v3 EDK2 realm guest firmware patches for 1.0-REL0 available since Nov 2024
- CCA 1.0 stack subject to changes to standardize DMA addressing of shared memory

Arm CCA 1.1 key features – needed for initial deployments

- Memory Encryption Contexts (MEC)
  - Physical memory contents of each realm protected using a unique key or tweak
  - TF-A, TF-RMM, Host KVM, kvmtool public branches available since Jan 2025
- Planes
  - Multiple privilege levels within a realm, orthogonal to traditional kernel / user-space split, e.g. vTPM use-case
  - TF-RMM WIP branch available; open-source enablement story for host and P_0 (most privileged plane) stack TBD
- Device Assignment (DA)
  - Enable trusted device functions to be admitted into a realm's TCB, and granted DMA
  - TF-RMM and Linux WIP branches available; early integrated branch coming in Apr
- Live Firmware Activation (LFA)
  - Update firmware image(s) while workloads continue to run, with minimal loss of availability, or…
  - … provision firmware (for example, in R-EL2) during boot with an image supplied by the non-secure host
  - Also relevant for non-RME/CCA deployments. Defined in separate Arm spec, BET published very soon
  - Early patches for LFA of TF-RMM to be made public shortly after (Apr)
- Boot sync (defined in RHI spec)
  - Enables sharing of secrets between realm and realm owner, e.g. for realm secure boot and encrypted disk boot
  - Internal EDK2 realm guest firmware patches on hold until CCA 1.0 patches merged
  - Deployed solutions may look significantly different to reference SW

CCA Software Deliverables ROADMAP

* Estimated upstream delivery, items without * refers to public availability



Roadmap updated: 19 Mar 2025

Depends on partner/external stakeholder collaboration

Completed

arm

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