arm

CoreCollective Confidential Compute Working Group

Dan Handley

2026-05-11

Public © 2025 Arm

Agenda

- Brief CCA reference SW update
- QEMU platform/VMM CCA status update, gap analysis and discussion
- In-realm paravisor enablement status and strategy discussion

Public © 2025 Arm

Arm CCA software status

CCA software 1.0 status

- RMM spec 1.0-REL0 released Sep 2024
  - Enables ”CPU-only” realms
  - Minimum Viable Product (MVP) but missing some features needed by lead partners
- TF-A / TF-RMM (tag rmm-spec-v1.0-rel0) upstream since Oct 2024
- Guest Linux patches merged to v6.13 in Jan 2025
  - Patches to support guest on host with large page support on list since Dec 2025
- Host KVM patches have been regularly pushed to the list for more than a year
  - Last 1.0-based v12 Host KVM patches on list Dec 2025 (addressed maintainer UABI feedback)
- PR to merge EDK2 realm guest firmware patches raised Mar 2026
  - Now split into several smaller PRs to facilitate upstreaming (see top-level PR for status)

Public © 2025 Arm

CCA software 2.0 status

- Baseline support:
  - Initial 2.0 TF-RMM support merged March 2026
  - Early 2.0 v13 Host KVM patches on list March 2026
- Foundation DA:
  - 2.0-BET1 stack
    - TF-RMM branch [TODO] available April 2026
    - v4 Guest Linux, Host KVM, IDE setup (Host), IOMMU-FD UABI for DA (Host) on list April 2026
  - 1.1-ALP17 stack
    - TF-RMM patches merged Dec 2025; use this branch to be sure of a working stack; integrated build/test instructions here
    - v3 Guest Linux, Host KVM, IDE setup (Host), IOMMU-FD UABI for DA (Host) on list March 2026
- Planes:
  - RMM spec 1.1 ALP14 TF-RMM patches merged Sept 2025
  - Matching v1 RFC Host KVM also available
  - Will need to be reworked/rebased on 2.0 base stack
- MEC:
  - TF-A / TF-RMM patches merged Sept 2025
  - Host KVM, kvmtool prototype branches available since Jan 2025
  - Obsoleted by 2.0 spec (VMID/MECID allocation will now be handled within RMM) – TF-RMM will need to be reworked
- LFA:
  - LFA of TF-RMM: TF-A / TF-RMM patches merged incrementally between June 2025 and Jan 2026
    - v2 Linux patches patches available since Mar 2026
  - LFA of BL31: TF-A public branch available since Mar 2026 (see here for usage info)
  - LFA of Secure Partitions (SPs): TF-A patches merged Mar 2026 (see here for usage info)
- Boot sync public branches available since Sept 2025
  - Enabling "encrypted disk boot" and "measured boot" use-cases

Public © 2025 Arm

In-realm Paravisors

Essentially 3 solutions on the table

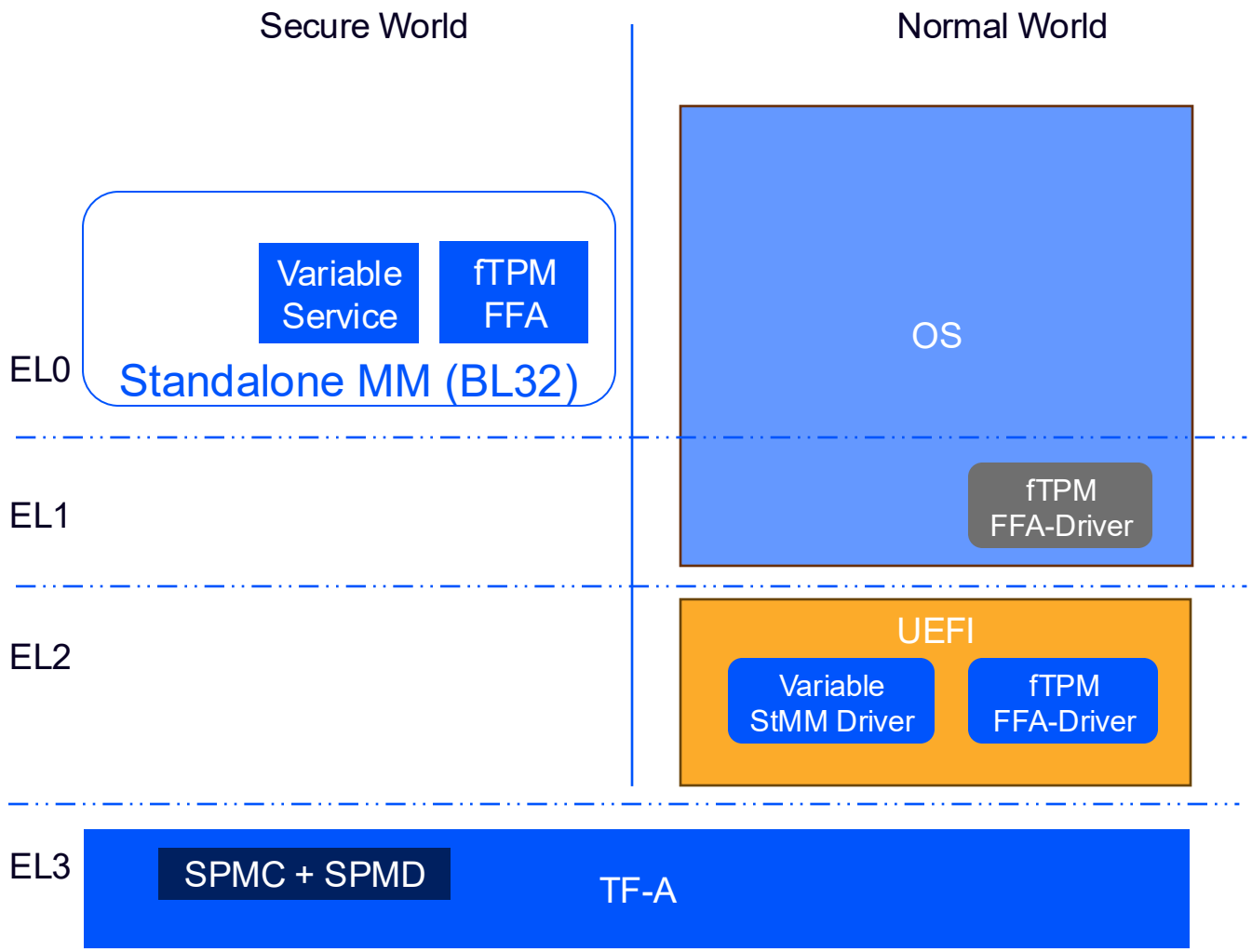
1. OpenHCL
   - Microsoft sponsored open-source project intended for Azure deployments
   - Designed to work with unenlightened Guest OS (Windows and Linux)
   - For production would always use Hyper-V
   - Arm working with Microsoft to enable OpenHCL in a KVM environment
     - For Arm CCA enablement and testing purposes only
2. P0-lite (lightweight paravisor)
   - See next slides
3. Coconut-SVSM
   - Provides rich set of paravisor services to enlightened OS
   - Currently tied to the AMD arch

Public © 2025 Arm

P0-Lite fTPM PoC

Existing host fTPM solution (equivalent to vTPM)

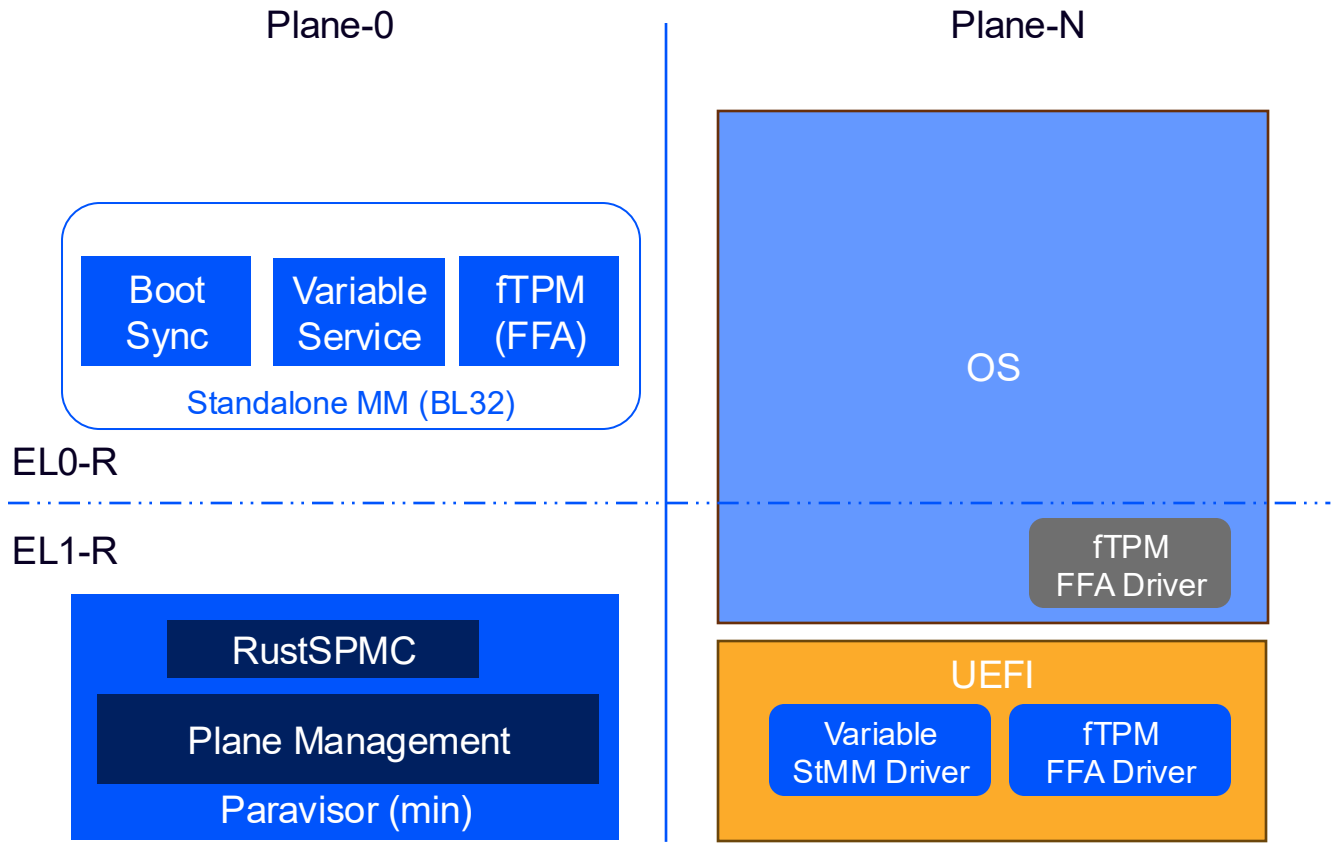
- Standalone MM (StMM) is a UEFI module that runs secure services
- StMM based fTPM over FF-A
  - fTPM - TCG reference TPM stack
    - Patches coming soon
  - ARM DEN0138 - TPM Service Command Response Buffer Interface Over FF-A
- UEFI fTPM driver
  - TPM Device Lib for TPM CRB over FF-A upstreamed
- TPM2 ACPI table
  - CRB over FF-A support upstream
  - Either use Tcg2AcpiFfa module or Dynamic Tables Generator
- TPM Linux kernel driver
  - Recent updates for CRB over FF-A
  - Already upstream



Public © 2025 Arm

Propose P0-Lite – Reuse existing fTPM solution in CCA Planes

- Paravisor
  - Minimal
    - Arch initialisation
    - Memory assignment for planes
    - All interrupts are handled by the OS Plane
  - Rust SPMC
    - Dispatching FF-A calls to StMM
  - Plane Management
    - Partitioning
    - Switching
    - Servicing RSI requests calls from other planes.
- Code reuse
  - Boot Sync
  - Variable Service
  - fTPM – CRB over FF-A
  - Rust SPMC.



Public © 2025 Arm

P0-lite status

- Arm shared Proof of Concept (PoC) at Q1 2026
- Features:
  - Boot flow across planes: P0-lite paravisor, StandaloneMM and Realm Guest UEFI
  - StandaloneMM hosting UEFI variable and vTPM services (currently ephemeral)
  - End-to-end boot of a Realm Guest Linux OS in Plane 1
- Arm will continue developing this PoC through to Q3 2026
- Will then review whether to take the PoC forward based on how well it works and partner feedback

Public © 2025 Arm

arm

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