Confidential Compute Working Group (WG)

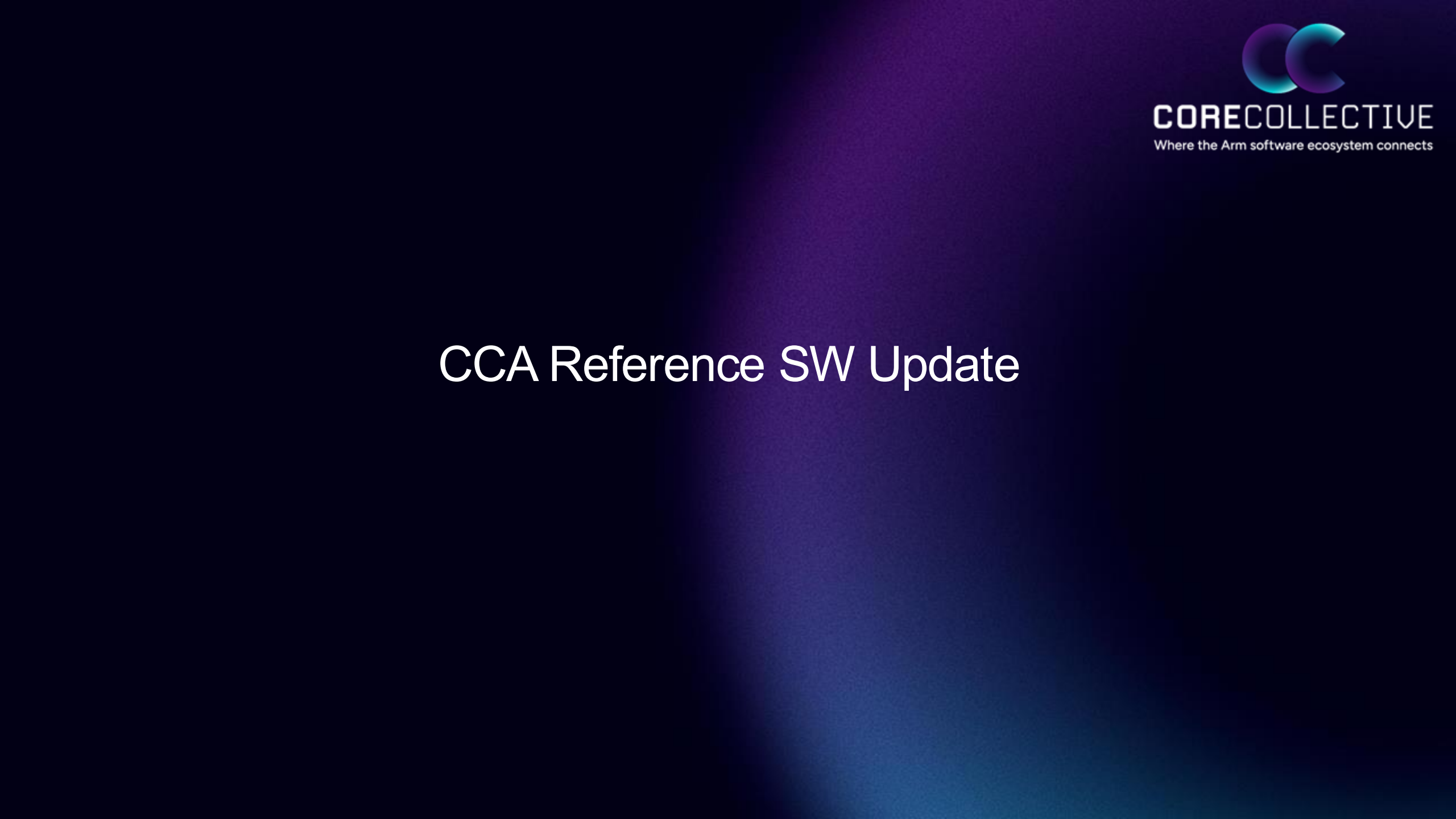


12 Oct 2026

Confidential Compute WG Agenda 12 Oct 2026

CORECOLLECTIVE
Where the Arm software ecosystem connects

- Arm CCA Reference SW Updates
- Early informal feedback from Plumbers?
- AOB


CORECOLLECTIVE
Where the Arm software ecosystem connects
CCA Reference SW Update

CCA software 1.0 status

COREcollective
Where the Arm software ecosystem connects

- 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 6.13 in Jan 2025
  - RFC v8 patches to support guest on host with large page support on list Sept 2026
  - Dependency SMCCC bus patches queued for 7.4
- Last 1.0-based v12 Host KVM patches on list Dec 2025 (addressed maintainer UABI feedback)
- EDK2 realm guest firmware (following PRs are split into smaller PRs to facilitate upstreaming)
  - Base PR raised Mar 2026; 8 of 14 series merged
  - Measured Boot PR raised April 2026, 3 of 4 series merged
  - Boot Sync PR (enabling Secure Boot and Encrypted Disk Boot) raised May 2026

CCA software 2.0 status

CORECOLLECTIVE
Where the Arm software ecosystem connects

- Baseline support:
  - Initial 2.0 TF-RMM support merged March 2026 and released in v0.9 May 2026
    - Dynamic granule tracking patches merged Sept 2026
  - 2.0 v23 Host KVM patches - queued for 7.4
    - Focusses on KVM arm64 enlightenment of different VM types and bare minimal realm VM support, plus
    - v22 Base RMI patches – queued for 7.4
    - v19 Host support for GPFs - queued for 7.4
    - v23 RMI driver and remaining realm enablement – off-list for now
- Foundation DA:
  - 2.0-BET3 based stack
    - TF-RMM patches merged Sept 2026
    - Shrinkwrap config available here
    - DMA layer changes merged in Linux 7.3
  - 1.1-ALP17 stack
    - (Superseded) TF-RMM patches merged Dec 2025; use this branch to be sure of a working stack; integrated build/test instructions here

CCA software 2.0 status [2]

CORECOLLECTIVE
Where the Arm software ecosystem connects

- 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
    - Obsoleted by 2.0 spec (VMID/MECID allocation will now be handled within RMM) – will need to be reworked
  - RFC v1 Host KVM patches (Fujitsu) available since July 2025
    - Based on v15 host baseline
    - Arm has proposed alternative ABI
- LFA:
  - LFA of TF-RMM: TF-A / TF-RMM patches merged incrementally between June 2025 and Jan 2026
    - v4 Linux patches patches available since Sept 2026
  - LFA of BL31: TF-A patches merged June 2026 (see here for usage info)
  - LFA of Secure Partitions (SPs): TF-A patches merged Mar 2026 (see here for usage info)

Kernel Upstream Update

CORECOLLECTIVE
Where the Arm software ecosystem connects

Feature	Notes
Base Host Support (KVM) **(3 Series Split)**	• Complexity/dependencies for this work has grown significantly due to upstream changes is guest private memory and pKVM • Maintainer has agreed to a merge plan to handle the increased complexity by **split into 3 independently mergeable series**. • Bare minimum host enablement is first unit to be **merged in Kernel 7.4**. • Allowing time for review, re-spin and merge of each series sequentially makes ~4 kernel cycles the realistic convergence window.
DA Foundation - Host **(2 Series Split, Community Driven)**	• Full DA is no longer a self-contained Arm kernel series. It depends on **Device Trust, netlink/interface definition, IOMMUFD, DMA-BUF and TDISP integration**, with contributors across **NVIDIA, AMD, Intel and Arm**. • **The delay reflects the slow progress made by the community** before the final host DA can be merged for any architecture. • IDE is deliberately separated as the first independently upstreamable DA building block. It can progress once the initial Host KVM patches are visible, without waiting for the complete Device Assignment architecture.
DA Foundation – Guest **(Community Driven)**	• Arm has Guest DA patches, but they sit above the Device Trust / host DA framework. • Until the framework has an agreed design, maintainer/PR path and upstream implementations, Guest DA cannot realistically converge independently.
MEC - Host	• MEC is **architecturally downstream of the Base KVM Host**. Its upstream work should follow a sufficiently stable host KVM rather than competing with or repeatedly rebasing on the KVM host changes. • Its exact merge timing also remains exposed to maintainer review latency.
Large Page / 64K	• Kernel guest changes are relatively mature; the additional schedule is primarily to align with the **TF-RMM 64K support**, so the upstream kernel change corresponds to a usable end-to-end implementation rather than an isolated patch.
Planes - Host	• Additional complexity that is sequenced behind higher-priority Base Host and DA work.
LFA – Live CCA Firmware Activation	• The kernel interface is self contained, but usable solution also requires firmware hardening, rollback/compatibility and further validation on real platforms. • The date therefore reflects end-to-end readiness rather than kernel code alone.
EDK2 Guest FW	• The +2-cycle is to align Guest FW with the revised Base CCA/guest enablement sequence • Guest firmware is purely reference, CCA deployments may use their specific firmware of choice

CCA Upstream Roadmap Update



Feature	RMM Spec	Previous Roadmap	Delta	Updated Roadmap	
				Kernel	TF-RMM & EL3
Base Host Support (KVM) Upstream Merge Queue	RMM 2.0 BET3	2026 Q4 (Kernel 7.4)	+3 Kernel Cycle	2026 Q4 Series 1 (Kernel 7.4) 2027 Q1 Series 2 (Kernel 7.6) **2027 Q2 Series 3 (Kernel 7.7)**	Upstreamed
DA Foundation (IDE) Host Support Upstream Merge	RMM 2.0 BET3	New Plan	-	**2027 Q1 Series 1 (Kernel 7.6)**	Upstreamed
DA Foundation Full Host Support Upstream Merge	RMM 2.0 BET3	2027 Q1 (Kernel 7.6)	+5 Kernel Cycle	**2028 Q1 Series 2 (Kernel 7.11)**	Upstreamed
DA Foundation Guest Upstream Merge	RMM 2.0 BET3	2026 Q3 (Kernel 7.3)	+8 Kernel Cycle	**2028 Q1 (Kernel 7.11)**	Upstreamed
Large Page Support Upstream Merge Queue	RMM 2.0 BET3	2026 Q3 (Kernel 7.3)	+2 Kernel Cycle	**2027 Q1 (Kernel 7.5)**	2027 Q3
MEC Host Upstream Merge Queue	RMM 2.0 BET3	2027 Q1 (Kernel 7.6)	+3 Kernel Cycle	**2027 Q4 (Kernel 7.9)**	Upstreamed
Planes Host Upstream Merge Queue	RMM 2.0 BET3	2027 Q1 (Kernel 7.6)	+5 Kernel Cycle	**2028 Q1 (Kernel 7.11)**	2028 Q1
LFA Upstream Merge	RMM 2.0 BET3	2026 Q3 (Kernel 7.3)	+2 Kernel Cycle	**2027 Q1 (Kernel 7.5)**	Upstreamed
EDK2 Guest FW Upstream Merge	RMM 2.0 BET3	2026 Q3 (Kernel 7.3)	+2 Kernel Cycle	**2027 Q1 (Kernel 7.5)**	N/A

CCA Software Deliverables Roadmap



Done

- **Planes** | RMM 1.1 ALP14 | TF-RMM (UQ) & KVM Host (PB) | P0-Lite PoC
- **MEC** | RMM 1.1 | TF-RMM (UQ) & KVM Host (PB)
- **LFA** | TF-RMM (UQ) | Kernel Host (PB) | SP Hafnium (UQ)
- **FIRME TF-A & TF-RMM** | Static L1 GPT | GPI_set Single Page Support
- **RMM 2.0 Base Support**| TF-RMM & Kernel Host (PB)
- **RMM 2.0 DA Foundation** | Initial Branch | Kernel Host
- **Planes** | P0-Lite PoC
- **RMM 2.0 DA Foundation** | TF-RMM PSMMU (UQ)

Q3 2026

- **RMM 2.0 Base Support** | TF-RMM (PB) BET2 + Delta BET3
- **RMM 2.0 DA Foundation | Kernel Host (PB)** BET2 + Delta BET3
- **RMM 2.0 MEC** | TF-RMM (UQ) | Kernel Host Initial Alignment
- **RMM 2.0 Planes** | Kernel Host Initial Alignment | P0-Lite PoC
- **P1 EDK2 Boot Sync** | Encrypted Disk Boot (UQ)
- **FIRME TF-A & TF-RMM (PB)**| GPI_Set | Long Running MM | IDE | MEC

Q4 2026

- **RMM 2.0 Base Support** | Kernel Host UQ Series 1/3 | TF-RMM (PB) BET2 + Delta BET3
- **RMM 2.0 DA Foundation | Kernel Host (PB)** BET2 + Delta BET3
- **RMM 2.0 MEC** | TF-RMM (UQ)
- **LFA** | Kernel Support (UQ)
- **P1 EDK2 Boot Sync** | Encrypted Disk Boot (UQ)
- **FIRME TF-A & TF-RMM (PB)**| Dynamic GPT
- **RMM 2.0 Planes** | P0-Lite PoC

Q1 2027

- **RMM 2.0 Base Support** | Kernel Host UQ Series 2/3 | TF-RMM (UQ) BET3
- **EDK2 Guest FW (UQ)**
- **FIRME TF-A & TF-RMM (UQ)**| Dynamic GPT | **RMM 1.0** | EDK2 Guest (UQ)
- **Large page support** | Guest on a host (UQ)
- **RMM 2.0 Planes** | Final P0-Lite PoC

Q2 2027

- **RMM 2.0 Base Support** | Kernel Host (UQ) Series 3/3
- **EDK2** | Measured Boot (UQ)
- **P3 EDK2 Boot Sync** | Encrypted Disk Boot (UQ)
- **Large page support** | TF-RMM (PB)

Future

- **RMM 2.0 DA Foundation** | Kernel Host & Guest (UQ)
- **RMM 2.0 Planes** | TF-RMM (UQ) | Kernel Host (UQ)
- **RMM 2.0 MEC** | Kernel Host (UQ)
- **RMM 2.0 Planes** | TF-RMM (UQ) | Kernel Host (UQ)
- **LFA** | Full System Update
- Firmware Activity Log
- **RMM 2.x Coherent DA** | P2P | RCIeP | PRI | S1 SMMU
- RMM 2.x CMEM CXL
- RMM 2.x Live Migration

Roadmap updated: 1 Oct 2026. Next Update Due by Jan 2027

- UQ - Estimate for Upstream Queue
- PB - Refers to Public Branch
- PoL – Patches on List
- RFC – Patches Ready for Comment
- Red – Changes on the roadmap vs Previous Update

CORECOLLECTIVE
Where the Arm software ecosystem connects

AOB