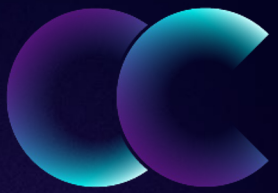
Confidential Compute Working Group (WG)



CORECOLLECTIVE

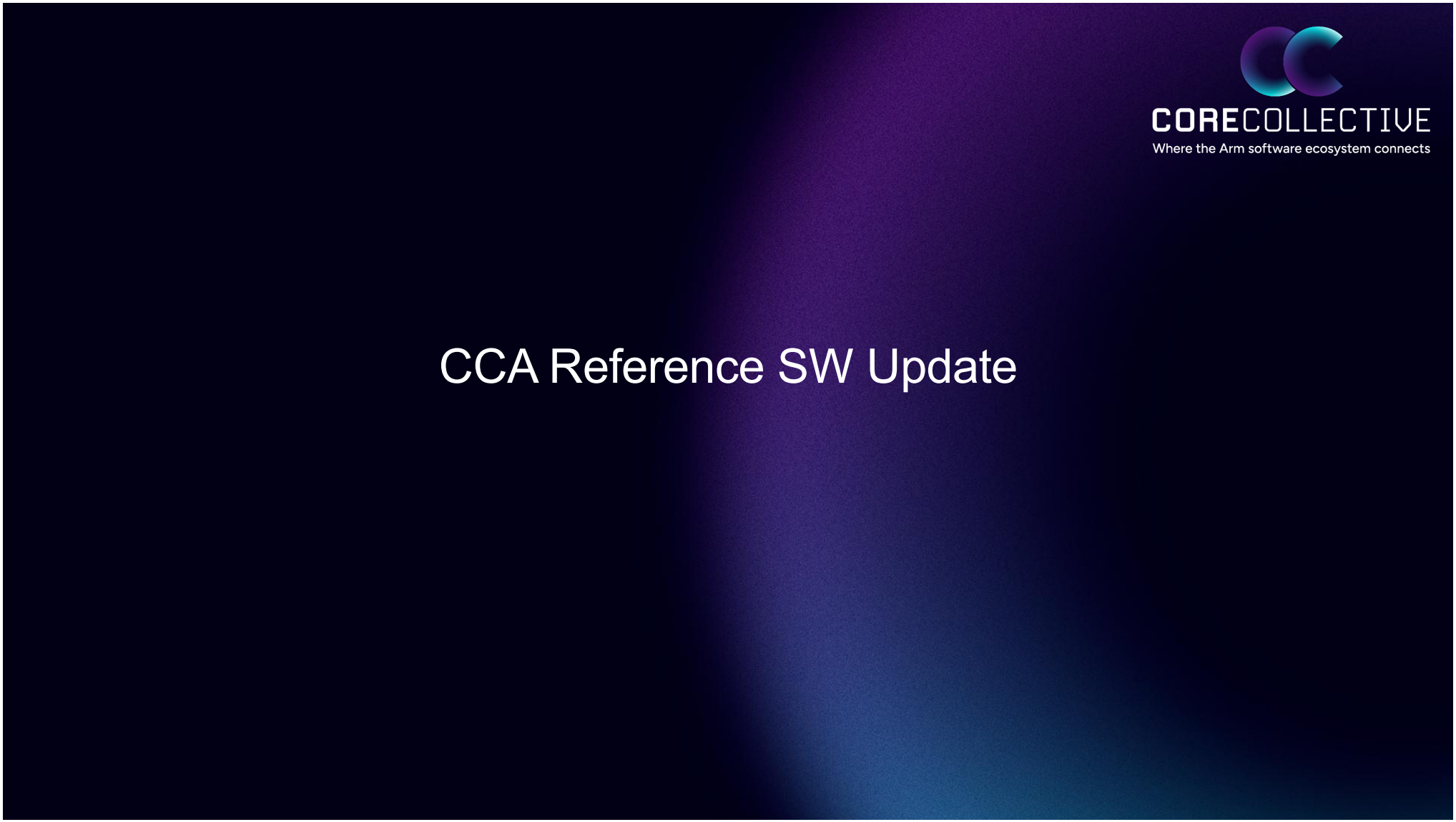
Where the Arm software ecosystem connects

14 Sept 2026

Confidential Compute WG Agenda 14 Sept 2026

CORECOLLECTIVE
Where the Arm software ecosystem connects

- Causeway Demo
- Linaro CCA Roadmap Updates
- Arm CCA Reference SW Updates
- Discussion Topic: Upstream delays and impacts on distro and deployment
  - how to collab together to progress


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 v6.13 in Jan 2025
  - v6 patches to support guest on host with large page support on list Sept 2026
- 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; 7 of 14 series merged
  - Measured Boot PR raised April 2026, 3 of 4 series merged
  - Draft Boot Sync PR (enabling Secure Boot and Encrypted Disk Boot) raised May 2026

CCA software 2.0 status

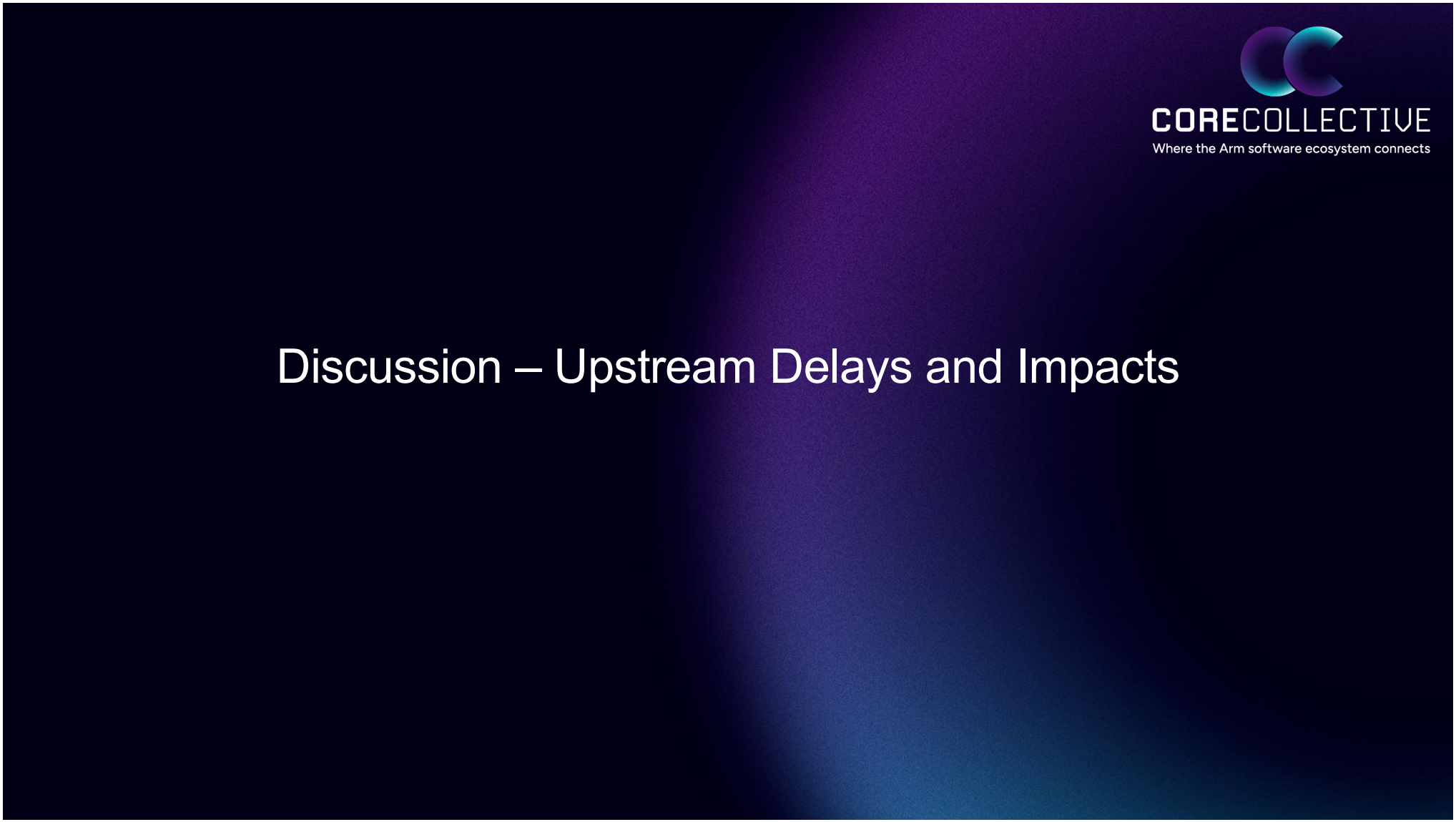


- Baseline support:
  - Initial 2.0 TF-RMM support merged March 2026 and released in v0.9 May 2026
  - 2.0 v17 Host KVM patches on list Sept 2026, now trimmed down with some chunks split out
    - Series now focusses on KVM arm64 enlightenment of different VM types and bare minimal realm VM support, plus
    - Base RMI patches
    - Host support for GPFs
    - RMI driver and remaining realm enablement – off-list for now
- Foundation DA:
  - 2.0-BET3 based stack (not fully spec aligned yet)
    - TF-RMM patches merged Sept 2026
    - Shrinkwrap config available here
    - DMA layer changes queued for 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
    - v3 Linux patches patches available since July 2026 (now depends on Aneesh's SMCCC bus patches)
  - 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)


CORECOLLECTIVE
Where the Arm software ecosystem connects
Discussion – Upstream Delays and Impacts

Discussion: Upstream delays and impacts



- CCA 2.0 Host baseline upstreaming
  - Plan agreed with maintainer to upstream this in smaller chunks
  - But now unlikely to be able to complete this upstreaming by end of 2026 as previously hoped
  - Replanning in progress
  - Likely to have knock-on impact on subsequent feature upstreaming and landing in distros...

- CCA 2.0 DA Foundation upstreaming
  - Depends on Device Trust Layer previously owned by Dan Williams
    - Maintainer is now JasonG (NVidia)
    - Ownership spread across the community (AMD, NVidia, Arm, Intel)
  - Replanning pending but likely to have an impact on overall upstreaming of feature...