
arm
Software Enablement Updates
Firmware A
Akanksha Jain
May 2024
Partner Restricted © 2024 Arm
AI-generated image

Agenda

- Recap and Delta
- TF-A : Architecture Flowers
- TF-A Release Highlights
- Component Roadmap – EL3, Hafnium, Arch IP
- CCA Enablement Updates
- TS + OPTEE Enablement Roadmap
- Other Highlights
- Q&A

Recap

- TF-A v2.9 Highlights
- Updated Roadmaps and Flowers
- TS + OPTEE bundled with other TF-A Components
- TF-A LTS 2.8 as 1st LTS Release
  - Next Steps
- TS v1.0 | Release last Quarter

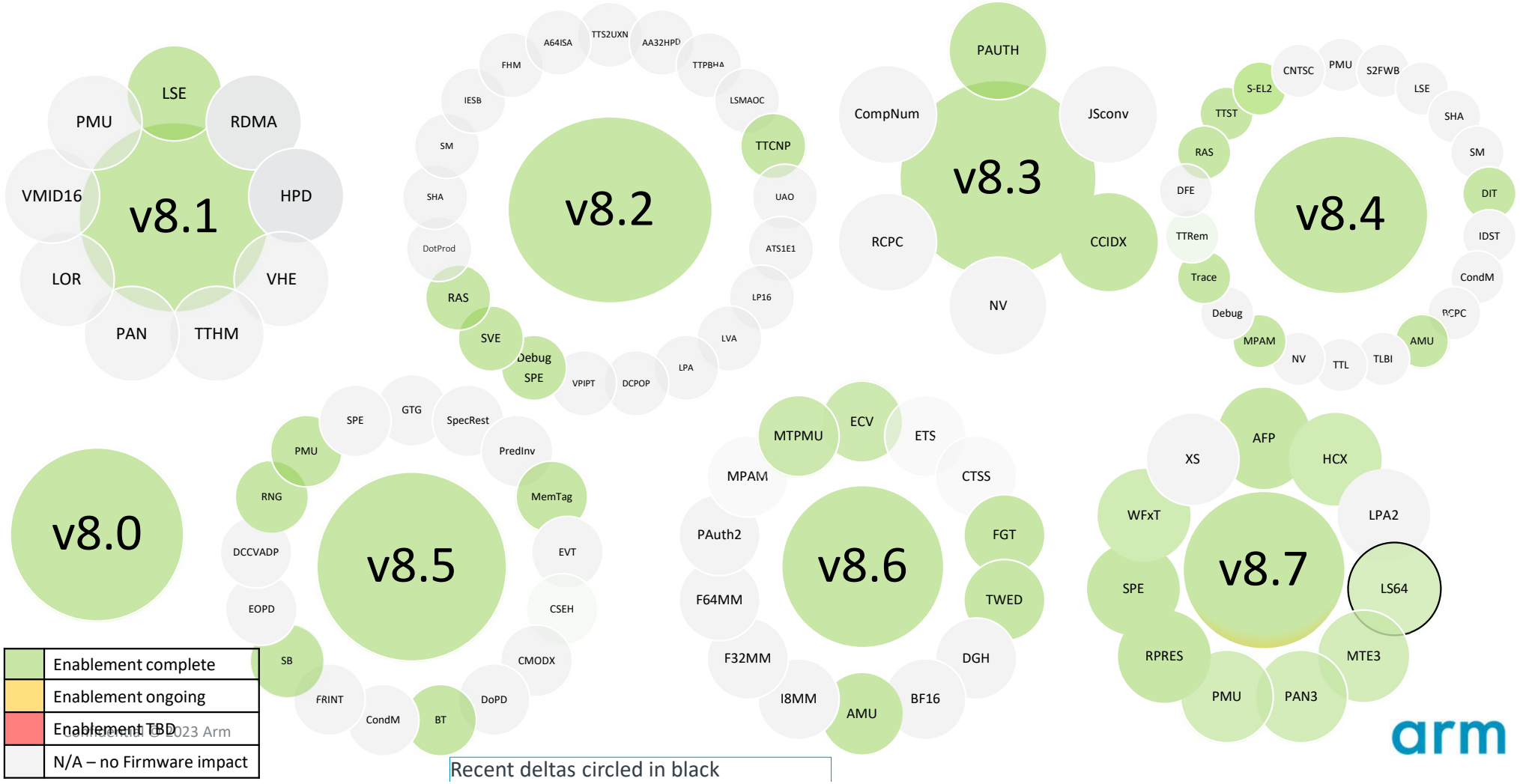
Deltas

- TF-A v2.10 Highlights
- Upcoming TF-A 2.11 | Highlights
- Updated Roadmaps and Flowers
- TF-A LTS 2.10.2 | 2nd Major LTS Release
- CCA Highlights

arm

TF-A
Architecture Enablement Story

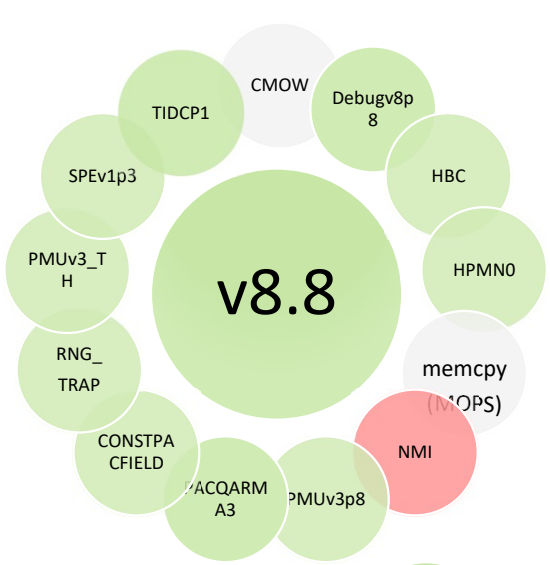
A-profile architecture – v8.x TF-A enablement recap

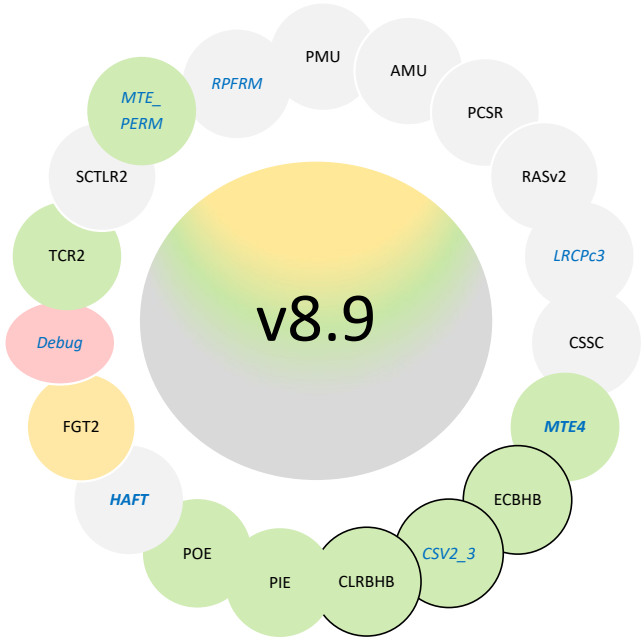


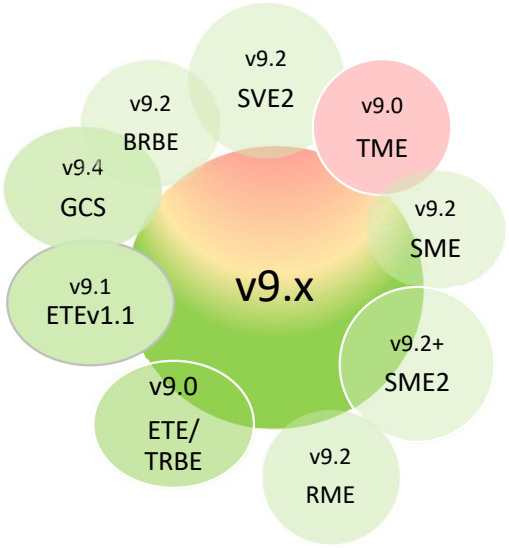
Recent deltas circled in black

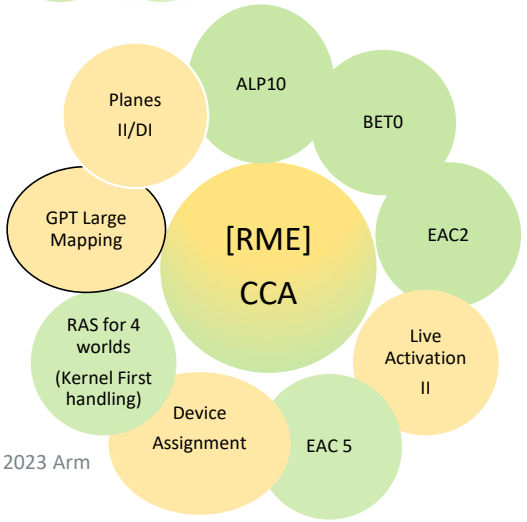
A-profile architecture TF-A

Recent Deltas circled in black









Armv8.9 :Priority to be given to this set of features (2024 Mobile CPUs)

	Enablement complete
	Enablement ongoing
	Enablement TBD
	N/A – no Kernel impact

TF-A Release Highlights

TF-A 2.10 Release | Highlights

- TF-A 2.10 | Nov'23 | 10 years and counting! ☺

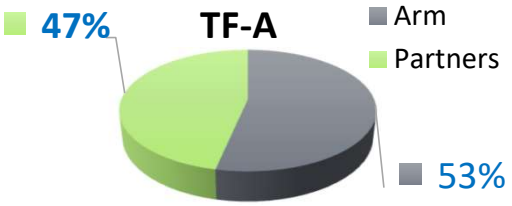
  - Continued support for 2022 Architecture extensions [HAFT,RPRFM, LRCPC3, MTE_PERM]
  - CPU support for Gelas, Nevis and Travis
  - Context management refactoring for RME/4 Worlds

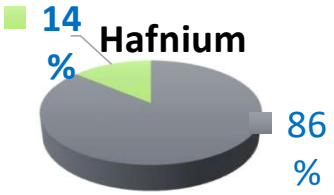
  - TF-RMM alignment against RMM 1.0 EAC5 spec
  - Non-Secure SME support in RMM
  - PAC+ BTI support enabled in RMM and Realm
  - Initial CBMC Support

  - Crypto-cell removal - 712/713 (deprecated since TF-A 2.9)
  - Enhanced FF-A 1.2 Support

  - Added support for 5 new platforms[Aspeed AST2700, NXP IMX93, Intel Agilex5,Nuvoton and ST]

  - For more details => Blog





Top External Contributors for v2.10 release cycle	• AMD • STM • Invisible Things Lab • Intel • Qualcomm • Mediatek • NXP • Nvidia • Google | TI
Next steps	• LTS 2.10 Prep • Prep for TF-A 2.11 • RMM spec v1.1 Next steps • UNDEF Injection | SMCCC v1.5 Support

TF-A 2.11 : Upcoming Highlights

EL3 Highlights

- MHUv3 doorbell driver support
- S/R support for DSU PMU registers
- v8.9 features enabled (CSV2, CLRBHB, ECBHB etc)
- UNDEF Injection : disable EL3 traps to support lower Els
- Renaming of TCS24 CPUs [Chaberton, BlackHawk] | Neoverse N3 [Hermes]

SPM | Hafnium

- **FF-A v1.2**: Direct messaging | Memory sharing descriptors update | setup and discovery interfaces | Multiple UUID per SP support
- Device memory sharing initial support.
- SME/SVE context S/R support for the NS-EL1 state, on entry from and exit back to the NWd.

System| Boot| Misc

- Enhanced Firmware handoff library |provide support BL1->BL2->Bl31 interface to use transfer list
- SMCCC 1.5 : Implemented vendor specific EL3 monitor calls
- Migration to mbedTLS v3.6.0
- DPE implementation
- Update DRTM implementation as per latest specification v1.0
- Migrate to FWU metadata version 2

Other Highlights

- TF-RMM | R-EL2
  - Arch Feature Support : Feat_DIT | Feat_LPA2
  - Introduced the 'arm' platform layer|used by any compatible SoC| enable a single binary across them
  - Reduced the `struct granule` data structure size; reducing its footprint from 16MB to 4MB for FVP
  - TF-A Tests
- *Core*
  - *Errata mgmt firmware interface |firmware handoff*
- *SPM/FF-A*
  - *Support SMCCCv1.2 registers set.*
  - *Test SMCCC compliance |non-secure phy instance*
  - *Test FF-A v1.2*
- *RMM*
  - *Added FPU/SVE/SME tests*
  - *Added multiple REC single CPU tests.*
  - *Added PAuth support in Realms tests.*
  - *Added PMU tests.*
- CPU Errata
  - 28 new CPU Errata implemented.
  - Fixed 3 errata implementation defects. (2xCortex-A715 + erratum wrongly to Cortex-A715 instead of Cortex-X3)
  - Implemented 1x GIC600 erratum
- Platform Support
  - Aspeed AST2700, NXP IMX93, Intel Agilex5, Nuvoton NPCM845x, QTI MDM9607, MSM8909, MSM8939, ST STM32MP2

arm

Roadmap

Trusted Firmware-A Roadmap

	2024 CQ1	2024 CQ2	2024 Q3	2024 Q4	Future
HW & IP	• TF-A 2.10 LTS Release	• TF-A 2.11 Release • 2022 Arch Enhanced Support • GPT large Mapping II/DI	• CC-3xx HW Offload • 2023 Features : II/DI • GIC v3.3 NMI II/DI	• TF-A 2.12 ? • 2023 Features Support • GIC vNext : II/DI	• CC-3xx HW offload (PSA Crypto driver API) • Granule Delegation | SMC Support • PSCI S/R MPAM MSC • GICvNext support
SPM & FF-A	• FF-A 1.1 | SMMU Support • FF-A 1.2 Enhanced Support	• FF-A 1.1 | Secure Timer II • FF-A 1.1 | RAS CI • FWU LA II/DI	• FF-A 1.1 ACS Compliance	• FWU LA| Proto on FVP • Secure timer virtualization • GICvNext Support |II	• FF-Av1.1 ACS compliance • Measured Boot: • TZ Hafnium fTPM/EventLog
System & Misc	• FW Handoff BL Stage • FWU Live A BL Stage • PSCI Imrovements	• mbedTLS 2.x Deprecation • mbedTLS 3.6 support • FWU Live Activation II	• FW Handoff : Arm Plat. Support • dTPM Proto : Review	• FW handoff • Partner Platform support • FWU Live Activation DI	• RSS-centric Bootflow • PSCI improvements • DRTM Phase 2 Support

arm

Trusted Firmware-A Roadmap

	Released	2024 CQ2	2024 Q3	2024 Q4	Future
Trsuted Services	• smm gateway – Auth. Variables • mbedTLS 3.5 • SP Logging Proto • RSS Com protocol	• BTI support • FWU|Proxy SP • Secure Interrupt Handling • FF-A Userspace • YP Recipe updates	• mbedTLS next • SDL Enhanced Support	• TS 1.1 [24Q4 Release] • OpenCI Support	FF-A Manifest | Tooling Secure Partition [RPMb PoC] Linux dm-crypt
OPTEE	• SPM Test suite – Enhancement	• OPTEE SPMC : Multiple VM support	• OPTEE SPMC : Multiple VM support		• FF-A ACS support • FF-A Boot Protocol [TF-A | OPTEE]

ChangeLog

Roadmap

arm

arm

CCA

Arm CCA 1.0 (also known as RMM spec 1.0)

- Enables protection of CPU state and memory contents owned by a realm
  - Minimum Viable Product

- Final RMM 1.0 spec (EAC5) released in Oct 2023

- TF-A / TF-RMM support upstream since Jan 2024
- Latest Linux/KVM patches based on v6.9-rc1 on list since Apr 2024
  - kvm-unit-test patches too
- Latest EDK2 patches (realm guest firmware) on list since Apr 2024

CCA 1.1 features – needed for initial deployments

Further strengthen the security guarantees provided to end users (Realm owners)

- Memory Encryption Contexts (MEC)
  - Physical memory contents of each Realm protected using a unique key or tweak
- Multiple signers
  - Require firmware image to be endorsed by multiple authorities, e.g. vendor plus a trusted auditor

Enable migration of workloads from non-secure VM to Realm, by providing feature parity

- Planes
  - Multiple privilege levels within a Realm, orthogonal to traditional kernel / userspace split
- Device Assignment (DA)
  - Enable trusted device functions to be admitted into a Realm's TCB, and granted DMA

Allow platform owners additional flexibility, in deploying and updating firmware

- Live firmware activation
  - Update firmware image(s) while workloads continue to run, with minimal loss of availability
  - Replace platform firmware (e.g. RMM) with an image supplied by the non-secure host

TF-A LTS

TF-A LTS Highlights | Next Steps

Recap

- Mailing List discussion
- LTS Proposal

- Gearing up for the next LTS Major Release (Q1'24) branched out of TF-A 2.10

- Gearing for TF-A 2.8.10 Minor Release | **Final Stages of Review**
  - Update mbedTLS to 2.28.5
  - LTS Public documentation Support
- Partner Engagement
  - Nvidia, Google, STM and Xilinx Maintainers
  - Strengthen the Ecosystem support | Deliberation

TF-A LTS 2.10 | Highlights |Next steps

- Building on the 1st TF-A LTS in 2023, the second major LTS version- LTS v2.10 [1], its first valid tag being lts-v2.10.2 [Feb'24]

- The LTS is branched out of TF-A 2.10, the second 2023 TF-A Release [Nov'2023]

  - **15 errata support** merged in last 3 months (Cortex-A78C, Cortex-A520, Cortex-A710, Cortex-X2, Cortex-X3 and Neoverse N2 CPU cores)

- For more details
  - [1] TF-A LTS 2.10.2 Release Note | Changelog

Release Cadence

- Major Release : Annual Cadence; Branched out of 2nd TF-A Release
- Minor Release: Generally targeted as a Fri Release on an ad-hoc basis
- Maintenance Window : 5-year Period
- LTS CI jobs : Twice a week | Wed and Sat

Ongoing Discussions | Challenges

- Ongoing discussion on openCI automation
- Scalability : With more LTS branches; leverage strong partner ecosystem support
- Initial estimates on the metrics gathered with TF-A LTS 2.8; could need revisit
- Long Term Performance Window: Forward Looking Strategy