Firmware A profile Roadmap Update

Oct 2023

CE-OSS Tech Management
Akanksha J. | Olivier D. | Gyorgy S.

Agenda

- Introduction
- Recap and Delta
- TF-A 2.9 Release Highlights
- Component Roadmap – EL3, Hafnium, Arch IP
- CCA Enablement Roadmap
- TS + OPTEE Enablement Roadmap
- TF-A LTS | Highlights and Next steps
- Q&A

Recap

- TF-A v2.8 Highlights
- Roadmap
- Architecture Enablement Flowers (2021 Extensions WiP)
- CCA Enablement Plans
- TS + OPTEE Roadmaps
- 1st RMM Public Release
- Initial Deliberation around LTS Release

Deltas

- 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

TF-A 2.9 Highlights

TF-A 2.9 Release | General Highlights

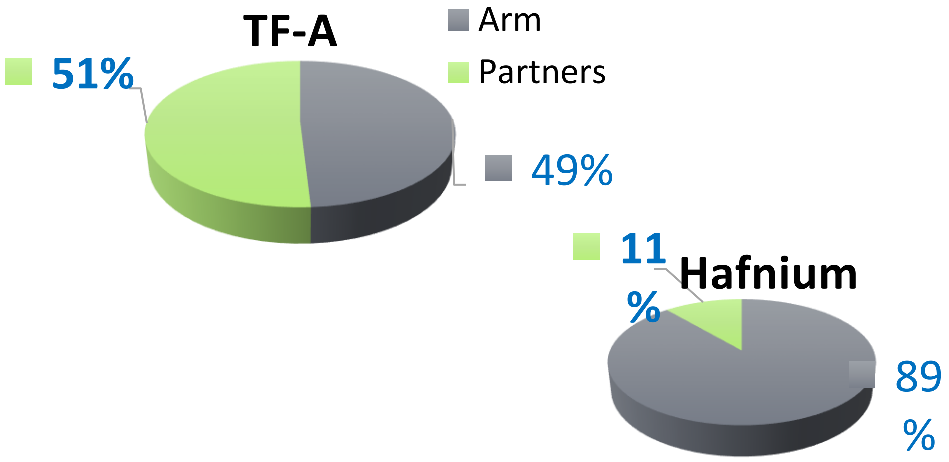
- ❑ First release done solely relying on [TrustedFirmware.org Open CI]
- ❑ Support for PSCI initiated mode | Active partner engagement in development and testing support
- ❑ Trusted Boot Support for TC22 platform | Migration to mbedTLS 3.x
- ❑ Support to create Realms which can make use of SVE hardware functionality
- ❑ EL3 Enablement Support for 2021 and 2022 Arch. Extensions

A profile Arch enablement

- ❑ CPU support for 2023 CPU Cores
- ❑ Support for PSCI OS initiated mode
- ❑ Architecture support for FEAT_TCR2, Guarded Control Stack (FEAT_GCS), Config Register Support for FEAT_HCX
- ❑ Save/Restore Support for FEAT_PIE/POE, FEAT_SME | SME2, FEAT_MPAM: runtime check
- ❑ Added dynamic detection of architecture feature enablement
- ❑ System registers access trap handler

Other merges

- ❑ Errata ABI 1.0 |REL support → merged in TF-A 2.9
- ❑ FF-A 1.2 Early Adoption | FF-A 1.1 Continued Support
- ❑ Ethos-N NPU Driver Added support for Protected Firmware Setup
- ❑ 18 CPU Errata Mitigations for Cortex-A510, A-78, X2, Neoverse V1, N2 cores |GICv3 bug fixes
- ❑ EL3 SPMC enhanced feature
- ❑ Arm CCA support | BET0 Alignment
  - ❑ *Support for Trusted Boot rooted into RSS RoT.*
  - ❑ *Support for PSA attestation scheme with Measured Boot rooted into RSS*
  - ❑ *General improvements and hardening of the boot and attestation support*



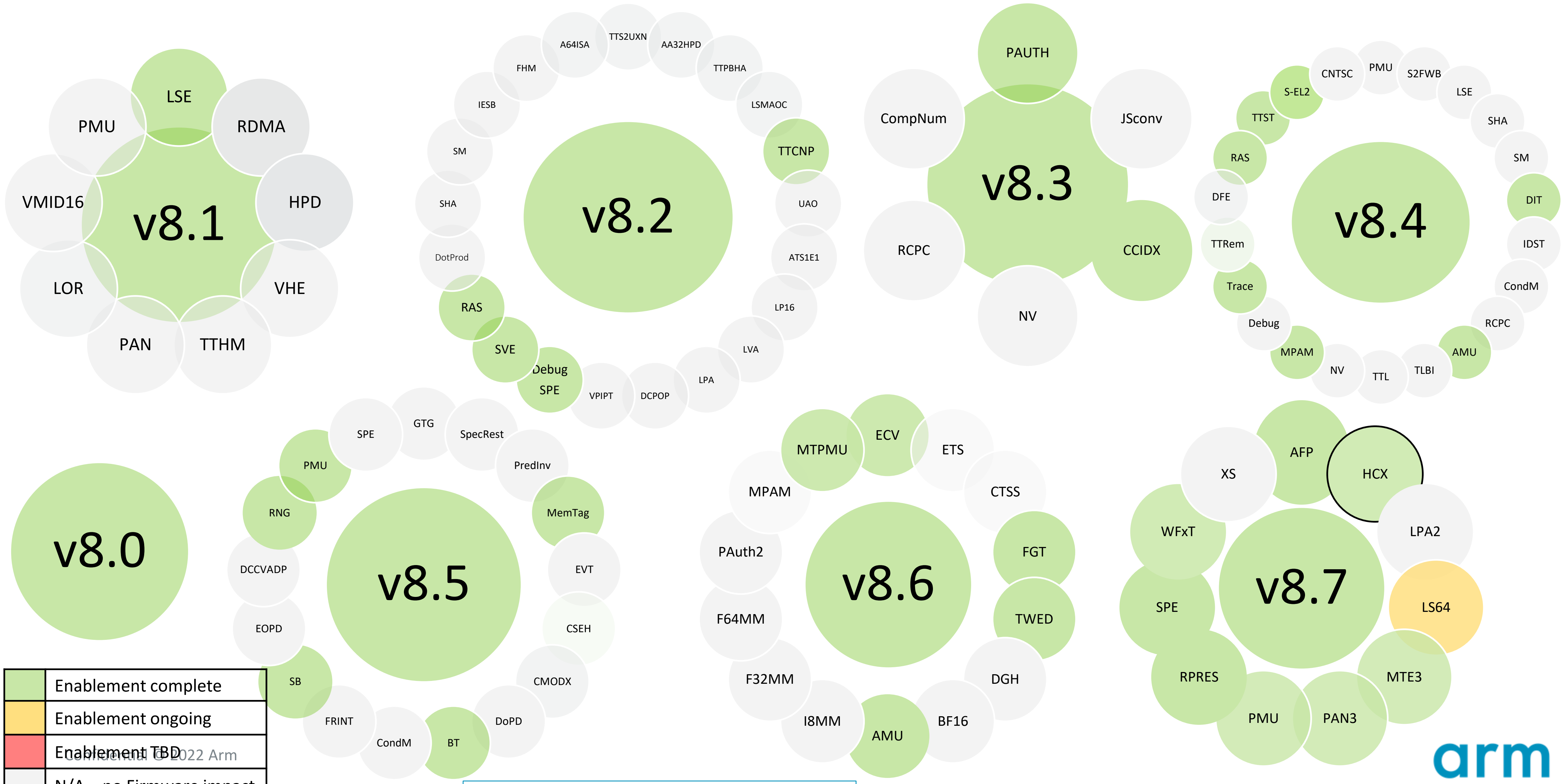
Top External Contributors for v2.9 release cycle	• AMD|Xilinx • STM • Nvidia • NXP • Google • Mediatek • Intel • Linaro | TI | QC
Next steps	• Prep for TF-A 2.10 |3.0 • RMMv1.0 (EAC spec alignment) Deprecation of CC 7xx series planned for TF-A release (Nov '23)

Trusted Firmware-A Roadmap

■ Released ● Adv. Planning
◆ Development ⬡ Concept

	2023 H1 ■	2023 CQ4 ◆	2024 CQ1 ●	2024 CQ2 ⬡	Future ⬡
HW & IP	• TF-A 2.9 Release • CC-7xx Dep. Announcement • 2023 Arm CPU Core Support • 2021 | 2022 Arch. Enablement Support	• TF-A 2.10 Release • CC-7xx Deprecation • 2024 Arm CPU Core support	• TF-A 2.10 LTS Release • GICv Next II/DI	• TF-A vNext • 2022 Arch Enhanced Support • GIC v3.3 NMI II/DI • GICv Next DI	• CC-3xx HW Offload • 2023 Arch Extensions :II/DI • GIC Support
SPM & FF-A	• FF-A 1.1 Support • FF-A |VHE S-EL0 Support • FF-A 1.2 Bypass Multi-borrower • Platform Device Assignment	• FF-A Mem Sharing | RME • SME 1|2 NS S/R • EL3 SPMC|SVE Support	• FF-A 1.1 | SMMU Support • FF-A 1.2 Enhanced Support	• FF-A 1.1 | Secure Timer II • GICvnext Support |II • FWU Live Activation II/DI	• FF-A 1.1 | RAS CI • FF-A 1.1 ACS Compliance • Secure Timer Virtualization
System & Misc	• SMCCC v1.4 support • RAS Support for 4 worlds • PSA Crypto API II/DI • FW Handoff spec | FVP | generic code Review	• mbedTLS 2.x Dep . Announcement • PSA Crypto API • DICE | DPE Attestation	• FW Handoff BL Stage • FWU Live A BL Stage • PSCI Imrovements	• mbedTLS 2.x Deprecation • FWU Live Activation DI	• RSS Centric Bootflow • DRTM | dTPM Proto Support • FWU TS Alignment | Update Agent

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

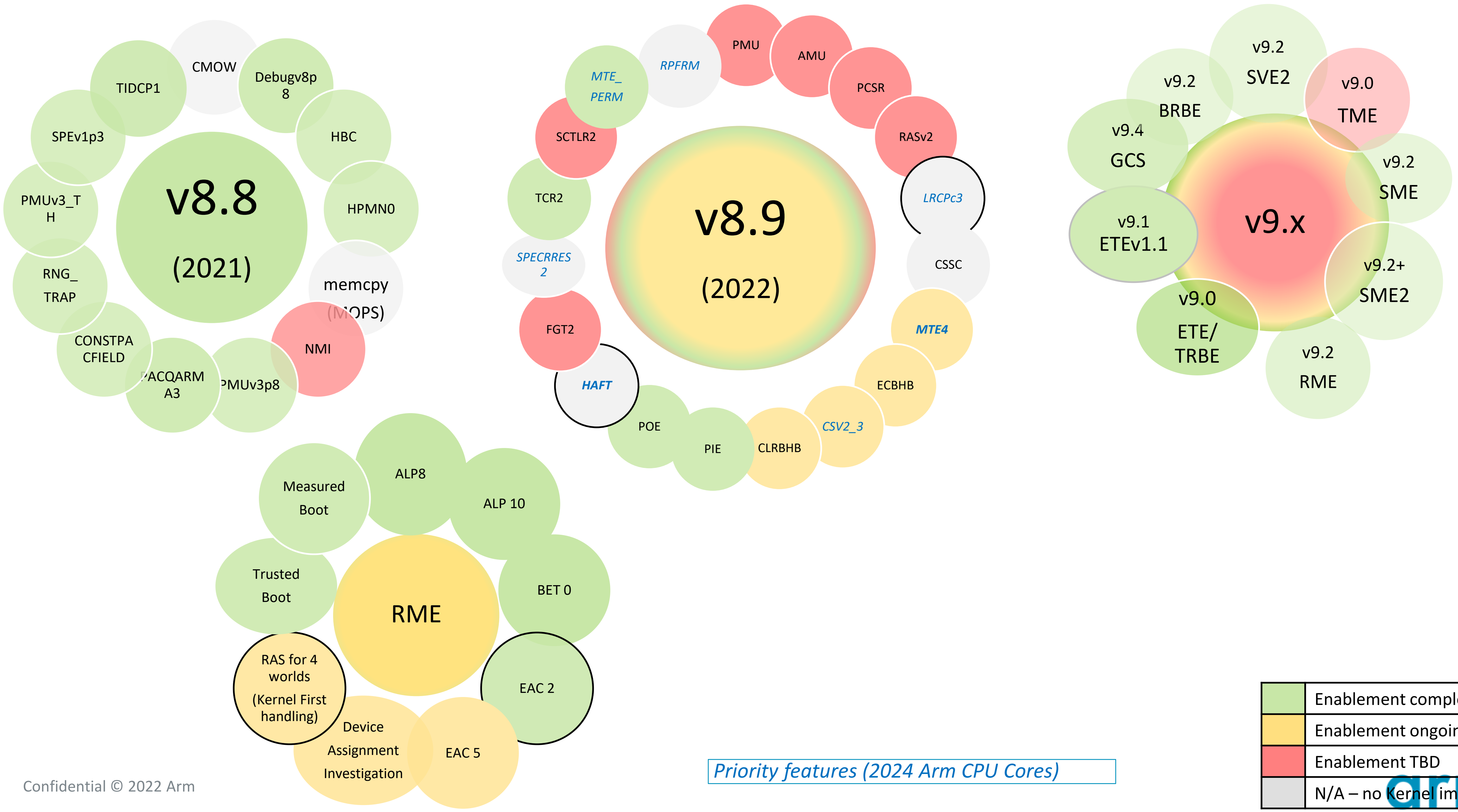


🟩	Enablement complete
🟨	Enablement ongoing
🟥	Enablement TBD
⬜	N/A – no Firmware impact

Recent Highlights circled in Black

A-profile architecture TF-A

Recent Highlights



v8.8 (2021)

CMOW, Debugv8p8, HBC, HPMN0, memcpy (MOPS), NMI, PMUv3p8, PACQARMA3, CONSTPACFIELD, RNG_TRAP, PMUv3_TH, SPEv1p3, TIDCP1

v8.9 (2022)

PMU, AMU, PCSR, RASv2, *LRCPc3*, CSSC, ***MTE4***, ECBHB, *CSV2_3*, CLRBHB, PIE, POE, ***HAFT***, FGT2, *SPECRRES2*, TCR2, SCTLR2, *MTE_PERM*, *RPFRM*

v9.x

v9.2 SVE2, v9.0 TME, v9.2 SME, v9.2+ SME2, v9.2 RME, v9.0 ETE/ TRBE, v9.1 ETEv1.1, v9.4 GCS, v9.2 BRBE

RME

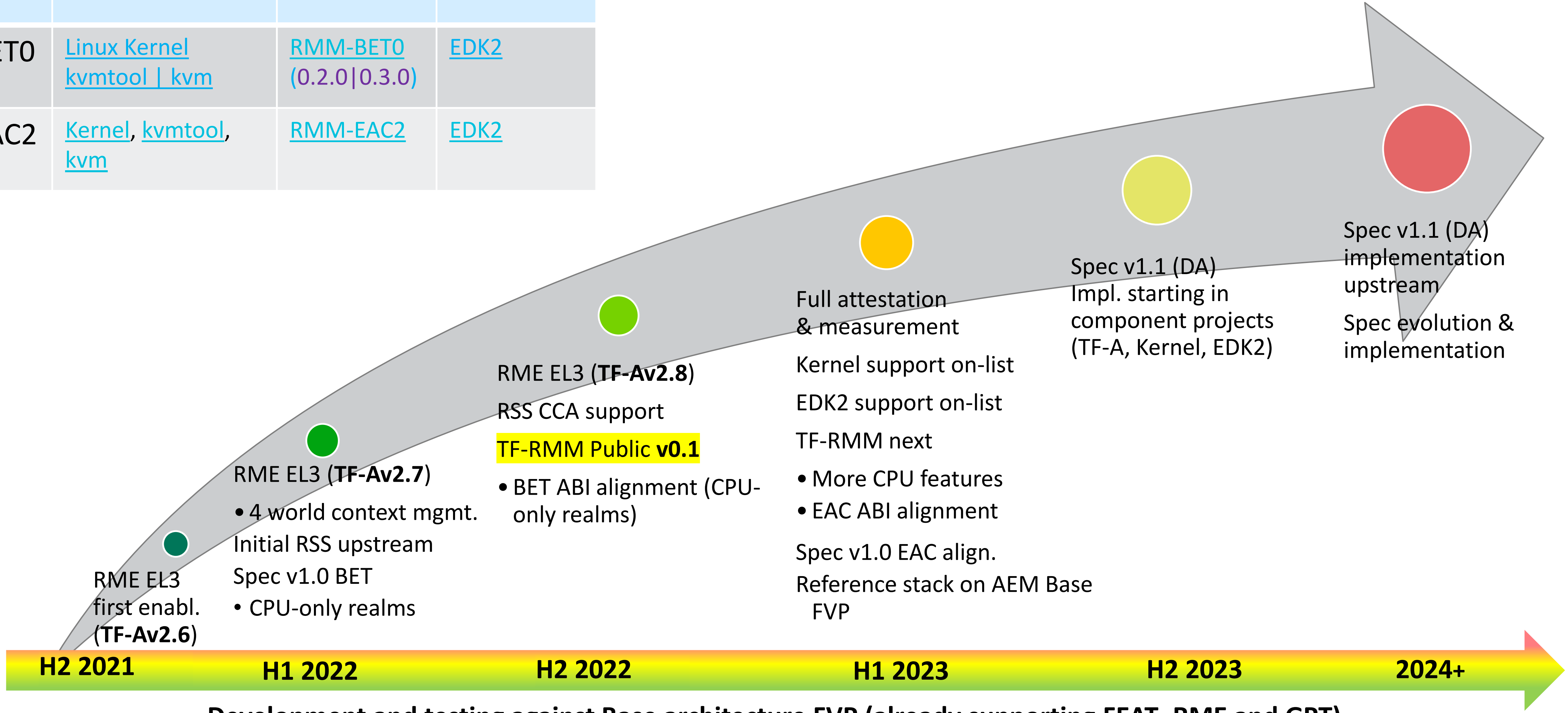
ALP8, ALP 10, BET 0, EAC 2, EAC 5, Device Assignment Investigation, RAS for 4 worlds (Kernel First handling), Trusted Boot, Measured Boot

Priority features (2024 Arm CPU Cores)

🟩	Enablement complete
🟨	Enablement ongoing
🟥	Enablement TBD
⬜	N/A – no Kernel impact

Arm CCA Upstream Enablement Roadmap

Spec	Kernel	RMM	EDK2
BET0	Linux Kernel kvmtool | kvm	RMM-BET0 (0.2.0|0.3.0)	EDK2
EAC2	Kernel, kvmtool, kvm	RMM-EAC2	EDK2



RME EL3 first enabl. (**TF-Av2.6**)

RME EL3 (**TF-Av2.7**)
- 4 world context mgmt.

Initial RSS upstream

Spec v1.0 BET
- CPU-only realms

RME EL3 (**TF-Av2.8**)

RSS CCA support

TF-RMM Public **v0.1**
- BET ABI alignment (CPU-only realms)

Full attestation & measurement

Kernel support on-list

EDK2 support on-list

TF-RMM next
- More CPU features
- EAC ABI alignment

Spec v1.0 EAC align.

Reference stack on AEM Base FVP

Spec v1.1 (DA) Impl. starting in component projects (TF-A, Kernel, EDK2)

Spec v1.1 (DA) implementation upstream

Spec evolution & implementation

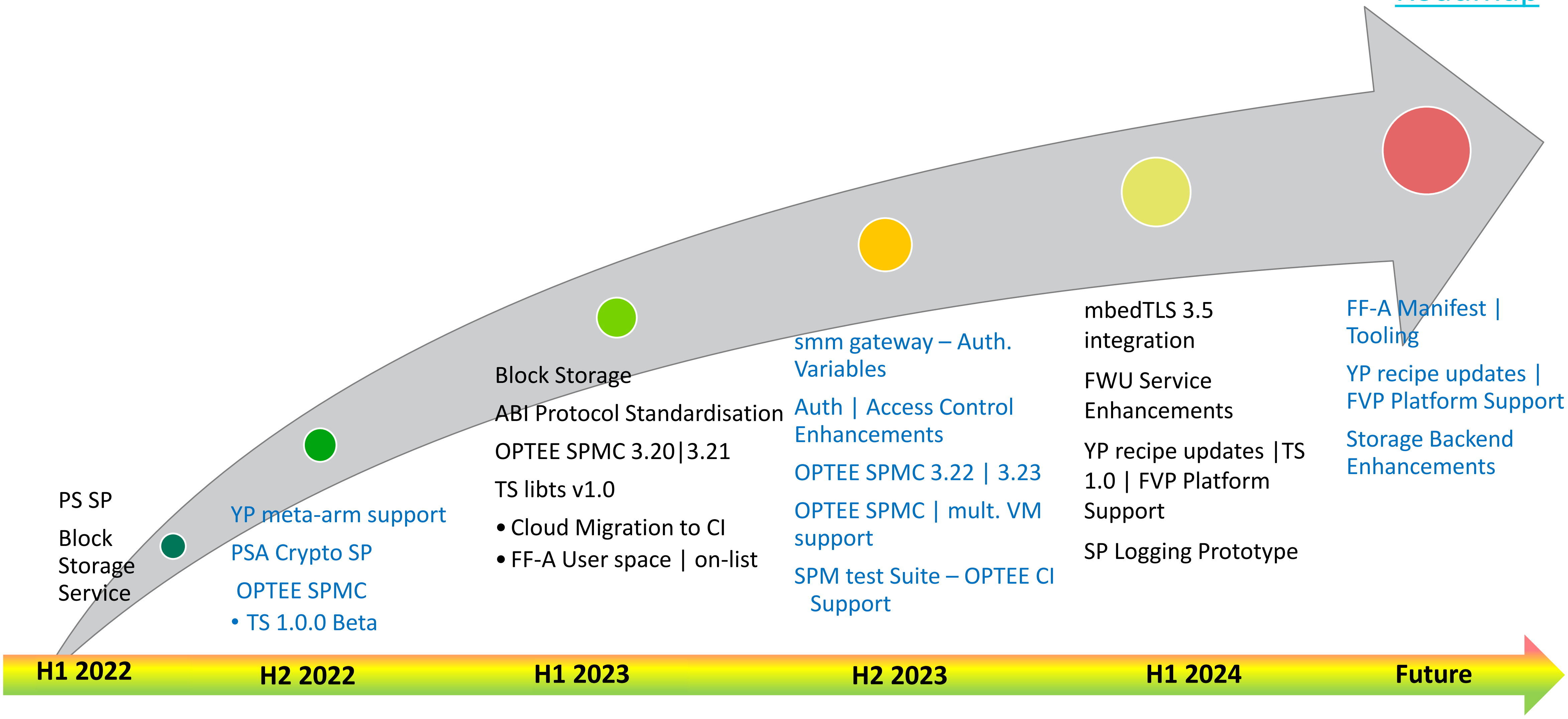
Development and testing against Base architecture FVP (already supporting FEAT_RME and GPT)

Additional Resources

- Linaro Connect London 26th-28th April 2023
  - LHR23-311-Arm Confidential Compute Architecture open-source enablement
  - LHR23-304-Runtime Security Subsystem [Arm CCA HES] – An overview
  - LHR23-120-Trusted Firmware (TF-RMM) Hacking Session
  - LHR23-319-Arm CCA Linux Support
  - LHR23-315-Confidential Containers(Coco) on Arm CCA
  - LHR23-301-Confidential Computing panel
- Linaro Virtual Connect Fall 8th-10th September 2021
  - LVC21F-311 Overview of Firmware Architecture for Arm CCA
- Linaro and Arm CCA tech event 23rd June 2021
  - Introduction to the Arm Confidential Compute Architecture
  - Software & Firmware Architecture
  - Attestation architecture
  - Developer Resources
  - TF-A Monitor Firmware (deep dive)
  - Confidential Compute, what's it all about? (Panel discussion)

Trusted Services + OPTEE Roadmap

Roadmap



H1 2022

PS SP

Block Storage Service

H2 2022

YP meta-arm support

PSA Crypto SP

OPTEE SPMC

- TS 1.0.0 Beta

H1 2023

Block Storage

ABI Protocol Standardisation

OPTEE SPMC 3.20|3.21

TS libts v1.0

- Cloud Migration to CI
- FF-A User space | on-list

H2 2023

smm gateway – Auth. Variables

Auth | Access Control Enhancements

OPTEE SPMC 3.22 | 3.23

OPTEE SPMC | mult. VM support

SPM test Suite – OPTEE CI Support

H1 2024

mbedTLS 3.5 integration

FWU Service Enhancements

YP recipe updates |TS 1.0 | FVP Platform Support

SP Logging Prototype

Future

FF-A Manifest | Tooling

YP recipe updates | FVP Platform Support

Storage Backend Enhancements

Trusted Services Release | v1.0.0

TS 1.0 Release | Blog

- The deltas from the Beta release include:
- Introduction to Block Storage Service and FWU services(to allow replacement of Firmware components)
- Refactoring the UUID policy
- Refactoring the discover service to remove the runtime overhead
- Normal World preemption capability in Secure Partition
- Arm 8.x CRC-32 support for the S|NS
- Continued support for FF-A1.1 and FF-A 1.2 spec
- mbedTLS version update to v3.4.0

TF-A LTS Highlights | Next Steps

Recap

- ❑ Mailing List discussion
- ❑ LTS Proposal

- ❑ TF-A LTS 2.8 Release majorly comprised
  - ❑ 1st LTS Release of the Project- Feb’23| Blog
  - ❑ Errata ABI and Errata Framework Support in 2.8.9 Minor release
  - ❑ More details in here

- ❑ Partner Engagement
  - ❑ Nvidia, Google, STM and Xilinx Maintainers
  - ❑ Strengthen the Ecosystem support | Deliberation

TF-A LTS Next Steps

- ❑ 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

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

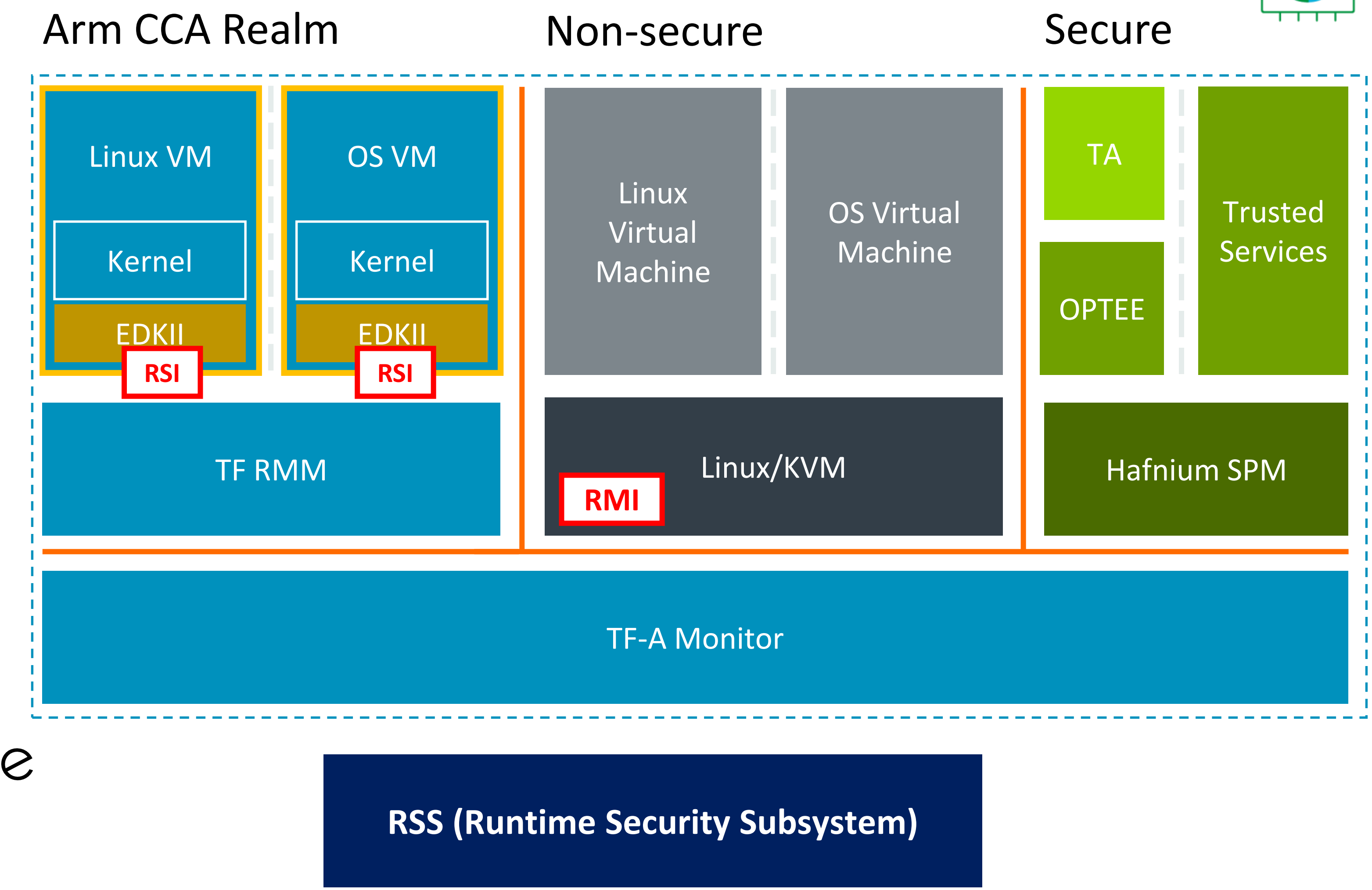
Ongoing Discussions | Challenges

- ❑ 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

Thank you

Additional Slides

Arm CCA Open Source Software enablement – Upstream components



Arm CCA Realm

Non-secure

Secure

Linux VM

Kernel

EDKII

RSI

OS VM

Kernel

EDKII

RSI

TF RMM

Linux Virtual Machine

OS Virtual Machine

Linux/KVM

RMI

TA

OPTEE

Trusted Services

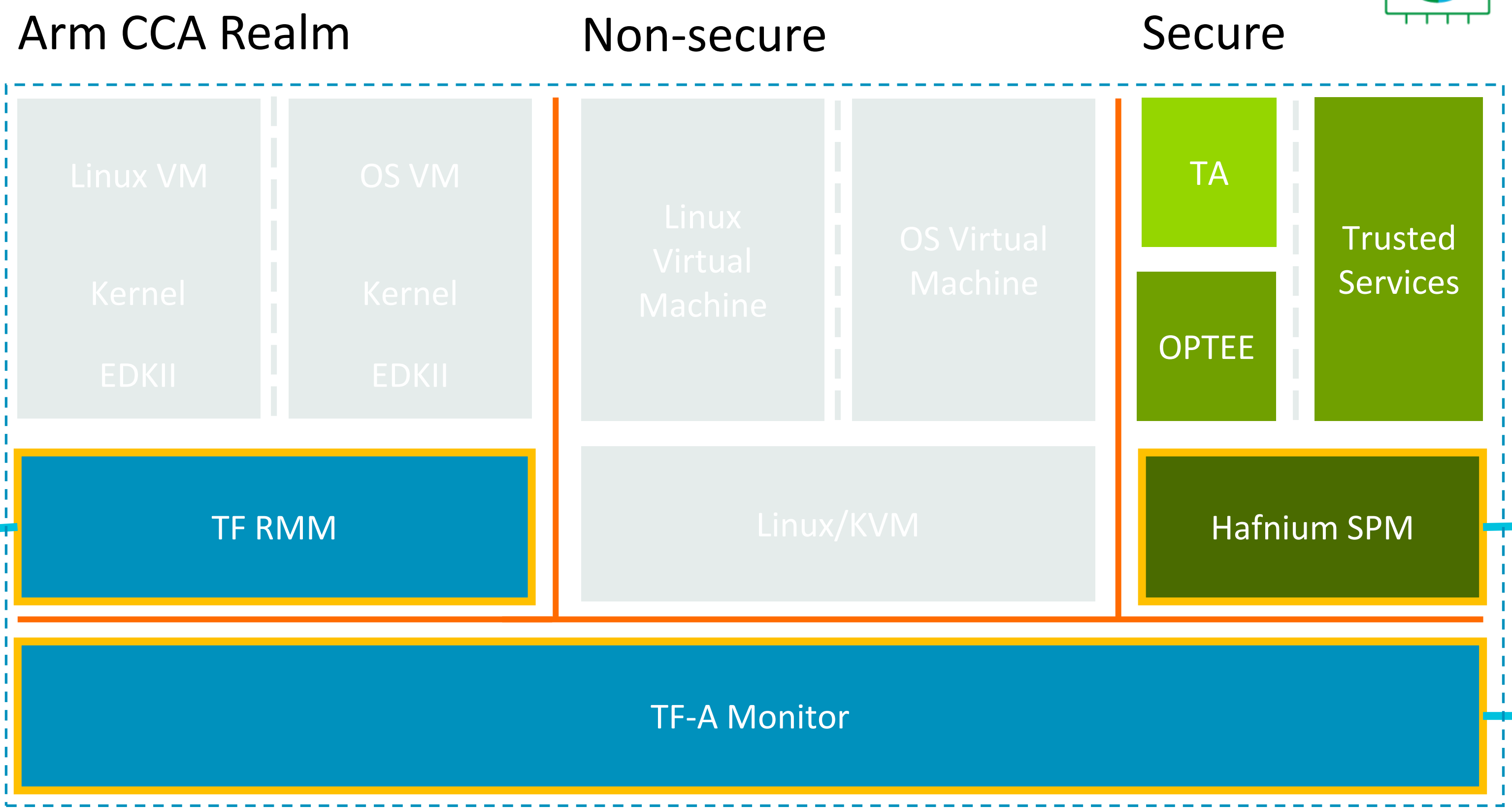
Hafnium SPM

TF-A Monitor

RSS (Runtime Security Subsystem)

Arm CCA Open Source Software – TrustedFirmware.org

TrustedFirmware .org



Brand new open source component

Dynamic Secure memory support

TF-A Monitor supporting FEAT_RME extension

RSS (Runtime Security Subsystem)

AP Measurements & Attestation RoT (part of TF-M code)

Introduction & Highlights

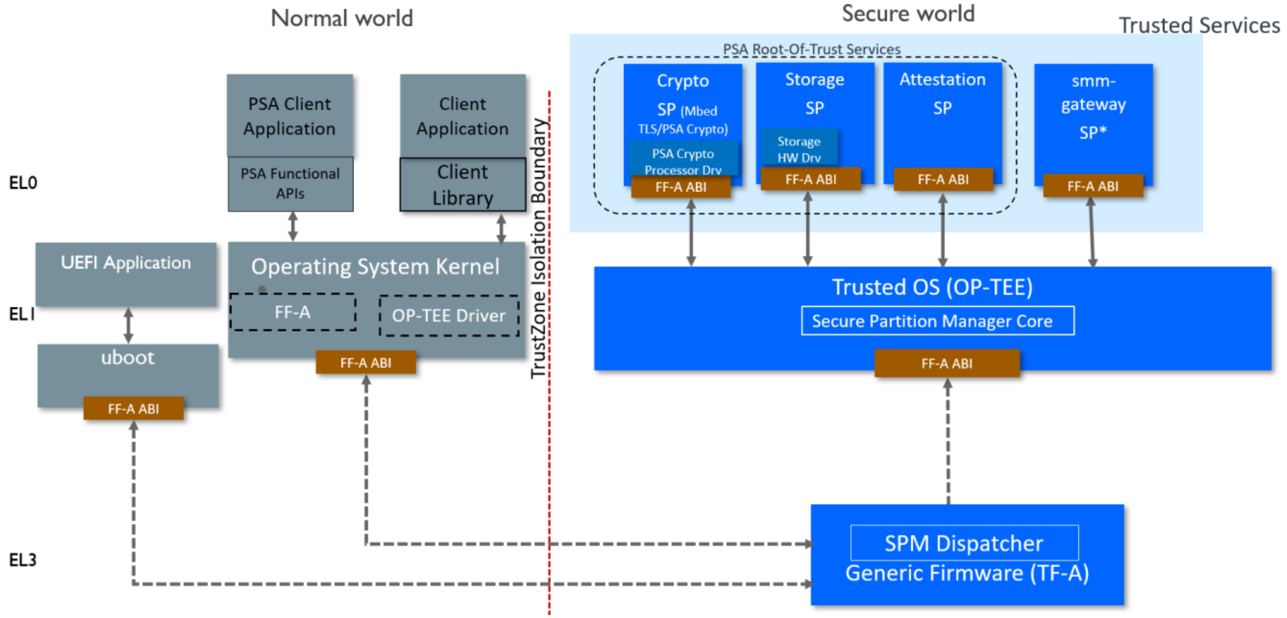
- Project to develop and deploy device root-of-trust services for A-profile devices
  - Works with other Trusted Firmware projects – TF-A, OP-TEE and Hafnium.

- Applications use Trusted Services for Security Operations using client/server model

- Uses Secure Partition Manager Core (SPMC) in OP-TEE to manage a set of secure partitions running at S-EL0.
  - FF-A used as transport layer.

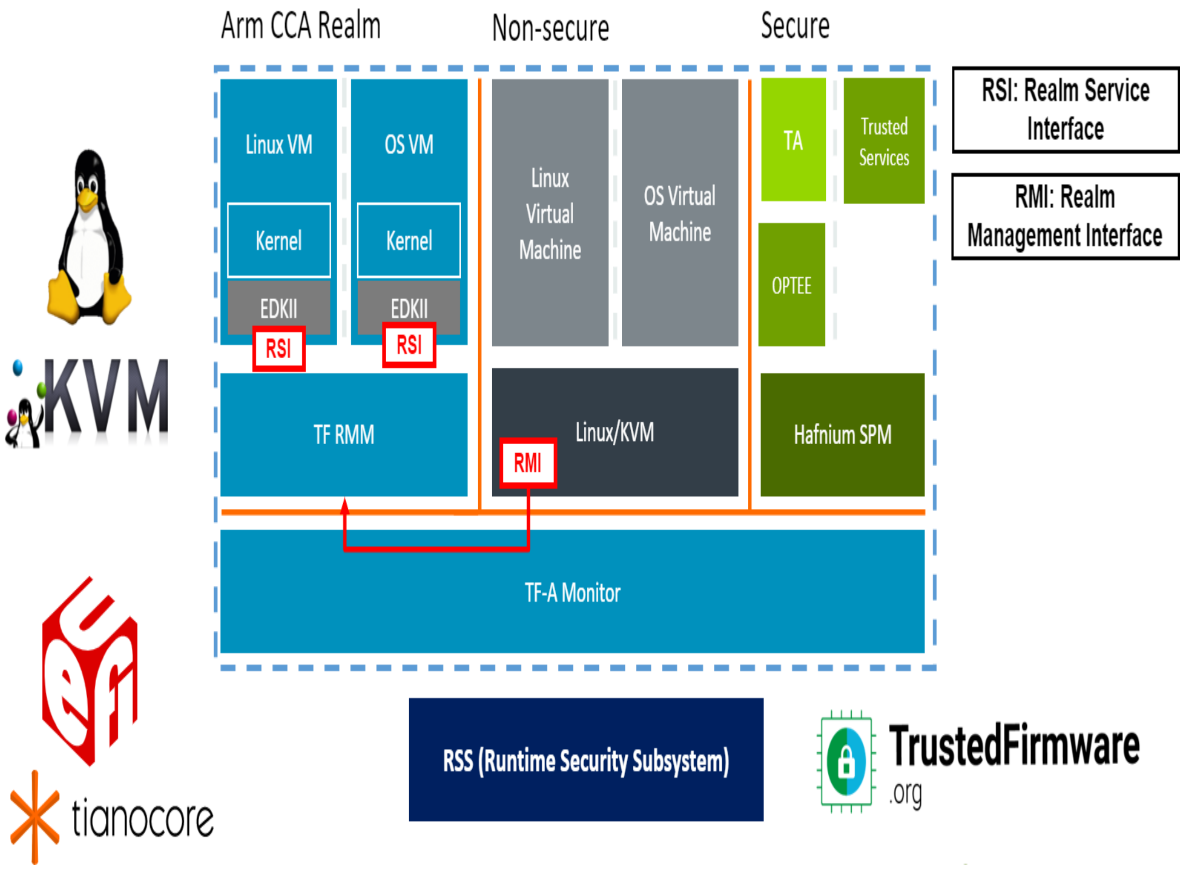
- First Release 1.0.0-Beta made this month
  - PSA Crypto, Storage and Attestation Secure Partitions
  - UEFI SMM services
  - OP-TEE in 3.17 and later releases support Secure Partition Manager Core (SPMC).

- Services under development
  - Block Storage
  - Firmware Update



Confidential Compute : Highlights!

OSS enablement – Upstream components



Arm CCA Realm

Non-secure

Secure

Linux VM

Kernel

EDKII

RSI

OS VM

Kernel

EDKII

RSI

Linux Virtual Machine

OS Virtual Machine

TA

Trusted Services

OPTEE

TF RMM

Linux/KVM

RMI

Hafnium SPM

TF-A Monitor

RSI: Realm Service Interface

RMI: Realm Management Interface

RSS (Runtime Security Subsystem)

- ❑ RME: Realm Management Extension
  - ❑ Arm 9.x Hardware extension to provide an isolated, dynamic, attestable and trustworthy execution environment
- ❑ Arm Confidential Compute Architecture
  - ❑ Builds on RME by providing a reference security and software architecture
- ❑ RSS : Runtime Security Subsystem
  - ❑ Hardware Encryption Scheme | Root of Trust Module | TF-M
- ❑ RMM : Realm Management Module
  - ❑ Dedicated mailing list and website section
  - ❑ Release tag against BET0 upstream
- ❑ BET0 Alignment | RFC patches on-list
  - ❑ Linux Kernel kvmtool | kvm
  - ❑ EDK2
- ❑ Arm CCA Reference Software Stack
  - ❑ Arm Neoverse Fremont Reference Design (RD) FVP
  - ❑ Armv8-A Base Architecture Fixed Virtual Platform (FVP) model
  - ❑ Arm CCA stack for Base FVP available now
- ❑ QEMU | on-list
  - ❑ TCG (Tiny Code Generator), interpreter/emulator | QEMU 8.1
  - ❑ VMM (Virtual Machine Manager) for KVM realm

Confidential Compute : Deeper dive – Linaro Sessions !

- ❑ The Arm CCA allows the hypervisor to control the VM, but removes the right to access the code, register state or data that is used by the VM

- ❑ LHR23-120-Trusted Firmware (TF-RMM) Hacking Session
- ❑ LHR23-311-Arm CCA Open-source enablement
- ❑ LHR23-319-Arm CCA Linux Support
- ❑ Runtime Security Subsystem (RSS) – CCA Overview
- ❑ LHR23-315-Confidential Containers(Coco) on Arm CCA

Next steps

- ❑ Enablement ongoing in 2023
- ❑ RSS firmware (HES) – feature complete
- ❑ TF-A EL3 firmware

Refactoring 4-world RAS handling and context management code, improved CPU feature mgmt

- ❑ TF-A boot firmware

Enabling Trusted/Measured Boot with RSS, more dynamic CoT, security hardening

- ❑ TF-RMM

Enabling CPU features in realms, e.g. PMU, PAuth, self-hosted debug, SVE

- ❑ Kernel

Handling invasive stage-2 changes in RMM BET1 spec

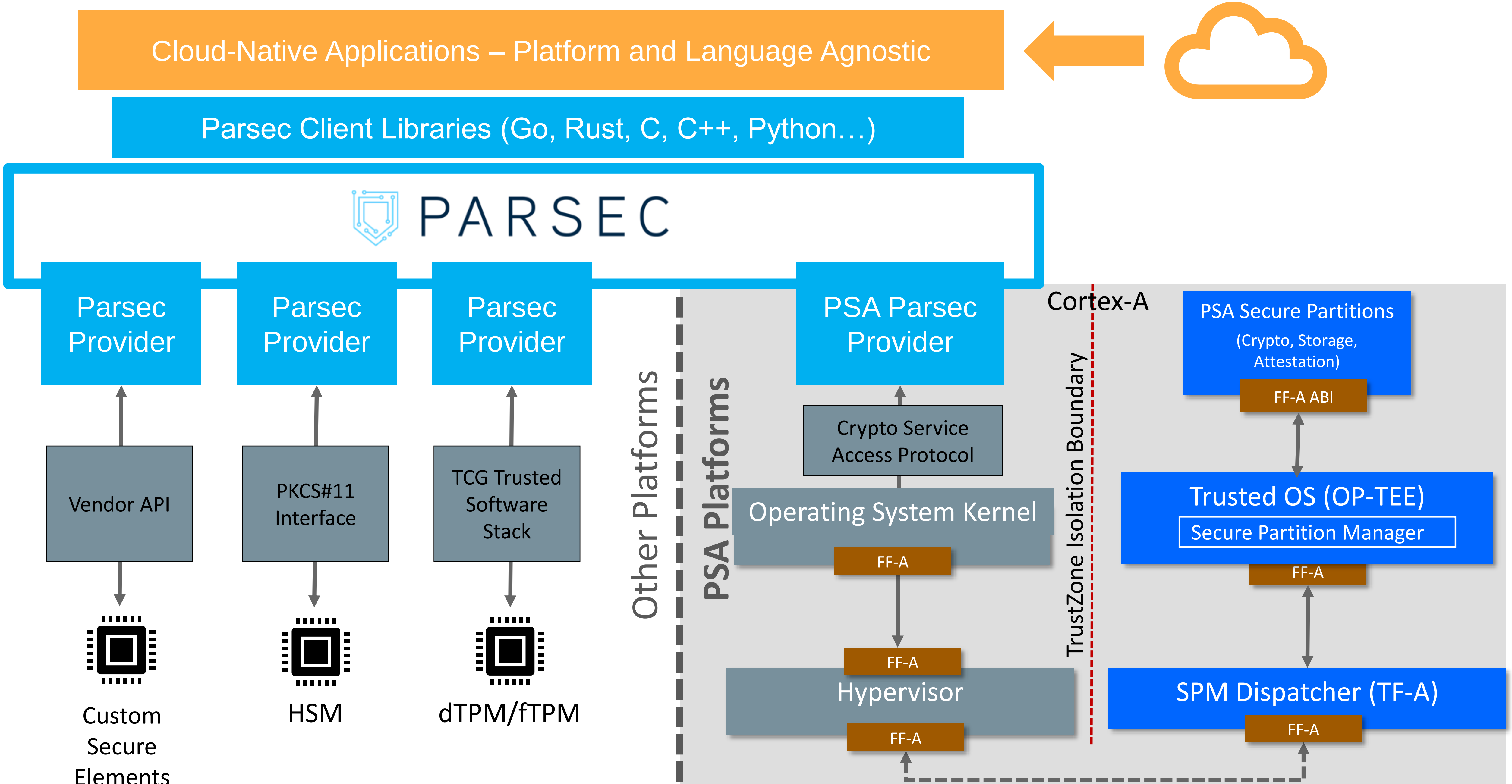
Post RMM v1.0 feature prototyping

- ❑ In-realm firmware

Continued upstreaming | Remote Attestation Proto work

Where possible, standardizing and aligning with other CC architectures

PARSEC and Trusted Services



Cloud-Native Applications – Platform and Language Agnostic

Parsec Client Libraries (Go, Rust, C, C++, Python…)

PARSEC

Parsec Provider

Parsec Provider

Parsec Provider

PSA Parsec Provider

Vendor API

PKCS#11 Interface

TCG Trusted Software Stack

Custom Secure Elements

HSM

dTPM/fTPM

Other Platforms

PSA Platforms

Crypto Service Access Protocol

Operating System Kernel

FF-A

FF-A

Hypervisor

FF-A

Cortex-A

TrustZone Isolation Boundary

PSA Secure Partitions

(Crypto, Storage, Attestation)

FF-A ABI

Trusted OS (OP-TEE)

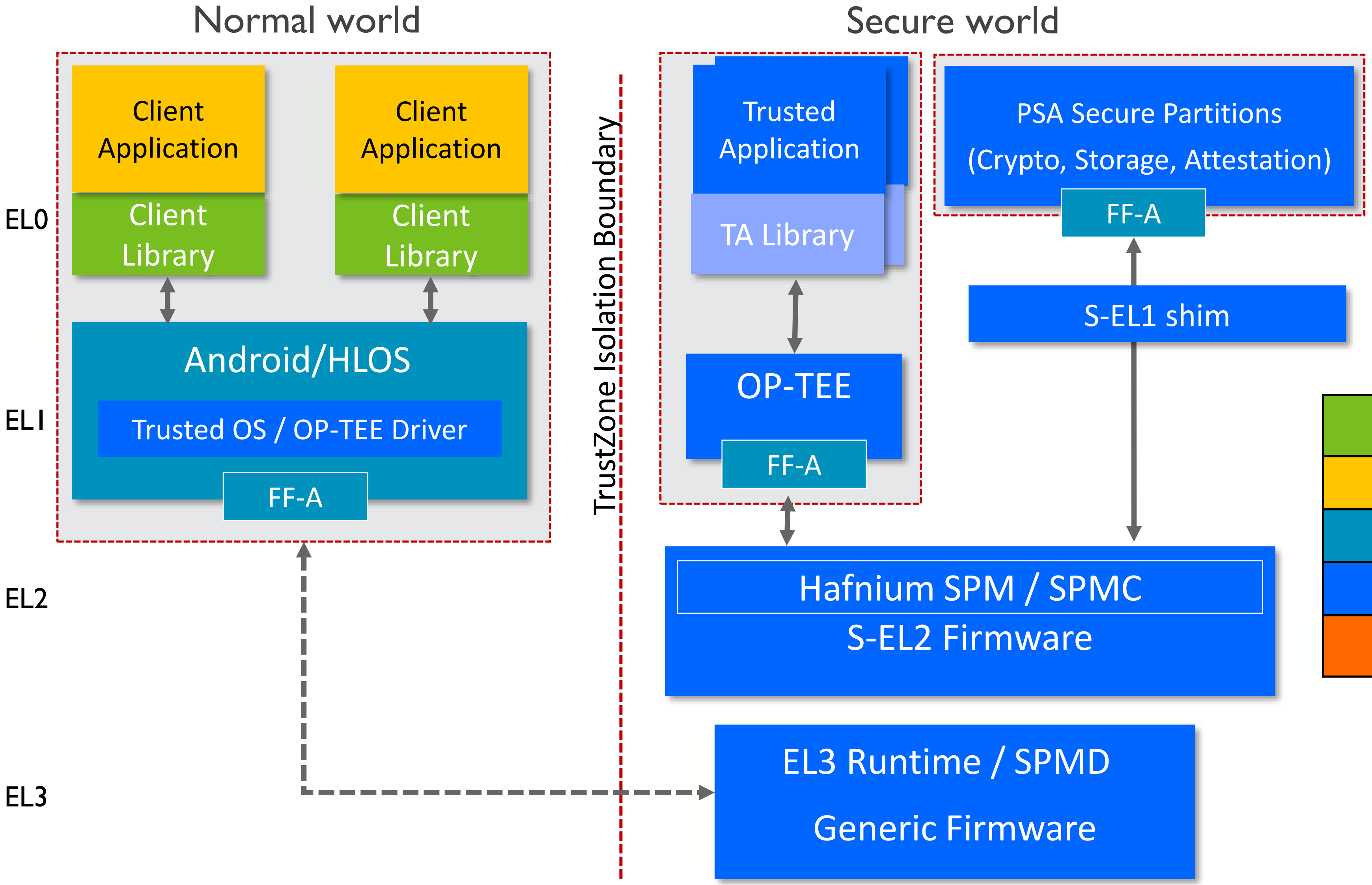
Secure Partition Manager

FF-A

SPM Dispatcher (TF-A)

FF-A

Trusted Services on Armv8.4/Secure EL2



Normal world

Secure world

EL0

EL1

EL2

EL3

Client Application

Client Library

Client Application

Client Library

Android/HLOS

Trusted OS / OP-TEE Driver

FF-A

TrustZone Isolation Boundary

Trusted Application

TA Library

OP-TEE

FF-A

PSA Secure Partitions (Crypto, Storage, Attestation)

FF-A

S-EL1 shim

Hafnium SPM / SPMC

S-EL2 Firmware

EL3 Runtime / SPMD

Generic Firmware

🟩	Application trusted OS specific
🟨	Application provider specific
🟦	Generic software
🟦	TrustedFirmware.org
🟧	Silicon Vendor specific software