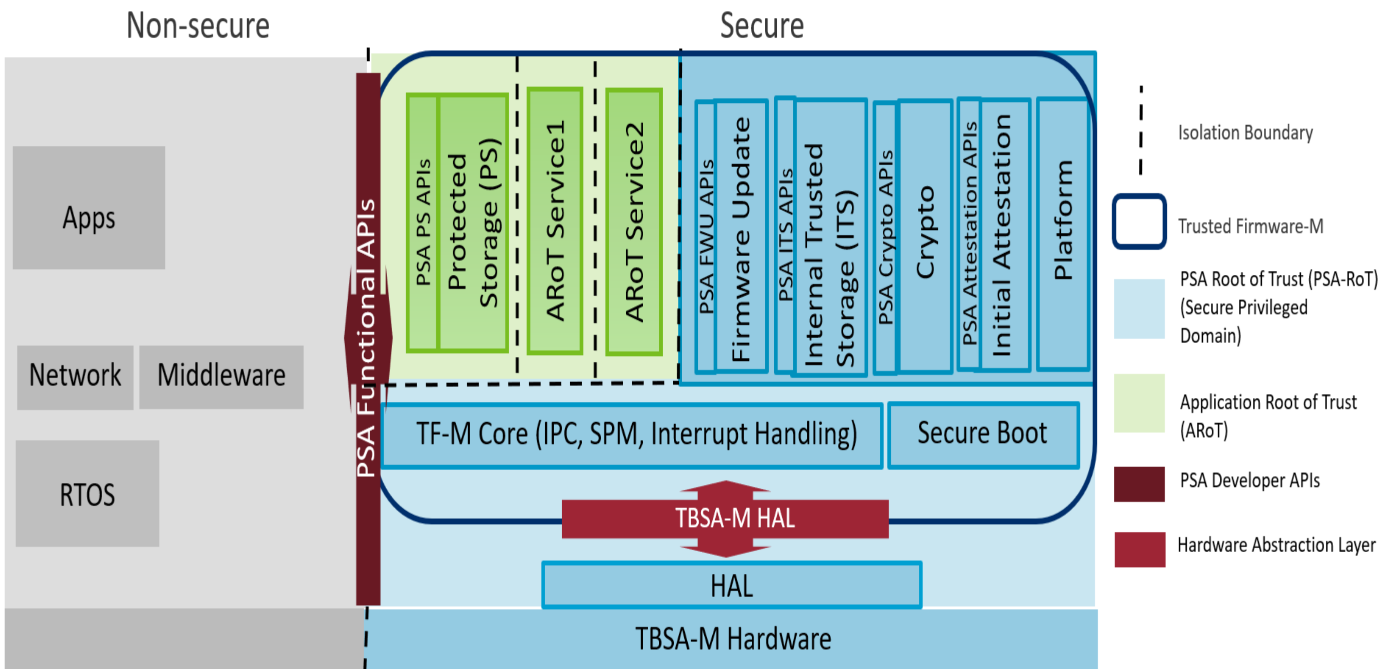
Trusted Firmware-M Roadmap Update

Shebu V. Kuriakose

Oct’22

Trusted Firmware-M v1.6

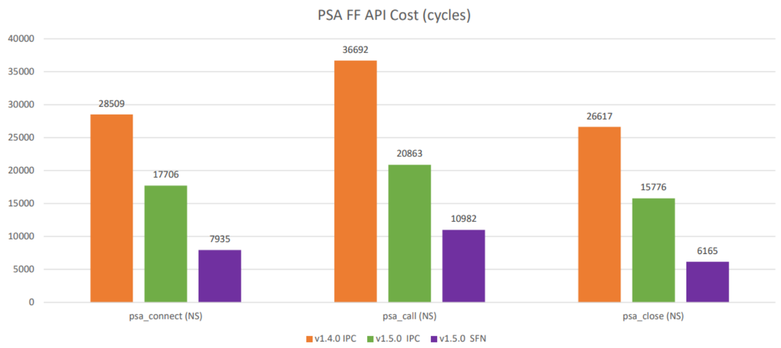
- PSA Crypto API (Mbed TLS 3.1)
- Firmware Framework v1.1
  - SFN, Stateless services, MMIOVEC, FLIH
- Documentation Improvements
- PSA Crypto Driver interface for Cryptocell
- Floating Point
- Corstone-300 (Cortex-M55),Corstone-310 (Cortex-M85) & Corstone-1000 (A35+Secure Enclave)



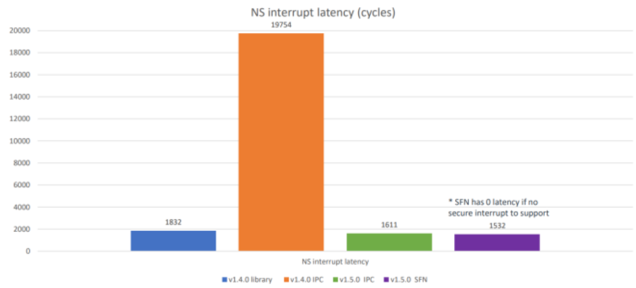
Optimizations

- Performance (2021)
  - Firmware Framework-M API
  - Non-Secure Interrupt Latency

PSA FF API Cost

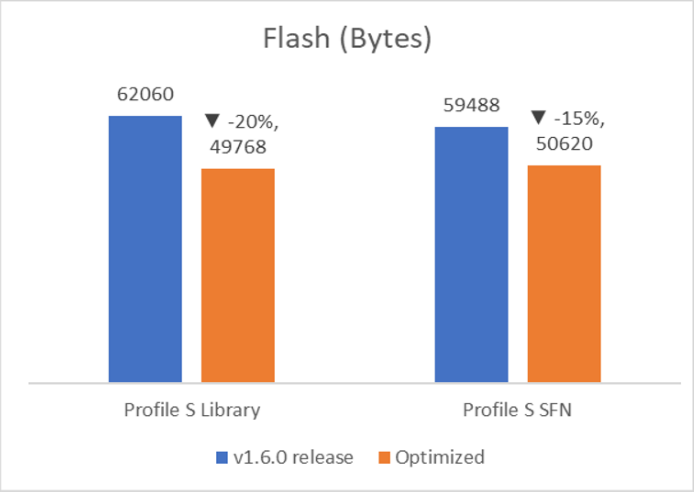


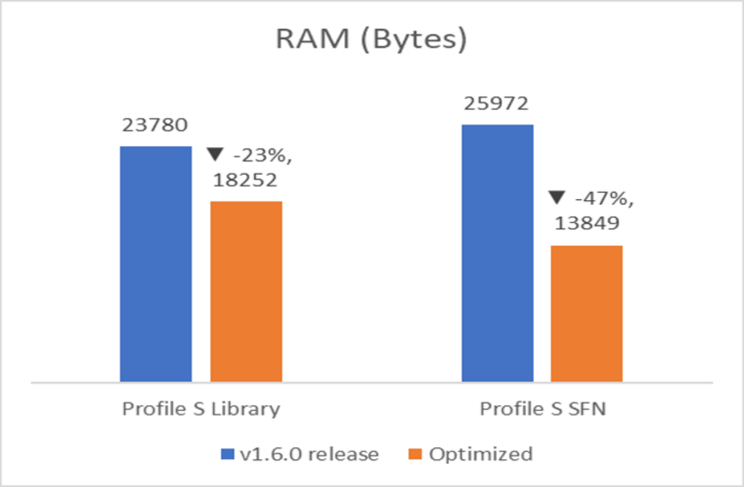
Non-Secure Interrupt Latency



- Memory (CQ2’22)
  - Initial Focus – Profile Small, SFN Mode

Based on software crypto (Mbed TLS)

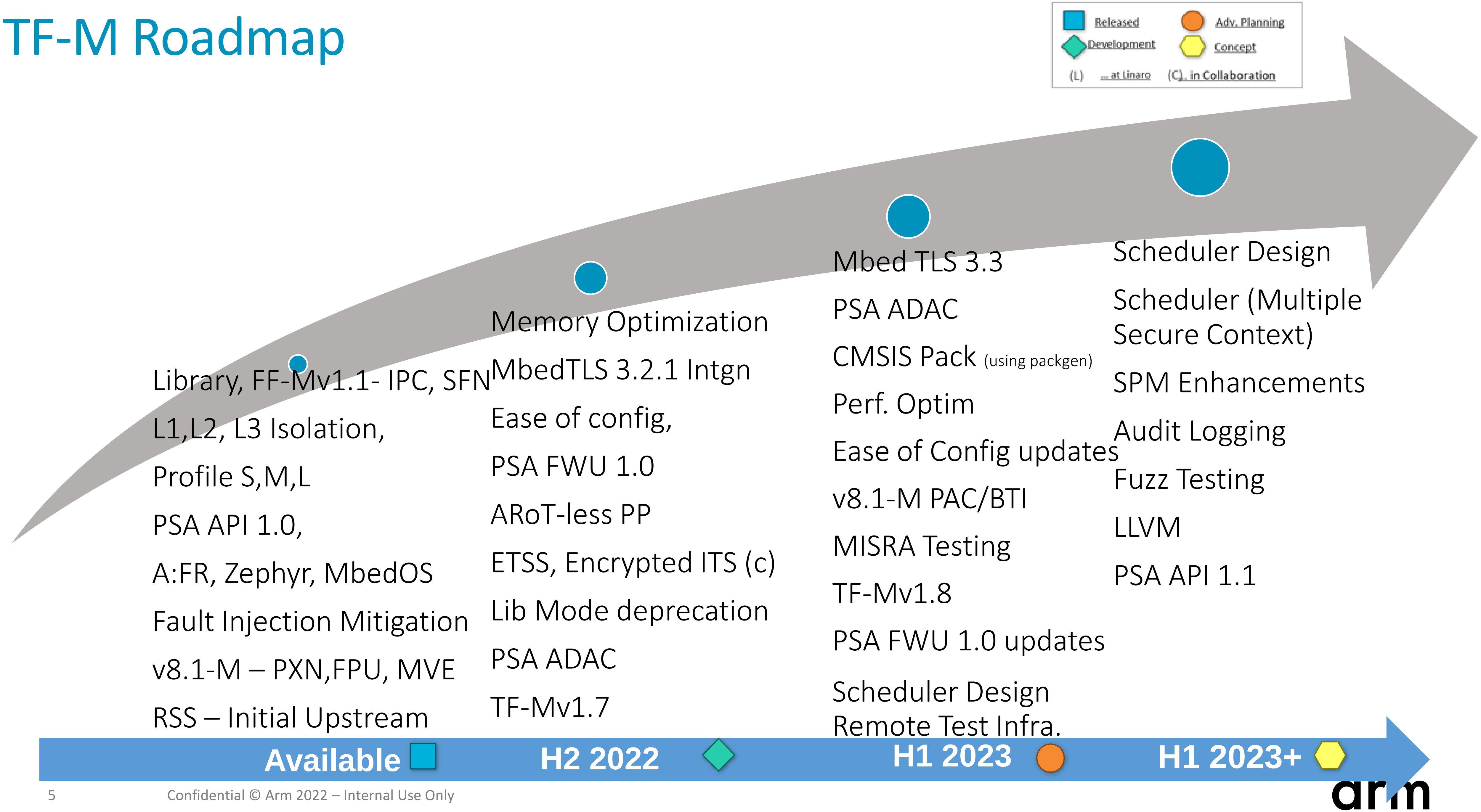




What’s coming in Trusted Firmware-M v1.7

- Change Default Config
  - Change to include SPM, Platform code only.
  - Profile Small, Medium and Large remain unchanged as reference & test profiles
- Remove Library Model
  - SFN and IPC defined in PSA FF-M will be the supported modes
- Introduce PSA L2 ARoT-less Protection Profile
  - New reference profile aligning with the new PSA certified protection profile
- Change/Simplify Configuration Mechanism
- Align with PSA FWU API 1.0
- Update Mbed TLS & mcuboot versions

TF-M Roadmap



🟦 Released
🔶 Development
🟠 Adv. Planning
⬡ Concept
(L) ...at Linaro
(C)... in Collaboration

Library, FF-Mv1.1- IPC, SFN

L1,L2, L3 Isolation,

Profile S,M,L

PSA API 1.0,

A:FR, Zephyr, MbedOS

Fault Injection Mitigation

v8.1-M – PXN,FPU, MVE

RSS – Initial Upstream

Memory Optimization

MbedTLS 3.2.1 Intgn

Ease of config,

PSA FWU 1.0

ARoT-less PP

ETSS, Encrypted ITS (c)

Lib Mode deprecation

PSA ADAC

TF-Mv1.7

Mbed TLS 3.3

PSA ADAC

CMSIS Pack (using packgen)

Perf. Optim

Ease of Config updates

v8.1-M PAC/BTI

MISRA Testing

TF-Mv1.8

PSA FWU 1.0 updates

Scheduler Design
Remote Test Infra.

Scheduler Design

Scheduler (Multiple Secure Context)

SPM Enhancements

Audit Logging

Fuzz Testing

LLVM

PSA API 1.1

Available 🟦 **H2 2022** 🔶 **H1 2023** 🟠 **H1 2023+** ⬡

Thank You

Danke

Gracias

Grazie

谢谢

ありがとう

Asante

Merci

감사합니다

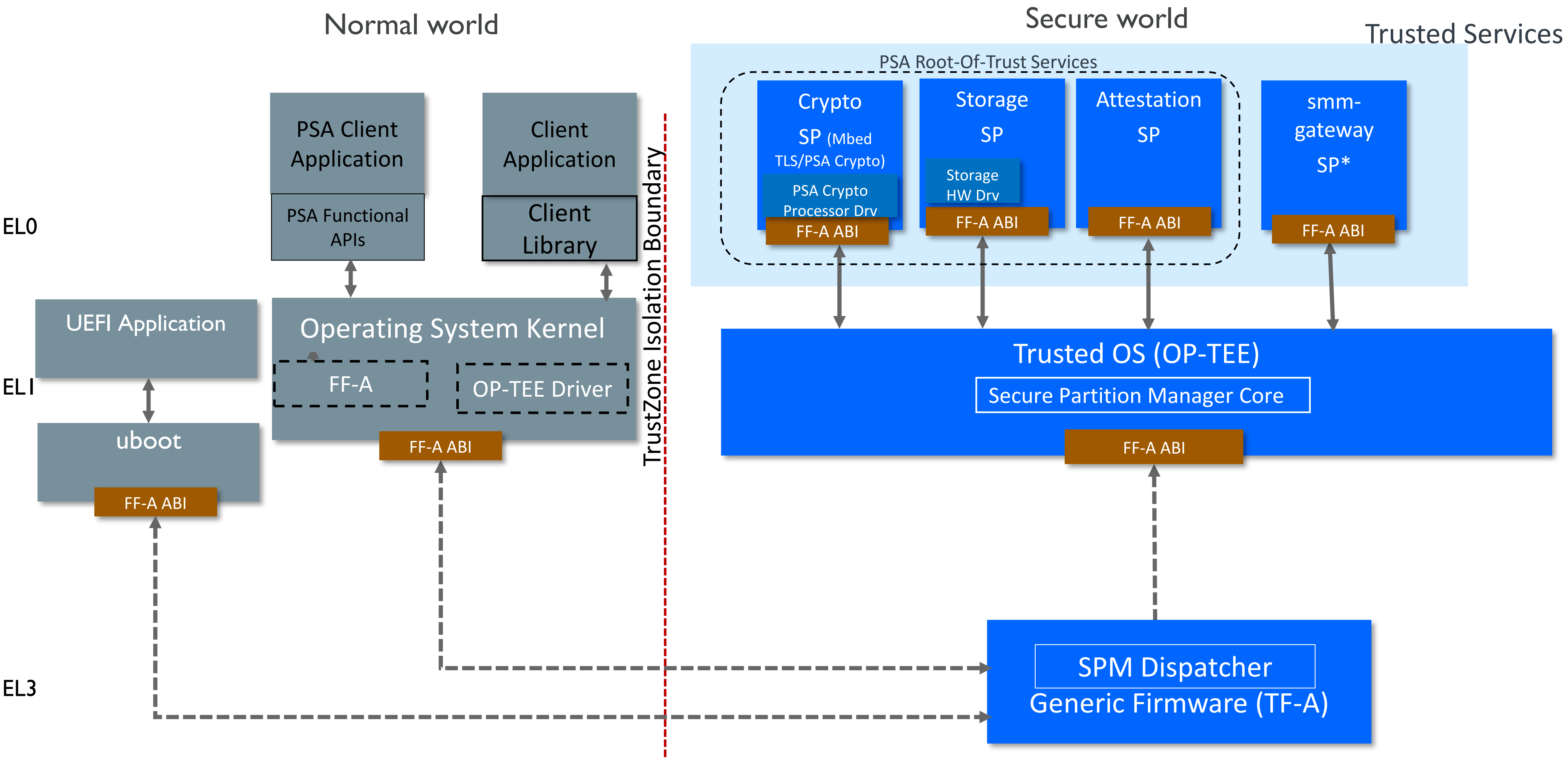
धन्यवाद

Kiitos

شكرًا

ধন্যবাদ

תודה



Normal world

Secure world

Trusted Services

PSA Root-Of-Trust Services

EL0

EL1

EL3

PSA Client Application

PSA Functional APIs

Client Application

Client Library

UEFI Application

uboot

FF-A ABI

Operating System Kernel

FF-A

OP-TEE Driver

FF-A ABI

TrustZone Isolation Boundary

Crypto SP (Mbed TLS/PSA Crypto)

PSA Crypto Processor Drv

FF-A ABI

Storage SP

Storage HW Drv

FF-A ABI

Attestation SP

FF-A ABI

smm-gateway SP*

FF-A ABI

Trusted OS (OP-TEE)

Secure Partition Manager Core

FF-A ABI

SPM Dispatcher

Generic Firmware (TF-A)

* Also possible to run StMM as a SEL0 SP

Mbed TLS, PSA Crypto

Trusted Firmware-M

Recent Highlights

- Mbed TLS 3.2.1 release with full PSA Crypto API support, TLS/X.509 Using PSA enhancements and TLS1.3.
- Open Test System
- PSA Crypto driver interfaces implemented for Cryptocell-312
- Collaboration on TLS/X.509 using PSA Crypto APIs

Ongoing Work

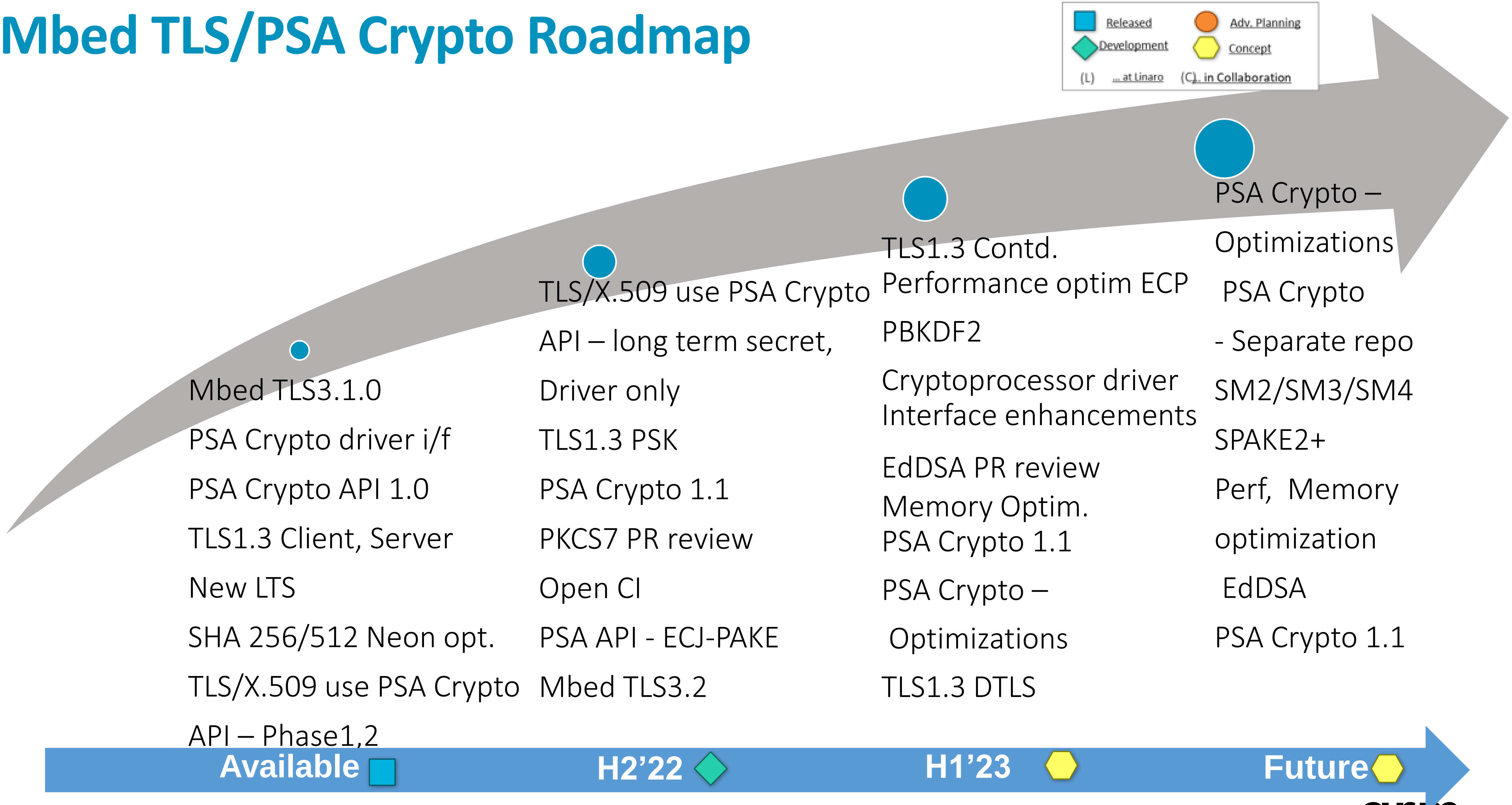
TLS/X.509 using PSA Crypto APIs fully

TLS1.3 – Beyond MVP

Performance Optimizations

Open CI

Mbed TLS/PSA Crypto Roadmap



▢ Released ◆ Development ● Adv. Planning ⬡ Concept

(L) ...at Linaro (C)... In Collaboration

Mbed TLS3.1.0
PSA Crypto driver i/f
PSA Crypto API 1.0
TLS1.3 Client, Server
New LTS
SHA 256/512 Neon opt.
TLS/X.509 use PSA Crypto API – Phase1,2

TLS/X.509 use PSA Crypto API – long term secret, Driver only
TLS1.3 PSK
PSA Crypto 1.1
PKCS7 PR review
Open CI
PSA API - ECJ-PAKE
Mbed TLS3.2

TLS1.3 Contd.
Performance optim ECP
PBKDF2
Cryptoprocessor driver Interface enhancements
EdDSA PR review
Memory Optim.
PSA Crypto 1.1
PSA Crypto – Optimizations
TLS1.3 DTLS

PSA Crypto – Optimizations
PSA Crypto - Separate repo
SM2/SM3/SM4
SPAKE2+
Perf, Memory optimization
EdDSA
PSA Crypto 1.1

Trusted Services

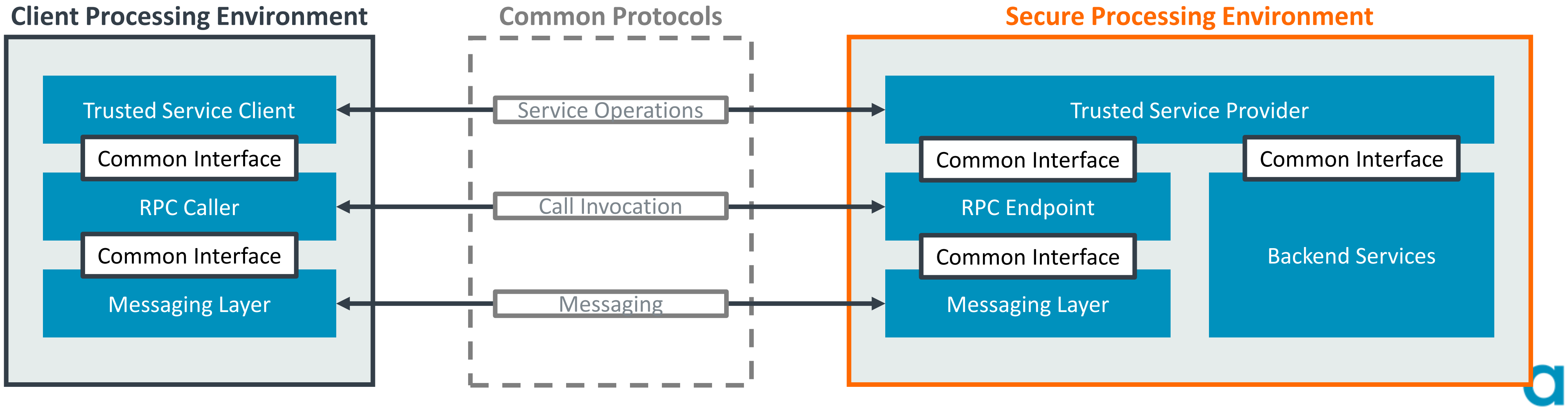
Trusted Services

- Project to develop and deploy device root-of-trust services for A-profile devices
  - Deployable over a range of Isolated Processing Environment (TEE)
  - Works with other Trusted Firmware projects – TF-A, OP-TEE.

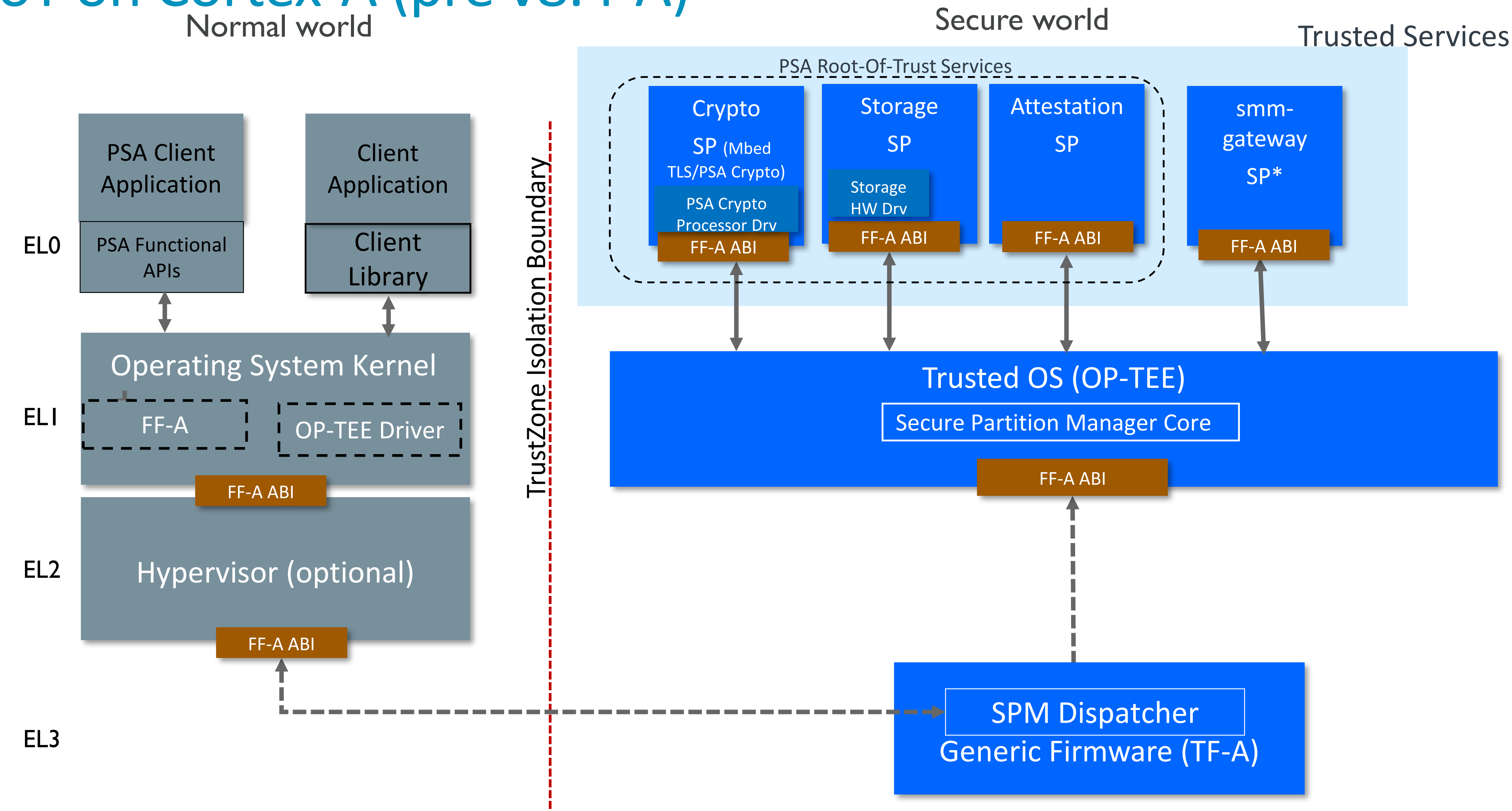
- Applications use Trusted Services for Security Operations using client/server model

- Reference implementation uses **Secure Partition Manager Core** (SPMC) in OP-TEE to manage a set of **secure partitions** running at S-EL0. Firmware Framework-A used as transport layer.

- Secure Partitions host PSA Services exposing PSA Functional APIs providing PSA RoT for Cortex-A devices.
  - Enables Cortex-A devices to meet PSA certification requirements



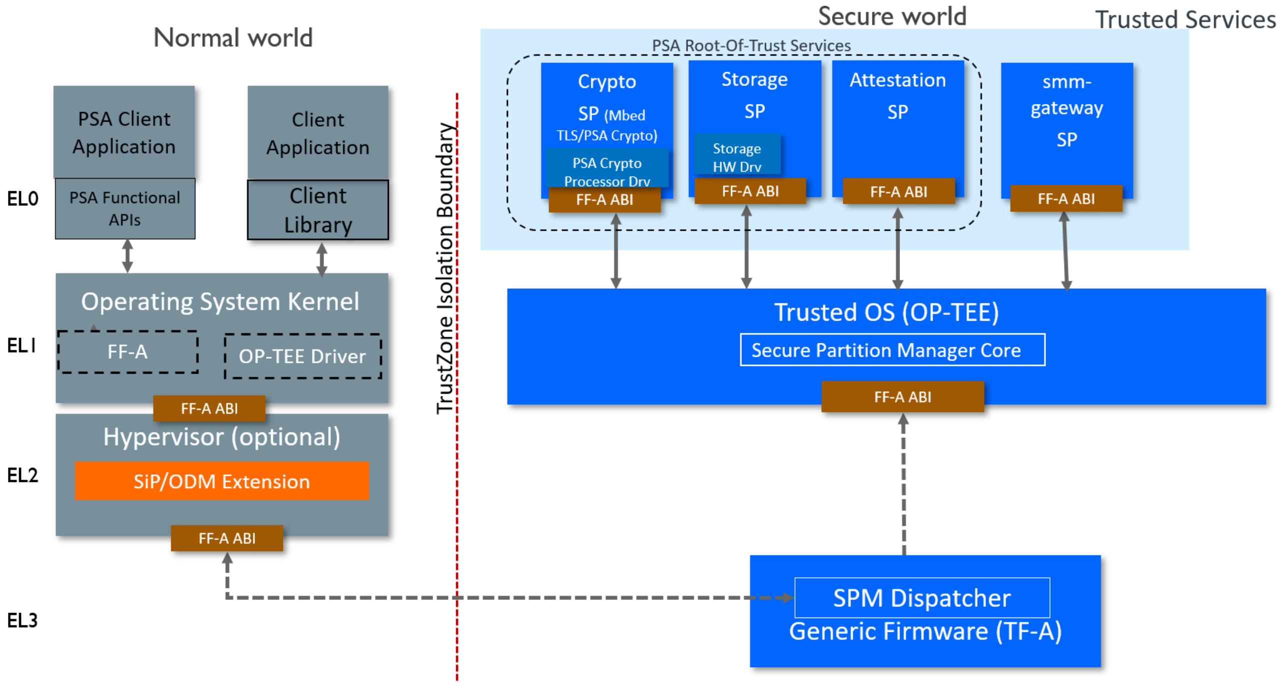
PSA RoT on Cortex-A (pre v8.4-A)



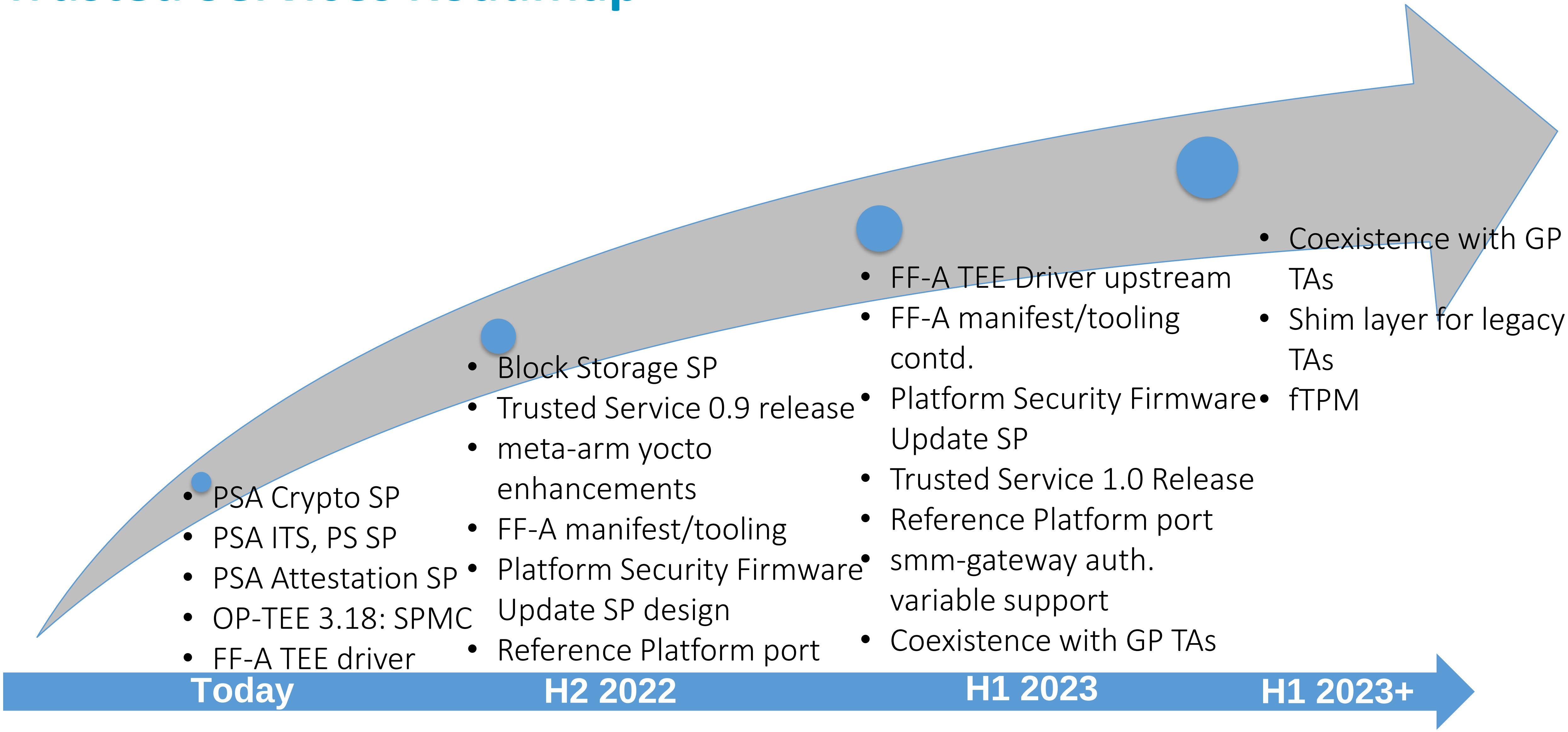
* Also possible to run StMM as a SEL0 SP

Recent Highlights

- SPMC support available in OP-TEE 3.17/3.18
  - PSA SPs can be run as S-EL0 SPs
- TEE FF-A driver exposing FF-A ABIs to userspace under review in lkml
- PSA SPs pass the PSA Functional APIs compliance tests
- Trusted Services starting to get ported on Cortex-A platforms inc. Arm reference platforms



Trusted Services Roadmap



Today

- PSA Crypto SP
- PSA ITS, PS SP
- PSA Attestation SP
- OP-TEE 3.18: SPMC
- FF-A TEE driver

H2 2022

- Block Storage SP
- Trusted Service 0.9 release
- meta-arm yocto enhancements
- FF-A manifest/tooling
- Platform Security Firmware Update SP design
- Reference Platform port

H1 2023

- FF-A TEE Driver upstream
- FF-A manifest/tooling contd.
- Platform Security Firmware Update SP
- Trusted Service 1.0 Release
- Reference Platform port
- smm-gateway auth. variable support
- Coexistence with GP TAs

H1 2023+

- Coexistence with GP TAs
- Shim layer for legacy TAs
- fTPM