Trusted Firmware-M Update

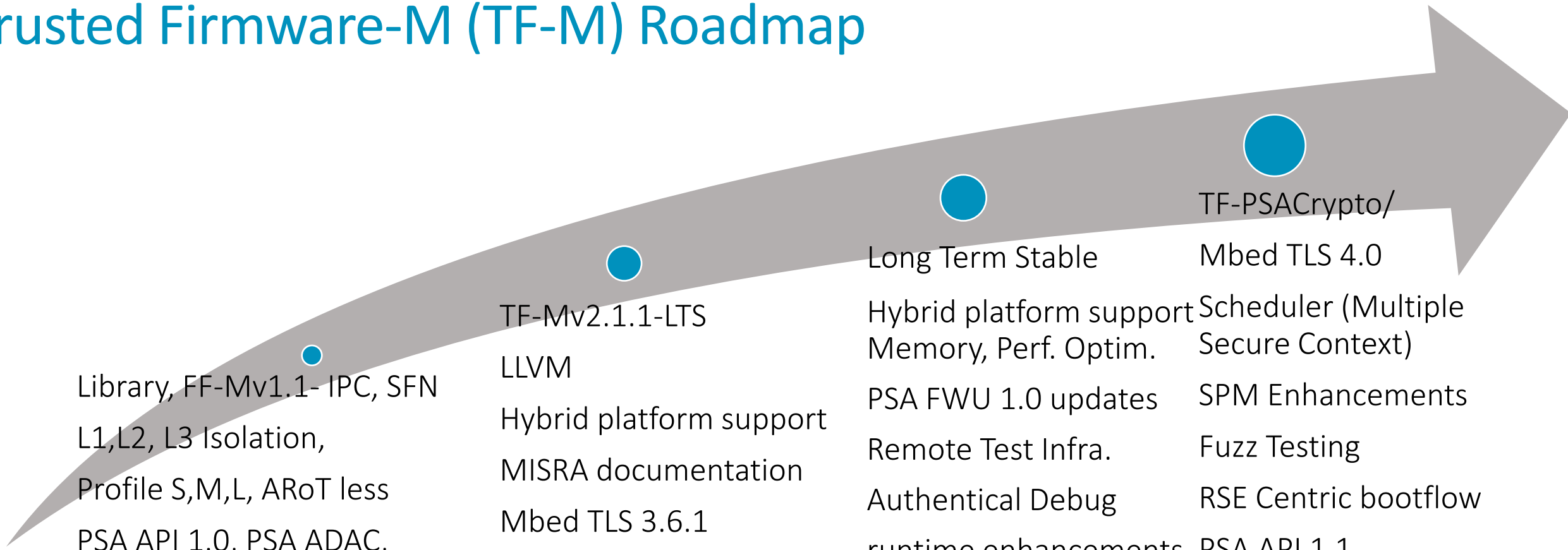
Shebu V. Kuriakose

Sept’24

Trusted Firmware-M Updates

- TF-M v2.1.0 released
  - First TF-M LTS release. Plan to maintain for 3 years with bug fixes, security fixes
  - Includes Mbed TLS 3.6.0 LTS
  - Aligns to the same PSA Crypto header as Mbed TLS
  - Initial Hybrid platform (A-profile + M-profile or M-profile + M-profile) support.
- TF-M v2.1.1 LTS will be submitted to PSA L2 evaluation in CQ4'24
  - Followed by delta evaluation for security and bug fixes
  - Allows platforms getting PSA certified on LTS branch to reuse the delta evaluation to keep certification upto date
- v8.1-M PAC/BTI enabled
- Work continues on Hybrid platform and Remote test infrastructure
- Enhancement for Runtime Security Engine (RSE)
  - DICE DPE, measured boot, ADAC runtime, Boot ROM

Trusted Firmware-M (TF-M) Roadmap



Library, FF-Mv1.1- IPC, SFN

L1,L2, L3 Isolation,

Profile S,M,L, ARoT less

PSA API 1.0, PSA ADAC,

A:FR, Zephyr, MbedOS

Fault Injection Mitigation

v8.1-M – PXN,FPU, MVE, PAC/BTI

Cryptocell driver refactoring

TF-Mv2.1.1-LTS

LLVM

Hybrid platform support

MISRA documentation

Mbed TLS 3.6.1

Upstream t_cose

Long Term Stable

Hybrid platform support Memory, Perf. Optim.

PSA FWU 1.0 updates

Remote Test Infra.

Authentical Debug

runtime enhancements

Image encryption via. PSA Crypto in mcuboot

TF-PSACrypto/

Mbed TLS 4.0

Scheduler (Multiple Secure Context)

SPM Enhancements

Fuzz Testing

RSE Centric bootflow

PSA API 1.1

Available | **H2 2024** | **H1 2025** | **H1 2025+**

Thank You!
Danke!
Merci!
谢谢!
ありがとう!
Gracias!
Kiitos!