

arm



Trusted Firmware-M Roadmap Update

Apr'23

© 2023 Arm

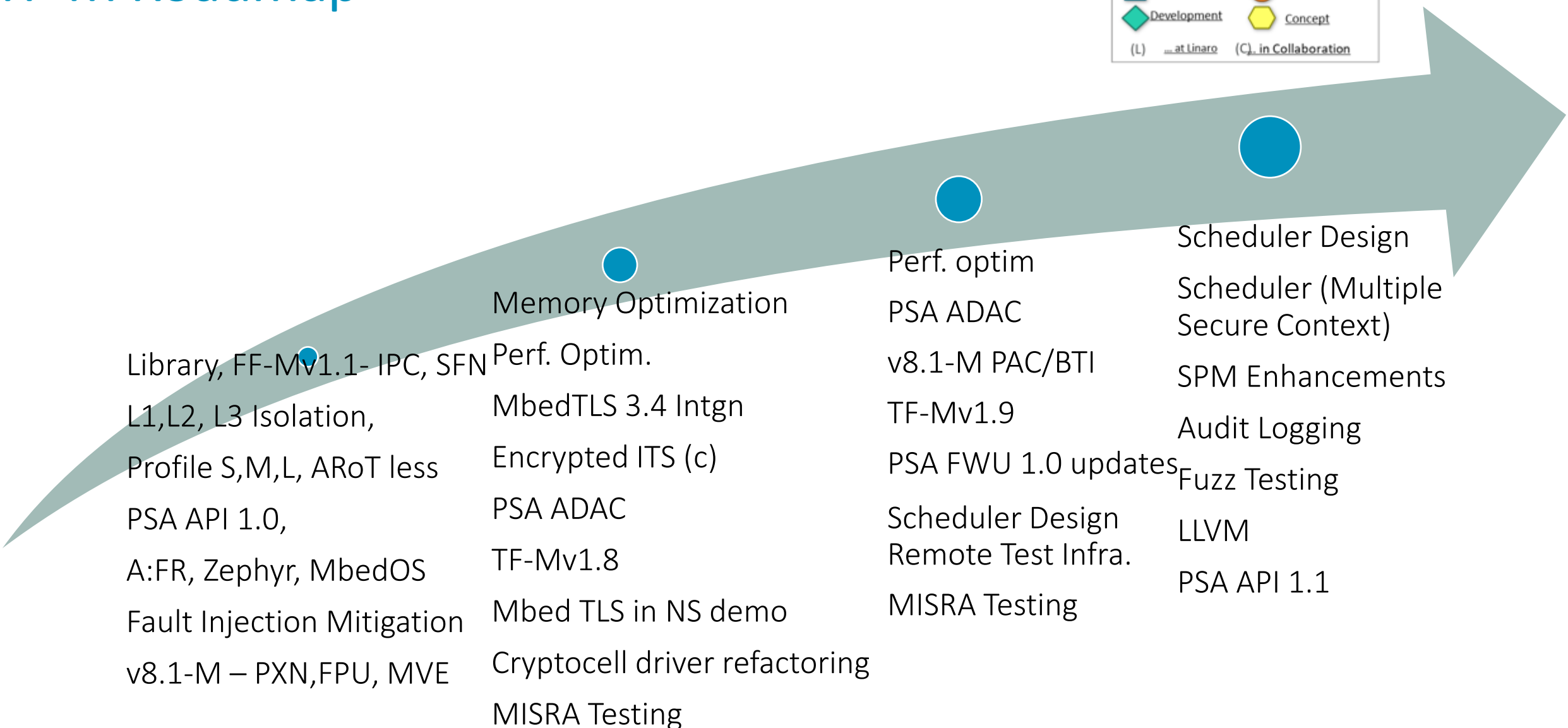
Trusted Firmware-M v1.8 Coming...

- + eRPC Test framework
- + Improvements to crypto library abstractions & integration with Mbed TLS/Mbed Crypto
- + Kconfig enhancements
- + PSA ADAC on MuscaB1
- + Upstream QCBOR
- + MCUboot v1.10
- + Mbed TLS 3.4

CQ2'23 Priorities

- + TF-M v1.8 release
- + Memory Optimization – SPM, Secure Storage and Attestation Services
- + Performance Improvements
- + Build System improvements
- + MISRA tool integration
- + Example integration of Mbed TLS in Non-Secure using PSA Crypto APIs in TF-M
- + GitHub Mirroring

TF-M Roadmap



Library, FF-Mv1.1- IPC, SFN
 L1,L2, L3 Isolation,
 Profile S,M,L, ARoT less
 PSA API 1.0,
 A:FR, Zephyr, MbedOS
 Fault Injection Mitigation
 v8.1-M – PXN,FPU, MVE

Memory Optimization
 Perf. Optim.
 MbedTLS 3.4 Intgn
 Encrypted ITS (c)
 PSA ADAC
 TF-Mv1.8
 Mbed TLS in NS demo
 Cryptocell driver refactoring
 MISRA Testing

Perf. optim
 PSA ADAC
 v8.1-M PAC/BTI
 TF-Mv1.9
 PSA FWU 1.0 updates
 Scheduler Design
 Remote Test Infra.
 MISRA Testing

Scheduler Design
 Scheduler (Multiple
 Secure Context)
 SPM Enhancements
 Audit Logging
 Fuzz Testing
 LLVM
 PSA API 1.1



Trusted Firmware Sessions @ Linaro Connect

- [LHR23-118-Trusted Firmware community project update](#) (inc. Celebrating 5 Years of TF-M)
 - **Wednesday**, Apr 26th 2.45pm-3.10pm
- [LHR23-120-Trusted Firmware \(TF-RMM\) Hacking Session](#)
 - **Wednesday**, April 26th 3:15pm - 3:40pm
- [LHR23-304-Runtime Security Subsystem \(Arm CCA HES\) – An overview](#)
 - **Friday**, April 28th 10:20am – 10:45am
- [LHR23-311 Arm CCA Open-source enablement](#)
 - **Friday**, April 28th 11:20am – 11:45am
- [LHR23-309 Exploring AIoT security solutions on high performance MCU](#)
 - **Friday**, April 28th 11:20am – 11:45am

arm

Thank You

Danke

Gracias

Grazie

谢谢

ありがとう

Asante

Merci

감사합니다

धन्यवाद

Kiitos

شكرًا

ধন্যবাদ

תודה