Trusted Firmware-M Update

Shebu V. Kuriakose

Jan’24

TF-M Update

- TF-M v2.0.0 and what’s coming
- Latest on TF-M LTS release
- Roadmap

TF-M v2.0.0 and what's coming

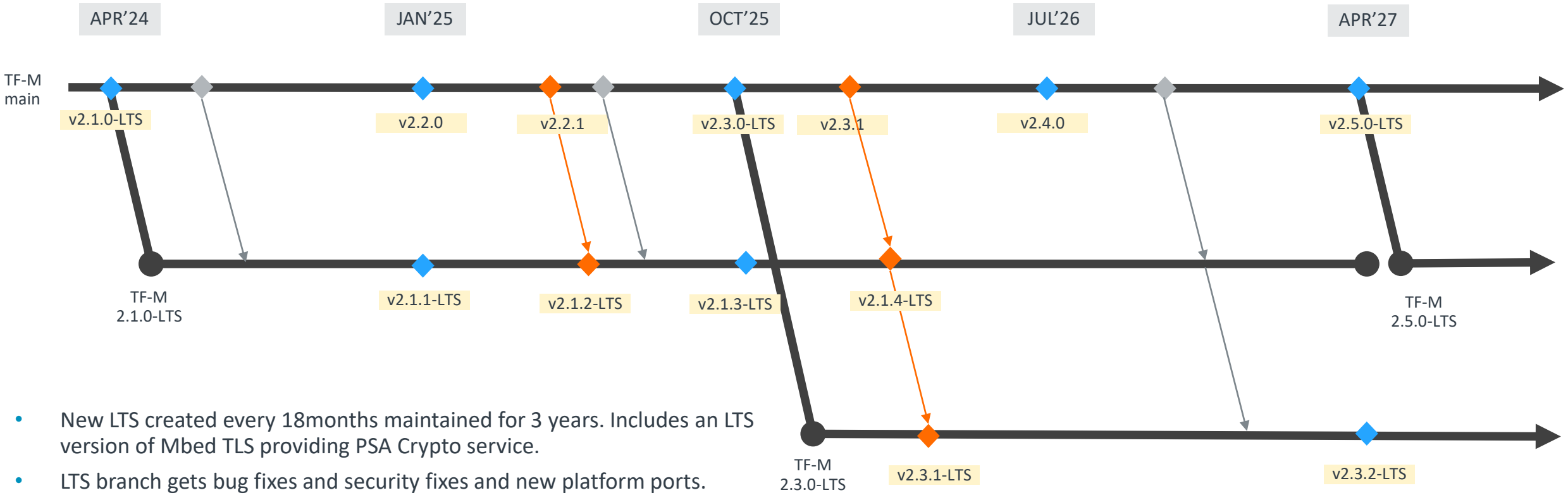
- v2.0.0 (Blog: https://www.trustedfirmware.org/blog/tf-m-v2-0-0)
  - 14k code size reduction by using an alternative ECC implementation in Mbed TLS
  - Moving from single build process to separate independent Non-Secure and Secure build
  - New mailbox Non-secure agent API for dual core and Hybrid platforms
  - Non-secure interrupt latency improvements for isolation level > 1
- Long Term Stable Releases
  - To make it easier for chip to update PSA Cert. with latest TF-M
  - Aligning with Mbed TLS LTS release
  - Feeding into RTOS LTSes
- RoT for Hybrid Platforms (e.g. Cortex-A/M + Cortex-M)
  - Providing Secure Services for multiple clients (on-core and off-core) on the SoC
  - Worked on Solution1, new engineers ramping up for further work due to team changes
- Demonstrate Key Usecases
  - TLS connection relying on PSA Crypto Service
- MISRA Testing
  - Enabled through Trusted Firmware.org Open CI

PSA Certified & TF-M Long Term Stable (LTS)

- Today chips are PSA Certified using a particular version of TF-M (PSA Updatable RoT)
  - No efficient way to update PSA certificate with future TF-M versions – Expensive & time consuming.
  - Certificate can be invalid once vulnerabilities found in TF-M

- TF-M LTS enables an efficient way to update PSA Certification of chips with latest TF-M security and bug fixes.
  - Chips are certified using a TF-M LTS release. Chips then update to future LTS updates after updates go through PSA Security evaluation
  - Certificate can be kept valid and latest TF-M shipped in chip vendor SDKs
  - End devices using the chips able to use latest TF-M that is PSA Certified.
- New LTS release created every 18 months and maintained for 3 years. During 3years of an LTS,
  - 9-monthly bug fix LTS update releases alongside the 9-monthly mainline releases
  - Ad hoc security fix releases
- Platform independent TF-M fixes are evaluated once & applicable to PSA Certified chips on the LTS release.
  - Platform specific changes would require chip specific evaluation.
- PSA Certification process to support LTS evaluation under review with Trust CB.

3 Year LTS; Created every 18months; Released every 9 months

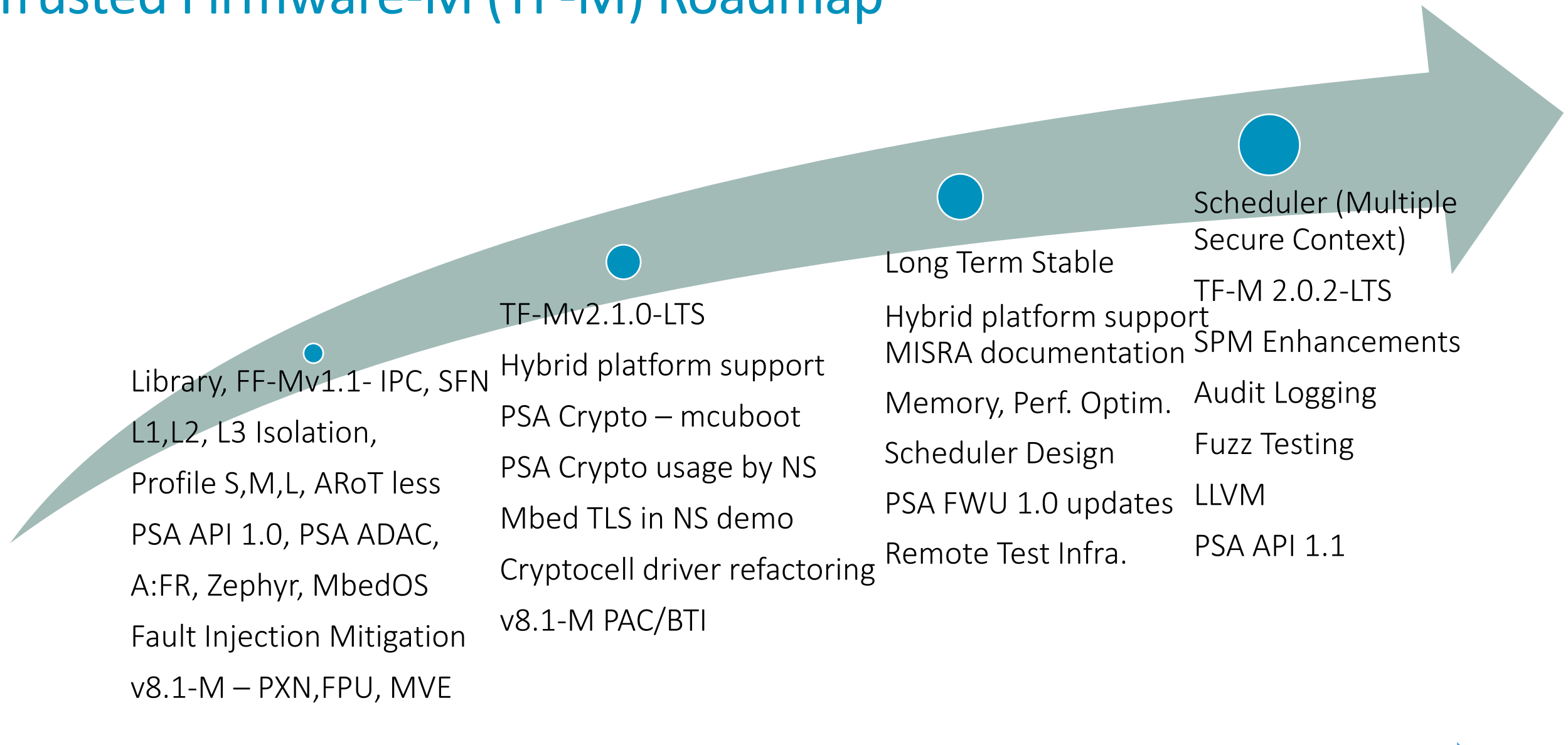


- New LTS created every 18months maintained for 3 years. Includes an LTS version of Mbed TLS providing PSA Crypto service.
- LTS branch gets bug fixes and security fixes and new platform ports.
- Mbed TLS/PSA Crypto LTS release updates gets integrated to TF-M LTS release
- Adhoc TF-M, Mbed TLS/PSA Crypto release to fix security issues
- TF-M 9-monthly LTS update releases alongside 9-monthly mainline releases
- Changes in every TF-M release go through PSA Cert. evaluation by Lab

Bug fixes, errata, new platform (no release)
9-monthly release
Adhoc security fix release
Versions are for illustration purpose only

arm

Trusted Firmware-M (TF-M) Roadmap



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