Trusted Firmware-M LTS & PSA Certified

Shebu V. Kuriakose

September 2023

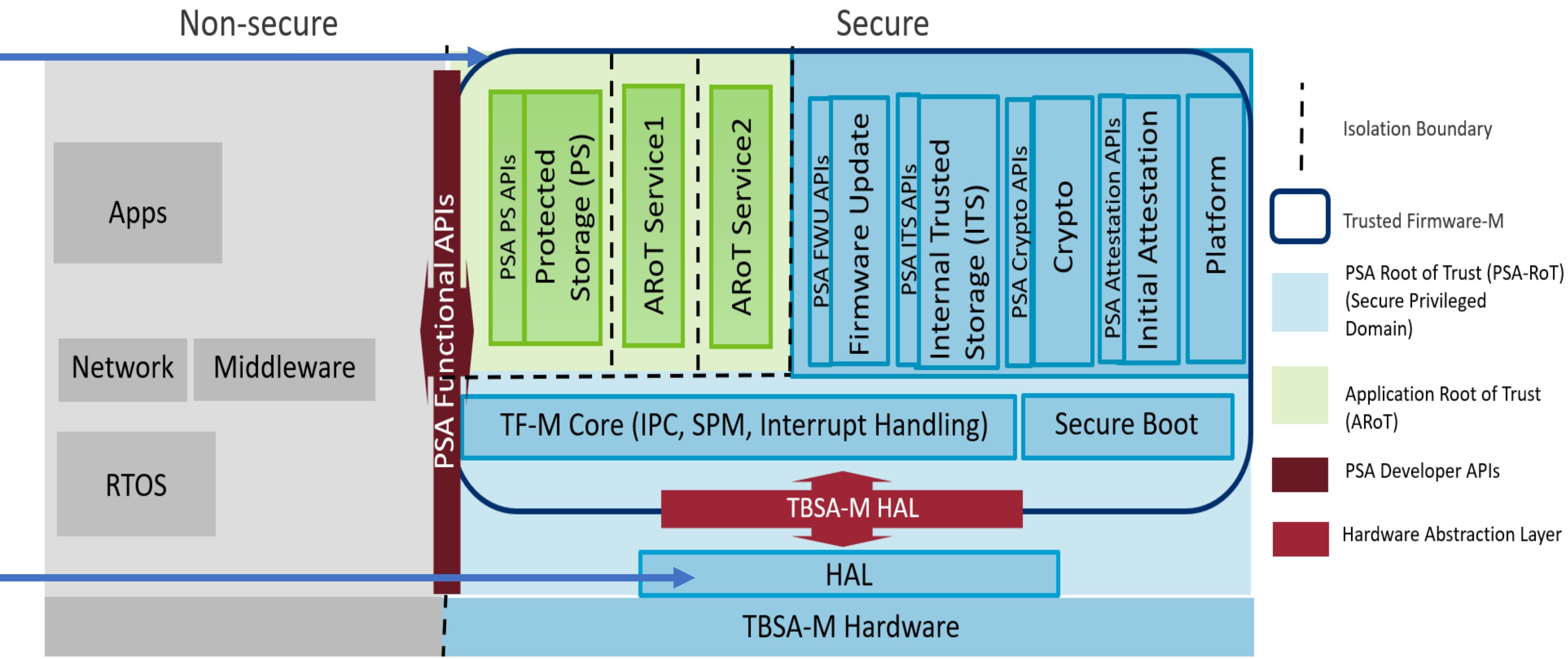
PSA Certified & TF-M Long Term Stable (LTS)

- 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,
  - 6-monthly bug fix update 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.

Trusted Firmware-M LTS – Generic & Platform Specific Changes

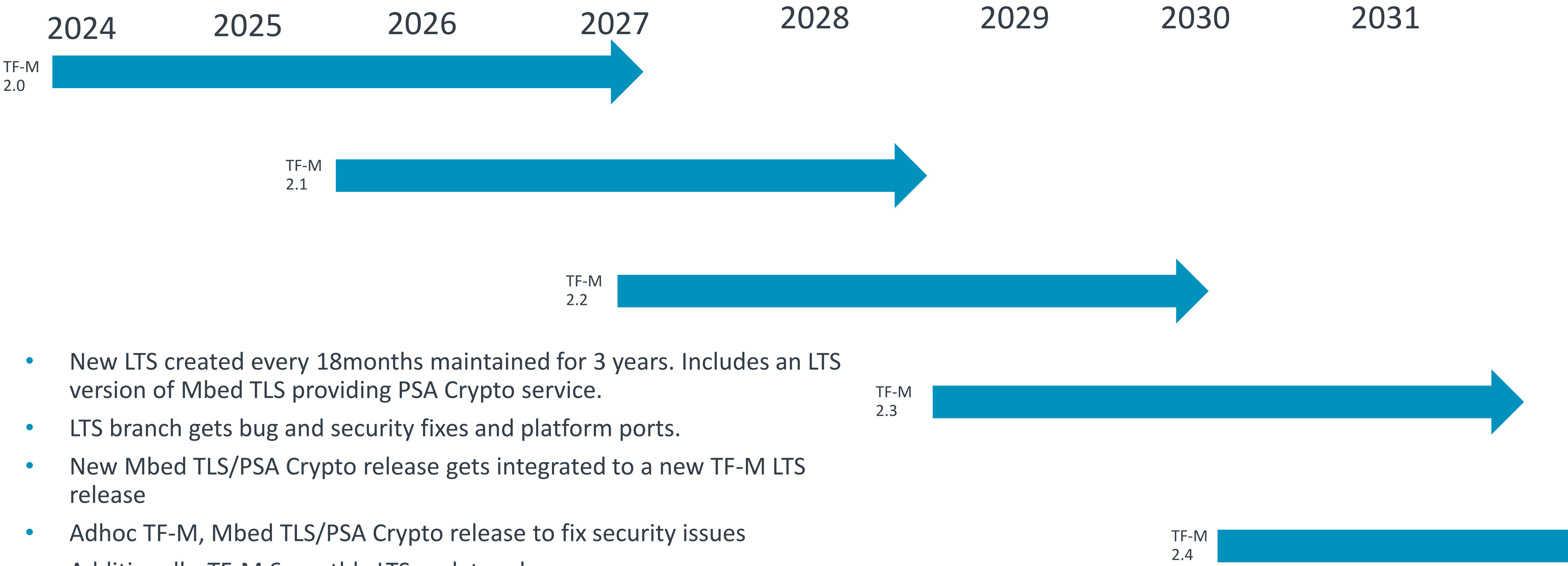
How the security evaluation happens?

- Platform independent TF-M fixes in LTS release evaluated once by Lab. and applicable to all PSA Certified chips based on the LTS release.
- Trustedfirmware.org & Arm will work with Lab and TrustCB to evaluate changes between LTS releases
- Chip vendors will have to undertake delta evaluation if changes in platform code



In most cases the chip LTS Trusted Firmware /SDK can be updated without affecting the certificate

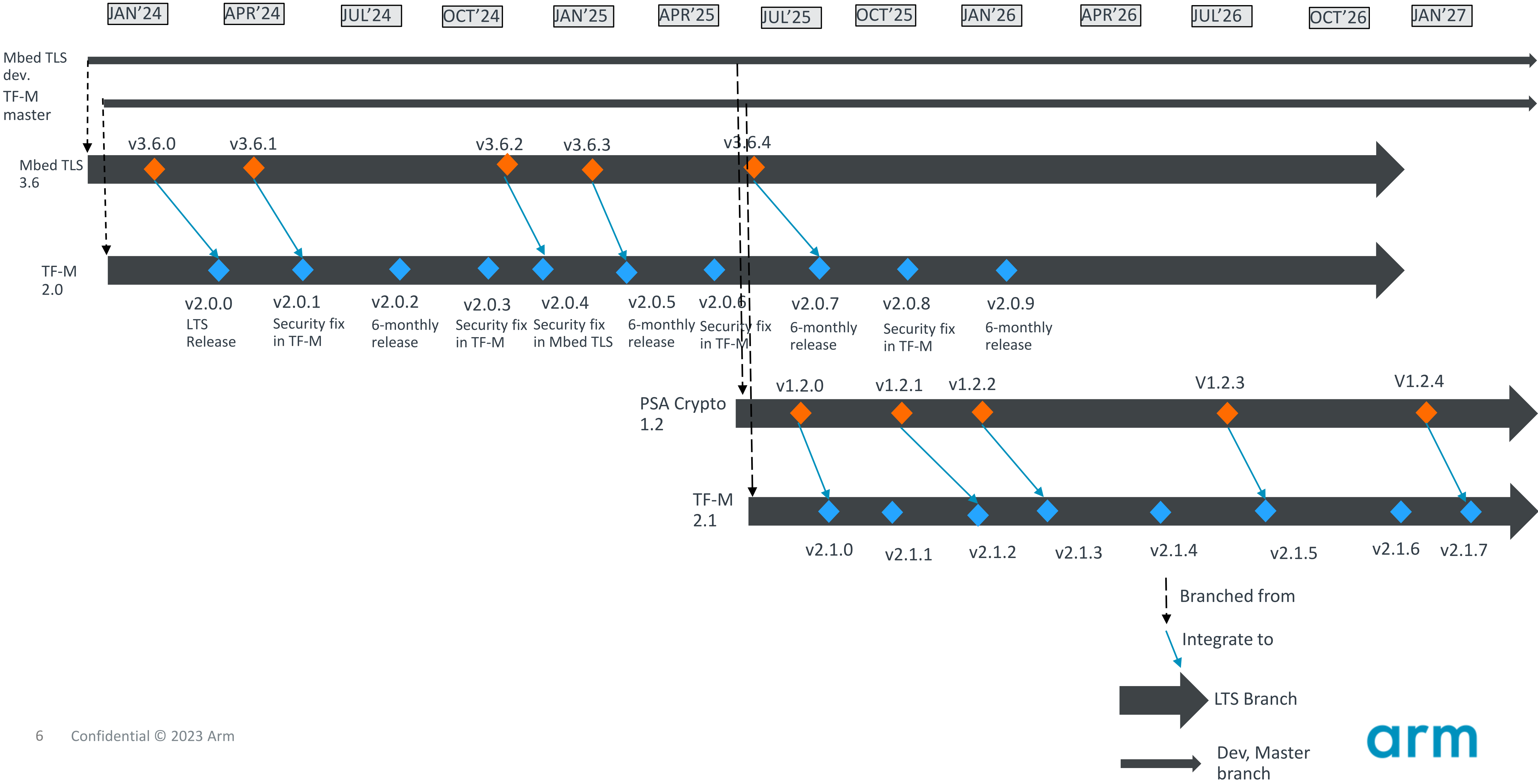
3Year TF-M LTS created every 18months



- New LTS created every 18months maintained for 3 years. Includes an LTS version of Mbed TLS providing PSA Crypto service.
- LTS branch gets bug and security fixes and platform ports.
- New Mbed TLS/PSA Crypto release gets integrated to a new TF-M LTS release
- Adhoc TF-M, Mbed TLS/PSA Crypto release to fix security issues
- Additionally, TF-M 6monthly LTS update releases
- Changes in every TF-M release go through PSA Cert. evaluation by Lab

Thank You
Danke
Gracias
Grazie
谢谢
ありがとう
Asante
Merci
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה

3 Yr Long Term Stable Releases – TF-M & Mbed TLS/PSA Crypto



JAN’24 APR’24 JUL’24 OCT’24 JAN’25 APR’25 JUL’25 OCT’25 JAN’26 APR’26 JUL’26 OCT’26 JAN’27

Mbed TLS dev.

TF-M master

Mbed TLS 3.6: v3.6.0, v3.6.1, v3.6.2, v3.6.3, v3.6.4

TF-M 2.0:

- v2.0.0 LTS Release
- v2.0.1 Security fix in TF-M
- v2.0.2 6-monthly release
- v2.0.3 Security fix in TF-M
- v2.0.4 Security fix in Mbed TLS
- v2.0.5 6-monthly release
- v2.0.6 Security fix in TF-M
- v2.0.7 6-monthly release
- v2.0.8 Security fix in TF-M
- v2.0.9 6-monthly release

PSA Crypto 1.2: v1.2.0, v1.2.1, v1.2.2, V1.2.3, V1.2.4

TF-M 2.1: v2.1.0, v2.1.1, v2.1.2, v2.1.3, v2.1.4, v2.1.5, v2.1.6, v2.1.7

Branched from

Integrate to

LTS Branch

Dev, Master branch