arm

TF-PSACrypto Project



Oct'26

© 2026 Arm

Project Update

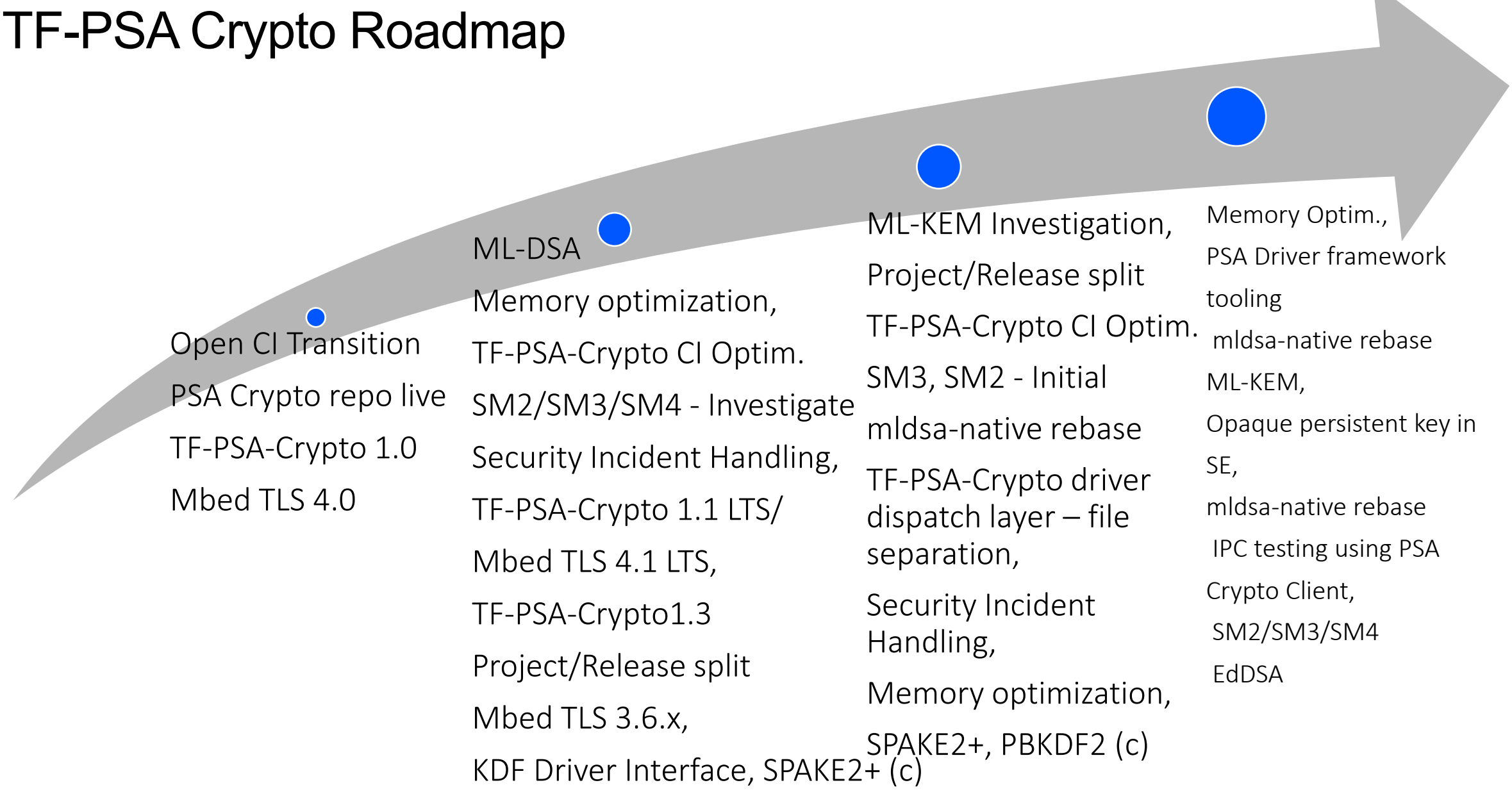
- Transition in the maintenance of TLS and X.509 libraries
  - Existing maintainers will cease their involvement in their development and maintenance from April’27
  - Welcome contributions from organisations and individuals interested in helping sustain Mbed TLS
  - Unless new maintainers have joined the project and ramped up by that time, security incident response, security fixes, and releases will cease from April 2027.
  - Discussions in board and wider community about potential future maintainership support

- Supported PSA API versions
  - Mbed TLS 3.6.x-LTS supports PSA Crypto 1.1 API Specification
  - Mbed TLS4.1.x/TF-PSA-Crypto1.1.x-LTS supports PSA Crypto 1.2 API Specification
    - Minor incompatibilities with PAKE
  - APIs updates beyond 1.2 being worked on e.g. ML-DSA
  - Mbed TLS releases expected to work only with the version of TF-PSA-Crypto it is shipped with
    - Doesn’t guarantee compatibility with a version of PSA Crypto Specification

- Higher volume of Security issues
- ML-DSA (PQC) support
- TF-PSA-Crypto Driver repository
- Mbed TLS 3.6.x LTS coming EOL in March’27

© 2026 Arm

TF-PSA Crypto Roadmap



Appreciate PR reviews from your engineers

arm

© 2026 Arm

arm

Tack
ಧನ್ಯವಾದಗಳು
Merci
Danke
Gracias
Grazie
谢谢
ありがとう
Asante
Thank you
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה
ధన్యవాదములు
Köszönöm