Mbed TLS, PSA Crypto Updates

Shebu V. Kuriakose

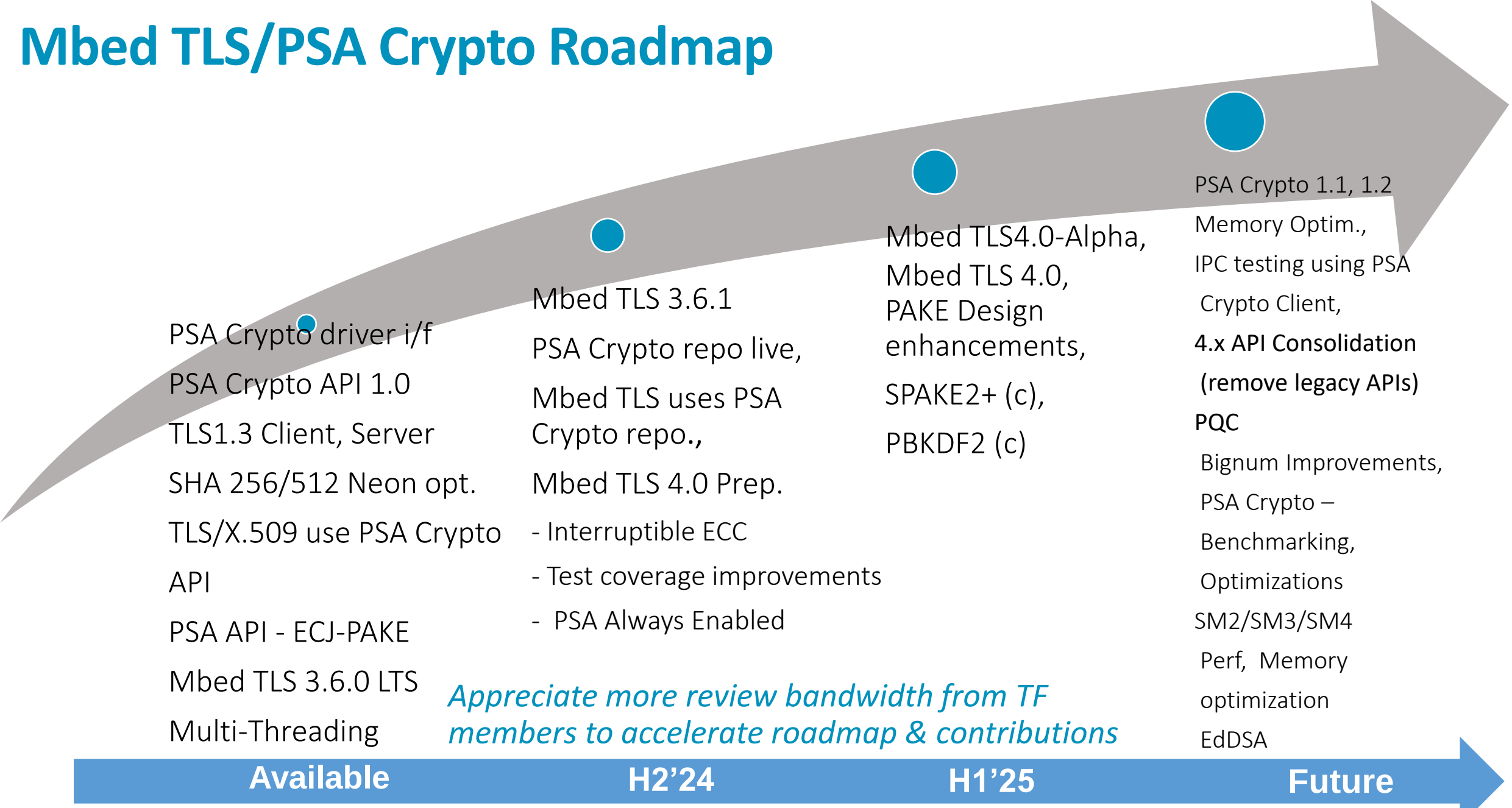
Oct’24

Mbed TLS, PSA Cypto Updates

- Mbed TLS 3.6.0 release
  - PSA Crypto thread safety, Arm v8-A crypto extn, TLS1.3 enabled in default config.
  - LTS release integrated into TF-M v2.1.0 LTS and Zephyr LTS releases.
  - No further major 3.x releases.
  - 3.6.1, 3.6.2 minor releases made

- Focus now on making TF-PSACrypto repository live and preparing Mbed TLS4.0
- TF-PSACrypto
  - Becomes development repository for PSA Crypto
  - Used by Mbed TLS for PSA Crypto
  - Expected latest by early next year
- Mbed TLS4.0
  - Recent rescoping to release by mid 2025.
  - Using TF-PSA Crypto repo., TLS/X.509 always uses PSA Crypto APIs in scope
  - Users based on PSA Crypto in 3.6 release will have same features and usecases supported in 4.0
  - Some of the legacy features not available in PSA Crypto today will be available only in subsequent 4.x releases
  - Removal of some of the legacy/deprecated APIs will also occur during 4.x releases.
  - Mbed TLS3.6 LTS supported for next 3 years for users yet to make switch to PSA Crypto

Mbed TLS/PSA Crypto Roadmap



PSA Crypto driver i/f

PSA Crypto API 1.0

TLS1.3 Client, Server

SHA 256/512 Neon opt.

TLS/X.509 use PSA Crypto API

PSA API - ECJ-PAKE

Mbed TLS 3.6.0 LTS

Multi-Threading

Mbed TLS 3.6.1

PSA Crypto repo live,

Mbed TLS uses PSA Crypto repo.,

Mbed TLS 4.0 Prep.

- Interruptible ECC
- Test coverage improvements
- PSA Always Enabled

Mbed TLS4.0-Alpha,
Mbed TLS 4.0,
PAKE Design enhancements,

SPAKE2+ (c),

PBKDF2 (c)

PSA Crypto 1.1, 1.2

Memory Optim.,

IPC testing using PSA Crypto Client,

4.x API Consolidation (remove legacy APIs)

PQC

Bignum Improvements,

PSA Crypto – Benchmarking, Optimizations

SM2/SM3/SM4 Perf, Memory optimization

EdDSA

Appreciate more review bandwidth from TF members to accelerate roadmap & contributions

Available | **H2'24** | **H1'25** | **Future**

arm