arm

Mbed TLS, PSA Crypto Roadmap

Nov’22

Recent News

- Open Test System (Open CI)
  - Performance Issues being investigated.
- New readthedocs documentation - https://mbed-tls.readthedocs.io/en/latest/
  - Most contents restored from old mbed website inc. knowledge base
- Project Matter support for PSA Crypto backend.
- Mbed TLS 3.2.1 release with full PSA Crypto API support, TLS/X.509 Using PSA enhancements and TLS1.3.
- Arm, Silicon Labs and Nordic PSA Crypto collaboration continues

Ongoing Work

PSA Crypto code size optimizations

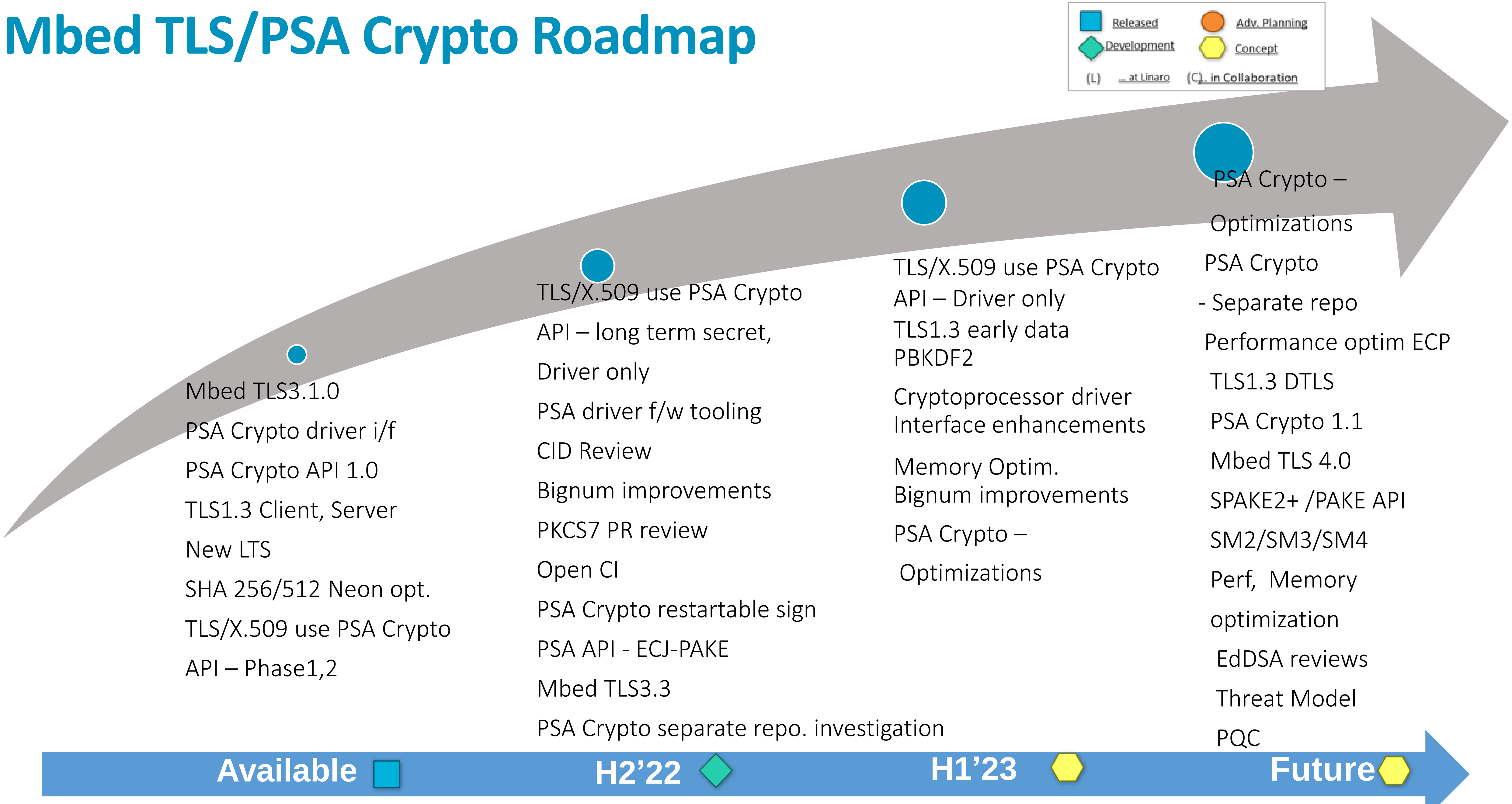
TLS1.3

Bignum Performance Improvements

Open CI

Mbed TLS 3.3 Release

Mbed TLS/PSA Crypto Roadmap



■ Released ● Adv. Planning
◆ Development ⬡ Concept
(L) ...at Linaro (C)... In Collaboration

Available ■

Mbed TLS3.1.0
PSA Crypto driver i/f
PSA Crypto API 1.0
TLS1.3 Client, Server
New LTS
SHA 256/512 Neon opt.
TLS/X.509 use PSA Crypto
API – Phase1,2

H2’22 ◆

TLS/X.509 use PSA Crypto
API – long term secret,
Driver only
PSA driver f/w tooling
CID Review
Bignum improvements
PKCS7 PR review
Open CI
PSA Crypto restartable sign
PSA API - ECJ-PAKE
Mbed TLS3.3
PSA Crypto separate repo. investigation

H1’23 ⬡

TLS/X.509 use PSA Crypto
API – Driver only
TLS1.3 early data
PBKDF2
Cryptoprocessor driver
Interface enhancements
Memory Optim.
Bignum improvements
PSA Crypto –
Optimizations

Future ⬡

PSA Crypto –
Optimizations
PSA Crypto
- Separate repo
Performance optim ECP
TLS1.3 DTLS
PSA Crypto 1.1
Mbed TLS 4.0
SPAKE2+ /PAKE API
SM2/SM3/SM4
Perf, Memory
optimization
EdDSA reviews
Threat Model
PQC