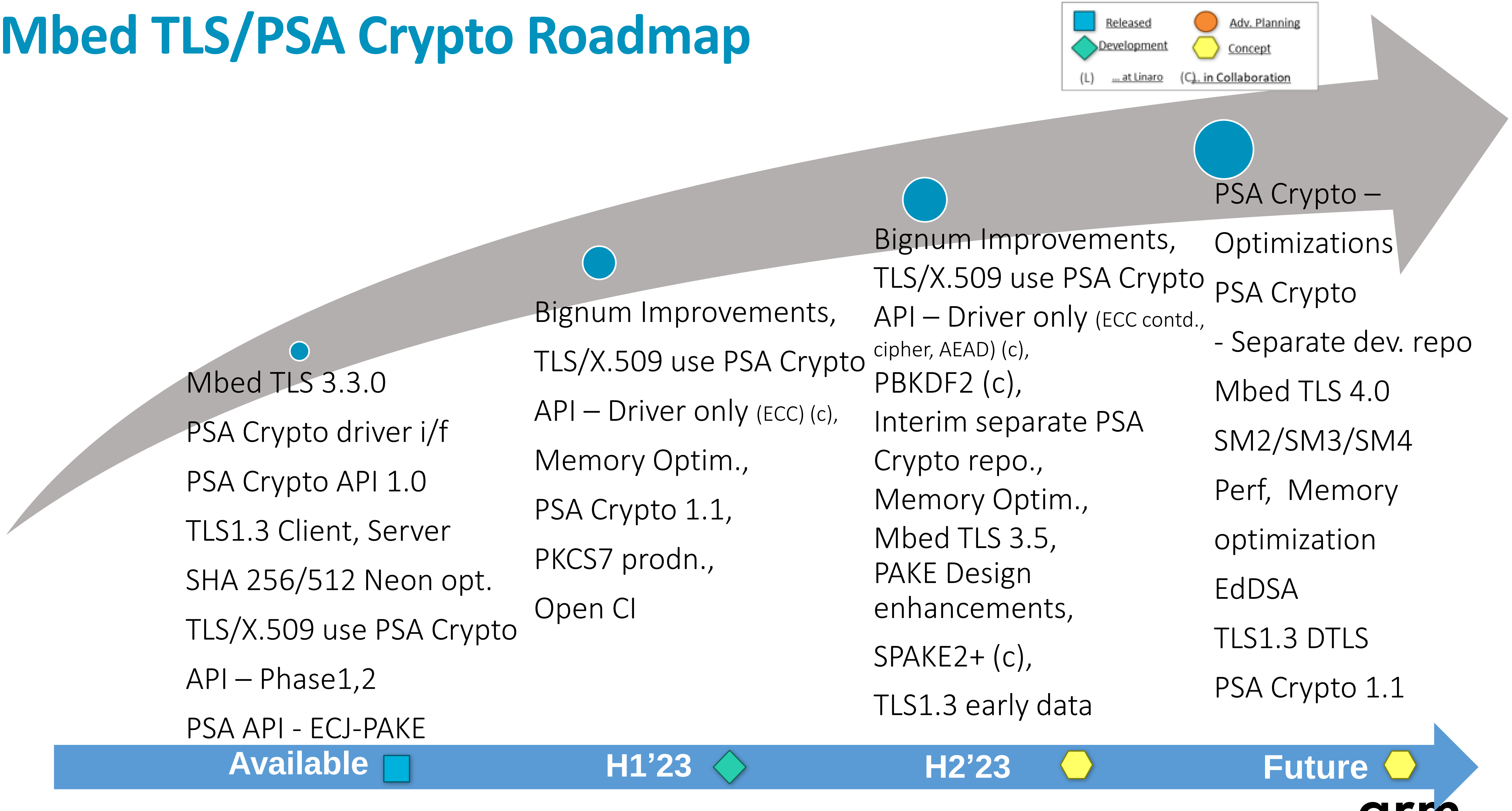
Mbed TLS Roadmap Update

May’23

Mbed TLS Update

- Mbed TLS 3.4.0 released
  - PSA Crypto driver dispatch layer for EC J-PAKE
  - Support disabling of ECDSA or EC J-PAKE implementation when PSA drivers present
  - PSA Crypto support for interruptible sign
  - Improvements to integration of PSA Crypto (Mbed Crypto) with its clients
  - Support for AES with the Armv8-A Cryptographic Extension on Aarch64
- Mbed TLS Open CI
- TLS and X.509 can use PSA Crypto APIs for crypto operations.
- PSA Crypto: Building library without software implementations when accelerators present (Driver only) progressing
- PSA Crypto Code size optimization kicked off.
- Working on creating PSA Crypto ‘interim’ repository

Mbed TLS/PSA Crypto Roadmap



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

Available ■

Mbed TLS 3.3.0
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 – Phase1,2
PSA API - ECJ-PAKE

H1’23 ◆

Bignum Improvements,
TLS/X.509 use PSA Crypto API – Driver only (ECC) (c),
Memory Optim.,
PSA Crypto 1.1,
PKCS7 prodn.,
Open CI

H2’23 ⬡

Bignum Improvements,
TLS/X.509 use PSA Crypto API – Driver only (ECC contd., cipher, AEAD) (c),
PBKDF2 (c),
Interim separate PSA Crypto repo.,
Memory Optim.,
Mbed TLS 3.5,
PAKE Design enhancements,
SPAKE2+ (c),
TLS1.3 early data

Future ⬡

PSA Crypto – Optimizations
PSA Crypto - Separate dev. repo
Mbed TLS 4.0
SM2/SM3/SM4
Perf, Memory optimization
EdDSA
TLS1.3 DTLS
PSA Crypto 1.1

Thank You

Danke

Gracias

Grazie

谢谢

ありがとう

Asante

Merci

감사합니다

धन्यवाद

Kiitos

شكرًا

ধন্যবাদ

תודה