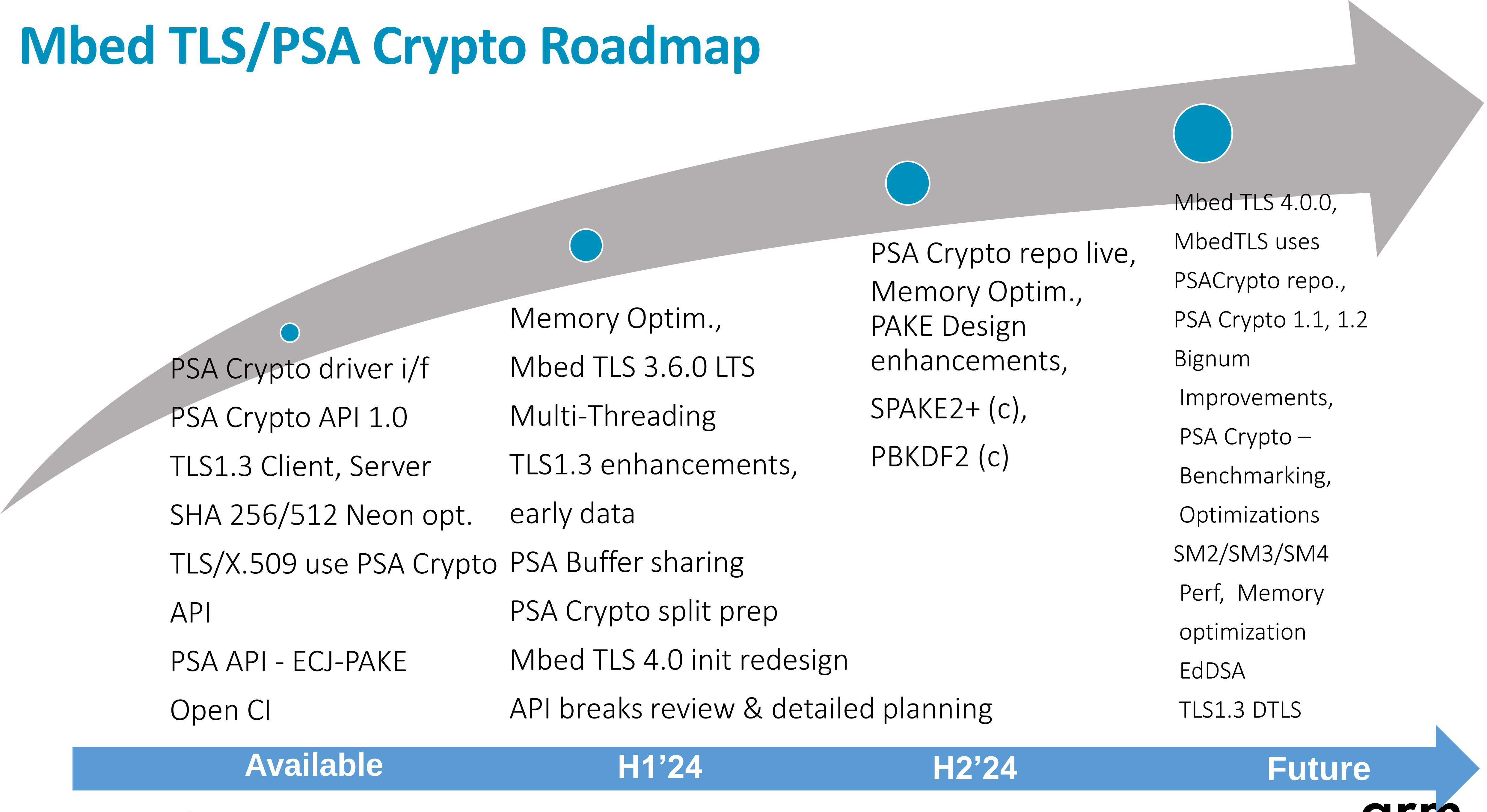
Mbed TLS Update

Mar’24

Mbed TLS, PSA Crypto Update

- Mbed TLS 3.6 LTS release imminent
  - PSA Crypto thread safety. Further testing and enhancements due in future
  - Building library without software implementations of AEAD or cipher when PSA drivers present
  - Armv8-A Cryptographic Extensions for AES, SHA-256 for Thumb (T32) or 32-bit Arm (A32)
  - TLS1.3 early data and other enhancements
  - TLS 1.3 protocol enabled in the default configuration
- Mbed TLS will create LTS every 18months and maintain for 3 years
  - Aligning with TF-M LTS release. TF-M LTS will include Mbed LTS
- Mbed TLS 4.0 release will be the next big focus
  - Release schedule pending detailed planning
  - Making PSA Crypto the main Crypto API. Deprecating/Internalizing legacy cipher APIs
  - TLS/X.509 always uses PSA Crypto APIs
  - Mbed TLS repository consumes the PSA Crypto APIs
  - PSA Crypto init subsystem
  - PSA Crypto driver interface enhancements, ALT interface deprecation (?)

Mbed TLS/PSA Crypto Roadmap



Available

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

Open CI

H1’24

Memory Optim.,

Mbed TLS 3.6.0 LTS

Multi-Threading

TLS1.3 enhancements,

early data

PSA Buffer sharing

PSA Crypto split prep

Mbed TLS 4.0 init redesign

API breaks review & detailed planning

H2’24

PSA Crypto repo live,
Memory Optim.,
PAKE Design
enhancements,

SPAKE2+ (c),

PBKDF2 (c)

Future

Mbed TLS 4.0.0,

MbedTLS uses

PSACrypto repo.,

PSA Crypto 1.1, 1.2

Bignum

Improvements,

PSA Crypto –

Benchmarking,

Optimizations

SM2/SM3/SM4

Perf, Memory

optimization

EdDSA

TLS1.3 DTLS

Thank You!

Danke!

Merci!

谢谢!

ありがとう!

Gracias!

Kiitos!