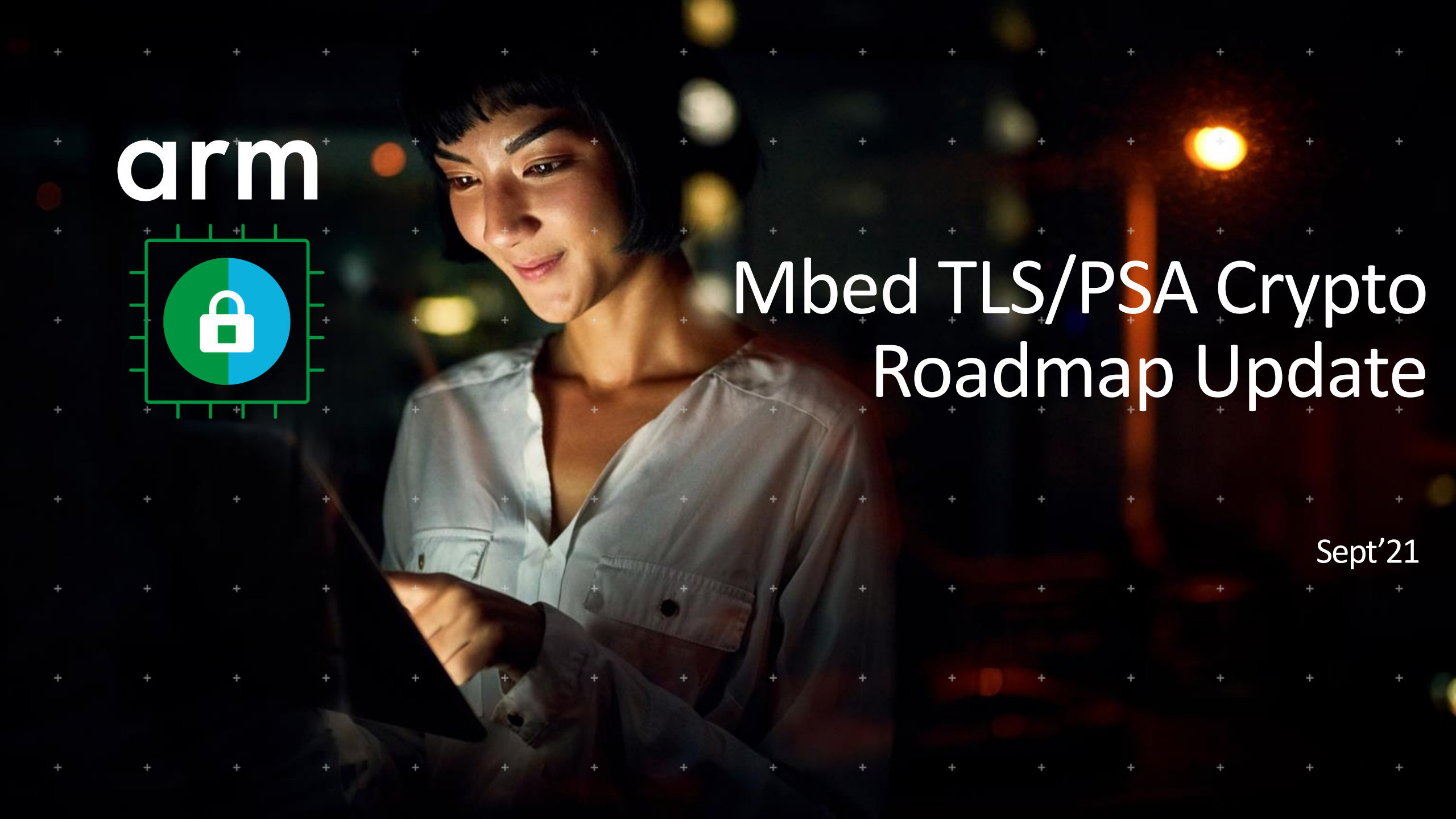

arm

Mbed TLS/PSA Crypto Roadmap Update

Sept'21

Mbed TLS/PSA Crypto – Ongoing Major Themes

- PSA Crypto APIs
- PSA Crypto Processor Driver Interface
- TLS1.3
- Open CI
- New LTS

https://developer.trustedfirmware.org/w/mbed-tls/roadmap/ - Updated start of every quarter

arm

Mbed TLS/PSA Crypto Roadmap

Mbed TLS3.0.0

Cryptoprocessor driver interface – Initial

PSA Crypto API 1.0 – Limited

PSA Crypto API1.0 –

Support Missing APIs

Cryptoprocessor driver

Interface enhancements

TLS1.3 MVP

New LTS

Open CI

Mbed TLS – Use

PSA Crypto - Investigation

Mbed TLS – Use

PSA Crypto – Phase1

TLS1.3

Cryptoprocessor driver Interface

-Performance

optimization

Community PR

EdDSA

Perf. Optimizations - Initial

Mbed TLS – Use

PSA Crypto

PSA Crypto –

Optimizations

SM2/SM3/SM4

SPAKE2+

PQC

Performance,

Memory

optimization

PSA Crypto 1.1

Available **H2'21** **CQ1'22** **Future**

arm