linaro™

Arm Solutions at Lightspeed

# Post Quantum Safe Firmware

Ilias Apalodimas , Senior Tech Lead,
Linaro

# Problem

- Quantum Computers are constantly improving.
- They are expected to excel at compromising certain aspects of traditional security, particularly by **breaking widely-used signature and asymmetric algorithms** like RSA and ECC.
  - Which are used in/for:
    - Software verification and distribution
      - Bootloader to verify binaries (secure/verified/trusted boot)
      - Package managers
      - Software update schemes
    - Secure communication:
      - Email, Messaging apps
      - Authentication (HTTPS, SSL/TLS)
    - Financial transactions
      - Including things such as Blockchain
    - Document signing
    - Voting systems
    - etc …
- Malicious actors harvest data and store large amounts of it → decrypt later!

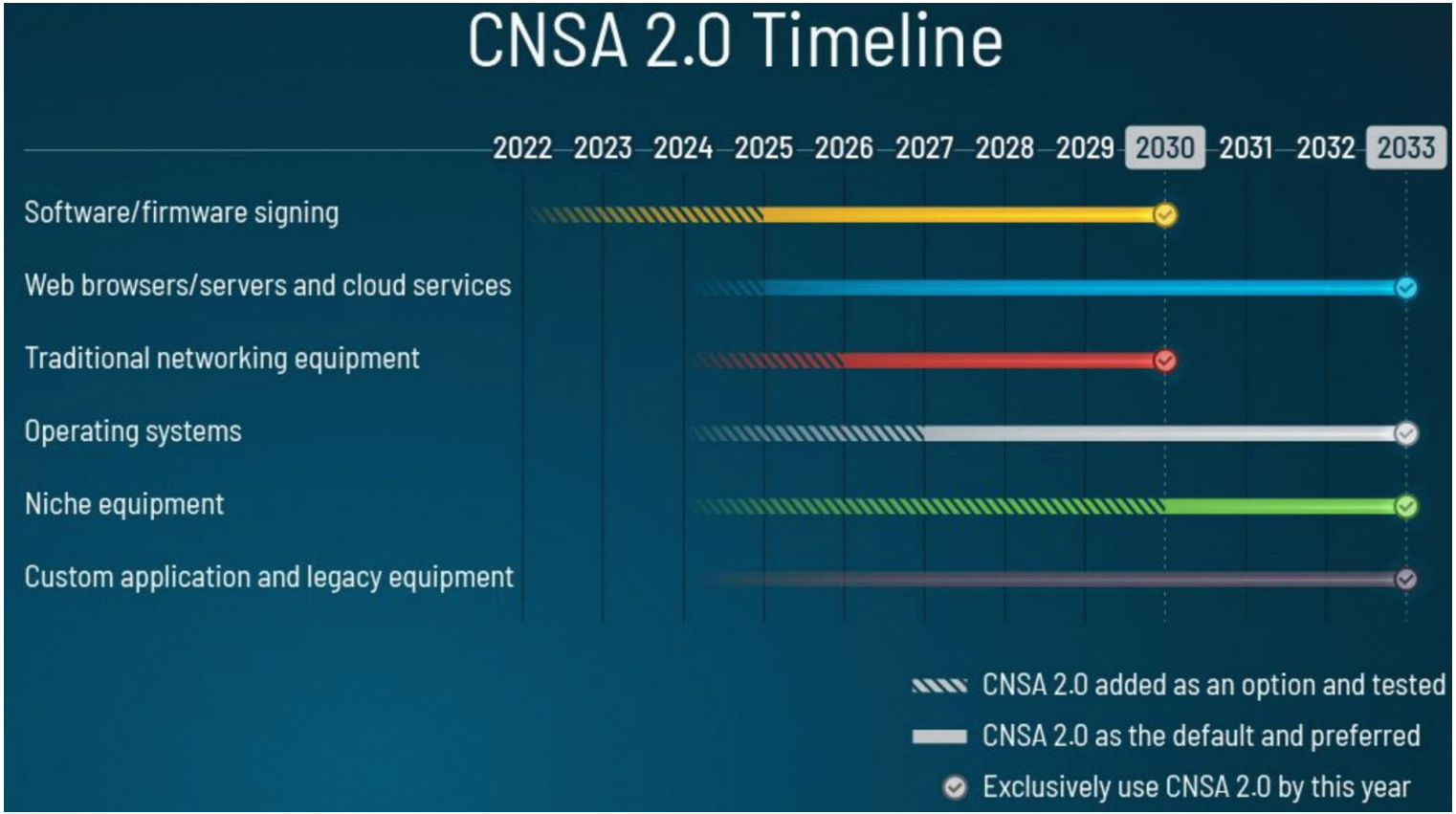
# Background

- **US Fed. Gov. / NIST** has published a set of quantum safe schemes (key encapsulation and signature)
  - Meant to replace RSA, ECC and ECDH
  - The White House wants the federal government to transition to PQC systems by 2035
- **National Security Agency (NSA)**
  - Created the "Commercial National Security Algorithm Suite 2.0" (CSNA 2.0) [FAQ]
  - It's about start using and enforcing Post Quantum Safe Cryptography
  - It also has timelines (see next slide) for various software and equipment.
  - The timeline for software/firmware signing is: start now, support/prefer by 2025, exclusive by 2030.
  - The bootloader ecosystem is late.
  - ***Note!*** NSA is not using these requirements to dictate to any other entity outside of National Security System (NSS) owners and operators

# Background

- **NCSC (UK)** has outlined a three-phase timeline for PQC migration
  - 2028, organizations should define migration goals and build an initial plan
  - From 2028 to 2031, high-priority upgrades should be executed
  - By 2035, the migration to PQC should be complete for all systems, services and products
- **CRYPTREC (Japan)** - Has similar requirements
- Etc…. you can find the per country initiatives here
- The UEFI Forum is about to update the specification with guidance on PQC

# NSA Timeline



# Not urgently affected by Quantum Computers

Symmetric encryption

- Increasing from AES-128 to AES-256 will be sufficient to be PQC ready

Hash, digests and Message Authentication Codes

- Use SHA-384 or SHA-512 will be sufficient to be PQC ready

# Summary of CNSA 2.0




**Public-key**

CRYSTALS-Dilithium → Replaces: RSA, ECC

CRYSTALS-Kyber → Replaces: ECDH

**Symmetric-key**

Advanced Encryption Standard (AES)

Secure Hash Algorithm (SHA)

**Software and Firmware Updates**

Xtended Merkle Signature Scheme (XMSS)

Leighton-Micali Signature (LMS)

# What is the suggestion?

- Phase1 - Crypto libraries
  - Check crypto libraries status - Do they have the needed algorithms (OpenSSL, Mbed-TLS, PSA Crypto …)
    - mbedTLS has ML-DSA prototype for Q1 2026
  - Alternatively use new libraries that already have implemented PQC algorithms
    - Liboqs, PQ code, PQCrypto Lib (commercial), kyberlib, … a longer list
- Phase 2 - Adopt PQC in bootloader components (use libraries from phase 1)
  - U-Boot
  - Trusted Firmware A/M
  - MCUBoot
  - EDK2
  - OP-TEE
- Phase 3 - Supply chain/distros (update layers and recipes to get phase 2 software)
  - Yocto integration
  - Linux distributions

# Software and firmware updates

Recommendation

LMS and XMSS are an option. However, the key management for these is cumbersome.

- Start with using LMS and XMSS (NIST SP 800-208, PDF)
  - Key management challenges as a key can only be used to sign a single image! (see section 1.2 and 9.1 in the NIST PDF)
  - Keys are larger ($2n^2$ bits) than traditional keys and generate larger signatures ($n^2$) compared to RSA and ECDSA
  - But SLH-DSA and ML-DSA keys are even bigger
- In the long run, when validated ML-DSA or SLH-DSA is widely available, we likely want to switch to use one of them (FIPS 204, PDF, FIPS 205)

# U-Boot proposal

- This video provides the latest updates wrt the UEFI spec
- Add a config option for Post Quantum Crypto support
- Bump symmetric crypto & hashing/MACs to 2x size of the current size – AES-256, SHA512 etc.
- Evaluate liboqs. If it's not adequate evaluate alternatives from this list.
  - The chosen library **must** support X.509 hybrid certificates
  - It **must** support NIST recommended algorithms
  - It **must** have a compatible license (GPLv2)
- Decide between stateful, stateless signature schemes
- Enhance UEFI secure boot with PQC algorithms
- Add self tests in the CI

# Open Questions

- Do we need to support key exchange as well (e.g ML-KEM)
- Are there speed and size requirements?


linaro
linaro
linaro