PQC Working Group Proposal



CORECOLLECTIVE

Where the Arm software ecosystem connects

v1 November 2026

Purpose Statement

CORECOLLECTIVE
Where the Arm software ecosystem connects

Ensure the open source components the Arm ecosystem depends on provide PQC on time

Problem / Gap Summary



- 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.
- Malicious actors harvest data and store large amounts of it → decrypt later!
- The legislation and timelines for supporting PQC in products keeps getting shorter

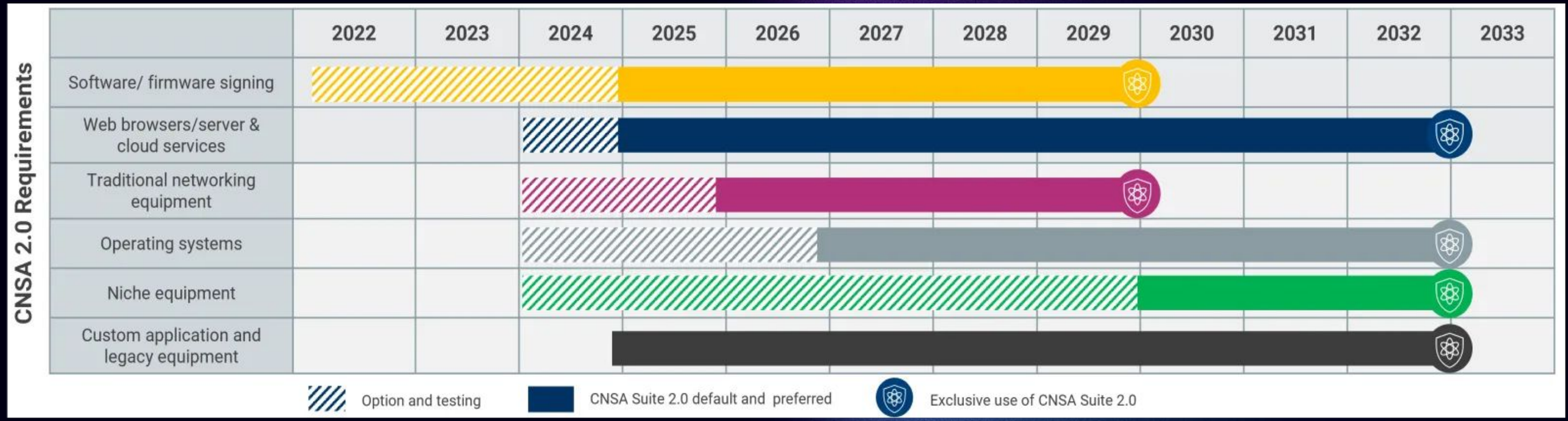
Problem / Gap Summary



- Multiple countries have published guidance for their PQC programs and every program uses NIST as its basis. But they differ in algorithm selection, enforcement dates, etc
- The vast majority prefers support by 2025. Exclusively used by 2030.
- The current plan is to deprecate ECC and RSA by ~2030 and banning them starting ~2035
- Different country regulations might make it difficult to pick just one algorithm.E.g NSA rejects SLH-DSA while BSI (Germany) and ANSSI (France) require it
- We are already late! E.g The CNSA 2.0 quantum-resistant requirements

Problem / Gap Summary

CORECOLLECTIVE
Where the Arm software ecosystem connects



Working Group Initial Focus

CORECOLLECTIVE
Where the Arm software ecosystem connects

- Regulatory alignment. Track PQC transition requirements and timelines from national and regional bodies (NIST, NSA CNSA 2.0, EU, BSI, ANSSI and others) and map them to the Arm software stack
- Constrained environments. Assess the impact of larger keys and signatures on early boot memory, secure world footprint, flash layout, image formats etc
- Identify gaps in the open source ecosystem with regards to PQC support. E.g, **Firmware and boot chain**. PQC and hybrid signature support across TF-A, OP-TEE, Zephyr, U-Boot, EDKII, UEFI Secure Boot, capsule updates, etc

Working Group Initial Focus

CORECOLLECTIVE
Where the Arm software ecosystem connects

- Cross-group coordination. Act as the PQC point of contact for other CoreCollective working groups
- Upstream integration. Build on existing projects and drive their integration into the Arm boot and runtime stack
- Deliverables and guidance. Provide reference PQC enabled stack

Targeted Initial Members

CORECOLLECTIVE
Where the Arm software ecosystem connects

The following companies have been approached and are interested in participating: Arm, AMD, Qualcomm

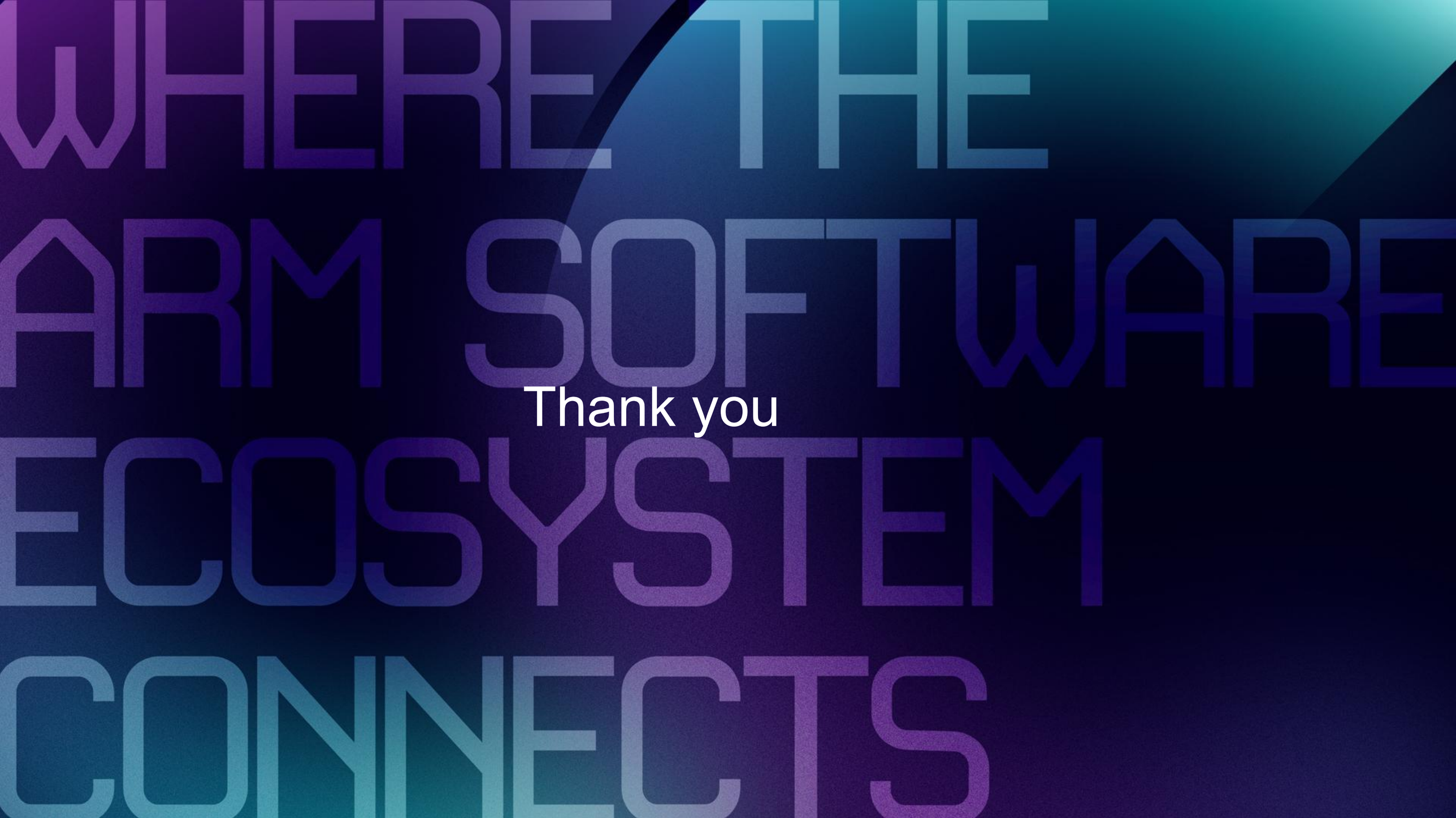
Company	**Potential Work item Interests**
ARM	PQC
AMD	PQC U-Boot
Qualcomm	PQC U-Boot, EDKII
Axis communications AB	PQC OP-TEE

Proposed WG Structure

CORECOLLECTIVE
Where the Arm software ecosystem connects

This WG would be expected to focus on executing of engineering Initiatives with the following details

- **Proposed Chair**: Interim, Ilias Apalodimas
- **WG Type**: Execution of Initiatives requiring Member sponsorship to perform Engineering tasks
- **Initiation Plans**: Collect needs and build a contribution model as supported by the members.



Thank you