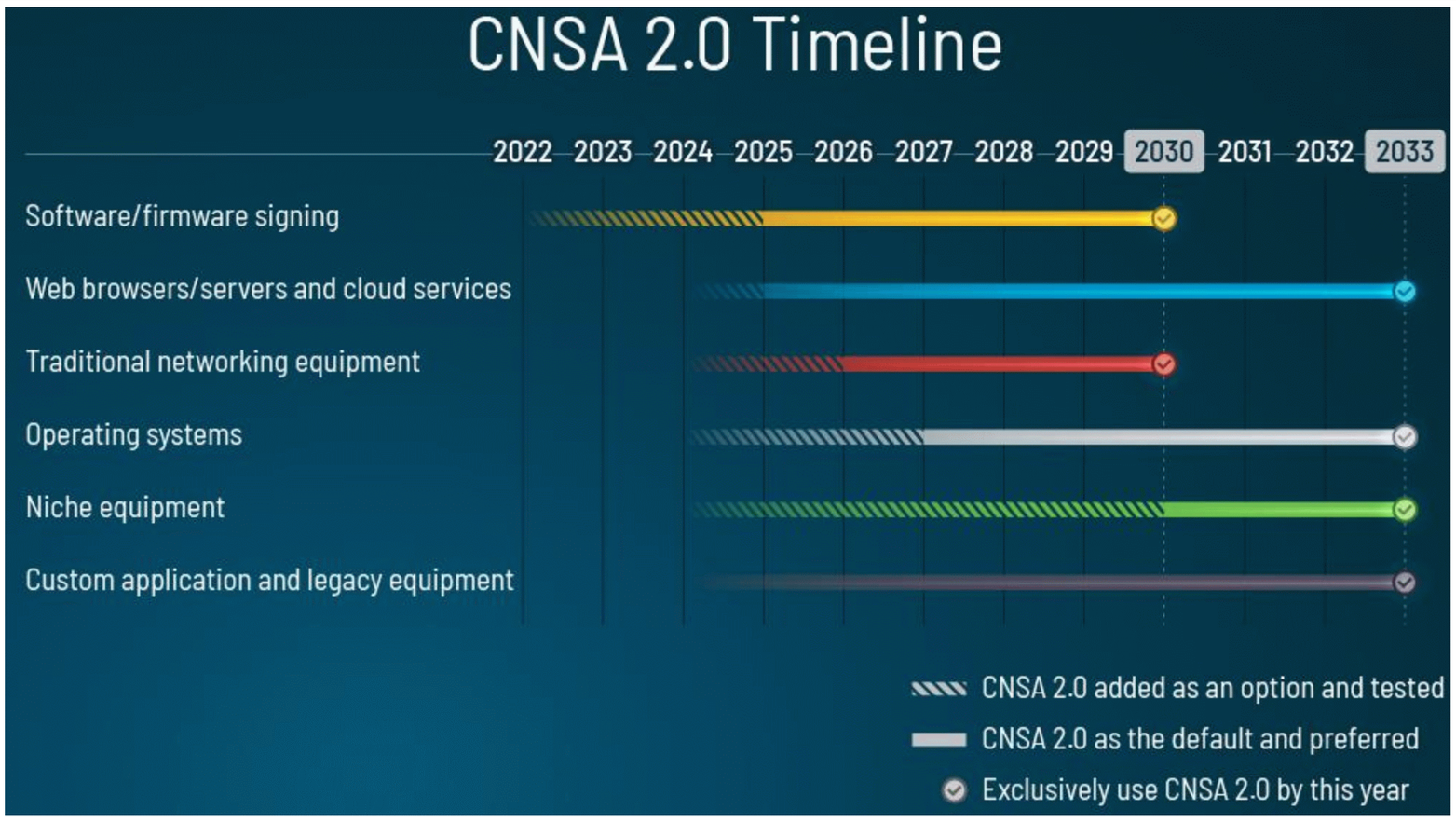
Post-Quantum Internet Browsing

Nouman Khan, Akif Mehmood, Francesco Rollo, Nicola Tuveri
Network and Information Security Group (NISEC)
Tampere University, FINLAND

QUBIP
Quantum-oriented Update to Browsers and Infrastructure for the PQ Transition

Why The Quantum Threat Is a Problem Worth Solving?



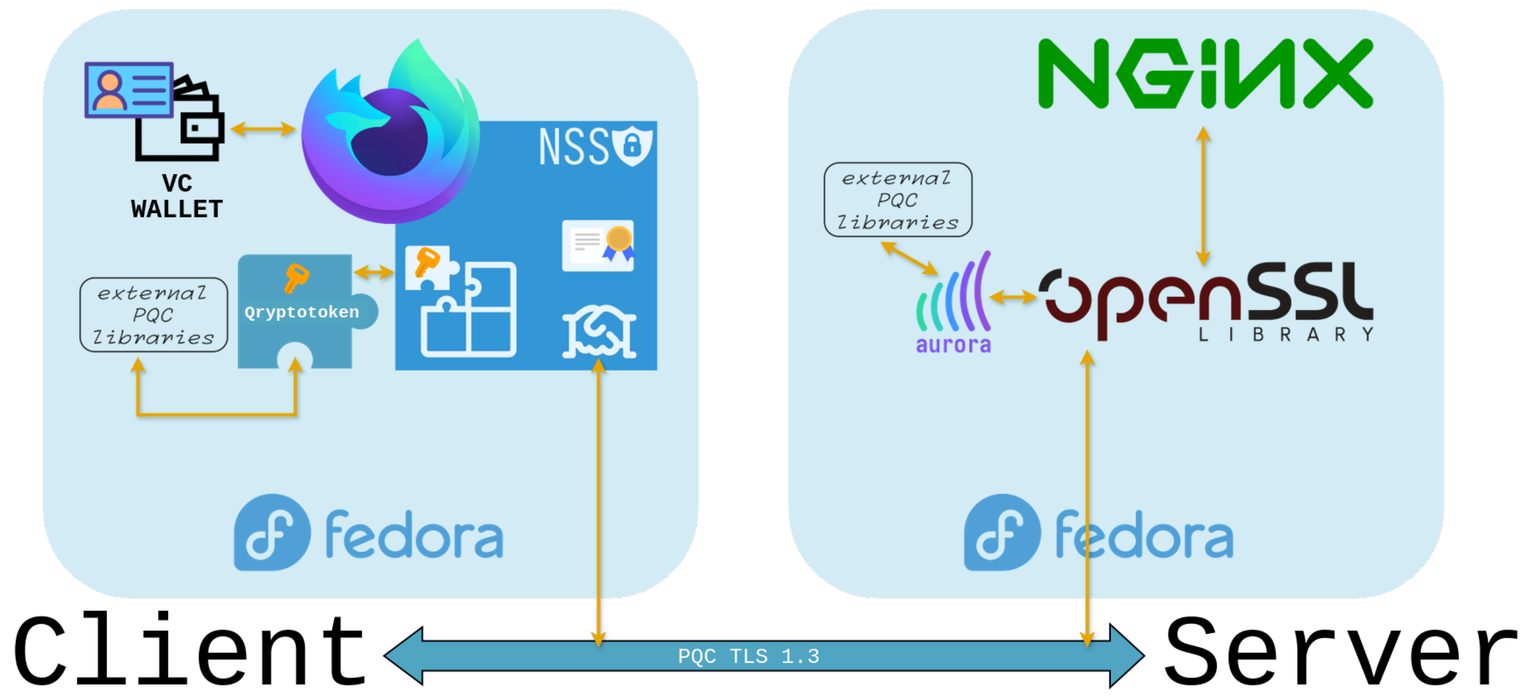
The rise of cryptographically relevant quantum computers (**CRQCs**) will ultimately **break** the traditional cryptographic algorithms which secure our communications today. Current policies mandate a transition to **post-quantum cryptography (PQC)** now, not later: examples include NSA CNSA 2.0, BSI TR-02102-1, guidance from ANSSI, and the PQC roadmap of the EU Commission.

But this shift is far from simple. A widespread adoption remains technically challenging due to the complexity of cryptography stacks and their integration across heterogeneous systems.

Shallow Modules: A Plug-and-Play Architecture

Instead of patching PQ cryptography into existing stacks, what if we could pull it out entirely?

Our proposal introduces **shallow modules**, lightweight, modular adapters that decouple cryptographic libraries from the rapidly evolving ecosystem of state-of-the-art PQ implementations and avoid invasive changes in the codebase of existing applications. They give us the freedom to experiment with PQ algorithms and implementations, iterate quickly, test different tradeoffs, and transparently reach most of the existing critical infrastructure.



Results

Key achievements in **OpenSSL**:

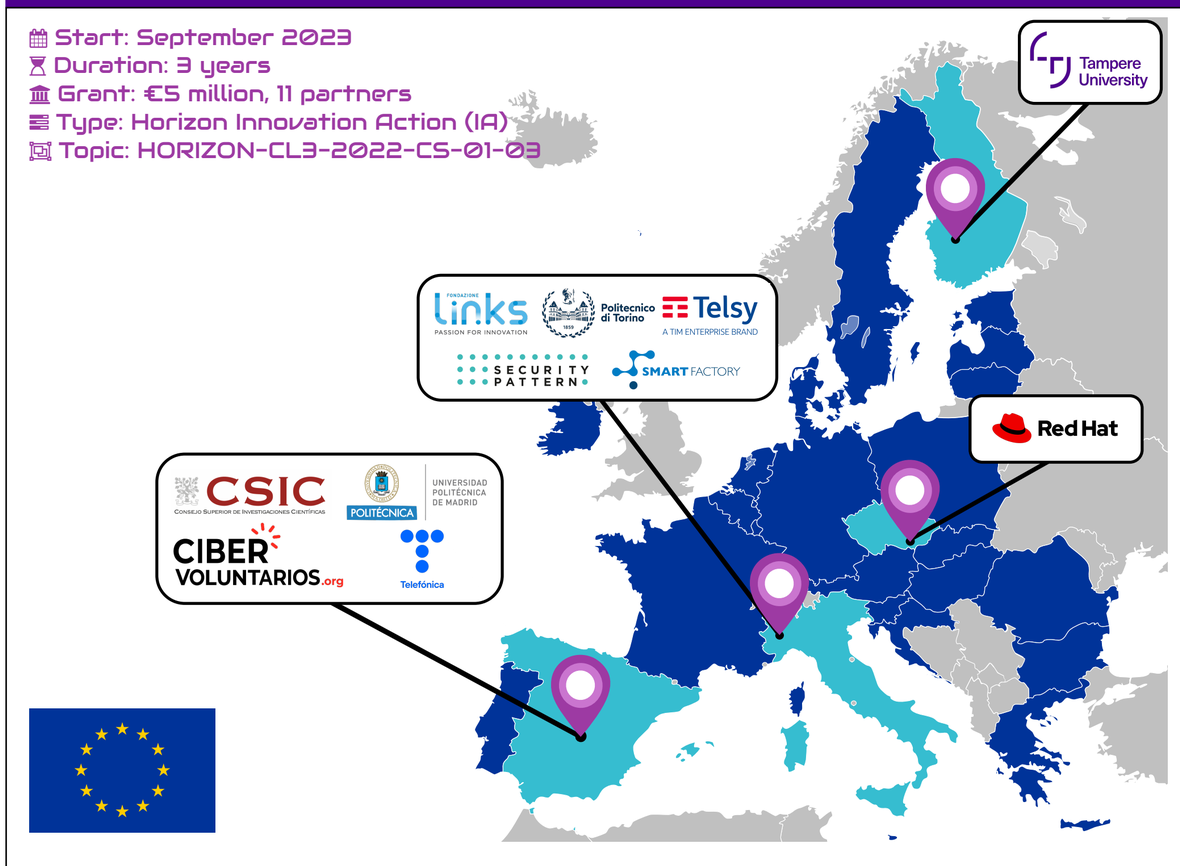
- OpenSSL v3.2 resolved key blockers. v3.5 delivered native PQC support.
- Released `aurora`, a Rust-based **`Provider`** which easily interfaces with various PQC implementations.
- Released **`openssl-provider-forge`**, a support crate to build Rust Providers

Key achievements in **Firefox/NSS**:

- Released **`qryptotoken`**, a Rust-based PKCS#11 token supporting:
  - ML-KEM-768 via NSS KEM interface
  - ML-DSA via NISEC extension
- Released an experimental build of Firefox supporting PQC key exchange and authentication in TLS 1.3.

About Us

Start: September 2023
Duration: 3 years
Grant: €5 million, 11 partners
Type: Horizon Innovation Action (IA)
Topic: HORIZON-CL3-2022-CS-01-03



QUBIP is a European project that leads the integration of PQ algorithms into the **protocols, networks, and systems** we use today.

We are a multi-disciplinary team of experts from different countries, connecting academia, industry, and end-users..

Our goal is to design and evaluate a reference and replicable post-quantum transition process.

Scan the QR code on the left to know more. **Want to see it in action?** Ask us how. We'll show you.

The QUBIP project is funded by the European Union under the Horizon Europe framework programme [Grant Agreement No. 101119746].

Tampere University