

OpenSSL
Conference
Prague 2025

Post-Quantum Crypto in Practice: Real-World Implementation with Firefox, OpenSSL, and Rust-Based Solutions



Akif Mehmood
Researcher
Tampere University

Francesco Rollo
Research Assistant
Tampere University



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

QUBIP Project



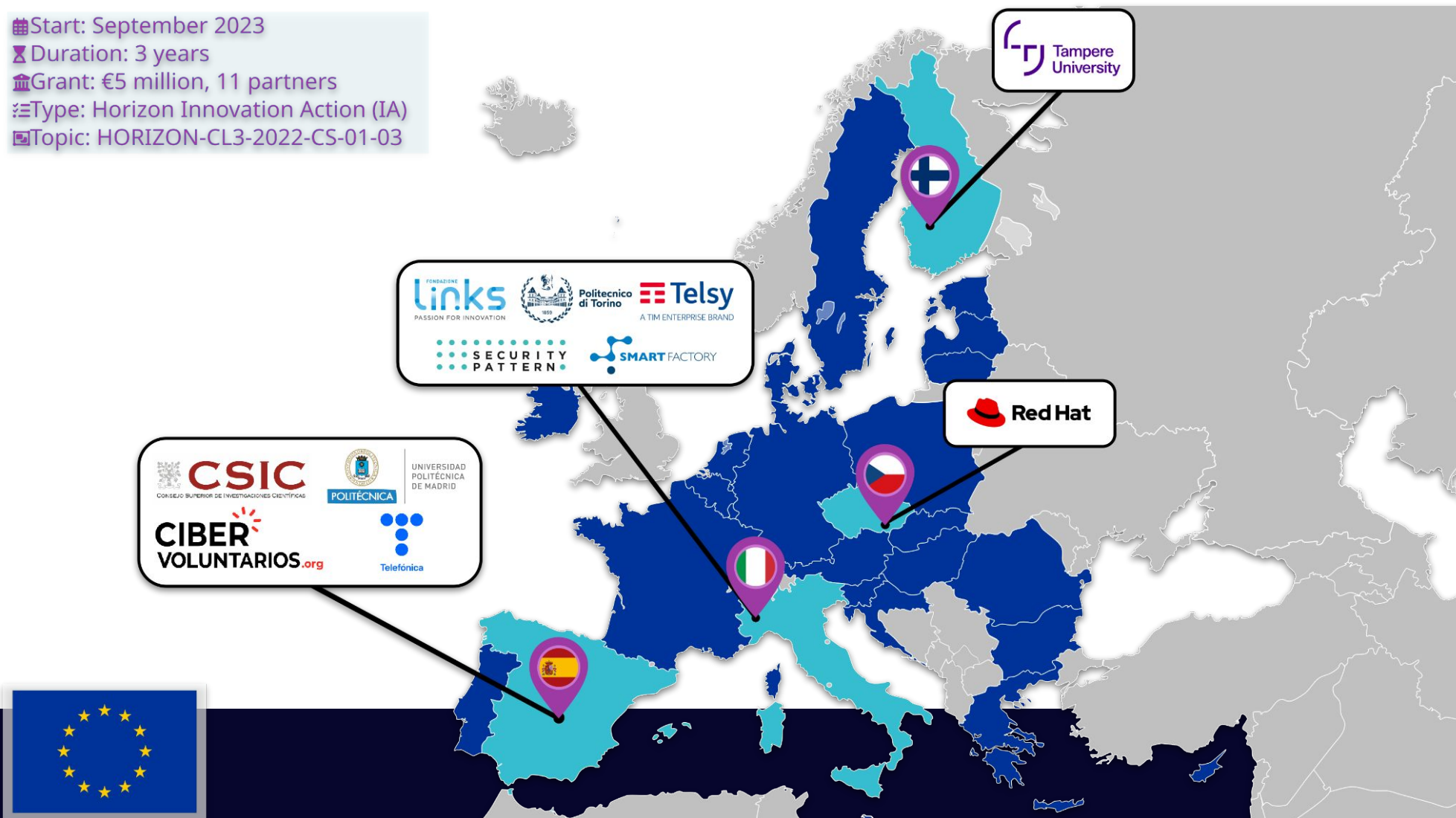
- [QUBIP](#) (**Q**uantum oriented update to **B**rowsers and **I**nfrastructure for the **P**Q transition) is designed to contribute to the EU transition to **PQC** with the aim of streamlining the process and creating a replicable transition model.
- [11 partners](#) contributing to the project, including Tampere University.
- TAU is responsible for integrating state-of-the-art PQC implementations in **OpenSSL** and **NSS** through shallow loadable modules.
- Our blog posts related to all the building blocks and their progress are accessible [here](#).

QUBIP Project

Quantum oriented update to **B**rowsers and Infrastructure for the **PQ** transition.



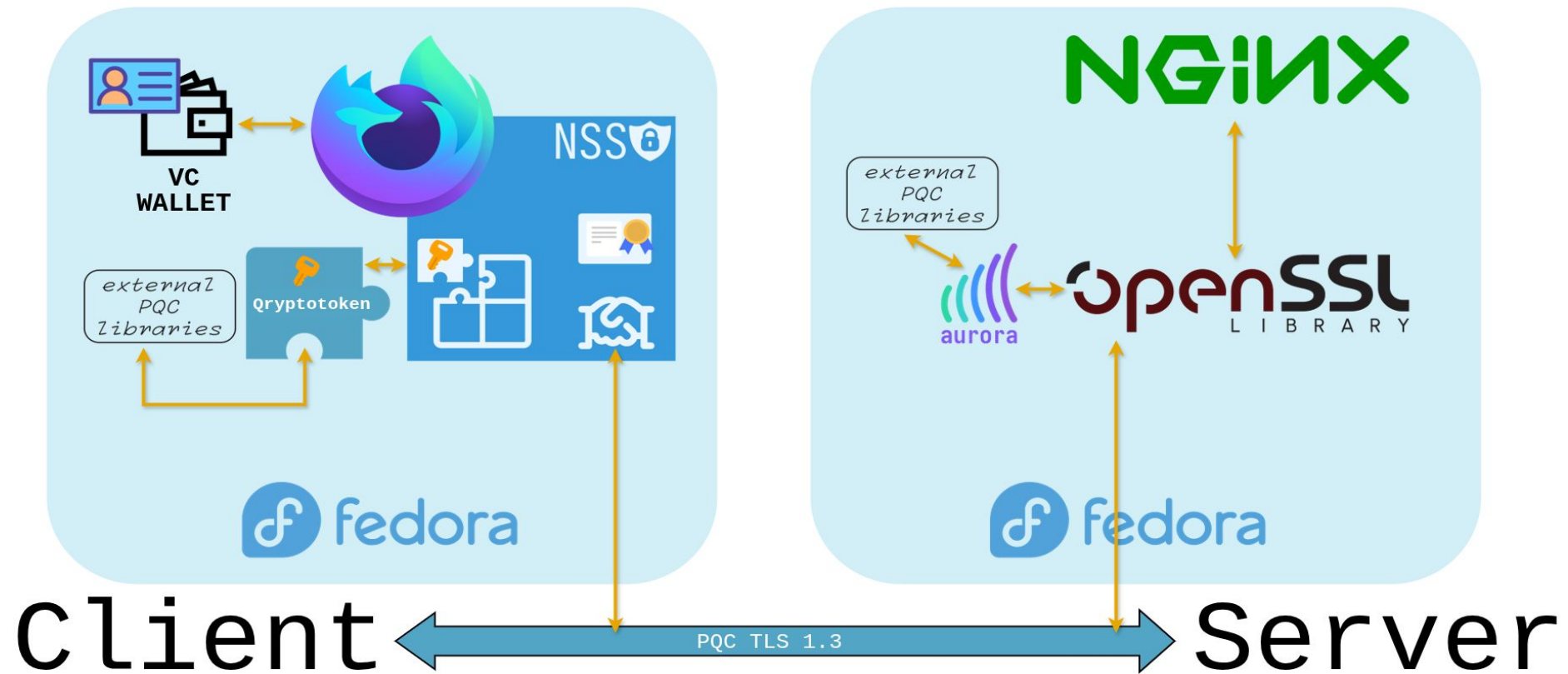
📅 Start: September 2023
⌚ Duration: 3 years
💰 Grant: €5 million, 11 partners
🔗 Type: Horizon Innovation Action (IA)
📄 Topic: HORIZON-CL3-2022-CS-01-03



A white abstract line graphic in the top-left corner, consisting of a single continuous line that curves and loops.

Pilot System Overview

Pilot system overview



3 use-cases



1. TLS-level server authentication
 - Our client (QUBIP's Firefox build) establishes a PQ-secure TLS 1.3 connection with a QUBIP server instance—located either in Finland or Italy—using qryptotoken (QUBIP's soft token). This should ensure that both the key exchange and authentication are demonstrably Post-Quantum secure.
2. App-level user authentication via plaintext PQ (or PQ/T hybrid) Verifiable Credentials
3. App-level user authentication via PQ Anonymous Credentials



Demo

Conclusions

before the final Q/A



- Recap
 - aurora and openssl_provider_forge for OpenSSL PQC Provider
 - cryptotoken for Firefox/NSS-compatible PKCS#11
- QUBIP blog posts
 - [Transition of OpenSSL for implementing PQ/T TLS](#)
 - [Fedora Linux Transition](#)
 - [NSS and Firefox Transition to PQC](#)
 - [QUBIP for post-quantum cryptography demos pilots for IoT, telco](#)
- Ongoing/future work
 - Firefox: match the new NSS once this is finalized (some already landed on NSS 3.116).
 - Enable mTLS and test keygen codepaths, likely to require small updates on cryptotoken
 - cryptotoken: rebase on latest kryoptic
 - aurora: showcase adapters using dynamic linking. Cleanup and maximize code reuse.



Q/A



Thank you!