Red Hat and Fedora: commercial and non-commercial way of moving post-quantum

Moving Post-Quantum
for customers and community

Workshop on Post-Quantum Cryptography: Principles and Challenges

March 27, 2025, VUT, Brno

Dmitry Belyavskiy, Principal Software Engineer

Who am I

Dmitry Belyavskiy
Red Hat Principal Software Engineer
Maintain: OpenSSL, OpenSSH

OpenSSL Technical Committee member since 2021

Current work: Post-Quantum transition in Red Hat

QUBIP Consortium

Quantum oriented update to **B**rowsers and **I**nfrastructure for the **P**Q transition, QUBIP.EU

Fondazione Links – Passion for Innovation

Coordinator

Politecnico di Torino 1859

Red Hat

Security Pattern

CSIC Consejo Superior de Investigaciones Científicas

Telefónica

Politécnica Universidad Politécnica de Madrid

Tampere University

Smart Factory

Ciber Voluntarios.org

Disclaimer: QUBIP project is co-funded by the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

Red Hat distributions

Fedora

Community based distribution

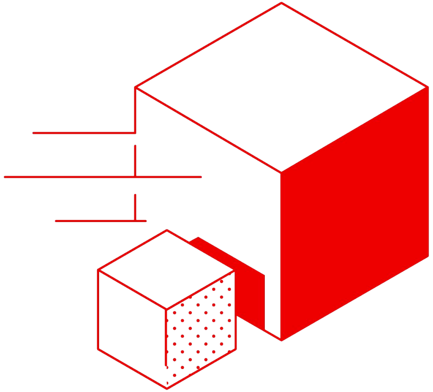
CentOS

A preview of RHEL

RHEL

Commercial distribution

Fedora Linux for PQ experiments



Components

liboqs + OQS provider by Open Quantum Safe

Low-level implementations

Multiple contributions

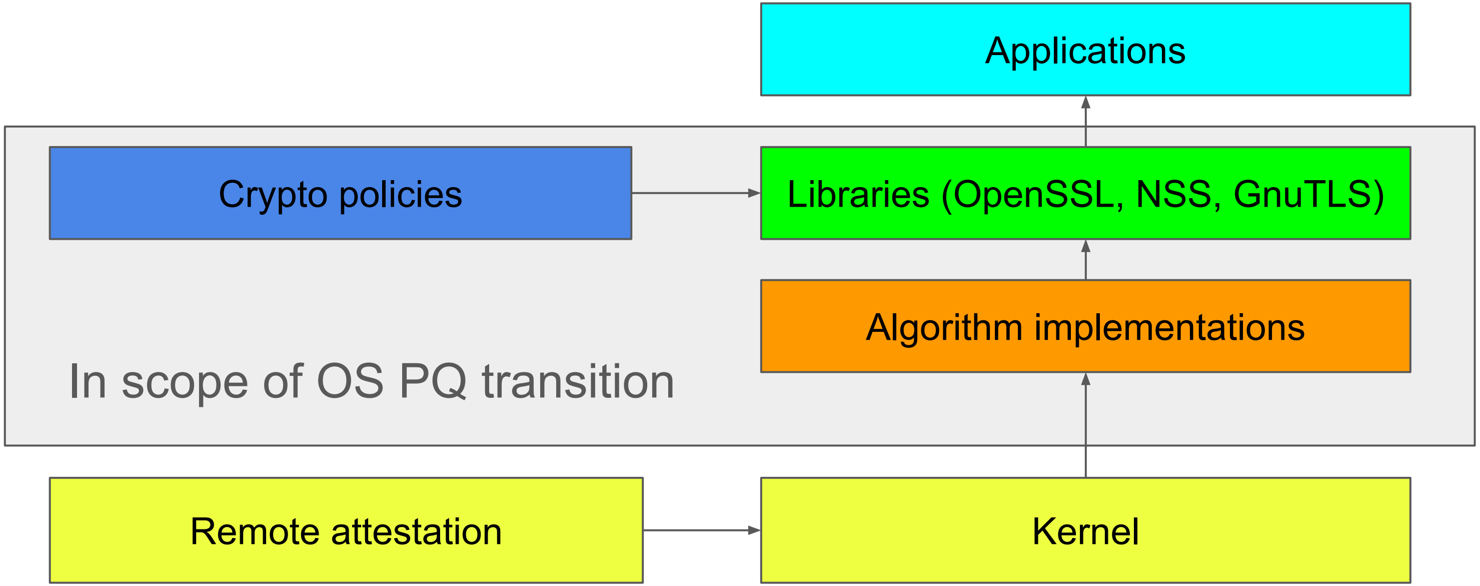
Container

https://github.com/QUBIP/pq-container

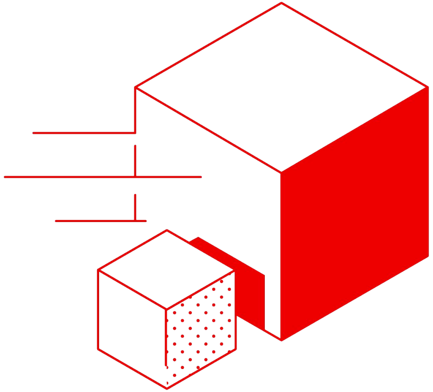
Algorithm migrations

Kyber => ML-KEM, Dilithium => ML-DSA

OS PQ transition: scope


Applications
Crypto policies
Libraries (OpenSSL, NSS, GnuTLS)
Algorithm implementations
In scope of OS PQ transition
Remote attestation
Kernel

Crypto policies: system-wide settings



Examples

DEFAULT, FIPS, LEGACY, FUTURE

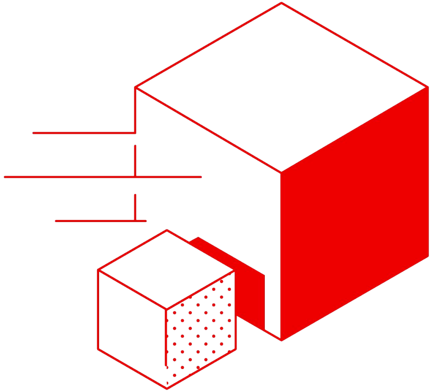
The way to configure

Config snippets

PQ experiments

TEST-PQ: enables PQ algorithms

Which algorithms to choose



Our algorithms choice

NIST standards (ML-DSA, ML-KEM, SLH-DSA)

Hybrid algorithms (ML-KEM, ML-DSA)

OpenSSH

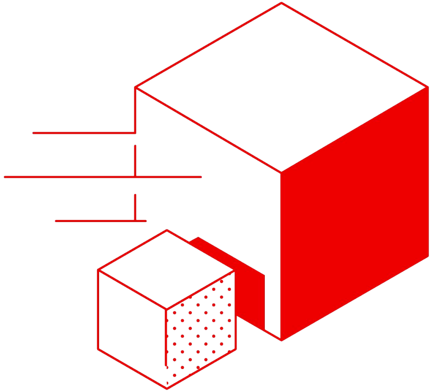
ML-KEM (9.9+) - own implementation

NTRU algorithm

Experimental status

We expect incompatibilities

Red Hat Enterprise Linux: commercial approach



RHEL choice

Inherited from Fedora

Includes post-quantum crypto policy

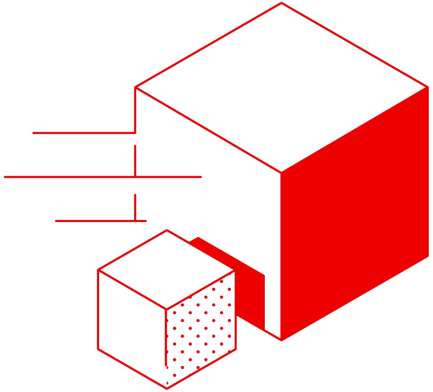
Status: Tech preview

RHEL challenges

PQ software will appear in RHEL 10

We have many customers that are still using RHEL 9, 8, 7…

Next steps



Supply chain PQ security

Package signatures and verification

Following upstreams

OpenSSL, GnuTLS, NSS

PQ algorithms in DEFAULT crypto policy

Extending PQ support

New algorithms, update protocols

IETF participation, writing code…

Certification

EU, US

Thank you

Red Hat is the world’s leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make
Red Hat a trusted adviser to the Fortune 500.

- linkedin.com/company/red-hat
- youtube.com/user/RedHatVideos
- facebook.com/redhatinc
- twitter.com/RedHat