



Connect
**Entering the Post-Quantum
Era with RHEL**





José Ángel de Bustos Pérez

EMEA Senior Specialist Solution Architect
Red Hat



Sebastian Mitterle

Principal Software Quality Engineer
Red Hat

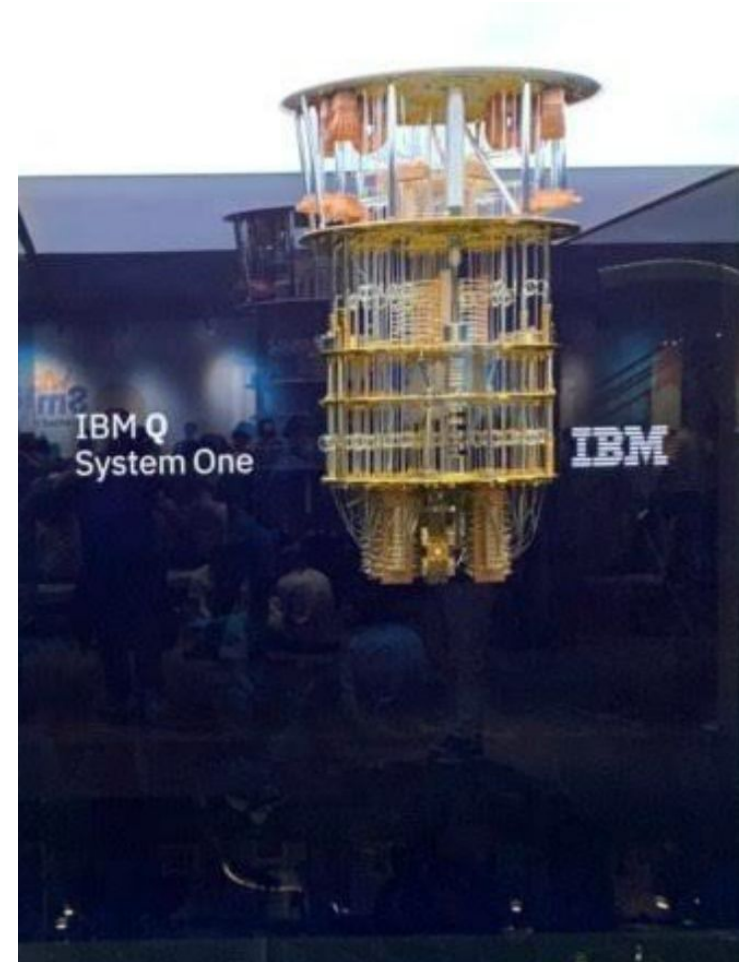


Why PQC?



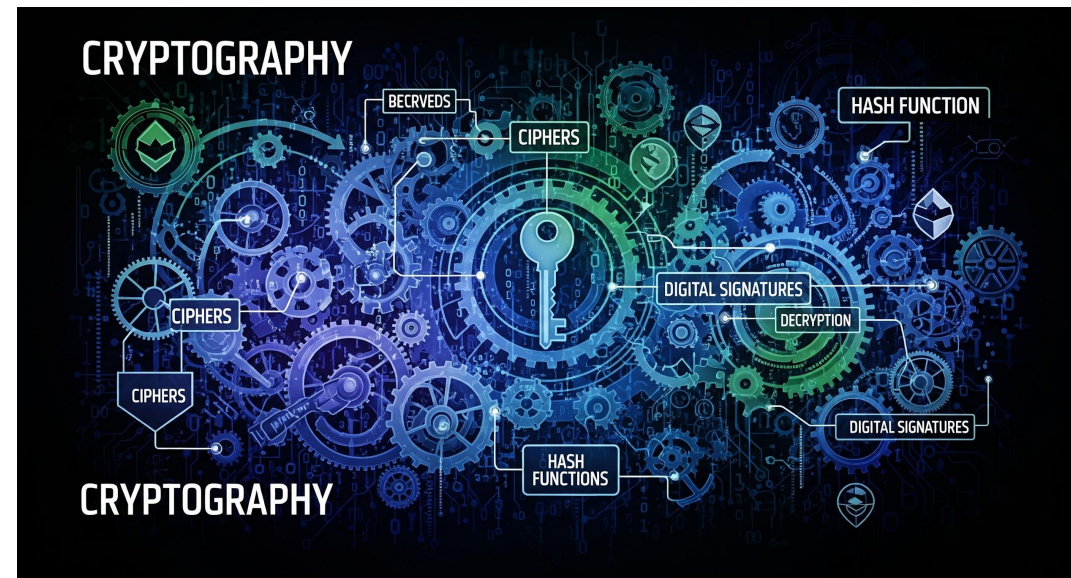
Quantum Computing

- Quantum computers are computers whose operation is based on quantum mechanics rather than classical mechanics.
- Quantum computers take advantage of quantum properties to solve problems that classical computers can't:
 - Superposition
 - Entanglement
 - Interference
- Quantum computers are real but they are quite limited today.



Cryptography

- Cryptography is the science of securing information by transforming it into an unintelligible string of data, ensuring confidentiality, integrity and authenticity.
- Cryptographic algorithms can be classified into:
 - Symmetric algorithms
 - Asymmetric algorithms
- Cryptographic algorithms are mainly used to:
 - Encrypt/Decrypt information
 - Key exchange
 - Digital signatures



Why Quantum Computing is a threat?

- Quantum computers are able to perform tasks that a classical computer would need millions of years to complete in only a few seconds.
- Shor's algorithm is available on quantum computers to factorize very big numbers which is not possible to perform using classical computers.
- Shor's algorithm is known since 1994 but at that time quantum computers were theoretical.
- Nowadays quantum computers are a reality although they are quite limited at the moment.
- As it is known that in a few years quantum computers will be able to break communication, today's encrypted communication could be stored to be broken in the future (Harvest Now, Decrypt Later).
- Algorithms based on prime number factorization or discrete logarithm (included the elliptic discrete logarithm problem) are at risk.



What cryptography is at risk ?

Asymmetric (Signatures,
Encryption, Key Exchange)



Schemes that depend on classical hard mathematical problems where public / private key pairs are used.

At Risk

Symmetric
Encryption



Ciphers that use a secret key to both encrypt and decrypt data.

Safe (with large enough keys)

Hashes, HMACs¹



Digest algorithms that are used for fingerprinting and compressing data into a short ID.

Safe (with large enough keys)

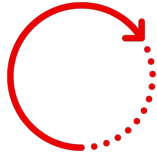


What is PQC?



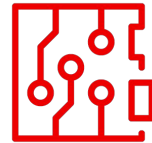
Post Quantum Cryptography (PQC) simplified

POST



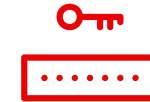
After...

QUANTUM



Refers to quantum computers which will be super fast¹ and able to crack today's security keys

CRYPTOGRAPHY



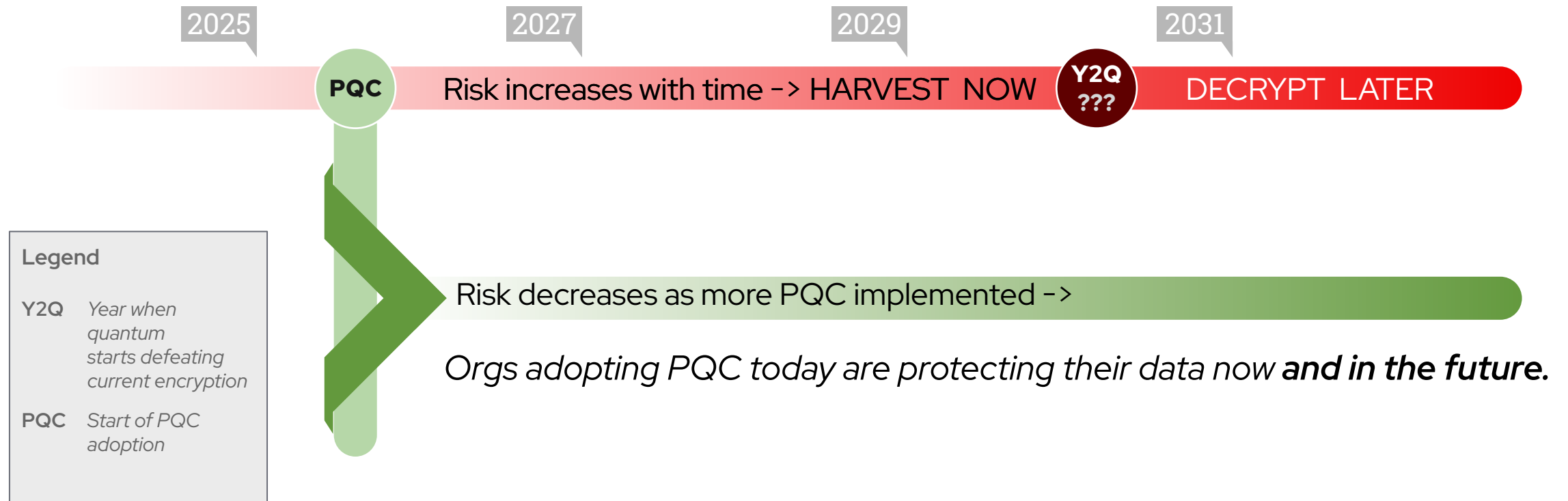
Refers to the process of protecting content and communications, keeping material authentic for intended users

Therefore, PQC simply refers to the ability to protect information after quantum computers become available.



Post-Quantum Cryptography (PQC) is a future challenge

But the threat is already here



Quantum Computing

- Nobody has a relevant quantum computer today.
- Three letter agencies have lots of storage.
- Store encrypted communications now, break them when a QC is available, get your passwords, medical records, etc. from today.

Booting Up: New NSA Data Farm Takes Root In Utah

SEPTEMBER 23, 2013 · 5:39 PM ET



Howard Berkes



The National Security Agency says its massive new data center near Salt Lake City will enhance the agency's ability to analyze the email, text message, cellphone and landline metadata it collects.

Rick Bowmer/AP



PQC will require changes to all software and hardware It's like Y2K, except... *we don't know the exact date*

Clock is ticking



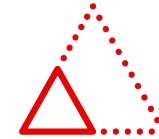
Gartner: By 2029, advances in quantum computing will make classic asymmetric cryptography unsafe and breakable by 2034.¹

Risk is real



Time to break RSA-2048 prime number factor encryption:
2020s computer: 300T years
Quantum computer: 10 sec.²

Demand is growing




The PQC market is estimated to grow from:

- 2024, 302.5 million USD
- 2029, 1.88 billion USD



PQC and EU



The screenshot shows the European Commission website. At the top, there is a navigation bar with the European Commission logo, a language selector set to 'EN', and a search bar. Below this is a blue header with the text 'Shaping Europe's digital future' and a menu with links: Home, Policies, Activities, News, Library, Funding, Calendar, Consultations, and AI Office. The main content area has a breadcrumb trail: Home > Library > A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography. Below this, it says 'POLICY AND LEGISLATION | Publication 23 June 2025'. The title of the document is 'A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography'. The text below the title states: 'The EU Member States, supported by the Commission, issued a roadmap and timeline to start using a more complex form of cybersecurity, the so-called post-quantum cryptography (PQC). Quantum computing has been identified as a threat to many cryptographic algorithms used to protect the confidentiality and authenticity of data. This threat can be countered by a timely, comprehensive and coordinated transition to Post-Quantum Cryptography (PQC). Therefore, on 11 April 2024, the Commission has published a [Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography](#). For the development of this Roadmap, the Commission recommended to establish a work stream on PQC with the NIS Cooperation Group. This document is the first deliverable and is meant to be a first high-level paper aimed at Member States. It includes a set of recommendations that Member States need to implement for a synchronised transition to PQC, as well as measures to ensure that all stakeholders are well informed on the quantum threat to cryptography.' To the right of the text is an image of a futuristic, glowing blue circuit board with a central glowing point. Below the image is the text 'AdobeStock © ipopba'. At the bottom left of the image area, it says 'Related topics'.

4. REVIEW

- (11) Member States should cooperate with the Commission to assess the effects of this Recommendation maximum three years after its publication, with a view to determine appropriate ways forward. This assessment should take into account the outcome of the work by the sub-group on Post-Quantum Cryptography of national experts.

Done at Brussels, 11.4.2024

For the Commission
Thierry BRETON
Member of the Commission



PQC and RHEL



Overall Implementation Strategy



Classical

Red Hat products and services use classical cryptography algorithms



PQ-Capable

Red Hat products or services include classical cryptography by default

PQC functions are configurable

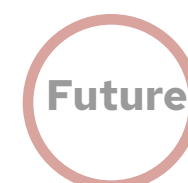
Classical and PQC available and both are supported (as available)



PQ-Ready

Red Hat products or services include PQC functions by default

Classical cryptography is configurable



Deprecation and Removal

Classical cryptography algorithms are marked as deprecated

Classical cryptography algorithms are removed

RHEL 10 will include the first installment of QRAs:

- ML-KEM [FIPS 203]
- ML-DSA [FIPS 204]



Red Hat Enterprise Linux 10

The first Linux distribution to be Post-Quantum Capable

- RHEL 10 includes the first installment of Post Quantum Cryptography algorithms OpenSSL, ML-KEM (FIPS 203), SLH-DSA (FIPS 205), and ML-DSA (FIPS 204) that enable secure key-exchange, encryption, and signing, with more functionality planned for subsequent releases.
- No need to change application code or configuration, **RHEL crypto-policies!**
- To our knowledge, there are no other enterprise level Linux distributions that are even close to matching RHEL's PQC capabilities and planned roadmap:
 - SUSE's 15 SP6 was released June 2024⁵, before NIST finalized the PQC algorithms
 - Canonical's Ubuntu uses codecrypt⁶, which does not implement the final NIST PQC algorithms

5: <https://www.suse.com/c/announcing-suse-linux-enterprise-15-sp6-the-linux-choice-for-security-and-compliance-in-a-reliable-it/>

6: <https://netbsd.pkgs.org/9/netbsd-aarch64/codecrypt-1.8nb1.tgz.html>



Implementations of PQC available in RHEL

All PQC algorithms in Red Hat Enterprise Linux 10.0 are available as Technology Preview.

RHEL 10.1 goes GA in 2025Q4 with these algorithms available **per default**.

Available on all platforms:

x86_64, aarch64, s390x, ppc64le



Key Exchange

key exchange where PQC protects confidentiality of communication against "harvest now, decrypt later" attacks



Signatures

PQC signature algorithms are available in Red Hat Enterprise Linux 10 to protect data integrity and authenticity.



Implementations of PQC available in RHEL



Post-quantum signature algorithm in **TLS**

PQC signature algorithms are available in Red Hat Enterprise Linux 10 to protect data integrity and authenticity.

TLS:

- ▶ TLS 1.3 required
- ▶ Graceful upgrades to PQC will be required for TLS for a while.
- ▶ Generally not yet supported by web browsers
- ▶ Prepare to support two certificates simultaneously.
 - two parallel certificate chains
 - supported with OpenSSL
- ▶ SHL-DSA not part of TLS due to performance impact (but available in OpenSSL)

- **Algorithms:** ML-DSA
 - ML-DSA-44
 - ML-DSA-65
 - ML-DSA-87
- **Classic:**
 - RSA-SHA256
 - ECDSA-SHA384
 - ...
- Supported: OpenSSL, LibNSS, GnuTLSz



Implementations of PQC available in RHEL



Post-quantum key exchange in **SSH**

key exchange where PQC protects confidentiality of communication against "harvest now, decrypt later" attacks

- **Algorithm:** mlkem768x25519-sha256
 - ML-KEM-768
 - Default by crypto-policy module
- **Algorithm:** sntrup761x25519-sha512
 - Not default, can be configured



PQC demo

1. exchange key:
 - a. establish connection and encrypt communication
 - b. ML-KEM per default from RHEL 10.1, e.g. with ssh
2. signature algorithm:
 - a. identify entity (server, client) uniquely
 - b. ML-DSA available for hybrid setup from RHEL 10.1, e.g. curl
 - i. no general browser support yet



exchange key

RHEL 9 (default)

```
[root@z15l43 ~]# ssh -v root@10.0.173.15 2>&1 | grep kex:
debug1: kex: algorithm: curve25519-sha256
debug1: kex: host key algorithm: ssh-ed25519
debug1: kex: server->client cipher: aes256-gcm@openssh.com MAC: <implicit> compression: none
debug1: kex: client->server cipher: aes256-gcm@openssh.com MAC: <implicit> compression: none
debug1: kex: curve25519-sha256 need=32 dh_need=32
debug1: kex: curve25519-sha256 need=32 dh_need=32
The authenticity of host '10.0.173.15 (10.0.173.15)' can't be established.
ED25519 key fingerprint is SHA256:VU/vSyrYXssaxfQqS4RAjw+bQz5639vfqAQKbKROFpI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? ^C
[root@z15l43 ~]# cat /etc/redhat-release
Red Hat Enterprise Linux release 9.7 Beta (Plow)
```

RHEL 10.1 (default)

```
root@rdu-z16-l28:~# ssh -v root@10.0.173.15 2>&1 |grep kex:
debug1: kex: algorithm: mlkem768x25519-sha256
debug1: kex: host key algorithm: ssh-ed25519
debug1: kex: server->client cipher: aes256-gcm@openssh.com MAC: <implicit> compression: none
debug1: kex: client->server cipher: aes256-gcm@openssh.com MAC: <implicit> compression: none
debug1: kex: mlkem768x25519-sha256 need=32 dh_need=32
debug1: kex: mlkem768x25519-sha256 need=32 dh_need=32
root@10.0.173.15's password:
root@rdu-z16-l28:~# cat /etc/redhat-release
Red Hat Enterprise Linux release 10.1 Beta (Coughlan)
```



signature algorithm

RHEL 9
(default)

```
[root@rhel-9 ~]# curl -k -v --cert-status https://192.168.122.21/index.html 2>&1 |grep -A6 "Server certificate"
* Server certificate:
*  subject: CN=localhost
*  start date: Sep 18 15:26:12 2025 GMT
*  expire date: Sep 18 15:26:12 2026 GMT
*  issuer: CN=RSA test CA
*  SSL certificate verify result: unable to get local issuer certificate (20), continuing anyway.
```

RHEL 10.1
(default)

```
[root@rhel-10 ~]# curl -k -v --cert-status https://192.168.122.21/index.html 2>&1 |grep -A6 "Server certificate"
* Server certificate:
*  subject: CN=localhost
*  start date: Sep 18 15:26:12 2025 GMT
*  expire date: Sep 18 15:26:12 2026 GMT
*  issuer: CN=ML-DSA test CA
*  SSL certificate verify result: unable to get local issuer certificate (20), continuing anyway.
*  Certificate level 0: Public key type ML-DSA-65 (15616/192 Bits/secBits), signed using ML-DSA-65
```



PQC and the European Union

- [A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography](#)
- [EU reinforces its cybersecurity with post-quantum cryptography](#)
- [Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography](#) (multi language documents), published on the April 11, 2025.
- [European Quantum Policies](#)
- [Post-quantum cryptography in Red Hat Enterprise Linux 10](#)
-





Connect

Thank you



linkedin.com/company/red-hat



facebook.com/redhatinc



youtube.com/user/RedHatVideos



twitter.com/RedHat

