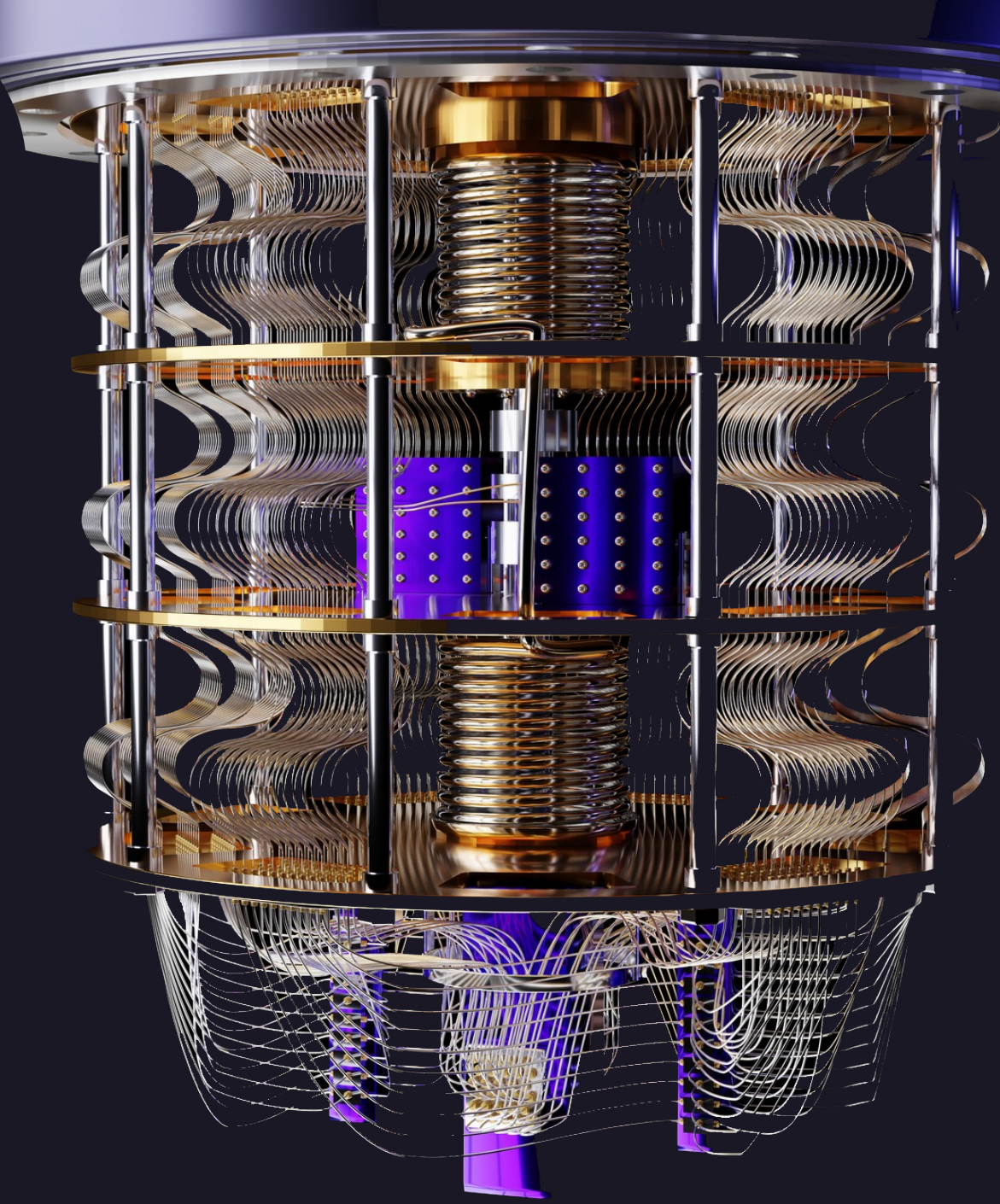
Quantum and PKI

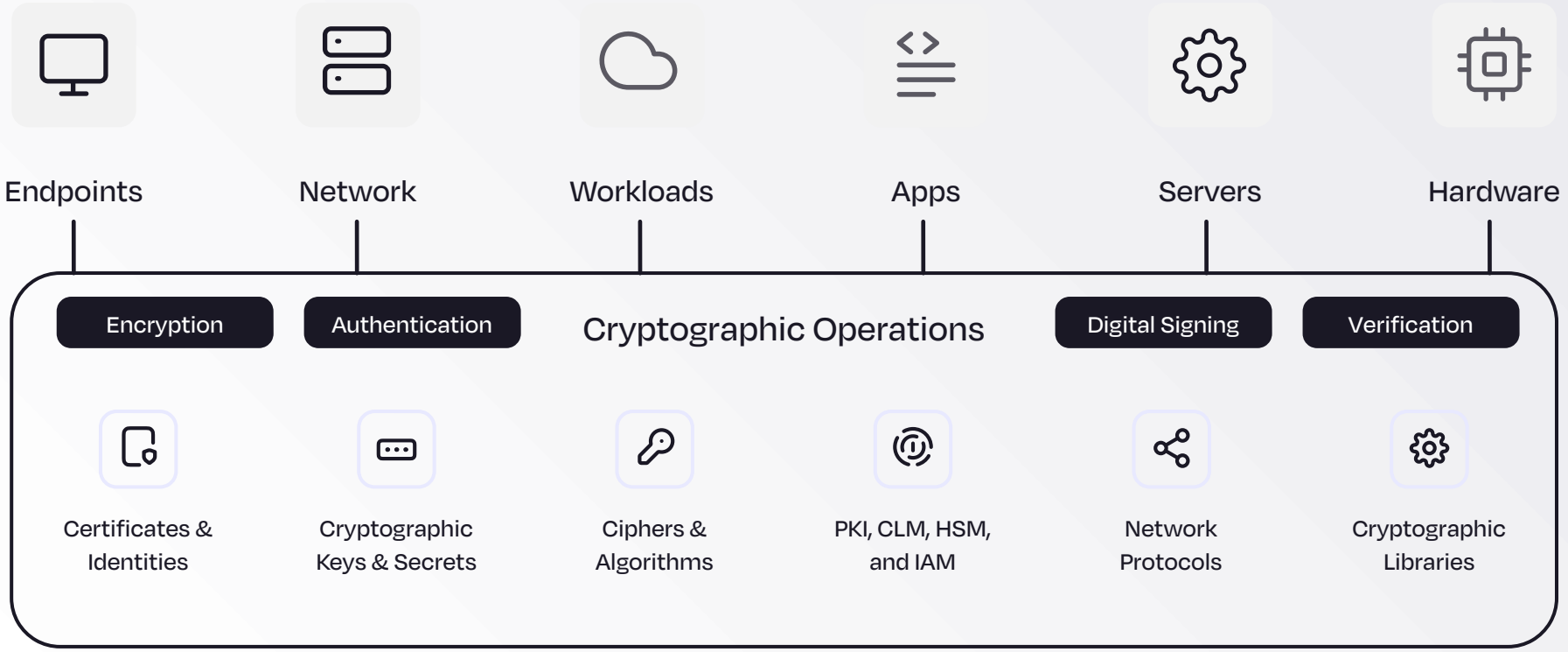
Preparing for Disruptive Changed in Digital Trust

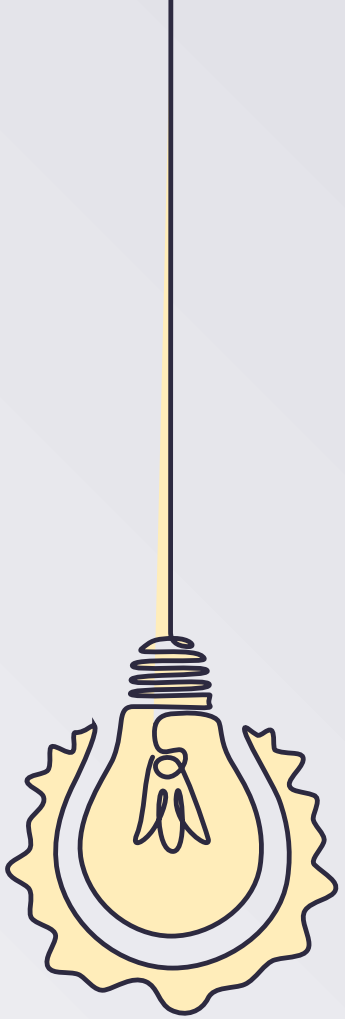
Tomas Gustavsson
Chief PKI Officer



/// DISRUPTION #3

Cryptography is Critical Infrastructure





“

According to Gartner, by 2029, advances in quantum computing will make conventional asymmetric cryptography *unsafe to use*.

Source: Gartner, How to Mitigate the Cryptography Risks Posed by Quantum Computing, By Thomas Lintemuth, Craig Lawson, Mark Horvath, 21 February 2025. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Gartner subscribers can access the report here: https://www.gartner.com/document/6199155

Quantum is the catalyst. Agility is the strategy.

Harvest Now, Decrypt Later

- Long-life data is already being targeted
- Archives and backups expand exposure
- Forward secrecy won't hold forever
- **Breach now. Impact later**

Trust Now, Forge Later

- Signed code, firmware and contracts at risk
- Certificate chains are vulnerable
- Trust can be forged at scale
- **Broken roots break everything**

A migration measured in years, not months

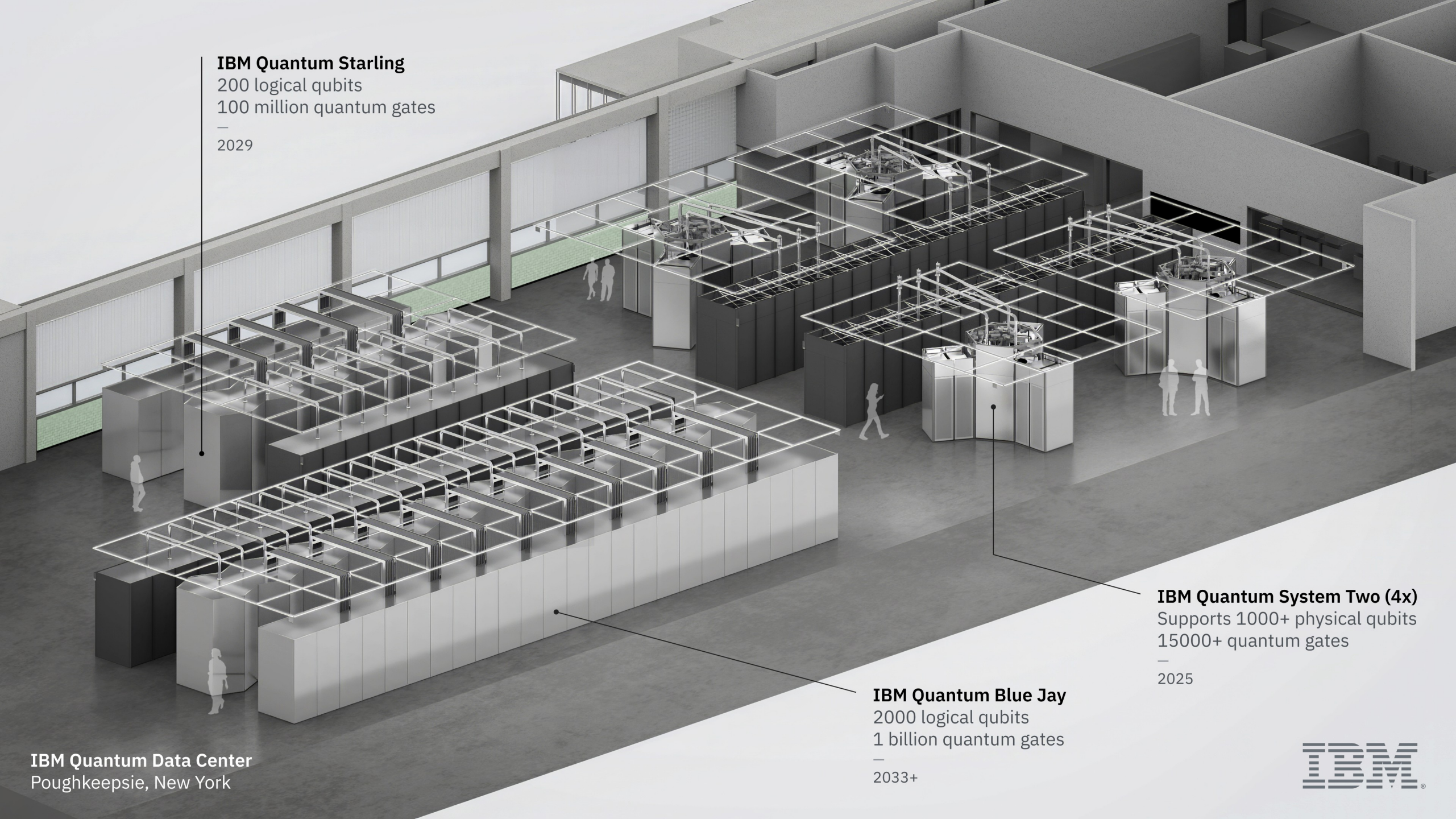
NIST has finalized post-quantum standards. The estate-wide swap — certificates, code signing, protocols, hardware roots — takes years, not a single release cycle.

KEYFACTOR

2029 ↴

Large-scale fault-tolerant systems

IBM Proprietary Information | © 2026 IBM Corporation


IBM Quantum Starling
200 logical qubits
100 million quantum gates
—
2029
IBM Quantum System Two (4x)
Supports 1000+ physical qubits
15000+ quantum gates
—
2025
IBM Quantum Blue Jay
2000 logical qubits
1 billion quantum gates
—
2033+
IBM Quantum Data Center
Poughkeepsie, New York

Official Deadline Approaching

1. By **31.12.2026**:
   - At least the *First Steps* have been implemented by all Member States.
   - Initial national PQC transition roadmaps have been established by all Member States.
   - PQC transition planning and pilots for high- and medium-risk use cases have been initiated.
2. By **31.12.2030**:
   - The *Next Steps* have been implemented by all Member States.
   - The PQC transition for high-risk use cases has been completed.
   - PQC transition planning and pilots for medium-risk use cases have been c pleted.
   - Quantum-safe software and firmware upgrades are enabled
3. By **31.12.2035**:
   - The PQC transition for medium-risk use ca
   - The PQC transition for low-risk us

EU Coordinate 2025

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	***Disallowed*** after 2035
	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035

IST IR 8

France to stop certifying products without quantum-safe encryption

45 47

PRESIDENTIAL ACTIONS

SECURING THE NATION AGAINST ADVANCED CRYPTOGRAPHIC ATTACKS

Executive Orders | June 22, 2026

…es organizations should treat 2029 as a p…
…ajor PQC migration activity for quantum-vulnerab…
Planning should begin now. This is not a prediction
fail in 2029. Rather, it is a advisory that, after 2029
before migrating to PQC should be viewed as add…

X9 Member News - Quantum Update – April 2026

ECCG Agreed Cryptographic Mechanisms v3 draft - 2 June; PQC becomes “state of the art cryptography”

KEYFACTOR

RSA/DH/ECDH ->
ML-KEM / FIPS 203

RSA/ECDSA ->
ML-DSA / FIPS 204

RSA/ECDSA ->
SLH-DSA / FIPS 205

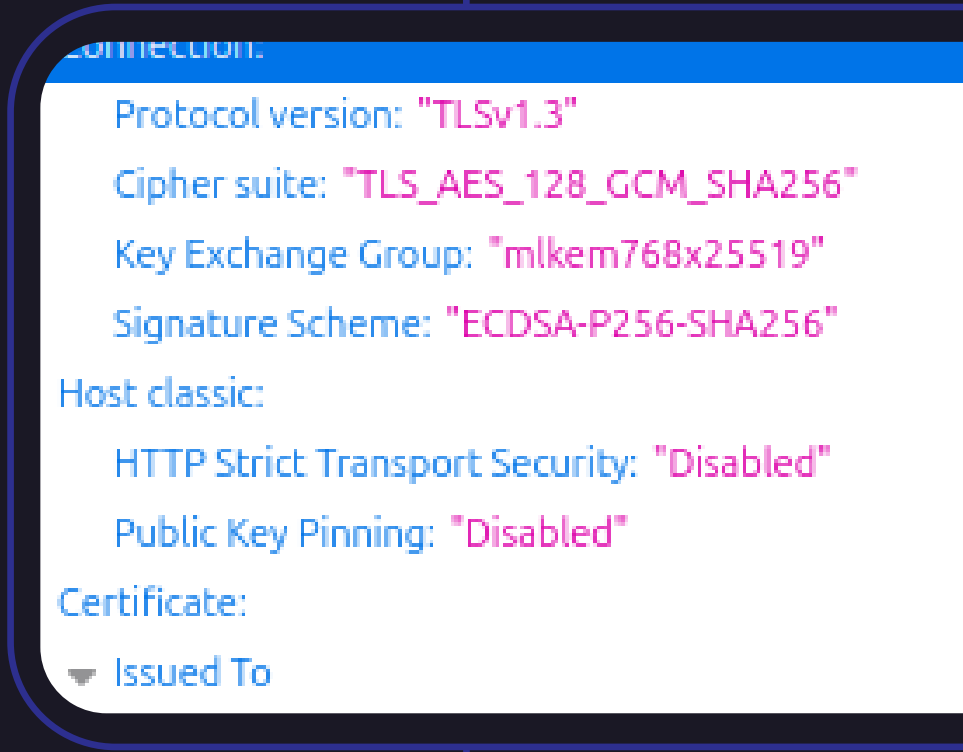
KEYFACTOR

Off-the-shelf TLS – OK

Ubuntu 26.04 - OpenSSL 3.5

- apt install apache2
- a2enmod ssl

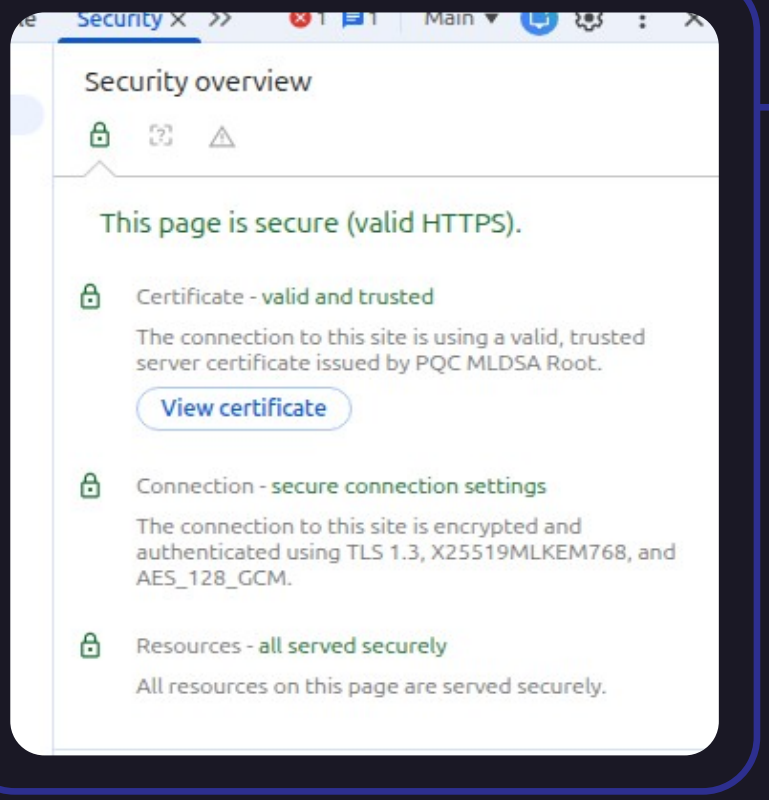
```
<VirtualHost *:443>
    ServerName www.classic.com
    DocumentRoot /var/www/classic
    SSLEngine on
    SSLCertificateFile /home/user/openssl/apache2/classic-cert.pem
    SSLCertificateKeyFile /home/user/openssl/apache2/classic-key.pem
    SSLCertificateChainFile /home/user/openssl/apache2/classic-ca.pem
</VirtualHost>
```

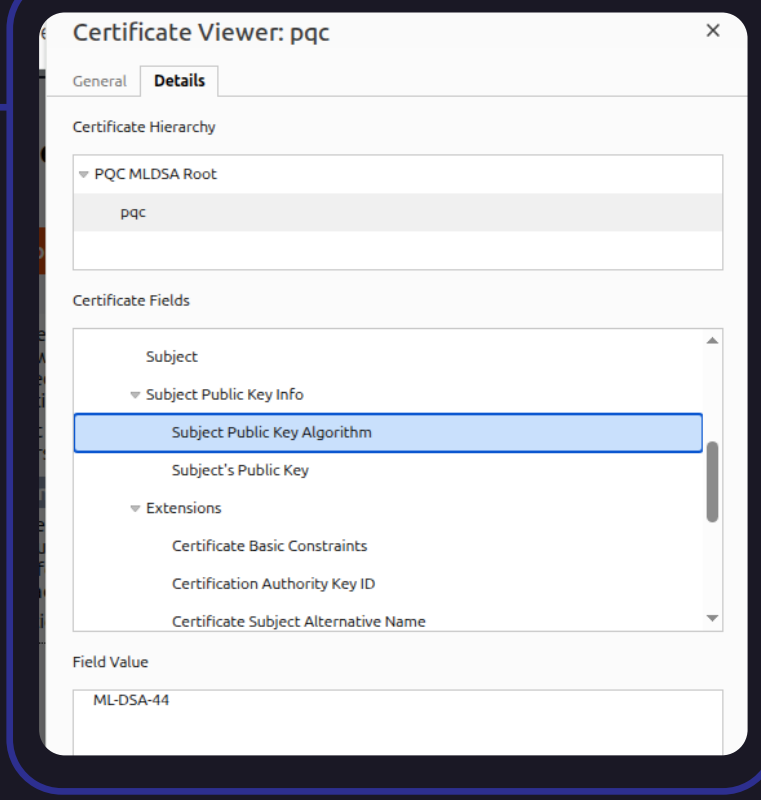


⚠ **Multiple SSLCertificateFile options work**

KEYFACTOR

Off-the-shelf TLS – OK





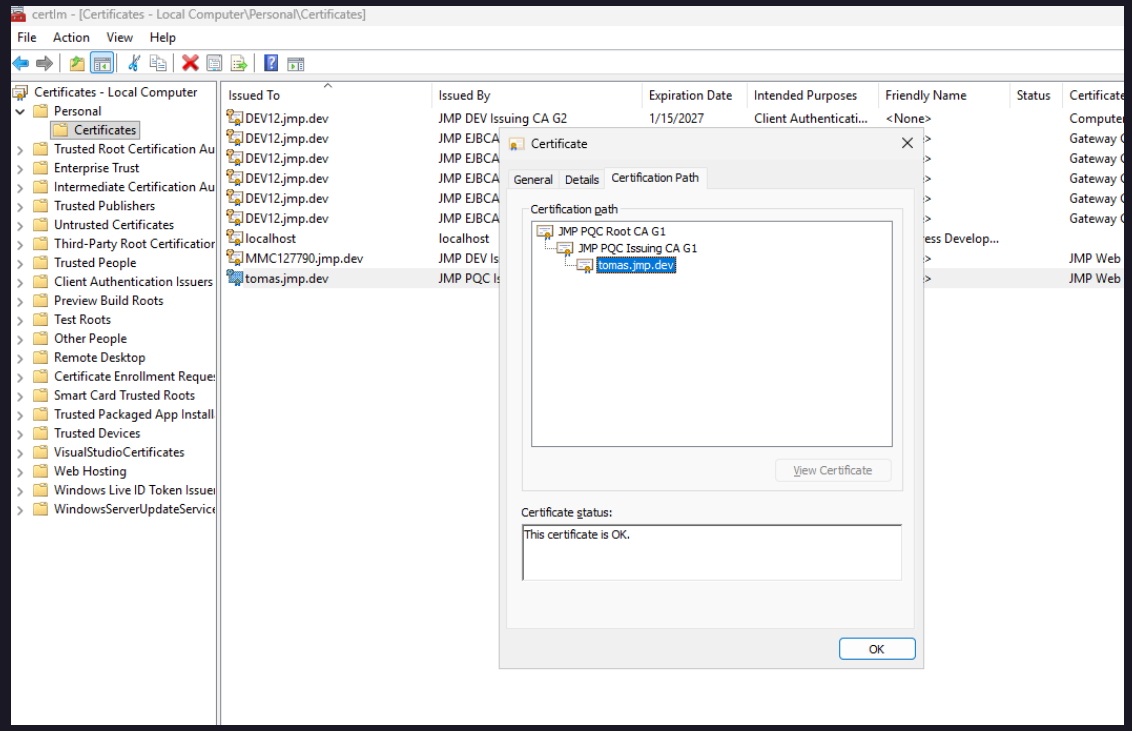
Chrome 150 – released end of June

KEYFACTOR

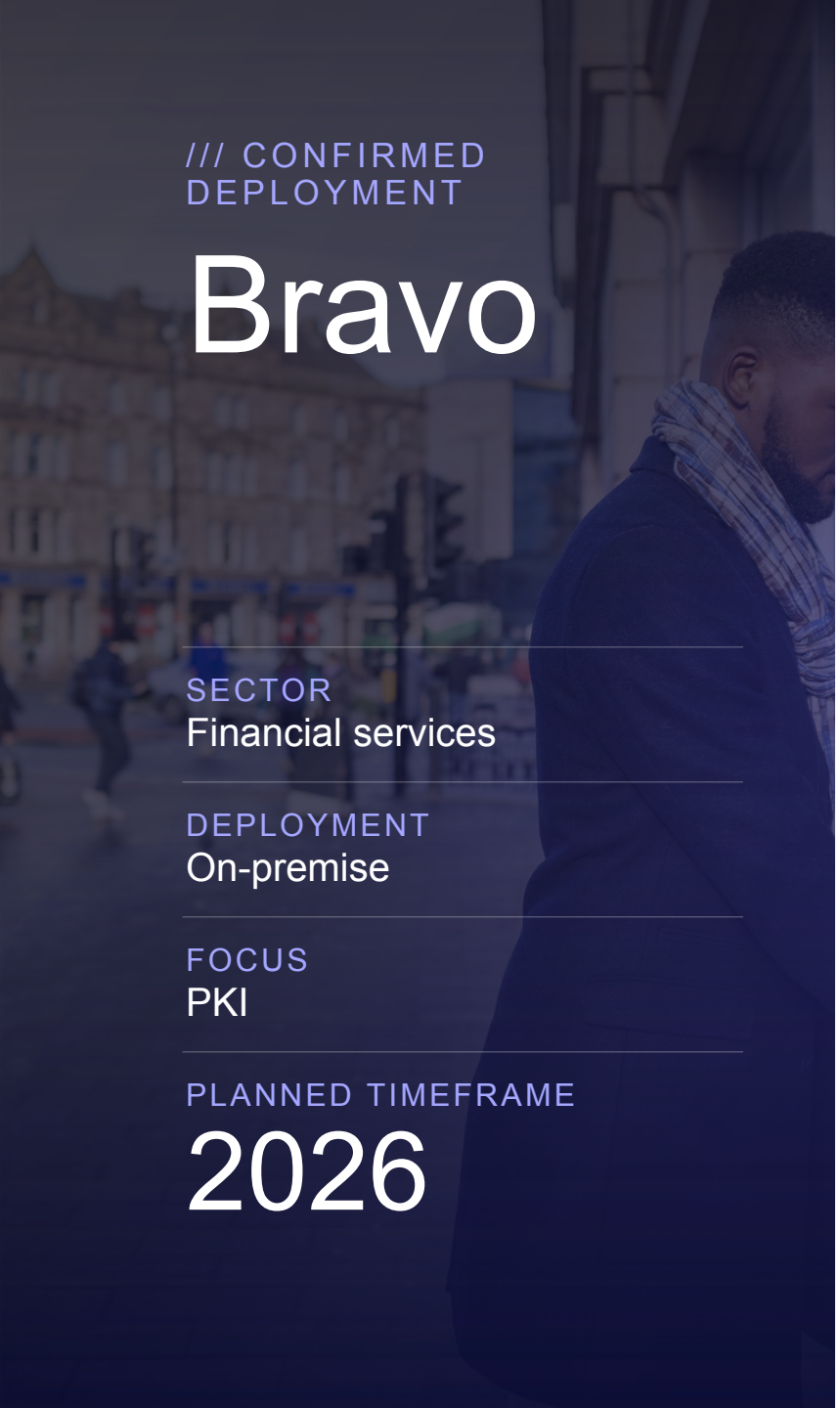
Off-the-shelf Windows

Administrator: Windows PowerShell

```
PS C:\WINDOWS\system32> certutil -store MY tomas.jmp.dev
MY "Personal"
================ Certificate 5 ================
Serial Number: 690000000ab0f5ac82d72c6f0c00000000000a
Issuer: CN=JMP PQC Issuing CA G1
 NotBefore: 5/21/2026 11:13 AM
 NotAfter: 5/20/2028 11:13 AM
Subject: CN=tomas.jmp.dev
Non-root Certificate
Template: JMPWebServerMLDSA44, JMP Web Server ML-DSA 44
Cert Hash(sha1): 2c52e093b5da30cf8aa4449f48763fdda5235259
  Key Container = te-JMPWebServerMLDSA44-ba17c7db-18d7-401f-a0a9-ea2e779cd42d
  Unique container name: 3be4889ec5b376efa50b7a290d20db8d_c23ac4d1-3357-4c96-9e3
  Provider = Microsoft Software Key Storage Provider
Private key is NOT plain text exportable
Signature test passed
CertUtil: -store command completed successfully.
PS C:\WINDOWS\system32>
```



KEYFACTOR



/// CONFIRMED DEPLOYMENT

Bravo

SECTOR
Financial services

DEPLOYMENT
On-premise

FOCUS
PKI

PLANNED TIMEFRAME
2026

Interoperability changed the choice

ML-DSA production root	Organizational trust enables full eco system migration
Pure PQC preferred	Chimera evaluation did not meet interoperability needs
Banking identity ecosystem	Tens of millions active certificates
Authentication and digital signatures	Wide RP eco system
Extensive previous testing	Speed, Validation, Relying parties

/// CONFIRMED DEPLOYMENT

Alpha

SECTOR
Consumer electronics

DEPLOYMENT
On-premise

FOCUS
PKI and time stamping

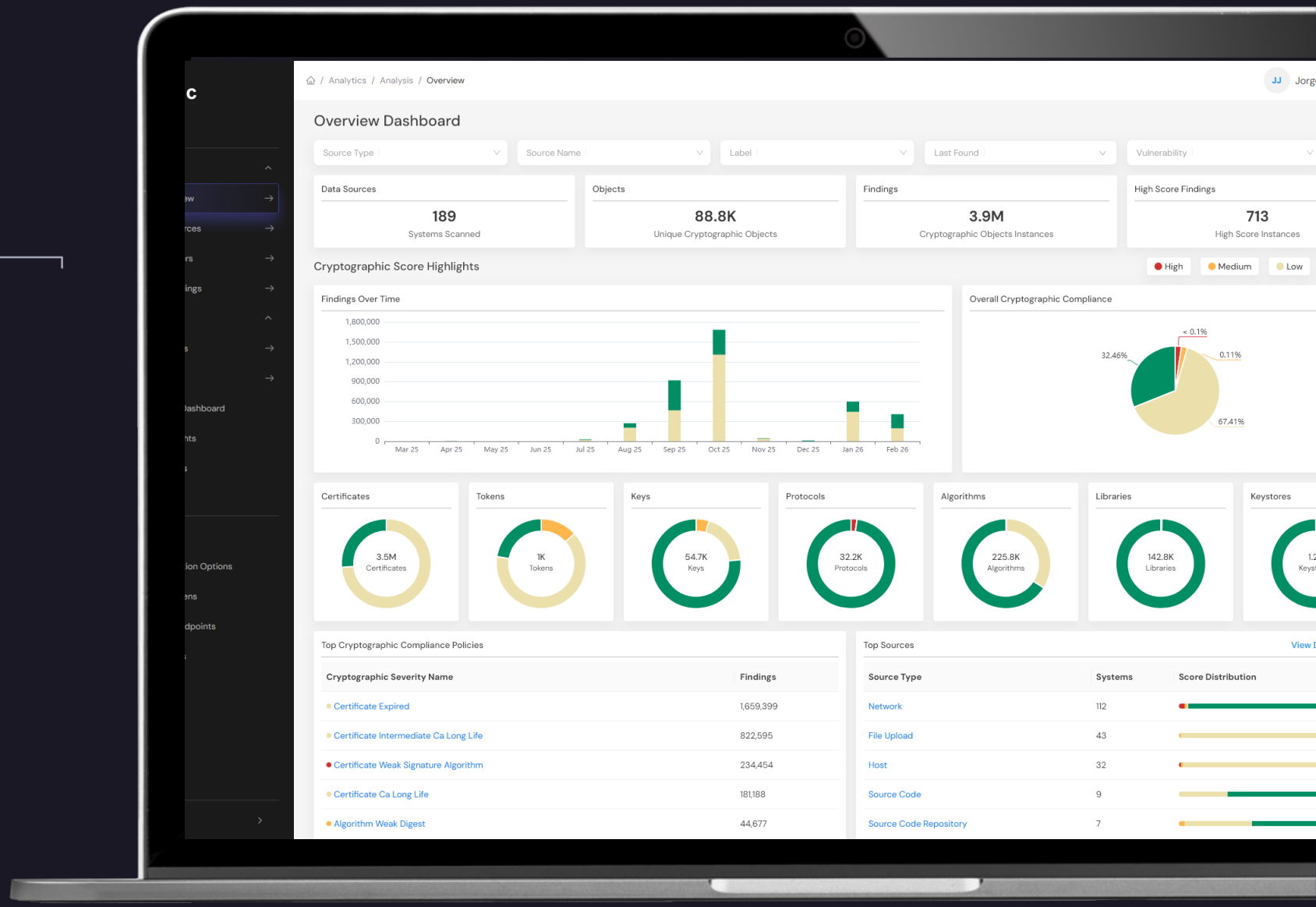
PLANNED TIMEFRAME
2026

Composite signing in production

- Composite CA in production first half of 2026 — RSA-PSS + ML-DSA, HSM backed
- Initial use cases: code signing — Minimal effect on signed software
- Composite time stamps also part of the design — Relatively low number of certificates and signatures
- Organizational trust enables multiple product teams — Control of the end-to-end supply chain
- Backwards interoperability — Requires device updates

Cryptographic Inventory

- X509 Certificates
- Tokens
- Keys
- Protocols
- Algorithms
- Libraries
- Keystores



Maturity Levels

> The PQCMM defines six maturity levels — from Level 0 (no PQC implemented) to Level 5 (fully optimised, PQC-by-default). Each level has precise criteria, assessment questions, and evidence requirements.

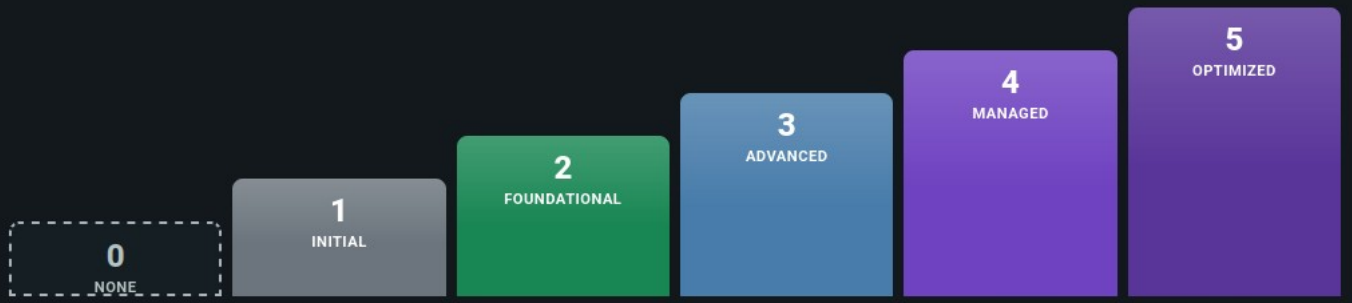
PQC MATURITY MODEL (PQCMM)

Maturity Levels
- 0 — None
- 1 — Initial
- 2 — Foundational
- 3 — Advanced
- 4 — Managed
- 5 — Optimized

Adopting the Model
Assessing a Product
Certified Products
Glossary
FAQ
Version History

Maturity Levels

The PQCMM defines **six maturity levels** (0–5) for post-quantum cryptography adoption in products and services. Each level builds on the previous one, defining what PQC readiness means in practice — from the complete absence of any quantum-safe activity, all the way to a fully optimised, PQC-by-default product or service.



LEVEL	NAME	SUMMARY
0 — None	No PQC implemented	PQC might be in the preparation phase, but no quantum-safe algorithms have matured into the product.
1 — Initial	Available for testing	PQC algorithms are available but for testing and evaluation only; not production-ready.
2 — Foundational	Production-ready	At least one quantum-safe algorithm is available in production and meets relevant standards.
3 — Advanced	Inventory & Agility	Cryptographic inventory (SBOM/CBOM) is in place, and the product supports crypto agility.

KEYFACTOR

PQC MATURITY MODEL (PQCMM)

Maturity Levels

0 — None
1 — Initial
2 — Foundational
3 — Advanced
4 — Managed
5 — Optimized

Adopting the Model
Assessing a Product
Certified Products
Glossary
FAQ
Version History

SWITCH VERSION

1.0.1 LATEST RELEASE

1.1.0 — Draft

Level 3 adds full cryptographic visibility and agility. Vendors can account for all cryptographic use cases and update algorithms with major redesign.

Criteria

A product meets Level 3 when all Level 2 criteria are met, plus:

Criterion 3.1.1

A **full cryptographic inventory** is maintained, covering all use cases within the product where cryptography is applied. The inventory address every applicable category in the **Cryptographic Inventory Taxonomy** below; categories that do not apply to the product mus marked *not applicable* with a written justification — categories may not be omitted.

Criterion 3.1.2

Non-quantum-safe features are **formally documented and flagged** — either for planned remediation, risk acceptance, or compensati controls.

Criterion 3.1.3

A **Software Bill of Materials (SBOM)** or equivalent component inventory is available, enabling consumers to identify cryptographic dependencies.

Criterion 3.1.4

Crypto-agility mechanisms exist for key product features: at least two algorithms can be selected for the same cryptographic role th configuration (for example two different signature algorithms, or a pure-PQC vs. hybrid option in the same role) without major archit redesign or a hardware refresh. Selecting only between parameter sets of the same algorithm (for example ML-KEM-768 and ML-KE does not by itself satisfy this criterion.

KEYFACTOR

Level 4 adds a CBOM, zero-legacy capability, and explicit hybrid/composite support. Suitable for high-assurance and regulated environments.

Criteria

A product meets Level 4 when all Level 3 criteria are met, plus:

Criterion 4.1.1

A Cryptographic Bill of Materials (CBOM) is maintained, detailing each algorithm in use, key sizes, protocol contexts, and usage purposes.

Criterion 4.1.2

Zero-Legacy Capability: the product can be configured to disable **all** non-quantum-safe algorithms throughout the product — including in low-level components such as boot, firmware update signing, hardware-bound operations, and internal diagnostics — while remaining fully functional. *Zero legacy means zero legacy.* If a non-quantum-safe algorithm cannot be disabled in any in-scope component, the product does not meet Level 4 for that component, and an assessment must record this as a finding that caps the product's level.

Criterion 4.1.3

Thank you!

For your attention and time