

Post Quantum Cryptography

Implications for eID 's and Trust Services

Date	25/09/2025
Location	17 th CA-Day, Split
Author	Jan Klaußner

**Who of YOU has actively
used PQC today?**

Everyone uses Post-Quantum-Crypto!

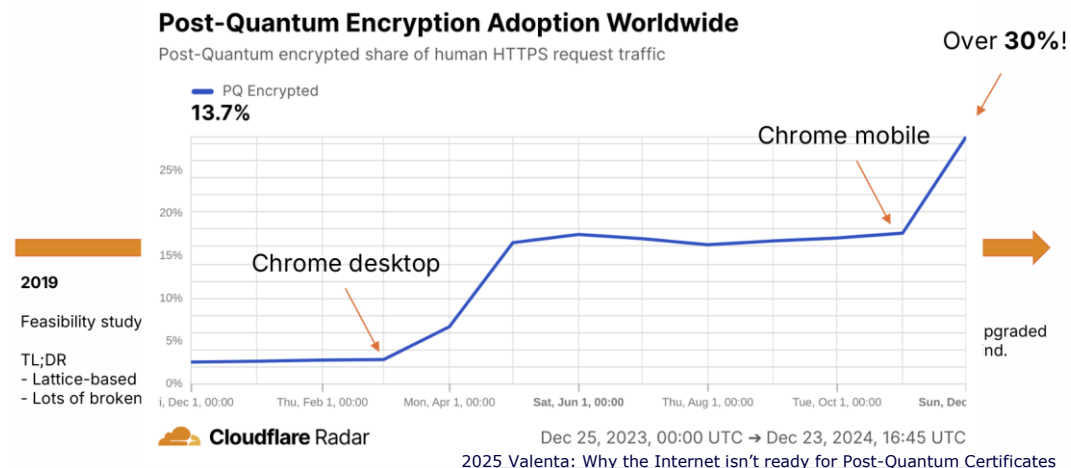
Messengers have adopted PQC

WhatsApp, Signal, iMessage adapted their protocols, use hybrid key exchange with ML-KEM

Big parts of the web adopted PQC

Chrome, Firefox, ... use hybrid key exchange with ML-KEM by default.

Content Delivery Network Cloudflare serves 20% of the web content and offers hybrid key exchange with ML-KEM



eIDAS

PQC Migration going well?

Heterogeneous system

Many different stakeholders with varying (performance) constraints and update cycles

Protocol ossification

Despite being designed to be upgradeable, any flexibility that isn't used in practice is probably broken, because of faulty implementations

Mixed signals

Massive amount of new work on PQC appears like it is still not ready, even for experts
Hybrids as European requirement



EU Roadmap following Commission's Recommendation on PQC

Milestones for high-risk and medium-risk use cases

Risk-based approach to planning

Starting date is not a moving target anymore



**A Coordinated Implementation
Roadmap for the Transition to
Post-Quantum Cryptography**

Part 1, Version: 1.1, EU PQC Workstream

11.06.2025

i Timeline for the transition to PQC**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 completed.
- Quantum-safe software and firmware upgrades are enabled by default.

3. By 31.12.2035:

- The PQC transition for medium-risk use cases has been completed.
- The PQC transition for low-risk use cases has been completed as much as feasible.

Do I need to act?



URGENT ADOPTERS

banks, hospitals, telecom providers, car manufacturers, etc.



REGULAR ADOPTERS

web shops, building companies, schools, etc.



CRYPTOGRAPHY EXPERTS

IT infrastructure providers, standard organizations, etc.

The PQC Migration Handbook, December 2024

Do I need to act?

NIS 2

**EU Implementing Regulation 2024/2690
aim for crypto agility**

**ENISA guidance
consider PQC**



URGENT ADOPTERS

banks, hospitals, telecom providers, car manufacturers, etc.

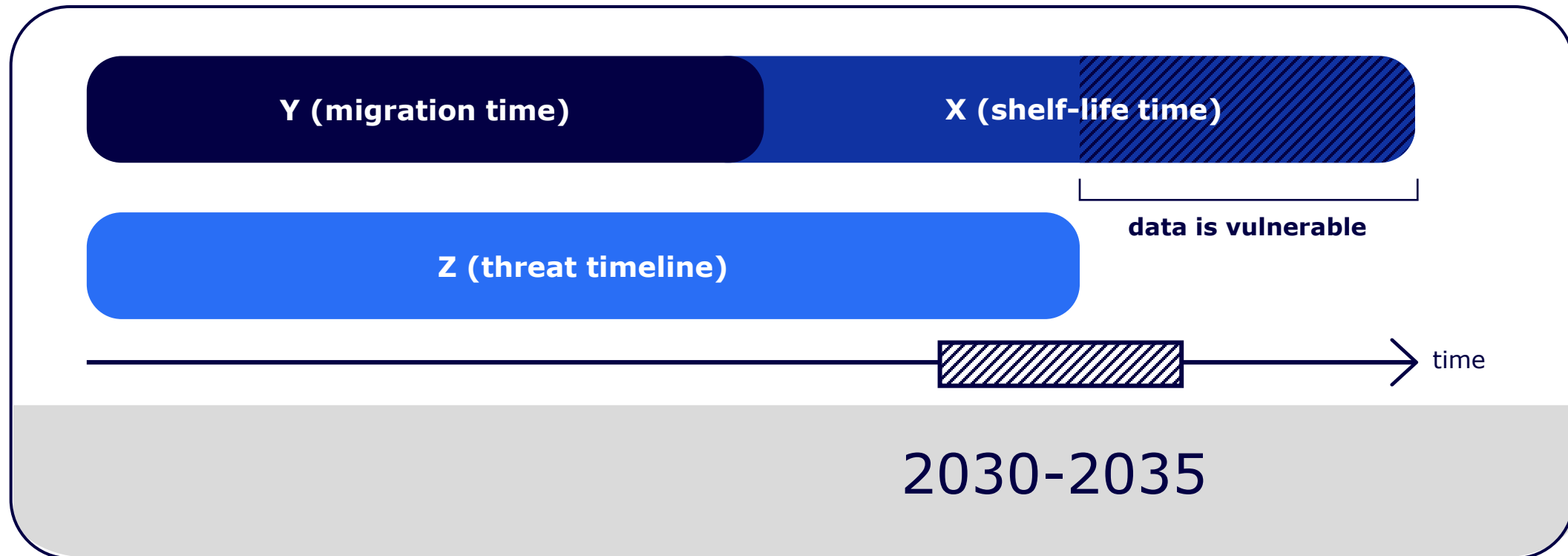


CRYPTOGRAPHY EXPERTS

IT infrastructure providers, standard organizations, etc.

The PQC Migration Handbook, December 2024

Mosca's Theorem and eIDAS



Prepare...

No regret moves

- Cryptographic asset and policy management
- Regulatory requirements
- Risk assessment
- Supply chain dependencies
- ...

and become Crypto Agile!

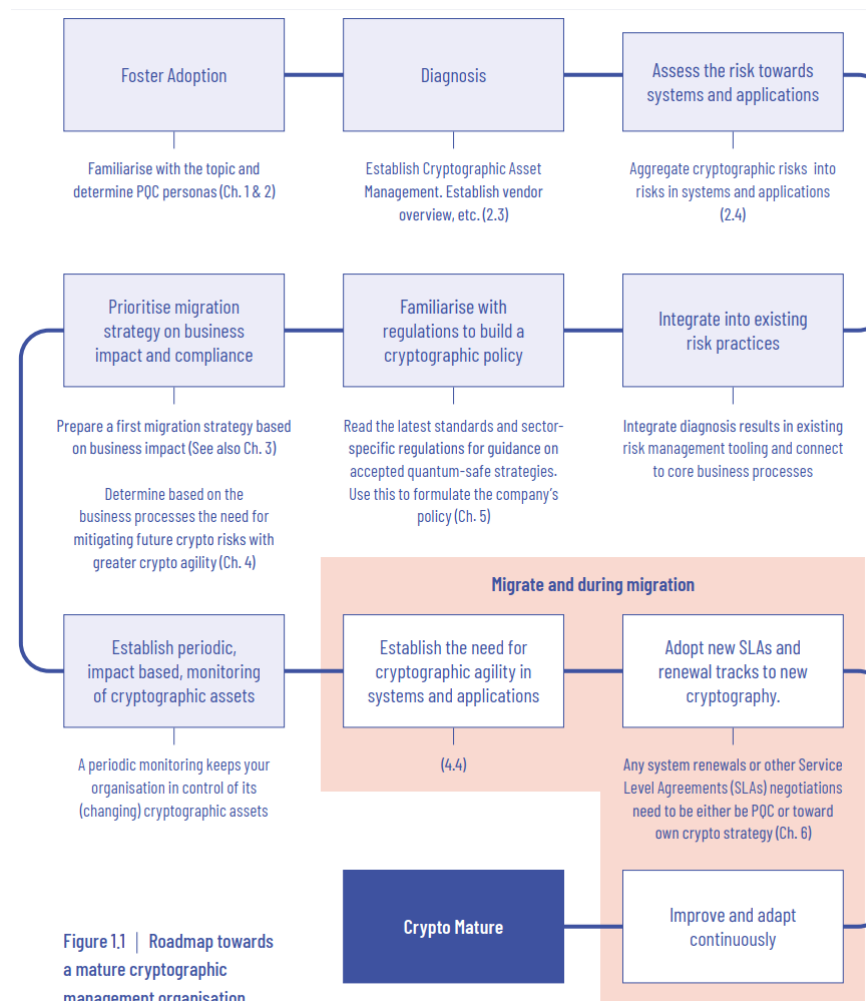


Figure 1.1 | Roadmap towards a mature cryptographic management organisation.

The PQC Migration Handbook, December 2024

Thank you.

Jan Klausner

Bundesdruckerei GmbH
Innovation
email: jan.klaussner@bdr.de

Please note: This presentation is the property of Bundesdruckerei GmbH.
All of the information contained herein may not be copied, distributed or published,
as a whole or in part, without the approval of Bundesdruckerei GmbH.
© 2025 by Bundesdruckerei GmbH