OPEN INDUSTRY 4.0 ALLIANCE

White Paper

Preparing for a Secure Future – Post-Quantum Cryptography

IMPRINT

Publisher

Open Industry 4.0 Alliance

Christoph Merian-Ring 12, 4153 Reinach, Switzerland

https://openindustry4.com

info@openindustry4.com

Status

File: Preparing for a Secure Future – Post-Quantum Cryptography

November 21st, 2025 – Version 1

Editor

Lucas Wolf (Open Industry 4.0 Alliance)

Authors

Andres Prieto (WIBU-SYSTEMS AG)

Bjoern Jansen (secunet Security Networks AG)

Florian Handke (Campus Schwarzwald)

Makan Rafiee (secunet Security Networks AG)

Introduction

Post-Quantum Cryptography (PQC) is gaining attention across industries, although initiatives appear to progress at different speeds. Activities are already visible in IT and enterprise systems, while comparable momentum in production and process technology seems less pronounced. The reasons for this may vary, and it is not yet clear whether this perception reflects the actual situation.

To establish a shared understanding and initiate an exchange within the Open Industry 4.0 Alliance, the Industrial Cybersecurity Working Group has compiled the following information on PQC. It is intended as both an initial and a complementary reference that helps us explore the questions: Where do we stand as Alliance members, what is our shared objective, and how do we get there?

Motivation

The security of today's digital systems relies fundamentally on classical asymmetric cryptography such as RSA and Elliptic Curve Cryptography (ECC). These methods derive their strength from mathematical problems that are considered infeasible to solve with the computational power available to conventional systems.

This foundation is challenged by the expected development of powerful quantum computers. Through specialized and efficient algorithms, most prominently the Shor algorithm, such machines will be able to break the mathematical assumptions that classical asymmetric cryptography depends on within practical time frames.

Asymmetric cryptography is affected most directly because its core security assumptions, such as the factorization of large integers in RSA or the discrete logarithm problem in ECC, become tractable under quantum algorithms. Symmetric cryptography, such as AES, is also impacted, but typically a longer key size is sufficient to compensate for the quadratic speed-up enabled by the Grover algorithm. Asymmetric cryptography, by contrast, requires a fundamental change in underlying mathematical constructions.

Given these developments and the potential long-term impact on industrial communication, secure device onboarding, digital identities, and cross-company data exchange, organizations need to address Post-Quantum Cryptography in order to maintain trust in connected systems over time.

Current Situation

Cryptographically relevant quantum computers are not yet available, but the concept of harvest now, decrypt later already presents a tangible risk. Attackers can intercept and store encrypted data today with the intention of decrypting it in the future once quantum capabilities mature. As a result, sensitive information, including data from industrial environments, is potentially at risk even before large-scale quantum computers exist.

The introduction of Post-Quantum Cryptography is required to secure authentication, digital signatures, communication channels, and firmware or software updates in the long term. The primary challenge is not the development of new algorithms but their integration into existing industrial infrastructures. Long-lived systems, such as those found in production environments and mechanical engineering, need an early migration strategy to maintain security and trustworthiness across the entire lifecycle.

As part of its international standardization process, the National Institute of Standards and Technology (NIST) selected three Post-Quantum Cryptography algorithms in 2024:

NOTE

ML-KEM (Module Lattice-based Key Encapsulation Mechanism) for key establishment and encryption

ML-DSA (Module Lattice-based Digital Signature Algorithm) for digital signatures

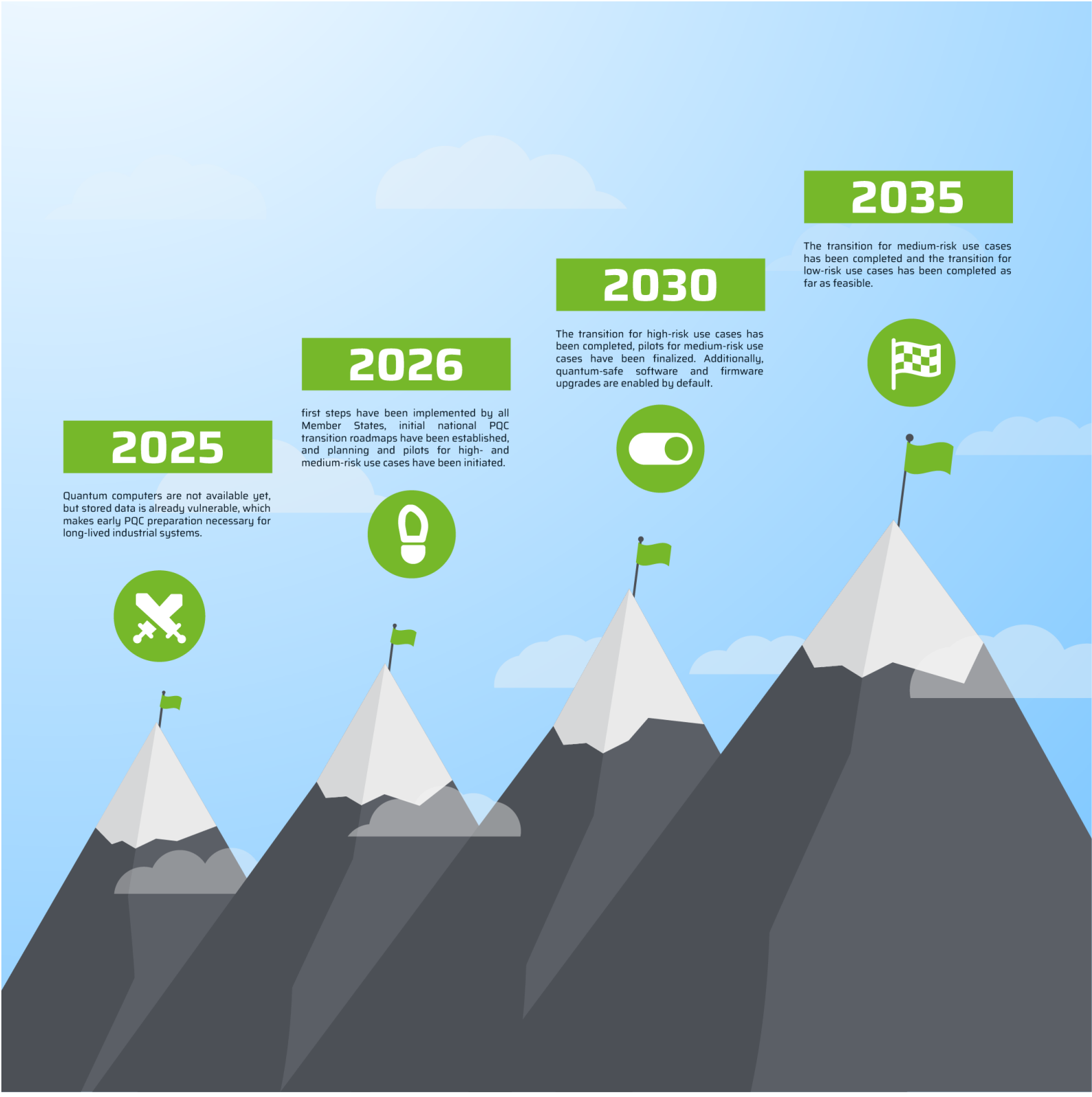
SLH-DSA (Stateless Hash-based Digital Signature Algorithm) for applications that require particularly high security levels

ETSI and the German Federal Office for Information Security (BSI) provide technical guidance and implementation recommendations to ensure a secure and interoperable adoption within Europe.

More insights can be gathered in the following sources:

- Computer Security Resource Center (CSRC)
- European Telecommunications Standards Institute (ETSI)
- Federal Office for Information Security (BSI)

Let us look at the roadmap and the milestones that lie ahead in the coming ten years. In the following, we'll provide an overview of how this development can be approached and which steps organizations may consider as they prepare for the long-term transition.


2025
Quantum computers are not available yet, but stored data is already vulnerable, which makes early PQC preparation necessary for long-lived industrial systems.
2026
first steps have been implemented by all Member States, initial national PQC transition roadmaps have been established, and planning and pilots for high- and medium-risk use cases have been initiated.
2030
The transition for high-risk use cases has been completed, pilots for medium-risk use cases have been finalized. Additionally, quantum-safe software and firmware upgrades are enabled by default.
2035
The transition for medium-risk use cases has been completed and the transition for low-risk use cases has been completed as far as feasible.

Challenges

Classical cryptographic methods such as elliptic curve cryptography and RSA have proven reliable for many years. They offer short keys, compact signatures and strong performance, which makes elliptic curve cryptography especially attractive for a wide range of applications. Post-Quantum algorithms perform noticeably worse in at least one of these categories. This creates challenges for systems with limited memory or low processing power. The impact is stronger for industrial systems than for typical web applications. A website that loads a second slower is acceptable, but a payment terminal that delays a transaction is not. Devices that are difficult or impossible to update are under particular pressure. Long-lived industrial equipment is therefore among the most affected, which increases the complexity of the migration.

For the migration, hybrid approaches will be required, as recommended by institutions such as BSI and NIST. The new algorithms are strong and standardized but have not been exposed to decades of operational experience like ECC and RSA, which have been in use for nearly fifty years. At the same time, the established methods remain efficient and reliable. Organizations need the ability to react flexibly if advances in quantum computing occur faster than expected. The goal is a controlled transition rather than a situation where cryptographic infrastructure fails unexpectedly.

To use hybrid methods, many technical foundations must be adapted. Protocols such as TLS or VPN require extensions, as do central standards such as certificate formats and PKI structures. Hardware components such as HSMs and cryptographic libraries also need updates. PQC migration is therefore not an isolated cryptographic task but a broad modernization effort across multiple layers of IT and operational infrastructure.

Outlook

This document can support organizations in starting their PQC planning. It provides an overview of the current state of the technology and outlines possible approaches. The actual planning process depends on individual needs, requirements and strategies, which means that no uniform guidance can be defined within this document. The Industrial Cybersecurity Working Group is available as a discussion partner for further exchange within the Open Industry 4.0 Alliance. Get in contact with us to discuss your options!