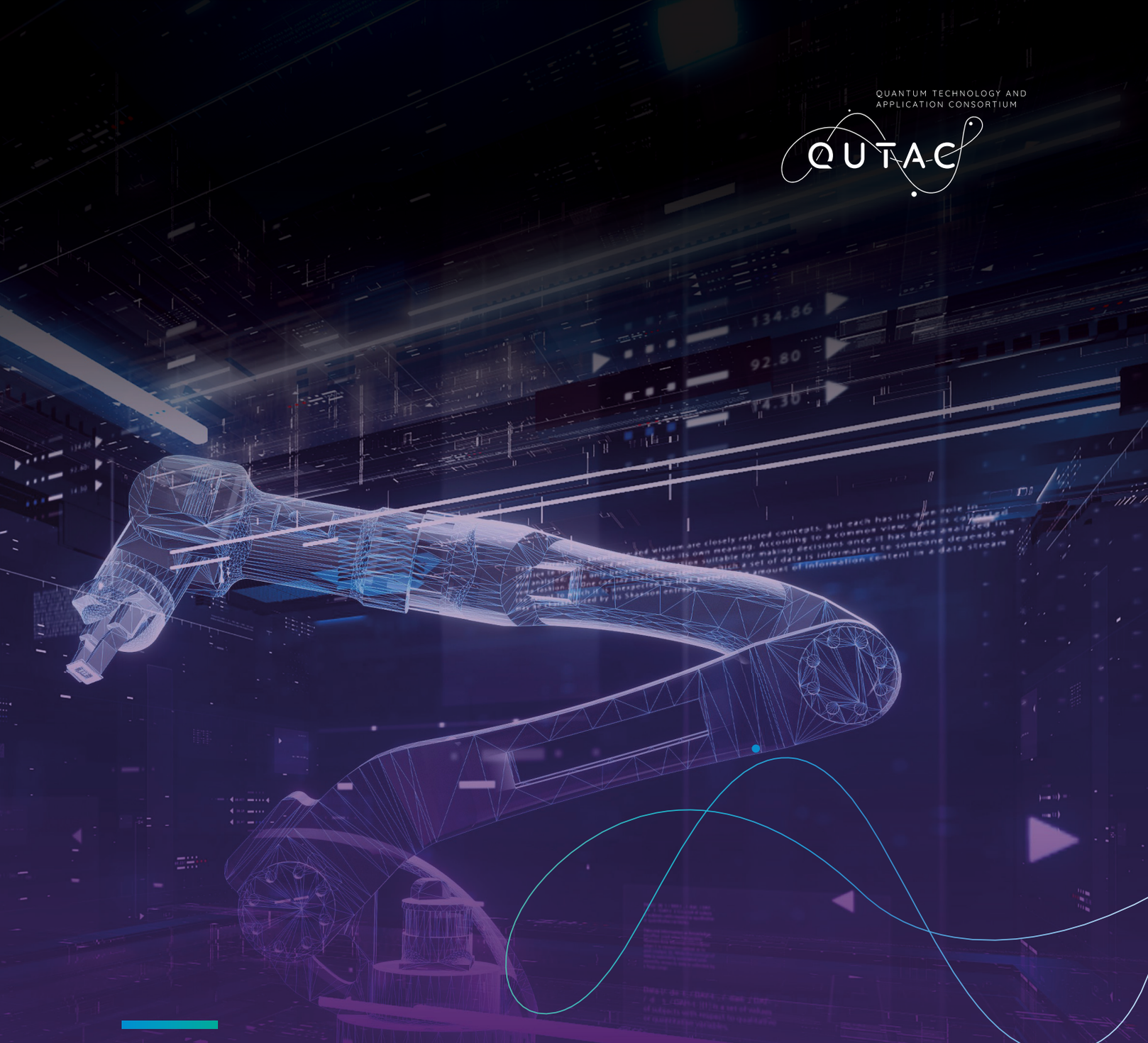

QUANTUM TECHNOLOGY AND APPLICATION CONSORTIUM

QUTAC

Introducing Post-Quantum Cryptography (PQC) to Industrial Systems

A Practical Guide for Business Leaders and IT Decision-Makers

October 2026

AUTHORS:

Harald Vogt[*1] (corresponding), Markus Ruppert[*2], Marvin Erdmann[*3], Sven Haueisen[*4], Wojciech Pawlak[*5], Sven Breitung[6]

[*]Quantum Technology & Application Consortium (QUTAC), [1]TRUMPF, [2]Lufthansa Industry Solutions, [3]BMW Group, [4]Volkswagen Group, [5]Deutsche Telekom, [6]VDMA

CONTRIBUTORS:

Christian Cohrs, Fabrizio Desantis, Florian Dommert, Christian Garske, Marc Geitz, Raoul Guiazon, Detlef Houdeau, Martin Hütter, Andreas Kind, Andre Luckow, Silke Müller, Sofia Todesca

October 2026
www.qutac.de

Table of Contents

1. Management Summary 4
2. Introduction 4
3. Key Use Cases 5
4. Threats and Risks 6
   - 4.1 Key Compromise 6
   - 4.2 Harvest Now, Decrypt Later 7
   - 4.3 Long-Lived Systems 8
   - 4.4 Signature Forging 8
   - 4.5 Regulatory Pressure 9
5. The Crypto Inventory: A Prerequisite for PQC Migration 10
   - 5.1 A Cryptography Bill of Materials 10
   - 5.2 Security-Sensitive Assets 11
   - 5.3 Managing the Crypto Inventory 12
6. Recommended Adoption Process 12
   - 6.1 PQC Adoption 12
   - 6.2 Step 1 — Establish Governance and Strategic Ownership 13
   - 6.3 Step 2 — Build and Maintain a Crypto Inventory 13
   - 6.4 Step 3 — Enable Crypto Agility as a Design Principle 14
   - 6.5 Step 4 — Deploy PQC and Hybrid Cryptography Pragmatically 14
   - 6.6 Step 5 — Continuous Improvement 14
7. Conclusion 15

References 16

1. Management Summary

Quantum computing is a promising technology from which many fields may benefit in the future—benefits are expected in areas such as complex simulations, optimization, and artificial intelligence. However, it poses a serious threat to established cryptographic technologies that provide the foundation of secure communications and data processing. Alternative algorithms have been designed and standardized, which provide quantum-safe encryption and authentication. First measures have been taken to integrate these algorithms in foundational tools such as web browsers. As the availability of capable quantum computers is approaching quickly, public and private organizations are called upon to take action and initiate a migration toward post-quantum cryptography. Machine and plant engineering has special challenges: long product lifecycles, installed bases that are distributed worldwide, industrial communication systems, limited test possibilities, and the dependency on complex supply chains.

We lay out the steps required to advance your organization and prepare it for the upcoming future where classical cryptography is becoming prone to adversarial activity. Since cryptographic technologies are deeply embedded in many software and IT systems, it will become a complex and time-consuming undertaking to not only replace the current technologies but also to ensure interoperability between new and legacy systems, and prepare for further upcoming changes to your cryptographic landscape. The long-term goal is not only to adopt the PQC mechanisms that are available today, but also to replace cryptographic mechanisms flexibly and economically in the future (crypto agility). Strict preparation and tight migration management are mandatory to succeed.

2. Introduction

Quantum computing is advancing rapidly. Once mature, it will be capable of breaking widely used classical cryptographic algorithms such as RSA and elliptic curve cryptography (ECC). International regulators foresee these algorithms becoming insecure by 2030[1].

Fortunately, quantum-safe (or post-quantum) cryptographic (PQC) algorithms are already available. They are widely considered adequate for protecting against classical and quantum-computing-based attacks. Large standardization bodies have put forward algorithms that can replace classical ones without compromising security today and that ensure security after sufficiently capable quantum computers have become available.

However, it is necessary to upgrade IT systems today so that they can use these mechanisms. Applications with a particularly high risk from a security compromise must have priority. This is urgent. The European Union recommends migrating high-risk use cases by 2030 and completing migration for all cases by 2035[2]. The German BSI continuously updates its recommendation for migration, putting an end to the sole use of classical cryptography by the end of 2031 for all use cases.

The market in general is already adapting to this development. Large companies, which are involved in developing quantum computers, are adopting strategies for migrating away from classical cryptography within the next few years. For example, Google has moved its own timeline for PQC migration forward to 2029[3]. Many large software vendors, such as SAP, IBM, or Salesforce, are currently integrating PQC functionality into their own product portfolios.

The members of QUTAC have committed to fostering the industrial application of quantum computing. However, QUTAC also acknowledges the responsibility to point out the risks associated with this new technology and wants to contribute to the preparation of organizations to thrive in this new environment.

There are clear indicators for organizations to act and adapt to new cryptographic conditions. As most organizations rely on the confidentiality and integrity of electronic data, they must ensure that these information assets are protected adequately. Quantum computers threaten core cryptographic primitives fundamental to authentication, digital signatures, and secure communications that organizations rely on daily. This means that a strategy must be established for upgrading systems that involve cryptographic mechanisms, and for migrating sensitive data under a new protective umbrella. The transition to PQC is not only a technical challenge but also a strategic imperative to maintain trust, operational resilience, and compliance.

Transitioning to a quantum-resilient setup is a complex effort that will affect nearly every system handling sensitive information. For organizations with heterogeneous, capital-intensive information technology (IT) and operational

technology (OT) environments, complete migration of all involved systems may take several years, high effort, and a substantial investment.

In this document, we outline how such a strategy can be put into action. Naturally, we will have to generalize. For any specific organization, the steps described need to be adapted to the needs of the organization. Our aim is to provide practical guidance for decision-makers, IT managers, and security leaders to prepare for PQC and execute a structured migration.

3. Key Use Cases

Public-key cryptography is the foundation of most cases of secure information exchange. It uses a combination of a private (secret) key and a public key to ensure both the confidentiality and the authenticity of information. For efficiency, these mechanisms are usually combined with symmetric encryption. Public-key cryptography is also the mechanism that is most threatened by the advent of the quantum computer. We therefore need to look at all use cases that rely on this mechanism. We list some examples, which will hopefully inspire you to identify the most relevant use cases in your organization.

Almost all organizations operate a distributed communication infrastructure: subsidiaries connect to headquarters, field workers access company resources online, documents are exchanged with external partners, and data is managed on external storage. Popular messaging services like e-mail or instant messaging are often used to discuss internal information or exchange sensitive information. The security of such communications relies on virtual private networks (VPN), encrypted web traffic (https), message encryption, and similar mechanisms, which are protected by asymmetric cryptography. The privacy of these networks will come under pressure with the availability of quantum computers. Even traffic ongoing today may be recorded and decrypted later—this is the harvest-now-decrypt-later attack, which we will describe below.

Not only the communication itself is susceptible to the capabilities of quantum computers but also documents that have been digitally signed because of their intrinsic value—such as business contracts and other legal documents. Signatures may be forged easily in the future. The public key is sufficient to reconstruct the private key. Thus, an attacker can create signatures that seem to come from the owner of the key. In effect, many digital signatures that are not confirmed by a quantum-safe mechanism become worthless. Therefore, adequate countermeasures should be taken early on.

Similar to this case, confidential documents, which are often encrypted and protected by a private key, would become openly readable by anyone with access to a quantum computer. Secret information, which should only be accessible in certain contexts and by certain users, would be widely accessible. A practical example of this is documents that are stored on backup media, where they might be encrypted—but would be accessible by unauthorized parties in the future. It must be assumed that all communication data with a long-term protection need can be at risk in the future.

Not only documents but also devices are affected. Many organizations operate devices in public spaces, such as vending machines, gas stations, traffic infrastructure, or surveillance devices. These rely on reliable communications: transactions must be performed accurately, sensor values must be correct, recordings must be protected against corruption. A cryptographic breach could lead to high financial costs and legal consequences. Upgrading such a setup relies on the capability of the supply chain of device providers, backend infrastructure, chip manufacturers, and software providers.

Both data that originates from such devices and data going into them must be protected. Software updates, configuration settings, payment transactions, functional upgrades (e.g., software-defined functions in cars), or updates to AI models are all critical to the correct functioning of these devices. Any breach of the integrity of such data may lead to harmful, even fatal consequences. These may have a very broad impact if critical infrastructure is affected, such as water systems or electrical grids.

As personal identification and authentication are moving to the digital domain, personalized services also become vulnerable. Tokens such as passports, identity cards, door keys, and similar items for high-security applications use public-key-based cryptography to avoid duplication or forging of tokens. For switching to a PQC infrastructure, these tokens must be replaced. However, due to their large numbers and capacity limits in manufacturing and distribution channels, replacing these tokens in the field may consume a significant amount of time.

The Cryptographic Risk Matrix: Classical Vulnerability vs. Quantum Defense

Currently, 90-95% of security mechanisms rely on RSA and ECC. Shor's algorithm allows quantum computers to break these foundations entirely, demanding an immediate shift to lattice- and hash-based mathematics.

	Underlying Math	Risk Today	Risk at Q-Day	Action Required
Legacy Asymmetric (RSA-2048 / ECC P-256)	Factoring / Discrete Logarithm	Medium	Critical (Complete Compromise)	Migrate
Legacy Symmetric (AES-128)	Unstructured Search	Low	High (Grover's Algorithm halves security)	Double key lengths to AES-256
Post-Quantum (ML-KEM / ML-DSA)	Lattice-based (Learning With Errors)	Low	Low (Quantum-Resistant)	Immediate hybrid integration

Figure 1 *Quantum computing demands adaptation of your cryptographic machinery. Classical asymmetric algorithms need replacement; symmetric algorithms can be improved to withstand quantum attacks.*

Another domain where quantum computers will lead to disruptions is the world of blockchains, which are used for supply chain verification, product identity management, and (most importantly) digital currency. As they have been adopted by global financial institutions, invalidating their cryptographic foundation may lead to significant financial losses and diminished information integrity.

These examples show that many organizations are susceptible to quantum-computer-based attacks on the confidentiality and integrity of their information assets. Broad and economical access to quantum computers may become reality only in the future. But this future is not as distant as it may seem. Transitioning to a full PQC-capable infrastructure and adequately protecting all information assets is a high-effort activity and requires careful planning and commitment.

4. Threats and Risks

4.1 Key Compromise

The foundation for most mechanisms for protecting information against unauthorized access or manipulation is the combination of private and public keys. A public key corresponds to a unique private key, and vice versa. The private key is held in secret, and the public key may be openly distributed. This is called "asymmetric cryptography", since the functions of both keys differ. There are two major use cases for such key pairs:

- Create a signature for a piece of data that can be verified by anyone holding the public key.
- Encrypt data that needs to be kept secret, which can only be read by the holder of the private key.

Usually, a cryptographic mechanism for protecting the confidentiality of data (or documents) works as follows. Since directly encrypting a complete document simply using the public key is very inefficient, first a "symmetric" key is generated. Encryption with a symmetric key can be done very quickly and efficiently. Only the symmetric key is encrypted using the public key. The holder of the private key now can first decrypt the symmetric key and then use this key to decrypt the complete document. As nobody else can decrypt the symmetric key, the document remains secret.

A quantum computer changes the game. Using "Shor's algorithm", the secrecy of the document can be broken.

As the attacker can easily get the public key, this algorithm allows the reconstruction of the corresponding private key. Using traditional computers, this is not computationally feasible in a limited amount of time. However, sufficiently equipped quantum computers can achieve this with relatively little effort.

Using the acquired private key, the attacker can now decipher the symmetric key that was used to protect the document and convert the encrypted document into a readable format.

The forging of a signature works similarly but is even simpler. If the attacker has access to the public key and a quantum computer, they can reconstruct the corresponding private key. This allows them to create signatures for documents of their own liking. For the verifier of a signed document, it becomes impossible to distinguish between an original and a forged document.

We have just described the technical threat that endangers the security of most information that is secured today by conventional cryptography. However, failing to upgrade systems so they can withstand this threat also bears further risks of regulatory and possibly legal nature.

Background

Since the idea of quantum computing was introduced in the early 1970s, researchers have found ways to make use of the great potential of quantum computers by formulating algorithms that theoretically outperform classical methods, including some that pose a significant threat to classical cryptography.

Shor's algorithm, discovered in 1994, enables quantum computers to factor large integers and compute discrete logarithms exponentially faster than classical algorithms. This threatens RSA, DH, and ECC, which rely on the hardness of these problems. For example, RSA-2048, which currently requires millions of years to factor classically, could be broken in days—or even hours[4]. Shor's algorithm uses the quantum Fourier transform and period finding to reduce factoring to a problem solvable on a quantum device, thus breaking the mathematical foundations of classical asymmetric cryptography.

Grover's algorithm reduces brute-force key search to roughly the square root of the classical effort. This is why it is often said to halve the effective key length and it may be advisable to double the used key length.[5] However, this is based on a theoretical query count, not on a realistic cost estimate. In practice, the required AES evaluations would run largely in sequence on a fault-tolerant quantum computer and would carry substantial circuit and error-correction overhead. Current resource estimates therefore conclude that, with existing techniques and plausible near-term hardware, Grover's practical impact on AES is very limited. Accordingly, NIST expects AES-128 to remain secure for "decades to come".[6]

Post-quantum cryptography (PQC) comprises cryptographic algorithms resistant to attacks by quantum computers, addressing the threat that quantum algorithms can break classical public-key schemes. The main families of PQC algorithms include:

- **Code-based Cryptography:** Based on error-correcting codes, such as the McEliece cryptosystem, leveraging the hardness of decoding random linear codes. These schemes offer strong security but often have large key sizes.
- **Lattice-based Cryptography:** Builds on hard lattice problems like Learning With Errors (LWE) and Ring-LWE. Lattice-based schemes (e.g., CRYSTALS-Kyber for encryption, CRYSTALS-Dilithium for signatures) provide efficient, scalable algorithms with reasonable key sizes and are NIST standards.
- **Hash-based Cryptography:** Primarily for digital signatures, relying on hash functions' one-way properties. Schemes like XMSS and SPHINCS+ offer strong security but can have large signature sizes and limits on the number of signatures per key.

Additional approaches include multivariate polynomial cryptography and supersingular elliptic curve isogeny cryptography, though these are less mature.

4.2 Harvest Now, Decrypt Later

As we have described, it will be possible to break conventional encryption using quantum computers. Even if they are not available today, attackers may collect encrypted communications or stored data now and decrypt them once sufficiently powerful quantum computers become available, potentially compromising sensitive information retrospectively.

This threat is especially critical for data that has been protected by conventional means today or in the past but

must remain confidential over extended periods due to regulatory mandates or business value.

This affects all information with long-term confidentiality requirements, including:

- Customer and personal data (including medical records)
- Intellectual property
- Engineering and product designs
- Contractual and financial documents
- Governmental communication
- Research data

The countermeasure against this attack would be to identify all documents that need long-term protection and move them to systems where they are encrypted using quantum-safe mechanisms.

4.3 Long-Lived Systems

Many organizations, e.g., in the automotive or telecommunication sector, operate OT, IoT, and embedded systems with operational lifetimes spanning 10 years or more. Such systems will still be in use once quantum computers are able to break current classical cryptographic security mechanisms. They often cannot be easily updated or replaced, increasing the urgency to implement PQC-compatible cryptographic mechanisms early in their lifecycle. Connected devices depend on secure cryptographic protocols for functions such as remote access, software updates, and telemetry. Ensuring these systems are quantum-resilient is critical to maintaining safety, privacy, and business continuity. For long-lived industrial plants, evaluate early whether quantum-safe mechanisms can be introduced through software updates or whether hardware changes are necessary.

Special Challenges in Machine and Plant Engineering

Machine and plant engineering has special challenges when it adopts post-quantum cryptography. Machines, production plants and industrial automation solutions have much longer lifecycles than conventional IT systems. Operators often use them for decades. Thus, the decisions that companies make today about the development, procurement, and design of products can have an effect long after powerful quantum computers become available.

Many machines and plants stay in operation for 10 to 30 years or longer. During this time, operators must operate, maintain and update them safely. Sometimes, they must also adapt them to new requirements. Frequently, a full replacement is not economical. Instead, operators modernize and retrofit the equipment. Thus, manufacturers must examine now whether they can change their products to new cryptographic procedures in the future.

Also, modern machines are increasingly connected. Remote maintenance, condition monitoring, digital services, software updates, cloud connections and digital twins are now important parts of many business models. The authentication, encryption and signature procedures for these functions frequently use cryptography that quantum computers can put at risk in the long term.

Another special aspect is the close connection between information technology (IT), operational technology (OT) and embedded systems. It is comparatively easy to update servers and workstations regularly. But industrial controllers, field devices and embedded components frequently have high requirements for availability, security and long-term support. Thus, you must plan changes to cryptography carefully. You must also agree on these changes with manufacturers, integrators and operators.

The global installed base is also a challenge. Operators frequently use machines for many years in different countries. Thus, it must be possible to apply security updates, certificate replacements and software migrations worldwide. Because of this, the technical capability to update cryptographic functions becomes an important criterion for future-proof products.

For machine and plant engineering, the adoption of PQC thus means more than a change to the company IT. It applies equally to products, service processes, supply chains and the full lifecycle of machines and plants. Early planning, crypto agility and close cooperation with suppliers and customers are necessary to ensure long-term security and to protect investments.

4.4 Signature Forging

As described above, using a quantum computer it is possible to construct the secret key matching a public key in a classical signature scheme. This enables a malicious party to create signatures that look legitimate. The verifier has no way to differentiate between a real, legitimate signature and a forged one. Under this condition, documents and data objects that have been signed using classical

signature schemes cannot be trusted once quantum computers become available.

Five consequences emerge from this:

- Valuable, legitimate documents, such as digitally signed business contracts, will be disputed. Business partners will not be incentivized to adhere to the contractual obligations.
- Illegitimate documents and data objects will be created and submitted to processing systems. The signature verification executed by these systems will be successful and these information items will be processed accordingly. Fraudulent business transactions will be executed, and compromised software updates will be installed.
- PKI certificates will become untrustworthy as attackers can either create their own certificates or imitate existing ones. Thus, the infrastructure cannot be trusted in general, even if compromised certificates are revoked.
- Signed software for customer-facing and non-customer-facing products faces multiple problems. Traceability (non-repudiation) is lost, as the digital signatures can no longer be used as evidence. This also leads to a loss of legal and regulatory compliance. In addition, supply chain attacks with manipulated or malicious firmware/software become possible.
- AI models and their lifecycle are no longer trustworthy as there will be poisoned models despite an authorized signature. Also, existing models can be manipulated by injected weights or backdoors. Signed training data, labels or artifacts are compromised.

Signatures created with classical algorithms will become practically worthless. All systems that rely on checking such signatures will be subject to a high risk of manipulation.

Not only documents will be affected by forged signatures. Since secure communication channels usually rely on certificates that are authenticated by signatures on multiple levels, forming a chain of trust, most of them will not be trustworthy once signatures can be forged. The identity of communication partners cannot be determined reliably.

4.5 Regulatory Pressure

Standardization and regulation play a critical role in ensuring interoperability, security assurance, and widespread adoption of post-quantum cryptography across industries. Without clear standards and regulatory guidance, organizations risk fragmented implementations, security gaps, and compliance challenges, potentially undermining the resilience of digital infrastructure against quantum-enabled attacks.

The United States National Institute of Standards and Technology (NIST) has led global efforts to standardize PQC algorithms through a rigorous multi-year evaluation process. In July 2022, NIST selected four primary algorithms for standardization: CRYSTALS-Kyber for public-key encryption and key establishment, and CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signatures. By August 2024, three of these algorithms were published as official Federal Information Processing Standards (FIPS), with the fourth (FALCON) expected soon. These standards cover essential cryptographic tasks, providing quantum-resistant alternatives to RSA and ECC[7].

NIST strongly encourages organizations to begin migrating to these new algorithms promptly. Federal civilian agencies are legally mandated to inventory vulnerable cryptographic systems and develop migration plans under the Quantum Computing Cybersecurity Preparedness Act of 2022. The White House's National Security Memorandum 10 (NSM-10) also sets a target for all federal systems to adopt quantum-safe cryptography by 2035. The National Security Agency (NSA) further requires National Security Systems to implement quantum-resistant algorithms, urging early transition planning.

At the European level, the European Commission issued the non-binding Commission Recommendation (EU) 2024/1101, calling on member states to develop coordinated national strategies with clear goals and timelines for PQC adoption, particularly in critical sectors. The recommendation highlights hybrid cryptographic schemes during the transition to ensure continuous security. In mid-2025, the NIS Cooperation Group turned it into the PQC transition roadmap with the ultimate deadline for the migration of high-risk use cases[8] set to December 31, 2030.

Cybersecurity authorities from 18 European countries jointly urged industry and public administrations to initiate the PQC transition[9] without delay, recommending "no-regret" measures such as asset inventories, risk-oriented roadmaps, and early hybrid deployments to improve overall cybersecurity while preparing for quantum threats.

While the EU has issued recommendations for the transition, national governments have issued their own recommendations and mandates.

Germany's Federal Office for Information Security (BSI) has published detailed guidelines incorporating PQC into its cryptographic recommendations. The 2026 Technical Guideline TR-02102-1 advises deploying PQC algorithms in hybrid mode alongside classical encryption during the migration phase to maintain security if any scheme is compromised.[10] In France, quantum-resistant encryption is required for procurement in government agencies starting as early as 2027. In contrast to NIST, hybrid mechanisms are required to qualify for certified systems.[11]

A similar approach is taken by the Netherlands. Critical infrastructure must be upgraded no later than 2030. Also, hybrid mechanisms are mandated. Dutch institutions were the main drivers behind the PQC Migration Handbook.

Other nations, including the United Kingdom, China, South Korea, and Canada, have developed their own PQC strategies and roadmaps aligned roughly with the 2030–2035 timeframe for migration. International standards bodies like ISO/IEC and the IETF are actively working to formalize PQC specifications and integrate quantum-safe algorithms into communication protocols such as TLS.

5. The Crypto Inventory: A Prerequisite for PQC Migration

The transition to Post-Quantum Cryptography begins with understanding where cryptography is used throughout the organization and which information assets depend on it. The term "Crypto Inventory" is often used to refer only to the cryptographic assets, such as the deployed algorithms, certificates, and keys. However, we will use the term to comprise both the cryptographic assets (documented as the Cryptography Bill of Materials) and the set of sensitive assets.

For many organizations, this visibility does not exist today. Cryptographic functions are embedded across applications, infrastructure, cloud services, operational technology, connected devices, and third-party products, often without explicit knowledge about dependencies, interoperability, and risks.

Consequently, many organizations lack visibility into their cryptographic assets. Existing tools often provide incomplete information, while gathering the required data involves significant coordination across multiple teams and technology domains. Nevertheless, building this inventory is an essential prerequisite for any successful PQC program. The Crypto Inventory provides several strategic benefits:

- It reveals where vulnerable algorithms are used.
- It exposes dependencies that must be migrated together.
- It enables risk-based prioritization.
- It provides measurable progress indicators.

Without a Crypto Inventory, organizations cannot effectively plan, prioritize, or execute a coordinated migration to quantum-safe cryptography.

5.1 A Cryptography Bill of Materials

To gain insight into the organization's cryptographic assets, a systematic overview must be established and maintained. Existing tools often provide sparse or inconsistent data, and gathering information involves significant manual effort. The information required to engage in a systematic cryptographic migration includes:

- Algorithms
- Keys, passwords and access tokens
- Certificates (including validity periods)
- Protocols
- Cryptographic libraries
- Encryption configurations
- Update mechanisms

Technically, this information can be captured in a Cryptography Bill of Materials (CBOM), which is a comprehensive directory of all cryptographic assets. For software systems, creation of a CBOM can be largely automated. However, for environments with legacy devices, manual effort is likely required. The CBOM serves as a foundation to identify weak algorithms or dependencies on cryptographic libraries, which need monitoring during the transitioning process. It is advisable to use a standardized format for capturing, documenting and versioning the CBOM, such as "CycloneDX". This is an open data description standard intended to capture in-

formation relevant to cybersecurity. It is widely supported by industry and can be used in most tools.

5.2 Security-Sensitive Assets

The assets protected by cryptographic means usually include:

- Design and engineering data (CAD, schematics, software source code) that provide a competitive advantage
- Plant configurations and machine parameters
- Research and development data containing intellectual property
- Customer and employment data protected by GDPR and similar regulations
- Financial and contractual data
- Operational data and telemetry
- Software code and software installation packages

In the future, more assets can become important, for example digital twins and simulation data.

For each asset, it must be recorded in which systems it is being stored or processed. These systems comprise:

- Storage systems such as databases for backup, archiving, and data processing, both on premises and cloud-based
- Communication channels such as VPNs and web traffic
- IoT devices, production equipment
- Blockchains

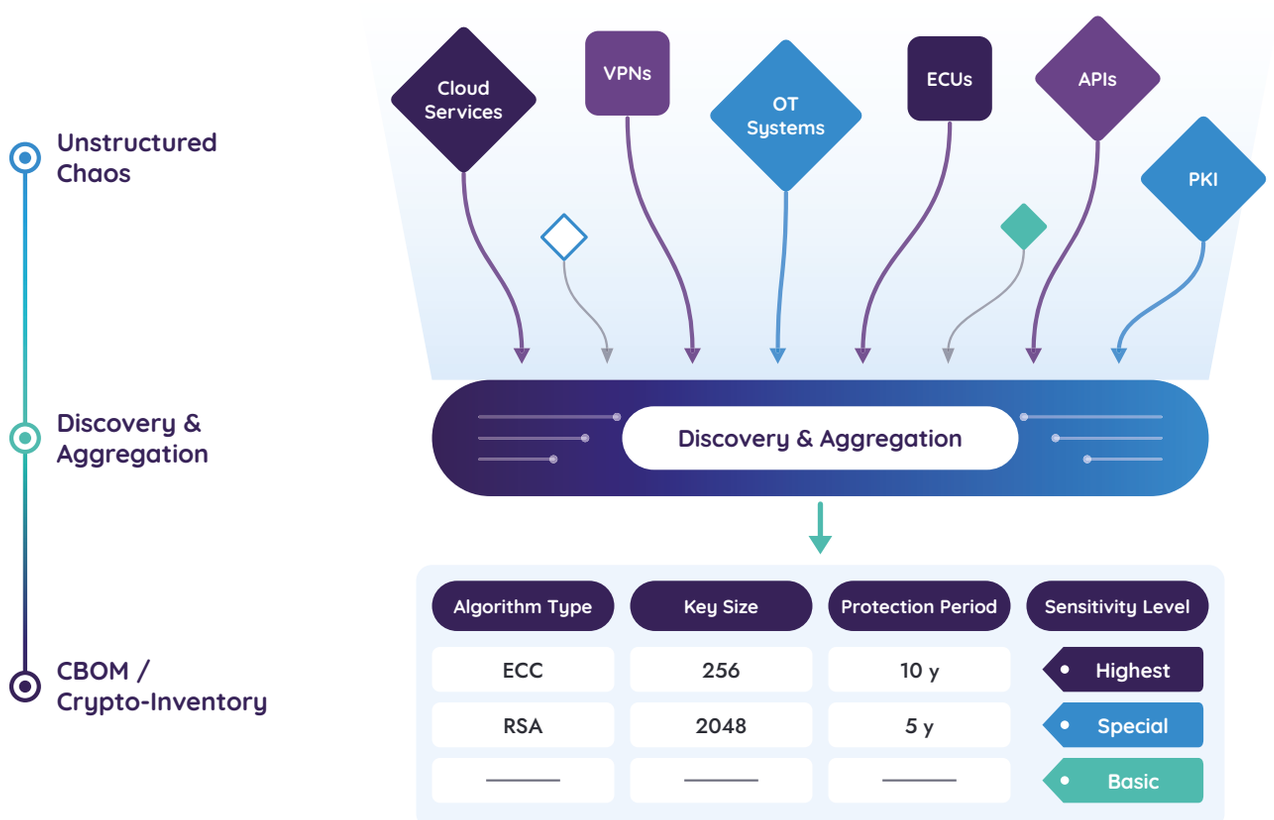

Figure 2 *A CBOM comprises all cryptographic and information assets that constitute the information security of your organization.*

As there may be a large number of assets, it is necessary to deal with them by priority. Priority is determined by the level of confidentiality and integrity, and the timespan over which the data is relevant. For example, session tokens are transient in nature and are only relevant for a single session. On the other hand, many data assets need to be protected over years or even indefinitely. Some requirements may be imposed by regulations such as GDPR, HIPAA, SOX, and PCI DSS.

5.3 Managing the Crypto Inventory

The Crypto Inventory needs to be established once but managed over time as the IT landscape evolves and the post-quantum migration proceeds.

Based on the classification of cryptographic assets, priorities can be set. Criteria for classification may be dependent on the organization, but as a general guideline, the following criteria are useful:

Sensitivity Level

- **Highest Protection:** Data with the greatest confidentiality and integrity requirements, such as cryptographic keys and intellectual property.
- **Special Protection:** Data requiring significant safeguards, including customer information and internal business documents.
- **Basic Protection:** Data with lower sensitivity but still subject to appropriate security controls.

Confidentiality Duration

- **Short Term:** Data requiring protection only during transmission or for a limited timeframe (e.g., session tokens).
- **Medium Term:** Data needing protection for months or a few years (e.g., project documentation).
- **Long Term:** Data requiring protection for many years or indefinitely (e.g., patents, financial archives).

Integrity and Authenticity Duration

- **Short Term:** Integrity needed only during transmission or brief periods.
- **Medium Term:** Integrity required for months or years.
- **Long Term:** Integrity to be maintained for extended periods, possibly as long as the data exists.

Regulatory and Compliance Requirements

Applicable laws, standards, and regulations (such as GDPR, HIPAA, SOX, PCI DSS) influence mandatory protection periods and security controls, shaping how data must be handled and secured. For example, medical records require protection for 6+ years under HIPAA.

Business Impact

- **Operational Impact:** Effects on business processes and continuity.
- **Financial Impact:** Potential monetary losses.
- **Reputational Impact:** Damage to brand trust and customer confidence.
- **Legal Impact:** Risks of fines, lawsuits, or sanctions.

6. Recommended Adoption Process

6.1 PQC Adoption

The transition to Post-Quantum Cryptography is not a single technical migration, but a multi-year transformation of an organization's cryptographic foundations and numerous external dependencies. Experience across industries shows that successful adoption depends less on the early deployment of specific algorithms and more on establishing transparency, governance, and crypto-agile structures first.[12]

The very first step is to create awareness of the increasing risk of exposure. Sensitive information may include intellectual property, personal information, customer information; even cryptocurrencies might be relevant to your organization. This awareness manifests itself in a clear assignment of responsibilities, including top management.

A next step is to identify the systems that are involved in storing and processing these information assets. Even if the "big" software solutions are covered, there are usually more IT and software systems in use at a company than the IT department knows of. Proprietary or custom-developed software may pose additional risk.

Once the foundation has been created, a migration plan can be drawn up. The organization should define the trigger point for starting the transformation. The plan can be executed in multiple steps that are decided based on the

risk involved. Eventually, the organization will end up fully transformed, using PQC throughout all relevant systems.

The following adoption process reflects a pragmatic, industry-oriented approach. It is designed to allow organizations to progress incrementally, manage risk, and align technical measures with business priorities and regulatory expectations.

6.2 Step 1 — Establish Governance and Strategic Ownership

The transition to PQC cuts across traditional organizational boundaries. Cryptography underpins authentication mechanisms, secure communications, machine-to-machine trust, software updates, and regulatory compliance. As a result, PQC migration cannot be delegated to a single technical team or security function alone.

At an early stage, organizations should establish **clear ownership and governance structures** for PQC adoption. This includes aligning responsibilities across IT leadership, information security, enterprise architecture, system owners, software development, procurement, and—where applicable—OT or product engineering.

Beyond assigning roles, this step serves a broader strategic purpose: It ensures that Post-Quantum Cryptography is understood as a business-critical, long-term risk management and resilience initiative, not merely as a future cryptographic upgrade. Management sponsorship is essential to set priorities, secure resources, and resolve trade-offs between security, performance, legacy constraints, and business continuity.

Equally important is the definition of decision-making principles. Organizations should clarify how cryptographic risks will be evaluated, which data categories and systems require priority protection, and how regulatory timelines will be translated into internal milestones.

Key decisions:

- Nominate a PQC sponsor or steering function at top management level
- Define cross-functional responsibilities (IT, security, architecture, procurement, OT)
- Agree on guiding principles: risk-based prioritization, crypto agility as a long-term goal
- Update the information security framework and associated policies to incorporate PQC-specific requirements

6.3 Step 2 — Build and Maintain a Crypto Inventory

A Crypto Inventory is the central enabler of any credible PQC strategy. Organizations cannot protect what they cannot see, and cryptography is often deeply embedded into systems, protocols, devices, and third-party components without explicit visibility.

The purpose of the Crypto Inventory is not solely documentation. Instead, it provides a living, structured view of how cryptography is used across the organization, including:

- which algorithms, protocols, certificates, and key materials are deployed
- where long-term confidential data is processed or stored
- how systems depend on and trust each other
- which assets are long-lived and therefore exposed to future quantum threats

In practice, many organizations discover that cryptographic information is fragmented across tools, teams, and vendors, often requiring significant manual effort in the early phases. This is expected and should not delay progress. The value of the inventory grows incrementally as coverage increases and data quality improves.

To ensure sustainability and interoperability, cryptographic information should be captured in a structured and standardized format, such as Cryptography Bill of Materials (CBOM). Over time, the Crypto Inventory becomes the foundation for impact analysis, compliance reporting, supplier management, and future cryptographic transitions.

What to do next:

- Start with high-risk and long-lived assets, not with completeness
- Identify systems handling data with long-term confidentiality and integrity requirements
- Capture cryptographic usage, dependencies, and trust relationships
- Establish the Crypto Inventory as a continuous process, not a one-off project

6.4 Step 3 — Enable Crypto Agility as a Design Principle

Post-Quantum Cryptography should not be treated as a one-time replacement of algorithms. History has shown that cryptographic assumptions evolve, and future vulnerabilities—quantum-related or not—cannot be excluded. Therefore, the strategic objective extends beyond PQC itself toward crypto agility.

Crypto agility refers to the ability to replace or adapt cryptographic mechanisms without major architectural changes, operational disruption, or lengthy migration cycles. For many organizations, this requires revisiting existing designs where cryptography is hard-coded, tightly coupled, or implicitly embedded into products and processes.

At this stage, organizations should assess where cryptographic flexibility already exists (e.g., configurable TLS stacks) and where constraints remain (e.g., embedded systems, legacy appliances). Introducing abstraction layers, standardized crypto libraries, and policy-driven configurations significantly reduces future migration effort.

Crypto agility also has organizational dimensions: procurement criteria, software development guidelines, and lifecycle management processes must explicitly support adaptability, not just compliance at the time of deployment.

What to do next:

- Identify systems with hard-coded or non-replaceable cryptography
- Introduce architectural patterns that isolate cryptographic components
- Update development and procurement guidelines to require crypto agility
- Treat PQC migration as one use case of a broader crypto-agile strategy

6.5 Step 4 — Deploy PQC and Hybrid Cryptography Pragmatically

Once transparency and crypto agility are established, organizations can begin the controlled deployment of PQC mechanisms. At present, hybrid cryptographic schemes—combining classical and post-quantum algorithms—represent the most robust and widely recommended transition approach.

Hybrid deployments ensure that security is maintained even if one class of algorithms is later found to be vulnerable. They also allow organizations to gain operational experience with post-quantum algorithms while preserving interoperability with existing systems.

Vendors of IT systems should be approached early on to provide information about their status and roadmap for supporting PQC mechanisms and their approach to crypto agility.

Initial deployments should focus on use cases where cryptographic change is operationally feasible and security impact is high, such as:

- secure communication channels (TLS, VPN)
- authentication and digital signatures
- internal trust relationships between services

Performance, interoperability, and operational stability should be closely observed. However, obstacles that occur must not put the whole project at risk. Instead, they must be addressed specifically. Early, contained deployments significantly reduce uncertainty and prepare teams for broader rollout.

What to do next:

- Identify "low-regret" use cases suitable for hybrid deployment
- Avoid full replacement strategies where standards or ecosystems are still evolving
- Coordinate PQC enablement with vendors, cloud providers, and integrators
- Treat early PQC deployments as learning steps, not final states

6.6 Step 5 — Continuous Improvement

PQC adoption is a long-term, continuous journey, not a milestone. Once initial deployments begin, organizations should shift focus toward measurement, governance, and refinement.

Key performance indicators derived from the Crypto Inventory help management understand progress, residual risk, and remaining dependencies. These indicators also support regulatory reporting, audit readiness, and internal decision-making.

As standards mature, ecosystem support increases, and regulatory expectations evolve, organizations should refine their roadmaps accordingly. The long-term objective is not

merely to "be PQC-ready," but to maintain cryptographic resilience as a permanent organizational capability.

What to do next:

- Define KPIs for quantum exposure and migration progress
- Regularly update the Crypto Inventory and reassess priorities
- Review vendor and supplier readiness over time
- Evolve from hybrid deployments to fully post-quantum solutions where appropriate

7. Conclusion

PQC migration is a strategic necessity since classical cryptography, the foundation for information security, will be broken in the foreseeable future. The period **2026–2030** is essential for preparation. Starting now ensures resilience, protects long-term confidentiality, and enables compliance with emerging regulations. It will also avoid higher costs for late adoption under increased pressure.

For a successful migration, an organization must answer two questions:

- Which objects need to be protected first and by which systems will this be achieved?
- Future changes will be coming, so how do we achieve cryptographic agility?

In the previous chapters, we have detailed the steps by which post-quantum security can be achieved. As a first step, a governance structure must be established with strong management buy-in. The second step is to establish a Crypto Inventory, which answers the following questions:

- In which systems do the critical information assets reside?
- Which cryptographic means are used for protecting these assets?

Based on this information, a risk-based migration strategy can be developed. Systems that are provided by external suppliers may require upgrading or replacement, based on the supplier's strategy. Additionally, adequate support for custom-developed software systems must be ensured.

Not only internal processes require consideration but also the products built and the services provided by the organization. In particular, long-lasting goods must be designed to be future-proof, and the special requirements of PQC must be considered, especially larger storage requirements for digital signatures and computational performance. Crypto agility, that is, the ability to update the cryptographic mechanisms also in products during their full lifecycle, decreases later retrofit costs, protects the installed base, and strengthens long-term competitiveness. Machine and plant manufacturers should consider this when they develop their products.

When migrating systems, interoperability between different systems must be ensured. Legacy elements in an information processing chain could lead to falling back to classical cryptographic mechanisms, which could expose vulnerabilities.

The efforts and budgets necessary to implement a PQC migration strategy are similar to upgrading your entire IT infrastructure to a new technology generation. Some elements may bring along PQC mechanisms quietly through regular updates. Others will need replacement. However, all will need configuration, integration and maintenance. Employees will require training and awareness, which is essential for effective application of security measures.

Implementing a full migration strategy could lead to activities spanning multiple years. Effective program management is required to carry out such a complex activity, and support by top management is essential. Progress should be transparent. At sensible milestones on the migration path, reviews should be performed to ensure proper usage of PQC mechanisms. Attention should be drawn to critical assets that are still protected by classical means.

In this paper, we provide a concise introduction to Post-Quantum Cryptography, why it matters to most organizations, and how to prepare for the time when quantum computers are sufficiently powerful and economically available to significantly threaten the security of public key cryptography.

The issue has been addressed on the regulatory level and there are guidelines available for planning and executing the migration to PQC mechanisms. Use these guidelines when you plan the migration. All organizations should start this work soon.

References

1. https://www.bsi.bund.de/EN/Service-Navi/Presse/Pressemitteilungen/Presse2024/241127_Post-Quantum_Cryptography.html
2. https://ec.europa.eu/newsroom/dae/redirection/document/117507
3. Google, "A timeline for cryptography migration," Google Blog, Mar. 2026. [Online]. Available: https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/. Google is one of the companies actively investing in building a quantum computer. In this posting, Google has moved its own timeline for PQC migration forward to 2029 and is integrating PQC into its own products such as Android.
4. Thé, Jesse Van Griensven, Victor Oliveira Santos, and Bahram Gharabaghi. 2026. "A Novel Hybrid Quantum Circuit for Integer Factorization: End-to-End Evaluation in Simulation and Real Quantum Hardware" Journal of Cybersecurity and Privacy 6, no. 2: 71. https://doi.org/10.3390/jcp6020071
5. BSI – Technische Richtlinie, Kryptographische Verfahren: Empfehlungen und Schlüssellängen. BSI TR-02102-1, January 23, 2026. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=15. This technical guideline describes in detail the cryptographic background of classical and post-quantum cryptographic algorithms. It targets developers of systems that employ cryptographic algorithms.
6. NIST – Post-Quantum Cryptography FAQs https://csrc.nist.gov/projects/post-quantum-cryptography/faqs
7. NIST Releases First 3 Finalized Post-Quantum Encryption Standards. August 13, 2024. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
8. NIS Cooperation Group. A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, June 11, 2025. https://ec.europa.eu/newsroom/dae/redirection/document/117507
9. Federal Office for Information Security (BSI) *et al.*, "Securing tomorrow, today: Transitioning to post-quantum cryptography," Partners from 18 EU Member States, Joint Statement, Nov. 27, 2024. Available online: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf
10. Quantum Technologies and Quantum-Safe Cryptography. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/quantentechnologien-und-post-quanten-kryptografie_node.html
11. https://cyber.gouv.fr/en/technological-and-cybersecurity-challenges/post-quantum-cryptography/
12. A. Amadori *et al.*, "The PQC Migration Handbook: Guidelines for migrating to post-quantum cryptography," AIVD, CWI, and TNO, Tech. Rep., 2nd ed., Dec. 2024. Available online: https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf. This book provides a comprehensive overview of the elements for an organizational migration strategy toward PQC. It also contains a wealth of deep technical information that is useful for raising awareness and understanding of the topic.

QUANTUM TECHNOLOGY AND
APPLICATION CONSORTIUM

QUTAC

www.qutac.de

