31-10-2025

Towards Quantum-Safe Networking

Grant Agreement No.:	101194278
Work Package:	WP6
Task Item:	T1
Nature of Document:	White Paper
Dissemination Level:	PU
Lead Partner:	FAU/DFN
Document ID:	GN5-2-25-634G7D

Authors:	Susanne Naegele-Jackson (FAU); Ane Sanz (EHU); Xavier Jordán Parra (i2CAT); Piotr Rydlichowski (PCSS); Ilias Papastamatiou (GRNET); Vincent Burkard (FAU); Guy Roberts (GÉANT); Ivana Golub (PCSS); Pavle Vuletić (AMRES)

Abstract

This document provides a step-by-step approach towards quantum-safe networks where PQC and QKD technology is applied and integrated over time to harden networks and ensure quantum-safe security.

Contents

Figures

Tables

Executive Summary

Quantum-safe networking refers to the adoption of cryptographic methods that are resistant to attacks by quantum computers. It involves the transition from classical cryptographic methods, which are vulnerable to quantum algorithms, to post-quantum cryptography (PQC) and quantum key distribution (QKD) systems that can withstand quantum threats.

As quantum computing evolves, the security of current cryptographic systems – such as Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC) – will be compromised. To mitigate this risk, National Research and Education Networks (NRENs) must adopt quantum-safe protocols and integrate quantum technologies, such as QKD and PQC, to maintain secure communication for research and educational data.

It is expected that the transition from quantum-vulnerable pre-quantum cryptography to quantum-resistant post-quantum cryptographic algorithms will take several years and will happen in stages. The EC therefore recommends starting out with standardised and tested hybrid solutions which include PQC, especially in high-risk scenarios, to replace vulnerable public-key encryption methods such as RSA or discrete logarithm-based algorithms wherever applicable. Such a gradual implementation approach is not only recommended when transitioning from pre-quantum cryptography to PQC, but also when integrating QKD and PQC into existing network infrastructures while the QKD standardisation and certification processes are ongoing and while QKD devices have limited terrestrial reach.

Additional aspects that need to be addressed include interoperability, scalability, integration with existing cryptography and crypto-agility as well as integration with network management, control and orchestration.

For the time being, therefore, it would seem that hybrid networks (defined here as the combination of PQC and QKD to offer quantum-safe resistance) offer the best path forward towards making networks more resilient and quantum-safe in the near future.

This document provides a step-by-step approach towards applying and integrating PQC and QKD technology into hybrid networks over time. It provides a series of recommendations for NRENs for the gradual implementation of these steps when transitioning from pre-quantum cryptography to PQC, as well as when integrating QKD and PQC into existing network infrastructures. These recommended steps are in line with the objectives of the Quantum European Strategy [1], the EuroQCI initiative [2] and the World Economic Forum [3].

Finally, a number of maturity models are examined that could help organisations assess their capabilities to implement hybrid networks using pre-quantum cryptography, PQC and QKD technologies and guide them during their transition towards quantum-safe networks.

1 Introduction

Quantum science has driven significant technological advancements since the early 20th century, including MRI diagnostics, semiconductor-based computing, and high-speed optical communications. Modern quantum technologies focus on harnessing deep-quantum phenomena such as superposition, no-cloning, and entanglement, which enable groundbreaking new capabilities.

Quantum computing offers computational power that exponentially increases with the number of qubits. With new algorithms such as Shor's algorithm for prime factorisation [4] [5], quantum computers are expected to break current public key cryptography (asymmetric cryptography) in the near future. This poses a "quantum threat" to the security of current internet communications. To counter this threat, mechanisms known as quantum-safe security (QSS) are being developed to ensure secure communications. It is interesting to note that not all public key schemes would be compromised by a quantum computer (lattice-based cryptography, for example, supports public key schemes); however, the most widely used ones today, such as RSA or elliptic curve, would indeed be compromised by the factorisation solved by Shor's algorithm.

The risk of breaking symmetric encryption algorithms such as Advanced Encryption Standard (AES) is lower, and these are considered secure if the key length is increased from the current maximum of 256 bits (AES-256) to larger keys of 384 or 512 bits. Many widely used encryption methods in current communication systems rely on the difficulty of factoring keys with current processing technologies. For example, RSA, which is based on public keys constructed from the product of two large prime numbers (typically 1024- or 2048-bit in length)., could potentially be broken by quantum computers using Shor's algorithm. While not all current cryptographic techniques may become vulnerable to this, this highlights the need for new, less sensitive cryptographic paradigms, known as Post-Quantum Cryptography (PQC).

From a cryptographic perspective, three key technologies are crucial towards developing quantum-safe security: (1) PQC: Using classical cryptography with new algorithms that offer computational complexity not solvable by known quantum algorithms within reasonable time and cost frames; (2) Quantum Random Number Generation (QRNG): Implementing true random number generators (TRNG) to replace commonly used pseudo-random software-based generators, promising better unpredictability and irreproducibility; and (3) Quantum Key Distribution (QKD): Also known as quantum cryptography, promising information-theoretic security (ITS) through quantum mechanics when combined with a one-time pad (OTP) encryption mechanism.

Other quantum cryptographic mechanisms include Quantum Secure Direct Communication (QSDC), Semi-Quantum Key Distribution (SQKD), Secure Multiparty Communication (SMPC), Quantum Blind Computing, Quantum Digital Signature, High-Dimensional QKD, or Position-Based Quantum Cryptography [6]. Of the different mechanisms mentioned, those that that can be classified as having greater technological maturity are based on QKD, QRNG, and PQC, and the rest of the document will be focused on these.

Deploying a quantum-safe network involves implementing QSS measures, i.e. using advanced cryptographic techniques designed to withstand threats such as those mentioned above. Key aspects of deploying quantum-safe networks are [7]:

- **PQC**: This involves using cryptographic algorithms that are resistant to attacks from quantum computers. These algorithms are designed to replace or complement existing encryption methods.
- **QKD**: QKD uses the principles of quantum mechanics to securely distribute encryption keys. This method ensures that any attempt to intercept the keys can be detected, providing a higher level of security.

- **Crypto-Agility**: This is the ability to quickly switch between different cryptographic algorithms as new threats emerge. It ensures that the network can adapt to future advancements in quantum computing.
- **Layered Security Approach**: This involves implementing multiple layers of security, including both classical and quantum-safe cryptographic methods, to provide comprehensive protection against various types of attacks.
- **Real-World Deployments**: Ensuring that quantum-safe solutions are scalable, adaptable, and cost-effective for practical use in real-world scenarios.

Migration to quantum-safe networks is becoming crucial for highly critical infrastructures such as power grids, nuclear power plant infrastructures or data centre networks, but also increasingly important for NRENs running nationwide research and education networks.

In February 2025, a short survey was run among 24 participants from 20 NREN organisations during the 34th Service and Technology Forum in Dublin, Ireland. Participants were asked about their priorities and activities related to making their networks quantum-safe, as well as about their short-term plans and the possibility for NRENs to work together in this area.

When asked "Is achieving quantum-safe security for your network currently a strategic priority for your organisation?", of 24 participants who responded two reported that they already undertake some activities in this area, and another two stated that they are following what is happening and/or are supporting their users who are carrying out some activities in this area. However, 19 of the NRENs reported that quantum-safe security was not yet a priority for them and a further two organisations were not sure about their status. Only three organisations provided answers to the second question about the steps they are taking to make their network quantum-safe: two indicated that there are not undertaking any activities in this area, while the third responded that quantum activities are not done on the existing "traditional" (TCP/IP) production network.

When it came to future plans, of 11 who responded, 6 organisations do not have any activities planned for the next 12 months related to quantum-safe networks, 3 are continuing with their existing activities such as "implementing PQC where possible" or "expansion of the national QCI network to take in a wider area and longer spans" and 1 organisation plans to focus on knowledge gathering and training.

Last but not least, participants have seen some opportunities for NREN collaboration, expressing the importance of the newly formed Special Interest Group for Quantum technologies – SIG-Quantum [8] in GÉANT for communication and collaboration, as well as training.

At the time of writing, the European Network and Information Systems (NIS) Cooperation Group [9] has also started a survey [10] on the EU Roadmap on Post-Quantum Cryptography and asked the European community for feedback on its PQC deliverable (first and next steps, please see section 2 below). The results of this survey are pending.

The remainder of this paper aims to set out a path forward towards quantum-safe networking by providing step-by-step descriptions for QKD and PQC migration. Section 2 first discusses the transition to post-quantum cryptography. Section 3 then describes the integration of QKD into networks, and the impact on orchestration, management and monitoring this will have. Section 4 provides a brief overview of the challenges of standardisation and certification relating to quantum-safe networking. Section 5 offers considerations for a roadmap for transitioning to quantum-safe networking with a brief checklist of recommendations. The focus of Section 6 is a discussion of maturity models and how an organisation may assess its progress when it comes to quantum-safe cryptography. Finally, Section 7 outlines the conclusions to this document.

2 Migrating to PQC

In April 2024, the European Commission (EC) published its recommendation on a coordinated implementation roadmap for the transition to post-quantum cryptography [11] [12]. As part of this publication the EC recommended establishing a work stream on PQC within the NIS Cooperation Group (NISCG). In June 2025, the NISCG published its first deliverable [13] [14] on how to proceed with first steps by the end of 2026 to initiate the transition to PQC, which will then be followed by next steps to ensure that this transition will be completed for as many systems as possible by 2035.

It is expected that the transition from quantum-vulnerable pre-quantum cryptography to quantum-resistant post-quantum cryptographic algorithms will take several years as interoperability and security standards across different platforms and devices must be maintained and as it will not be possible to transition all public-key cryptography in use in one instance. The EC therefore recommends starting out with standardised and tested hybrid solutions which include PQC to replace vulnerable public-key encryption methods such as RSA or discrete logarithm-based algorithms wherever applicable. Especially in high-risk scenarios, vulnerable public-key cryptography should not be used as a stand-alone mechanism after 2030 (and after 2035 for medium-risk scenarios).

The recommended EC timeline for a successful migration to PQC is based on the three basic quantum risk levels “low”, "medium" and "high", with factors that depend on the weakness of the cryptographic mechanism used, the expected impact if the mechanism were to be broken and the estimated time and effort it would take for the migration to PQC. It refers to the *PQC Migration Handbook* [15] from December 2024, where risk assessment can be judged as medium or high whenever confidentiality requires protection (high risk if confidentiality needs to be protected for more than 10 years) and if the migration effort is expected to take more than 8 years (high risk if it is expected to take more than 8 years and the impact of an attack would be high).

The **first steps** of the transition, which are recommended to be undertaken immediately, are:

- Identify and involve all types of stakeholders: Providers, users, consulting companies, representatives of science and research, CTO, CISO, and CIO stakeholders from ministries, governmental bodies, and standardisation organisations.
- Investigate market readiness.
- Identify obstacles impacting the migration to PQC.
- As an organisation, investigate your cryptographic assets, create and maintain cryptographic inventories.
- Create dependency maps that help you assess both internal, third party and supply-chain dependencies when it comes to products and applications and makes it possible to set priorities and also to take cross-border alignment for interoperability at the EU level into account.
- Conduct a quantum risk analysis (assess your organisations risk of vulnerabilities when it comes to quantum threats), and include it in your cyber security risk reports
- Talk to your suppliers about integration of PQC and cryptographic agility (i.e. the ability to replace a cryptographic mechanism in an agile manner with very little effort).
- Raise national awareness of the urgency to start now and develop product/service roadmaps in alignment with the PQC roadmap across the EU.
- Share knowledge and develop an implementation plan to help synchronise the PQC migration not only within each member state but in the EU as a whole in order to ensure readiness and be quantum-safe in time.

The recommended **next steps** to be approached as soon as possible include:

- Offering a quantum-safe upgrade path for products and supporting crypto-agility.
- Allocating resources for the transition (not only budget but also trained personnel).
- Adapting certification schemes that take quantum threats into account.
- Evolving regulations and cryptographic policies ensuring that they are systematically updated with the latest recommendations for PQC.
- Evolving the ecosystem with funding and training, including capacity building for NRENs, cross-border cooperation, and pilot use cases over test infrastructures to ensure interoperability.
- Cooperating across borders on research and training and ensuring that transversal activities are included throughout the creation and implementation of the roadmap and support PQC standardisation working groups.
- Testing international interoperability of PQC solutions for a seamless and smooth PQC migration across the EU and performing pilot use cases over test infrastructures.

According to the recommendation, adhering to these steps and timelines will avoid chaotic transitions that could possibly introduce new vulnerabilities stemming from solutions that are insufficiently tested.

In the US, the National Institute of Standards and Technology (NIST) provides very similar guidelines for the integration of PQC into existing infrastructures in their Cybersecurity Framework Version 2.0 [16] [17] [18]: The framework lists 5 core functions for organisations to manage cybersecurity risks. These include:

- *Identify*: learn your organisation's quantum-related risks and how they could impact your data, systems, assets (including supply chain risks) and services, develop a strategy to transition to PQC, and set priorities for critical components.
- *Protect*: use protective technology that supports PQC when it comes to hardware and also software upgrades and make sure that all your cryptographic mechanisms are regularly updated to integrate PQC. Protect identity management systems and access systems with PQC algorithms and also extend this to your data (in transit and at rest). Focus on awareness and training.
- *Detect:* implement processes that will let you identify anomalies and unusual events that could be part of a quantum-related cybersecurity activity. Monitor continuously to be able to detect possible breaches of your cryptographic systems and keep all systems up to date with regular audits and reviews.
- *Respond*: Test and implement response plans to be able to react to attack incidents and have communication protocols in place that will allow you to inform stakeholders about the threat and its mitigation. Analyse incidents and try to learn from them in order to be able to improve your strategies.
- *Recover*: Develop plans that will allow you to maintain resilience and be able to restore your services after an incident and keep stakeholders informed about recovery status for transparency.

Aydeger et al. [19] describe these core functions of the NIST Cybersecurity Framework version 2.0 but go a bit further by offering concrete case studies, recommendations for implementation and best practices from early adopters. The authors recommend hybrid cryptographic approaches where classical cryptographic algorithms and PQC algorithms are combined.

Classical cryptography distinguishes between:

- Asymmetric-key algorithms such as ECC and RSA (which use two different keys – a public key and a private key – to encrypt and decrypt data); and

- Symmetric-key algorithms such as AES (where the same secret key is used to encrypt and decrypt a message).

PQC algorithms (see also Section 4 on standardisation) are categorised into:

- Hash-based cryptography (algorithms such as SPHINCS+ [20][21]).
- Lattice-based cryptography (algorithms such as Kyber and Dilithium [22]).
- Multivariate quadratic equations (MQE)-based cryptography [23]) and algorithms such as classic McEliece [24], which remain research efforts as there are some practical issues with them (e.g. huge keys for McEliece).

By combining classical and PQC algorithms in hybrid approaches, compatibility can be ensured, and security can be provided against current threats while preparing against future vulnerabilities.

Aydeger et al. [25] list the following hybrid use case examples:

- **Authentication:** Combine classical key exchange algorithms (RSA, Diffie Hellman) with PQC algorithms such as lattice-based key exchange.
- **Encryption:** AES in connection with hybrid key encapsulation mechanism (KEM) to secure the symmetric key with both classical and PQC algorithms [26].
- **Digital signatures:** Both classical (such as RSA or ECC) and PQC algorithms can be employed for digital signatures.

As early adopters, the authors mentioned Google's combination of PQC (NewHope key exchange algorithm) and classical ECC in an experiment with its Chrome browser [27]. Other hybrid approaches described were Cisco's Virtual Private Network (VPN) solutions with both classical and PQC algorithms for encryption to secure data transmissions.

Adopting hybrid solutions and a phase-in approach for the new PQC algorithms seems to be the best way forward [28], as it ensures backward compatibility while the implementation challenges of PQC are still being ironed out: PQC faces challenges with standardisations and regulatory issues, but also compatibility issues with legacy systems and in cross-border environments. PQC algorithms often lead to the management of larger key sizes and requirements for more computation, hardware acceleration, optimisation or parallel processing. Performance tests should be conducted in pilot environments to assess any transition process.

3 Migrating to QKD

While PQC seems to be quantum-safe for now, it still has to pass the test of time. Just recently, the SIKEp434 algorithm, which had been one of the candidates in round 4 of the PQC standardisation process run by NIST, was broken [29]. Therefore, the option to make networks quantum-safe based on QKD is appealing as it relies on quantum mechanics rather than complex algorithms to generate keys without modifications or eavesdropping. Although QKD has been shown to be information-theoretic secure it is still unclear – due to a lack of certification – exactly what level of security the currently available physical QKD systems can offer.

Another problem with QKD devices is that their terrestrial reach is still rather limited and long distances require intermediate trusted nodes to relay QKD keys to distant endpoints and satellite transmissions. However, satellite transmissions have their own set of issues, ranging from interference due to weather, sunlight and atmospheric impairments to satellite availability (orbit periodicity and geometry, pointing agility and accuracy) [30].

For the time being, therefore, it would seem that hybrid networks (defined here as the combination of PQC and QKD to offer quantum-safe resistance) are the way forward, i.e. step-by-step integration of QKD into existing infrastructures while employing PQC algorithms whenever possible as a way to make networks more resilient and quantum-safe for the near future.

Klicnik et al. [31] [32] describe a real-world deployment of QKD in an academic network and the challenges that were encountered with multiplexing classical and quantum channels within the same wavelength band. Viksna et al. [33] studied another use case example of how QKD can be integrated step by step into a hybrid classical-quantum network: in their hybrid network, users wishing to communicate using quantum key distribution are connected to their nearest QKD service node originally via links protected by classical encryption such as TLS.

These links are then hardened by the PQC algorithms SPHINCS+ for certificate signatures and FrodoKEM for key exchange. In addition, they propose a new protocol where half-keys of the QKD session keys are relayed crosswise in a butterfly fashion between two QKD service nodes, meaning each node contributes and exchanges part of the key so that the final session key is jointly established (assuming that there is added security since an eavesdropper would have to compromise both links). More information on this approach can be found in [34].

But when considering the integration of QKD into existing classical networks, providers still face a number of challenges in areas such as:

- Interoperability and scalability
- Integration with existing cryptography and crypto-agility
- Integration with network management, control and orchestration

As traditional network frameworks do not handle the particularities of quantum-resistant cryptographic mechanisms, which introduce new computational requirements, increased key sizes, different trust models, and new network elements, these changes impact key management, authentication and secure communication, requiring the adaptation of management mechanisms or even the definition of novel approaches that ensure seamless integration with existing infrastructures.

The following sections will provide more details on these issues and how such integration can be addressed in hybrid networks where QKD is being slowly introduced.

3.1 Interoperability and Scalability

A key element for network providers is **interoperability**. As organisations transition from classical to quantum-resistant systems, it is unlikely that this migration will occur uniformly across all domains. Therefore, quantum-safe solutions must be designed to not only interoperate with other quantum-safe systems, but also to interoperate seamlessly with legacy systems.

This includes support for dual-stack protocols capable of handling both classical and quantum cryptographic operations. Ensuring interoperability helps maintain continuity of operations during the transitional phase and enables mixed environments where classical and quantum-safe endpoints can securely communicate, which is essential in large, distributed infrastructures like government networks, financial institutions, and telecom providers.

Another critical aspect is **scalability**, particularly in light of the increased computational and storage demands introduced by post-quantum algorithms. It could be argued that many PQC schemes require significantly larger key sizes, longer handshake durations, and more memory-intensive operations than their classical counterparts. QKD networks (QKDNs) also introduce unique scalability challenges, such as managing key relays between distant nodes or provisioning quantum links within the physical constraints of the optical infrastructures.

To meet these demands, quantum-safe architectures should incorporate intelligent orchestration layers capable of dynamically allocating resources, prioritising traffic, and offloading cryptographic workloads. Moreover, cryptographic operations should be optimised to leverage hardware acceleration where possible, allowing the infrastructure to absorb the impact of more demanding cryptographic primitives without degrading performance.

The practical deployment of QKD also presents a significant scalability challenge in itself: QKD typically generates keys in a point-to-point form and presents some physical limitations such as distance, which hinders the scalability and integration into existing communication infrastructures. To overcome these constraints, QKD networks allow keys to be relayed across intermediate QKD nodes, enabling secure key sharing even between parties that are not directly connected by a QKD link. This approach requires a well-structured key management framework to ensure E2E security.

NREN use case: Scalability and interoperability in connection with EuroQCI, National QCIs and R&E Networks

With the arrival of the QKD technology NRENs need to address both interoperability and scalability issues: ***interoperability*** is a major concern when it comes to cross-domain infrastructures such as EuroQCI [35]. The EuroQCI infrastructure will consist of individual National Quantum Communication Infrastructures (QCIs) and EU-QCI infrastructure. The EU-QCI ecosystem will include the SpaceQCI infrastructure, QuantumHub and interface to Terrestrial QCI infrastructure that can later connect to individual National QCIs (see Figure 3.1).

From the European Commission's perspective, EuroQCI is intended to evolve starting from 2027 to a fully operational infrastructure with the IRIS2 integration in mind. Given that certification and standardisation issues will be solved, the infrastructure should be able to handle up to EU-Secret classification material and data.

The current view presented in the EuroQCI ConOps document [36] outlines different elements of the EuroQCI infrastructure:

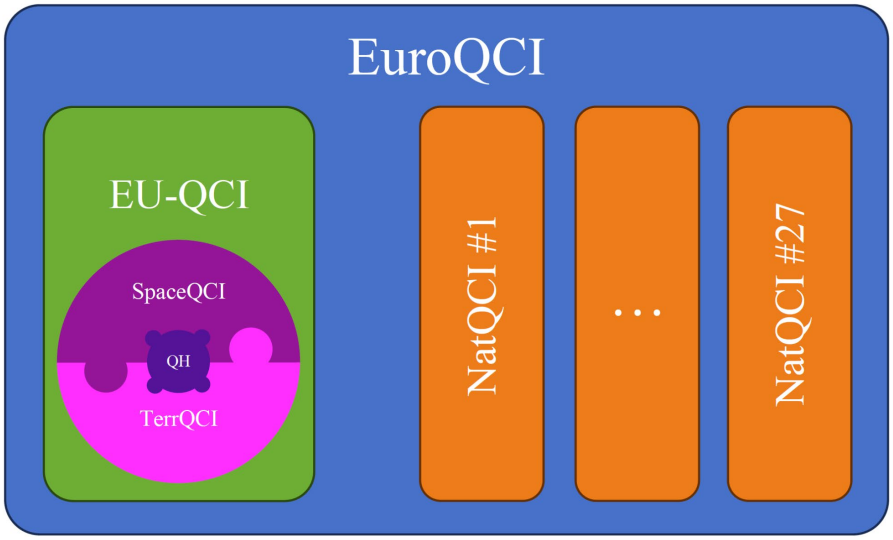

Figure 3.1: EuroQCI ecosystem

National Quantum Communications Infrastructures (NatQCIs) have broad autonomy and can use various scenarios and ways to interconnect with EU-QCI or other NatQCIs. It is up to the individual Member State and its NatQCI to decide how it is governed, used and interconnected with other systems and networks. It is important to note that individual NatQCIs can interconnect with each other independently of the EU-QCI infrastructure. **The requirement here is to ensure appropriate Key Management Services (KMSs) and connectivity between KMSs used in specific NatQCIs**.

From a research and development point of view, this is a desired option as it allows to set up and run independent KMS infrastructures and services for specific projects or activities, for example between the NRENs. This gives flexibility and separation from the infrastructure that requires EU-Secret or EU-Restricted classification and procedures and thus provides ***scalability*** for NRENs. The interested parties that want to engage in R&D activities with respect to QCI activities need to dedicate resources and prepare compatible KMS infrastructure that will allow them to work with the desired QKD infrastructure. In case of incompatible QKD infrastructure, a gateway KMS can be prepared to relay the KMSs, to allow for the inter-KMS interconnection. This approach allows for multi-layer setup for inter-KMS connectivity.

3.2 Integration with Existing Cryptography and Crypto-Agility

One of the most critical challenges in encryption is **key management**, including the functionalities of key generation, distribution, storage, synchronisation and renewal. In the quantum era, key management must accommodate both PQC and QKD for hybrid networks, and effectively managing and orchestrating these mechanisms is essential for enabling secure and scalable quantum-safe networks. Also, QKD does not solve the problem of user and device authentication, and additional mechanisms have to be in place to ensure identity verification.

For QKD key management, the ITU-T has published several recommendations such as the ITU-T Y.3802 [37], which defines the functional architecture of QKDNs, and the ITU-T Y.3803 [38], which defines fundamental key management operations for QKDNs, addressing key reception, storage, relay, synchronisation, and deletion.

QKDNs often rely on a centralised controller to monitor network status and manage key distribution efficiently. To support these functionalities, a QKDN key management system must handle the following operations:

- **Key acquisition, authentication and storage**: receiving keys from QKD modules, ensuring proper formatting, and temporarily storing them in secure buffers.
- **Key request processing from cryptographic applications**: authenticating applications that request QKD keys.
- **Key relay across QKD nodes**: managing the secure relay of keys when no direct QKD connection exists, with the route controlled by the QKDN controller.
- **Key supply to cryptographic applications**: delivering keys securely to authorised applications.
- **Key lifecycle management**: overseeing key transitions across all phases, including reception, storage, formatting, synchronisation, authentication and deletion.

On the other hand, in quantum-safe networks, traditional key exchange mechanisms such as RSA and ECC must be replaced, or possibly combined, with quantum-resistant alternatives such as PQC algorithms. In this case, effective management of PQC keys must address several areas:

- **PQC-enabled PKI**: Public Key Infrastructures must evolve to support post-quantum algorithms such as CRYSTALS-KYBER, CRYSTALS-Dilithium, SPHINCS+ and FALCON to follow the standardisation put forward by NIST (see also section **Error! Reference source not found.**). This includes upgrading Certificate Authorities (CAs) to support issuance and validation of certificates that use post-quantum signature algorithms. Backend cryptographic libraries must also be adapted to support PQC or hybrid certificate formats, and the root and intermediate CA migration strategies must be carefully designed, as these entities form the trust backbone of digital infrastructures.
- **Scalable key distribution mechanisms**: given the larger key sizes and higher processing demands, efficient and scalable mechanisms for securely distributing PQC-based keys are crucial.
- **Key revocation policies**: PQC schemes must support fast and reliable revocation and update strategies, especially due to the likelihood of evolving algorithm standards in the early adaptation phase. This requires robust and adapted mechanisms for Certificate Revocation Lists (CRLs) distribution, Online Certificate Status Protocol (OCSP) for real-time checking of a certificate revocation status directly from a Certificate Authority (CA)'s OCSP Responder, and possibly new revocation frameworks tailored to PQC if needed.
- **Hybrid key management strategies**: during the transition to quantum-safe systems, hybrid models that combine classical and quantum-safe algorithms are essential. Key management frameworks should support managing these coexistence schemes while preserving security and backward compatibility.

For practical deployment, a unified key management architecture must support both PQC and QKD, ensuring seamless integration within existing infrastructures. This involves several functionalities:

- **Policy-based key selection**: administrators may define context-aware policies for selecting keying mechanisms, enabling adaptive use of PQC, QKD or hybrid schemes based on availability, performance, security level, or compliance requirements.
- **Interoperability mechanisms**: the architecture must bridge classical, PQC, and QKD-based systems, providing translation layers, hybrid certificate formats, and cross-domain trust models.
- **Key synchronisation and consistency**: to ensure secure communication, the quantum-safe networks must include protocols and tools to verify and synchronise keying material across distributed systems.
- **Monitoring, logging, and auditability**: key management should include secure logs, audit trails, and real-time monitoring dashboards to ensure compliance, detect anomalies and support incident response.

- **Scalability and automation**: integration with orchestration systems enables the automated provisioning, renewal, and decommissioning of keys at scale. This is essential for dynamic environments such as 5G/6G networks, edge computing, and cloud-native infrastructures.
- **Resilience and fault tolerance**: unified systems must offer high availability, support disaster recovery, and maintain secure fallback mechanisms in case of QKD link failure or PQC algorithm deprecation.

Closely related to key management, and also critical for the management of quantum-safe networks, is the need for **crypto-agility**, which can also be understood as the ability of a network to dynamically switch between classical and quantum-safe cryptographic algorithms. This requires updates in the network management systems to support new cryptographic mechanisms and protocols and ensure seamless interoperability between traditional and quantum-safe systems.

3.3 Network Management, Control and Orchestration

Network control, management and orchestration play a crucial role in current communication infrastructures as they enable efficient operation, optimisation and automation of increasingly complex services. **Network control** focuses on real-time decision making, such as packet routing, bandwidth management and QoS policy enforcement. It ensures that networks can dynamically adapt to changing conditions and user demands.

Network management, on the other hand, encompasses the tools and techniques to monitor and maintain the network, including fault detection, performance monitoring and network configuration.

Orchestration takes these concepts further by automating the deployment, coordination and lifecycle management of network resources and services. It integrates technologies like Software-Defined Networking (SDN) and Network Functions Virtualisation (NFV) to dynamically allocate resources, provision and scale services, and ensure seamless operation across heterogeneous environments. Together, these components enable networks to be efficient, operational and scalable according to the demands of current applications and services.

Integration with Network Management: Monitoring, Maintenance and Operation

Monitoring and policy enforcement play an increasingly important role in securing and managing a quantum-ready environment. As the cryptographic surface of a network expands, so too does the need for visibility and control over how cryptographic assets are used. Monitoring systems must track algorithm usage, certificate validity, key lifecycles, and protocol negotiation outcomes across the network in real time. This data can be used not only for compliance and auditing, but also to detect anomalies, enforce security policies, and ensure cryptographic agility is functioning as intended. Integrating monitoring and enforcement directly into programmable network infrastructure allows for responsive and automated mitigation, helping ensure that the entire system remains resilient.

Ensuring continuous and reliable operation of quantum-safe networks requires updating maintenance frameworks, evolving operational tools, and adopting new best practices for system adaptation. These efforts must address the unique challenges introduced by both PQC and QKD, including cryptographic complexity, interoperability requirements, and lifecycle management of cryptographic assets.

In a quantum-resilient environment, cryptographic maintenance becomes a core operational responsibility. Operators must manage multiple cryptographic schemes concurrently: classical, PQC, and potentially hybrid. At the same time, they must ensure the secure and efficient lifecycle handling of cryptographic materials. This includes:

- Periodic key renewal in accordance with security policies and algorithm-specific lifetimes.
- Certificate update and revocation as part of Public Key Infrastructure (PKI) operations.

- Monitoring the state and availability of QKD keys, including buffer levels, key age, available key rate in each link, etc.

Thus quantum-safe networks introduce additional layers of complexity that must be monitored, logged, and analysed in real-time. Detailed telemetry and alerting mechanisms [39] are needed to manage aspects including QKD link status (link quality, synchronisation, key rate, QBER, etc.), key usage and expiry events, including certificate validation failures or key supply exhaustion. Monitoring frameworks must be enhanced with cryptography-specific telemetry, extending existing protocols such as:

- **gNMI** (gRPC Network Management Interface) for streaming real-time state information.
- **YANG data models**, which may require extensions to model quantum-specific parameters (e.g., qkd-key-status, pqc-algorithm-profile, hybrid-certificates).
- **SNMP or REST-based APIs**, where backward compatibility with legacy monitoring systems is necessary.

In this context, the maintenance of quantum-safe networks depends heavily on the availability of **well-defined, standardised APIs** that allow integration, automation and interoperability across multivendor environments. APIs are essential for both human and machine interaction with network components, especially in environments built on SDN and NFV. Several interfaces play a critical role, such as the OpenConfig and gNMI, which are widely used in NREN environments for telemetry and configuration management, and some other interfaces defined by both the ETSI and the ITU-T regarding the orchestration and control APIs for QKD networks.

For example, in a hybrid quantum-safe network, a QKD-aware entity might expose a RESTful northbound API enabling integration with a central SDN orchestrator (Figure 3.2). This API would support operations such as requesting a key relay path, querying buffer availability or pushing key distribution policies. Similarly, a PQC-aware Certificate Authority may expose an API for issuing hybrid certificates using PQC and classical. These APIs must also support revocation operations using Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) distribution with PQC compatibility.

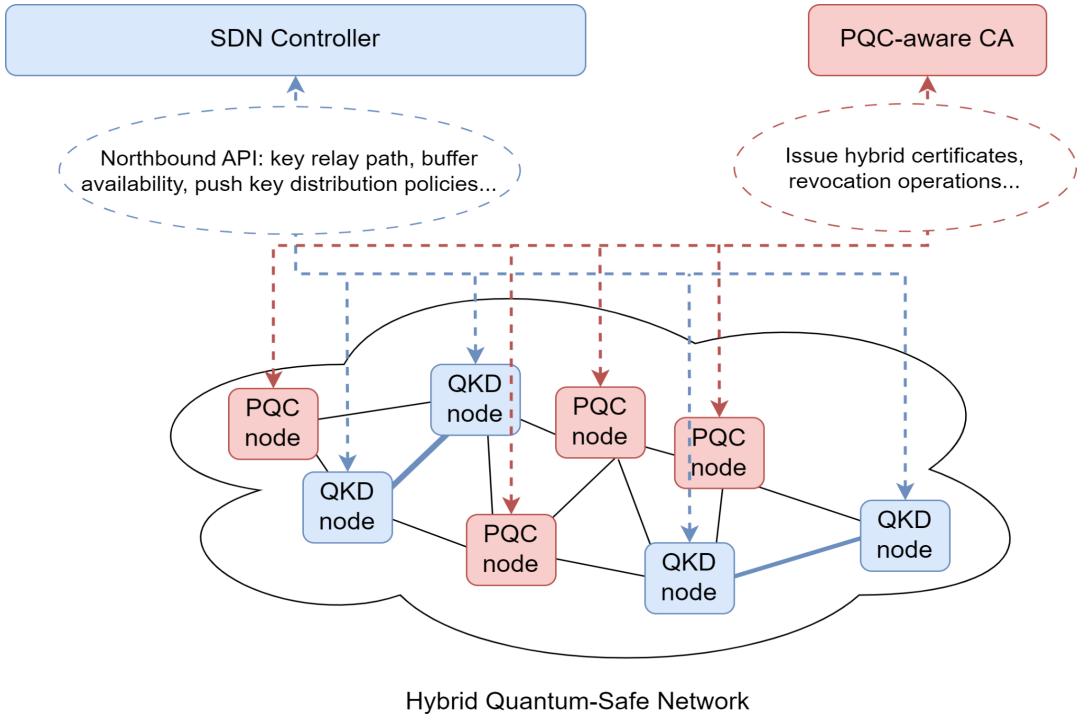

Figure 3.2: Hybrid quantum-safe network

On the other hand, operational frameworks must support adaptability over time, as cryptographic standards evolve and network infrastructures scale. Adaptation mechanisms include:

- Automated algorithm migration: Tools and workflows to transition endpoints from classical to hybrid and fully quantum-safe configurations without service interruption.
- Service chaining and policy adaptation: Dynamic reconfiguration of security services (firewalls, VPNs, etc.) to use appropriate cryptographic mechanisms based on policy and context.
- Hardware and software readiness tracking: Maintaining inventories of cryptographic capabilities across devices to support adaptive configuration.

The operationalisation of quantum-safe networking requires an additional layer comprised of maintenance routines, operational toolsets, and adaptation strategies. This includes the introduction of new telemetry models, integration of standardised and programmable APIs, and automation of cryptographic lifecycle management, among others. Existing standards and technologies such as gNMI, YANG, OpenConfig, and REST/gRPC interfaces must be extended to support quantum-era requirements, while new protocols and data models will emerge through standardisation efforts, and operations and maintenance of the classical network must continue through the transition to the fully quantum-safe networks.

Integrating Quantum-Safe Networks with SDN and NFV

As described in this section, quantum-safe networking introduces a new layer of cryptographic complexity that requires careful coordination across various infrastructure components. SDN and NFV, widely extended in traditional networks, offer the orchestration capabilities necessary to manage this complexity, providing centralised control, automation, and agility. SDN controllers can dynamically route traffic based on cryptographic requirements, selecting between PQC services, QKD-based keys, or hybrid mechanisms. This real-time programmability ensures that cryptographic functions are aligned with evolving policies, application needs, and threat conditions.

NFV complements this by virtualising cryptographic services, such as key distribution agents, PQC engines, etc., allowing them to be instantiated on demand. This elastic deployment model supports the automated scaling of cryptographic capacity, for instance during a rekeying event or under heavy load. Integrated orchestration platforms can manage the full lifecycle of these virtualised services, coordinating key generation, relay, revocation, and logging workflows across the network in a unified manner.

Beyond automation, SDN and NFV also enable more granular service differentiation. Through network slicing and dynamic service chaining, different flows or tenants can be assigned specific quantum-safe protections tailored to their sensitivity. Orchestration frameworks serve as the glue that binds together policies, resources, and services, ensuring that quantum-safe mechanisms are deployed consistently and efficiently across the network. As such, SDN and NFV are not just enablers but the operational backbone of quantum-safe network orchestration.

This orchestration landscape aligns closely with international standardisation efforts, such as the ITU-T Y.3804 [40] or the ITU-T SG13 Y.QKDN_SDNC [41] recommendation on QKD network control and management and SDN control in QKD networks.

These documents define the architectural functions and reference points needed to orchestrate QKD-specific elements across multiple layers, quantum, key management, and service, within a QKD network. It outlines a hierarchical model that includes a dedicated control layer and a management layer responsible for cross-layer coordination, policy enforcement, and interworking with external systems. The recommendation reinforces the importance of multi-layer orchestration in QKDNs, mirroring many of the principles already being applied through SDN/NFV paradigms in broader quantum-safe network architectures.

Orchestrators for harmonising control of classical and quantum resources currently exist mostly in the context of cloud-based hybrid workloads. Examples are Qonductor [42] for hybrid quantum-classical applications running on heterogeneous hybrid resources, or QFOR [43] for quantum scheduling and quantum fidelity-aware orchestration of tasks across heterogeneous quantum nodes.

Similarly, Q-Orchestrator [44] enables the execution of quantum circuits in different providers. Other examples of orchestrators include Quantum Machines [45] for hybrid control of quantum and classical operations or Amazon Braket [46] with a fully managed service for running hybrid quantum-classical algorithms; Orquestra [47] for integrating PQC; and Qoro [48] for streamlining quantum workflows.

4 Standardisation and Certification

From the perspective of standardisation bodies, both the European Telecommunications Standards Institute (ETSI) and International Telecommunication Union (ITU) are consistent in defining a quantum-safe network as implementing technologies and standards to protect data against the potential threats posed by quantum computing, with a focus on deploying quantum safe cryptography mechanisms such as PQC and QKD.

ETSI standardisation

ETSI focuses on different aspects of Quantum-Safe Cryptography (QSC), which aims to develop cryptographic algorithms resistant to attacks from both classical and quantum computers. Their efforts include:

- PQC: Developing and standardising cryptographic algorithms that can withstand quantum attacks.
- QKD: Using quantum mechanics principles to securely distribute encryption keys, ensuring any interception attempts are detectable.
- Practical Implementation: Assessing and recommending quantum-safe cryptographic primitives, protocols, and implementation considerations for real-world deployment.

It is important to highlight the work of the ETSI QSC Working Group, which has led to the publication of Technical Report TR 103 619 in 2020 [49]. This report outlines migration strategies and provides recommendations for the adoption of quantum-safe schemes, as well as actions to raise cybersecurity awareness across all sectors. Also noteworthy is the extensive work carried out by the Industry Specification Group (ISG) on QKD, which has, for over a decade, produced numerous documents that serve as de facto standards for the development of QKD devices, functional blocks, and interfaces [50].

ITU standardisation

ITU's approach includes developing standards for networks that support quantum-safe encryption and authentication. Key aspects covered include:

- QKD: ITU standards describe the networking concepts to underpin QKD, enabling secure encryption and authentication even in the presence of quantum computing.
- Security Guidelines: ITU provides guidelines for applying quantum-safe algorithms in various systems, such as IMT-2020 (5G) networks, to mitigate threats posed by quantum computing.
- Interoperability and Best Practices: ITU focuses on creating standards for the interoperability of QKD equipment from different vendors and codifying best practices for QKD network implementations.

Examples of released ITU documentation about QKD include [51] Y.3800 ‘Overview on networks supporting quantum key distribution’, which describes the basic conceptual structures of QKD networks as the first of a series of emerging ITU standards on network and security aspects of quantum information technologies, such as [52] X.1811, which relates to PQC strategies.

CEN-CENELEC standardisation roadmap

In 2023, the CEN-CENELEC Focus Group on Quantum Technologies published a Standardisation Roadmap on Quantum Technologies [53], which also includes a section on the standardisation needs for quantum communication systems, including QKD technology.

This extensive document covers:

- QKD protocols
- QKD transmitter and receiver modules
- Generic QKD components
- Single-link QKD
- Basic standards related to QKD and quantum communication
- Security evaluation/certification of quantum key distribution
- Quantum repeaters

Detailed analyses and considerations are given for existing and projected standards, as well as standardisation gaps and additional standardisation needs that must still be addressed.

NIST standardisation

In 2015, NIST started work on selecting and standardising quantum-resistant algorithms; at first four algorithm standards were selected and then approved as Federal Information Processing Standards (FIPS) by the US Secretary of Commerce: CRYSTALS-Kyber, CRYSTALS-Dilithium, Sphincs+ and FALCON. Three of these first draft standards were published in 2023 [54]. The fourth draft standard based on FALCON is currently (October 2025) pending release. A fifth algorithm – HQC – was selected in March 2025; this standard is expected to be published in 2027 [55] [56].

The first four FIPS include:

- FIPS 203 [57]: primary standard for general encryption
- Standard based on the **CRYSTALS-Kyber** algorithm (Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)); small encryption keys for easy exchange between two parties.
- HQC (fifth algorithm to be standardised in 2027) will become the backup algorithm for general encryption.
- FIPS 204 [58]: primary standard for protection of digital signatures
- Standard based on the **CRYSTALS-Dilithium** algorithm (Module-Lattice-Based Digital Signature Algorithm (ML-DSA)).
- FIPS 205 [59]: intended as backup method for digital signatures
- Standard that uses the **Sphincs+** algorithm (Stateless Hash-Based Digital Signature Algorithm (SLH-DSA)). Employs a different math approach from ML-DSA in case ML-DSA turns out to be vulnerable.
- FIPS 206 [60]: under development – Built around the **FALCON** algorithm (FFT (fast-Fourier transform) over NTRU-Lattice-Based Digital Signature Algorithm (FN-DSA)).

Certification

While having standards as documented guidelines is a prerequisite first step, certifying systems to confirm that that they meet the required standards in practice can present challenges. In January 2025, the first QKD product to receive an official national security approval was the Clavis XG Series of ID Quantique [61], which obtained the certification from the National Intelligence Service (NIS) of South Korea. The evaluation of the optical and digital subsystems also included the protocols and software stack of the Key Management System used (Clarion KX).

The European Union has adopted the Common Criteria-based Cybersecurity Certification Scheme (EUCC) as a process to certify hardware and software [62] [63]. Certification efforts are also driven by the German Bundesamt für Sicherheit in der Informationstechnik (BSI) [64].

5 Transitioning to Quantum-Safe Networking

As highlighted in the previous chapters, the challenges in implementing quantum-safe networking are wide-ranging and transitioning to quantum-safe networks using emerging technologies requires a careful, step-by-step approach. Since this process will require time, the best way forward is to initially use a hybrid approach, not only when it comes to moving from pre-quantum cryptography to PQC, but also when integrating QKD and PQC into existing network infrastructures.

This section summarises recommended steps and provides a short-term, medium-term and long-term timeline towards the implementation of quantum-safe networking for network providers , in line with the objectives of the Quantum European Strategy [65], the EuroQCI initiative [66] and the World Economic Forum [67].

- **Recommendation 1: Identify and Prioritise Quantum-Safe Cryptographic Algorithms**
  - Understand the computational requirements and performance impacts of adopting post-quantum algorithms, which may have higher latency or resource consumption.

- **Recommendation 2: Implement Quantum-Safe Cryptography and QKD in Network Infrastructure**
  - Quantum-safe protocols: Begin integrating post-quantum algorithms for secure communication, like Lattice-based algorithms and hash-based cryptography, into NRENs' networking and security protocols.
  - QKD implementation: Deploy QKD infrastructure in pilot locations, focusing on high-value research applications, and gradually expand this network to cover more campus and research institution connections. Use fibre-optic networks for early-stage deployment, as fibre provides the most mature platform for QKD.
  - Work on hybrid cryptography: combining classical encryption for routine traffic with QKD for high-priority or sensitive communication, ensuring that traditional networks can interoperate with quantum-safe techniques.

- **Recommendation 3: Foster Collaboration and Knowledge Sharing**
  - Engage in collaborations with international research bodies, industry and governments to ensure up-to-date adoption of quantum-safe technologies. Notably, integrate QKD as part of these discussions to align with global standards.
  - Participate in national and global initiatives such as the European Quantum Flagship, the EuroQCI Initiative, and Quantum Internet Alliance, which are focused on building quantum-safe infrastructures, including the development of QKD systems.

- **Recommendation 4: National Quantum-Safe Transition Timeline**
  - *Short-Term (2025–2026)*: Conduct an assessment of the current NREN infrastructure and perform initial trials for PQC and QKD. Begin the process of integrating quantum-safe protocols for specific use cases (e.g., secure key exchange in VPNs, securing sensitive research data). Conduct a comprehensive risk assessment to identify quantum computing threats and evaluate current NREN vulnerabilities. Begin PQC pilot programs for key services (e.g., secure key exchange in VPNs). Launch initial QKD pilot projects to test the feasibility of secure communication using quantum keys. Some recommended guidelines to follow include the EU Cybersecurity Act and ENISA guidelines on quantum-safe cryptography [68], ETSI GS QKD and PQC standards or NIST Draft Guidance (SP/IR) SP-800-227 [69], IR 8547 [70], and IR 8528 [71].

- *Medium-Term (2027–2030)*: Expand the integration of quantum-safe protocols and QKD in more NREN segments. Foster collaboration with other NRENs to ensure interoperability and shared learnings. Begin replacing legacy cryptographic systems in key infrastructures:
  - PQC Integration: Begin wider adoption of quantum-safe protocols for secure communication in more critical NREN services, ensuring robustness against quantum attacks.
  - QKD Expansion: Roll out QKD-based secure key exchanges across regional networks and expand QKD infrastructure to more campuses and partner research institutions. Foster collaboration and share lessons learned across NRENs to enhance collective capabilities.
- *Long-Term (2030–2035)*: Achieve a fully quantum-safe NREN infrastructure, with robust adoption of QKD in core and edge networks, including between universities and across international research collaborations. Achieve full integration of quantum-safe protocols across all NREN infrastructures, ensuring complete protection against quantum threats. Establish national quantum-safe network standards to ensure consistency and interoperability across NRENs and international research communities. Ensuring interoperability across national quantum communication infrastructures – particularly in cross-border scenarios envisioned by initiatives like EuroQCI –presents a highly technical and political challenge. Achieving seamless interconnection between diverse implementations of QKD and PQC requires consensus on architecture, orchestration, and key management systems.
- *Post-2035:* Stay ahead of quantum advancements by continuously researching PQC and QKD technologies, updating systems as needed to keep pace with emerging quantum computing developments. Expand QKD networks globally to create a seamless quantum-safe global communications infrastructure.

- **Recommendation 5: Training and Education**
  - Develop specialised training and make certification programs available to network engineers, administrators, and security professionals, focusing on post-quantum cryptography and QKD technologies [72].
  - Host workshops, seminars, and webinars for researchers to educate them on the future of quantum-safe networking and the role of QKD in securing sensitive academic research data.

6 Assessing Maturity of Quantum-Safe Networks

Maturity models [73] are used to assess the capabilities of an organisation, for example when it comes to processes, services or management structures and how well these practices match with a specific purpose or goals.

This approach is not only valuable for current network provider services but can be especially useful when it comes to emerging technologies or complicated processes such as migrating from PQC to QKD. The following section describes notable maturity models for both QKD networks and PQC.

Maturity considerations for PQC

A Post-Quantum Cryptography Maturity Model was proposed by DigiCert [74], with levels ranging from PQC Novice and Apprentice to PQC Practitioner and Master. There are also two dimensions to this maturity model that represent two important factors: how much an organisation understands and knows when it comes to quantum threats and how much preparation is actually carried out as a defence against such threats.

The PKI consortium [75] suggests the use of a Post Quantum Security Maturity Index to continuously monitor progress when it comes to improving quantum defences and to fine-tune actions that should be prioritised vs. budget considerations. Eight maturity levels (stages) are used in their suggested model (see Figure 6.1), where of the first 3 levels, level 1 deals with risk analysis and strategy, level 2 focuses on discovery (random numbers, PKI cryptography), and level 3 defines an ecosystem with vendors, tools, services and open source for interoperability. Level 4 in the PKI consortium maturity model refers to a Post-Quantum Encryption (PQE) Architecture; this is elevated to a PQE test environment in level 5 and to limited trials and prototypes for crypto agility in level 6. Level 7 describes the rollout and network implementation of crypto agility, while the final level 8 encompasses management of threats and algorithms, as well as management of new automation and APIs.

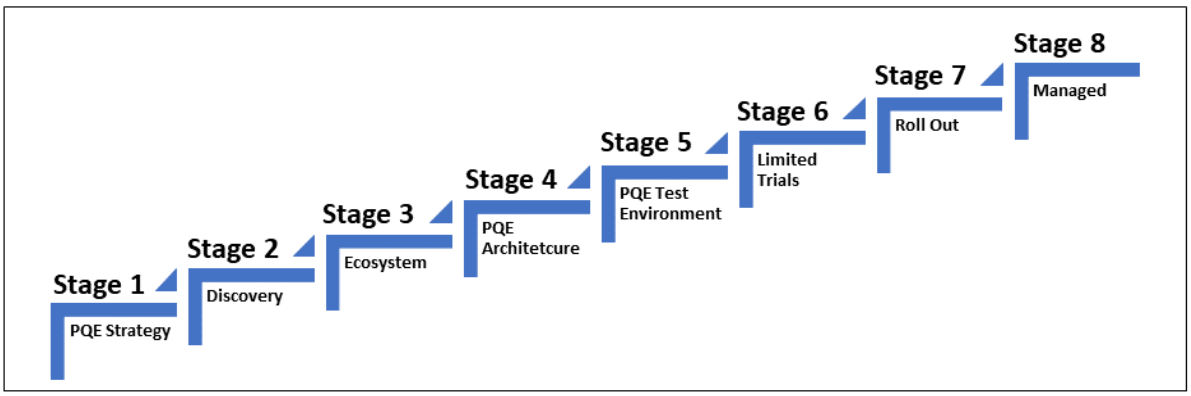

Figure 6.1: Post Quantum Encryption (PQE): Increasing maturity and effectiveness in 8 stages [76]

Hohm et al. [77] describe a Crypto-Agility Maturity Model (CAMM) with five levels: level 0 'Initial/Not Possible'; level 1 'Possible'; level 2 'Prepared'; level 3 'Practiced'; and level 4 'Sophisticated'. These levels describe the ability of an organisation to select security algorithms with very little effort in an agile way in real time. This includes the ability to add new cryptographic features or algorithms to software and hardware and the ability to retire systems that have become vulnerable or are no longer needed. In order to reach the next higher maturity level, certain requirements (see Table 6.1) have to be met: the requirements are grouped under three categories: Knowledge (K), Process (P), and System property (S).

Levels	0: Initial / Not Possible	1: Possible	2: Prepared	3: Practiced	4: Sophisticated
Knowledge	N/A	System knowledge, cryptographic inventory	Algorithm IDs	Performance, awareness, security	
Process	N/A	Updateability, reversibility		Policies, testing, enforceability, transition mechanism, effectiveness	Automation, scalability, real-time
System property	N/A	Extensibility	Cryptographic modularity, algorithm intersection, algorithm exclusion, opportunistic security	Hardware modularity, backwards compatibility,	Context independence, interoperability

Table 6.1: Requirements for reaching higher maturity levels [78]

The Cybersecurity Framework 2.0 [79] of the National Institute of Standards and Technology is also worth mentioning in the context of maturity models, although NIST does not have a specific PQC maturity framework in place. Instead, the framework identifies four tiers to describe an organisation's governance and management practices when it comes to cybersecurity risks, preparing systems and adopting new standards. The tiers are 'Partial' (tier 1), 'Risk-Informed' (tier 2), 'Repeatable' (tier 3) and 'Adaptive' (tier 4).

Maturity considerations for QKD

As quantum technologies comprise very different fields such as quantum computing, quantum sensing and quantum communication, it is beneficial to distinguish these areas when it comes to the discussion of technology readiness levels (TRLs) and maturity.

Quantum communication technology, which includes QKD, is one of the fields that is experiencing rapid advancements, although there are still hurdles to clear before it can become a fully employed production technology. According to Purhoit et al. [80] a Quantum Technology Readiness Level (QTRL) of 'seven' could be applied to quantum communication networks which corresponds to prototype demonstrations in operational environments.

Li et al. [81] do not rely on QTRLs to describe the quantum readiness for QKD Networks but instead use a six stage maturity model consisting of developmental stages (see Figure 6.2). In a first stage, QKD networks must be able to distribute keys while still relying on trusted nodes for repeaters between distant nodes. A second stage would allow end-to-end QKD without the use of trusted nodes by relying on hop-by-hop preparation and measurement (PMNs, Prepare and Measurement Networks).

In stage 3, Entanglement Distribution Networks (EDNs) must be used to realise end-to-end entanglement with device-independent application protocols.

The authors describe stage 4 as Quantum Memory Networks (QMNs), with local quantum memories at each node so that a deterministic transmission of unknown qubits between any pair of quantum nodes would be possible.

Stage 5 would then be Fault-Tolerant Qubit Networks (FQNs) where all operations can be performed in a fault-tolerant way, enabling high-accuracy quantum computation and protocols. The final stage 6 of Quantum Information Networks (QINs) will be a network where each node will have the ability to prepare, store, manipulate and transmit qubits.

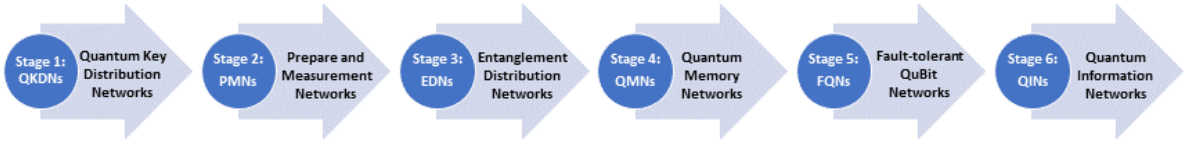

Figure 6.2: Maturity stages of entanglement-assisted quantum networks [82]

Similar stages based on functionality of the technology are also used initially by Wehner et al. [83] to assess the development of a future large-scale quantum internet.

7 Conclusions

For current cryptography, NRENs predominantly rely on RSA, ECC, and other classical cryptographic protocols to secure their communication channels. However, these are vulnerable to quantum computing's ability to break these systems using algorithms such as Shor's. Quantum computers could break the cryptographic primitives widely used today, making it essential for NRENs to prepare for these threats by moving to quantum-safe methods before large-scale quantum computers become a reality. The integration of post-quantum cryptographic algorithms and Quantum Key Distribution offers the most promising defence mechanisms in this scenario. QKD uses quantum mechanics to securely exchange cryptographic keys, which are immune to attacks from quantum computers.

Transitioning to quantum-safe networking presents a range of complex challenges that NRENs must carefully navigate. Some of those challenges that lie ahead include:

- One of the most significant challenges lies in the transition from existing cryptographic standards, such as RSA and ECC, to PQC algorithms. Widespread adoption will require extensive protocol updates and software modifications.
- Initially, small pilot testbeds and smaller-scale deployments will be needed to ensure interoperability and shared learnings towards bringing about the establishment of essential common guidelines and reference architectures.
- The relative maturity and availability of quantum-safe technologies also present obstacles. While promising developments are underway with current NIST PQC standardisations, QKD technologies, on the other hand, are commercially available but differ widely in terms of compatibility, performance, and interoperability. The lack of standardised, vendor-neutral benchmarks and test environments further complicates comparative assessments and strategic planning.
- Integrating QKD into existing network infrastructures presents additional complexities. QKD systems demand high-quality physical infrastructures, including low-loss optical fibre and closely spaced trusted nodes, which may not align with the current network topology of many NRENs. Moreover, ensuring the coexistence of classical encryption with QKD through hybrid models introduces the need for rigorous testing and architectural redesign to guarantee both performance and security.

A possible path forward is set out in this document to tackle these challenges using a step-by-step approach that is two-fold:

- Towards hybrid networks employing both pre-quantum cryptography and PQC during a transition period to harden the systems until all components are quantum-secure with PQC algorithms.
- Towards hybrid networks slowly integrating QKD technology and PQC over time.

The document also provides a very short overview of where things currently stand with standardisation and certification. The included checklist-oriented roadmap and timeline describe a series of objectives to focus on in this transition period. Maturity models that NRENs may use to assess their progress as well as future steps are discussed.

Since it is expected that the transition to quantum-safe networks will take years, during which interoperability and security standards across different platforms and devices will have to be maintained, the EC recommends starting out with standardised and tested hybrid solutions wherever applicable. It is also recommended that these steps should be taken without delay.

Glossary

AES	Advanced Encryption Standard
API	Application programming interface
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate Authority
CAMM	Crypto-Agility Maturity Model
CEN	European Committee for Standardization (CEN, French; Comité Européen de Normalisation
CENELEC	European Committee for Electrotechnical Standardization
CRL	Certificate Revocation List
E2E	End-to-end
ECC	Elliptic Curve Cryptography
EDN	Entanglement Distribution Network
ENISA	The European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
EUCC	Common Criteria-based Cybersecurity Certification Scheme
FIPS	Federal Information Processing Standards
FQN	Fault-Tolerant Qubit Network
gNMI	gRPC Network Management Interface
gRPC	A cross-platform remote procedure call (RPC) framework
ISG	Industry Specification Group
ITS	Information-theoretic security
ITU	International Telecommunication Union
KEM	Key encapsulation mechanism
KMS	Key Management Service
MQE	Multivariate quadratic equation
MRI	Magnetic Resonance Imaging
NatQCI	National Quantum Communications Infrastructure
NFV	Network Functions Virtualisation
NIS	National Intelligence Service; Network and Information Systems
NISCG	NIS Cooperation Group
NIST	National Institute of Standards and Technology
NREN	National Research and Education Network
OCSP	Online Certificate Status Protocol
OTP	One-time pad
PMN	Prepare and Measurement Network
PQC	Post-Quantum Cryptography
PQE	Post-Quantum Encryption
QCI	Quantum Communication Infrastructure
QIN	Quantum Information Network
QKD	Quantum Key Distribution
QMN	Quantum Memory Network
QRNG	Quantum Random Number Generation
QSC	Quantum-Safe Cryptography
QSDC	Quantum Secure Direct Communication
QSS	Quantum-safe security
QTRL	Quantum Technology Readiness Level
REST	Representational State Transfer

RSA	Rivest–Shamir–Adleman public-key cryptosystem
SDN	Software-Defined Networking
SMPC	Secure Multiparty Communication
SNMP	Simple Network Management Protocol
SQKD	Semi-Quantum Key Distribution
TRNG	True random number generator
VPN	Virtual Private Network
YANG	Yet Another Next Generation

References

[1] Quantum European Strategy https://digital-strategy.ec.europa.eu/en/library/quantum-europe-strategy

[2] EuroQCI https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

[3] World Economic Forum, *Transitioning to a Quantum Secure Economy*, White Paper, September 2022 https://www3.weforum.org/docs/WEF_Transitioning%20to_a_Quantum_Secure_Economy_2022.pdf

[4] Shor, P. W. (1994): Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science. 35th Annual Symposium on Foundations of Computer Science. Santa Fe, NM, USA, 20-22 Nov. 1994: IEEE Comput. Soc. Press, pp. 124–134, https://ieeexplore.ieee.org/document/365700

[5] Shor, Peter W. (1995): Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. DOI: 10.48550/arXiv.quant-ph/9508027, 28 pages, LaTeX. This is an expanded version of a paper that appeared in the Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, Nov. 20--22, 1994. Minor revisions made January 1996 https://arxiv.org/abs/quant-ph/9508027

[6] A. Kumar y S. Garhwal, "State-of-the-Art Survey of Quantum Cryptography", Arch Computat Methods Eng, vol. 28, no. 5, pp. 3831-3868, ago. 2021, DOI: 10.1007/s11831-021-09561-2

[7] https://www.nokia.com/industries/quantum-safe-networks/#explore

[8] SIG-Quantum https://community.geant.org/sig-quantum/

[9] *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*, Part 1, Version: 1.1, EU PQC Workstream, 11.06.2025, https://ec.europa.eu/newsroom/dae/redirection/document/117507

[10] Survey - EU Roadmap on Post-Quantum Cryptography, August 11, 2025, https://digital-strategy.ec.europa.eu/en/news/survey-eu-roadmap-post-quantum-cryptography

[11] *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*, June 23, 2025, https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[12] 'EU reinforces its cybersecurity with post-quantum cryptography', June 23, 2025 https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography

[13] NIS Roadmap 2025 – see [9]

[14] EPC - *A Quantum Cybersecurity Agenda for Europe II: Enabling policy and investment options for the quantum transition* https://www.epc.eu/publication/A-quantum-cybersecurity-agenda-for-Europe-II-60c188/

[15] P*QC Migration Handbook* https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf

[16] *The NIST Cybersecurity Framework (CSF) 2.0*, February 26, 2024 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[17] *Quantum-Readiness: Migration to Post-Quantum Cryptography*, CISA, USA, August 21, 2023 https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography

[18] *Quantum Networking: Findings and Recommendations for Growing American Leadership*, National Quantum Initiative Advisory Committee, September 2024, USA https://www.quantum.gov/wp-content/uploads/2024/09/NQIAC-Report-Quantum-Networking.pdf

[19] Aydeger, Abdullah; Zeydan, Engin; Yadav, Awaneesh Kumar; Hemachandra, Kasun T.; Liyanage, Madhusanka (2024), 'Towards a Quantum-Resilient Future: Strategies for Transitioning to Post-Quantum Cryptography', 2024, in *15th International Conference on Network of the Future (NoF)*. Castelldefels, Spain, 10/2/2024 - 10/4/2024: IEEE, pp. 195–203.July 8, 2024 https://www.researchgate.net/publication/382077518_Towards_a_Quantum-Resilient_Future_Strategies_for_Transitioning_to_Post-Quantum_Cryptography

[20] SPHINCS+ https://sphincs.org/

[21] NIST, Post Quantum Cryptography https://csrc.nist.gov/projects/post-quantum-cryptography

[22] NIST, PQC – see [21]

[23] Takanori Yasuda, Xavier Dahan, Yun-Ju Huang, Tsuyoshi Takagi, and Kouichi Sakurai, *MQ Challenge: Hardness Evaluation of Solving Multivariate Quadratic Problems* https://eprint.iacr.org/2015/275 , https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/papers/session7-yasuda-paper.pdf

[24] Classic McEliece https://classic.mceliece.org/nist.html

[25] Aydeger et al. – see [19]

[26] Ricci, Sara; Dobias, Patrik; Malina, Lukas; Hajny, Jan; Jedlicka, Petr (2024), 'Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography', in *IEEE Access 12*, pp. 23206–23219. DOI: 10.1109/ACCESS.2024.3364520 https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10430098

[27] Kaizu, T.; Margolius, H. S. (1975), 'Studies on rat renal cortical cell kallikrein. I. Separation and measurement', in *Biochimica et biophysica acta 411 (2)*, pp. 305–315. DOI: 10.1016/0304-4165(75)90310-4. https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_alkim.pdf

[28] Perttu Saarela, Xiphera, *Hybrid models connect the post-quantum with the classical security*, August 16, 2022 https://xiphera.com/hybrid-models-connect-the-post-quantum-with-the-classical-security/

[29] Castryck, W., Decru, T. (2023), 'An Efficient Key Recovery Attack on SIDH', in Carmit Hazay, Martijn Stam (Eds.): *Advances in Cryptology – EUROCRYPT 2023*, vol. 14008. Cham: Springer Nature Switzerland (Lecture Notes in Computer Science), pp. 423–447 https://eprint.iacr.org/2022/975.pdf

[30] EuroQCI ConOps (Concept of Operations), Nov. 21, 2024 https://digital-strategy.ec.europa.eu/en/miscellaneous/euroqci-conops-concept-operations

[31] O. Klicnik et al. (2023), 'Deploying Quantum Key Distribution into the Existing University Data Infrastructure', in *2023 IEEE AFRICON*. Nairobi, Kenya, 9/20/2023 - 9/22/2023: IEEE, pp.1–3 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10293655

[32] O. Klicnik, K. Turcanova, P. Munster, T. Horvath (2025), 'Integrating Quantum Key Distribution into Academic Network: Practical Challenges and Solutions'. In F. Skopik, V. Naessens, B. de Sutter (Eds.): *Availability, Reliability and Security*, vol. 15998. Cham: Springer Nature Switzerland (Lecture Notes in Computer Science), pp. 61–369 https://link.springer.com/chapter/10.1007/978-3-032-00642-4_21

[33] J. Viksna, S. Kozlovics, E. Rencis (2023), POSTER: 'Integrating Quantum Key Distribution into Hybrid Quantum-Classical Networks'. In J. Zhou, L. Batina, Z. Li, J. Lin, E. Losiouk, S. Majumdar et al. (Eds.): *Applied Cryptography and Network Security Workshops* vol. 13907. Cham: Springer Nature Switzerland (Lecture Notes in Computer Science), pp. 695–699, https://link.springer.com/chapter/10.1007/978-3-031-41181-6_42

[34] S. Kozlovičs, K. Petručeņa, D. Lāriņš, J. Vīksna (2023), 'Quantum Key Distribution as a Service and its Injection into TLS'. In W. Meng, Z. Yan, V. Piuri (Eds.): *Information Security Practice and Experience*, vol. 14341. Singapore: Springer Nature Singapore (Lecture Notes in Computer Science), pp. 527–545 https://link.springer.com/chapter/10.1007/978-981-99-7032-2_31

[35] EuroQCI https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

[36] EuroQCI ConOps – see [30]

[37] ITU-T Y.3802 'Recommendation ITU-T Y.3802 (2020), Functional architecture of the Quantum Key Distribution network' https://www.itu.int/rec/T-REC-Y.3802

[38] ITU-T Y.3803 'Recommendation ITU-T Y.3803 (2020), Key management for quantum key distribution network' https://www.itu.int/rec/T-REC-Y.3803/_page.print

[39] Long-term Parameters Monitoring of the IDQ Clavis 3 QKD System https://ieeexplore.ieee.org/document/9911354?arnumber=9911354

[40] ITU-T Y.3804 'Recommendation ITU-T Y.3804 (2020), Control and Management for Quantum Key Distribution Network' https://www.itu.int/rec/T-REC-Y.3804/en

[41] ITU-T SG13 Y.QKDN_SDNC 'Software Defined Networking Control for Quantum Key Distribution Networks' https://www.itu.int/rec/T-REC-Y.3805/en

[42] E. Giortamis et al. (2024), *Orchestrating Quantum Cloud Environments with Qonductor* https://arxiv.org/abs/2408.04312

[43] H. T. Nguyen, M. Usman, R. Buyya, (2025), *QFOR: A Fidelity-aware Orchestrator for Quantum Computing Environments using Deep Reinforcement Learning* https://www.arxiv.org/abs/2508.04974

[44] J. Alvarado-Valiente et al. (2024), 'Orchestration for quantum services: The power of load balancing across multiple service providers', in *Science of Computer Programming* 237, p. 103139. DOI: 0.1016/j.scico.2024.103139, https://www.sciencedirect.com/science/article/pii/S0167642324000625

[45] https://www.quantum-machines.co/

[46] https://aws.amazon.com/braket/

[47] *ORQESTRA: Orchestrating the Operational Deployment of Quantum Resistant Services for Next-Generation Secure Defence Systems and Communications*, 2024 https://defence-industry-space.ec.europa.eu/document/download/5a308169-efa7-498f-a090-78fbb26e3adc_en?filename=FACTSHEET_EDF_2024_LS_RA_DIS_QUANT_STEP_101224573_ORQESTRA.pdf

[48] https://qoroquantum.net/

[49] ETSI TR 103 619 V1.1.1 (2020-07), *Migration strategies and recommendations to Quantum Safe schemes* https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

[50] Industry Specification Group (ISG) on Quantum Key Distribution (QKD) https://www.etsi.org/committee/1430-qkd

[51] ITU Y.3800 'Overview on networks supporting quantum key distribution', (10-2019) https://www.itu.int/rec/T-REC-Y.3800-201910-I

[52] ITU X.1811 'Security guidelines for applying quantum-safe algorithms in IMT-2020 systems', (04-2021) https://www.itu.int/rec/T-REC-X.1811-202104-I/en

[53] CEN/CENELEC, *Standardization Roadmap on Quantum Technologies* https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Quantum%20technologies/Documentation%20and%20Materials/fgqt_q04_standardizationroadmapquantumtechnologies_release1.pdf

[54] https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[55] https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption

[56] https://csrc.nist.gov/projects/post-quantum-cryptography

[57] FIPS 203 https://csrc.nist.gov/pubs/fips/203/final

[58] FIPS 204 https://csrc.nist.gov/pubs/fips/204/final

[59] FIPS 205 https://csrc.nist.gov/pubs/fips/205/final

[60] 'NIST Announces Post-Quantum Cryptography Standards', *IEEE Spectrum* https://spectrum.ieee.org/post-quantum-cryptography-2668949802

[61] 'Clavis XG Series QKD obtains National Security Certification' https://www.idquantique.com/clavis-xg-series-qkd-obtains-national-security-certification/

[62] ENISA, EUCC Certification Scheme, December 2024, https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en

[63] 'ENISA to operate the EU Cybersecurity Reserve' https://digital-strategy.ec.europa.eu/en/news/enisa-operate-eu-cyber-reserve

[64] *Securing Tomorrow Today: Transitioning to Post-Quantum Cryptography*, BSI, Germany https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement-2025.pdf?__blob=publicationFile&v=3

[65] Quantum European Strategy https://digital-strategy.ec.europa.eu/en/library/quantum-europe-strategy

[66] EuroQCI https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

[67] World Economic Forum, *Transitioning to a Quantum Secure Economy*, White Paper, September 2022 https://www3.weforum.org/docs/WEF_Transitioning%20to_a_Quantum_Secure_Economy_2022.pdf

[68] ENISA – see [63]

[69] SP-800-227 https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information

[70] NIST IR 8547 https://csrc.nist.gov/pubs/ir/8547/ipd

[71] NIST IR 8528 https://csrc.nist.gov/pubs/ir/8528/final

[72] *Quantum Technologies Conceptual Framework Programme*, German Federal Ministry for Research, Technology and Space https://www.bmftr.bund.de/SharedDocs/Downloads/DE/2024/2024-12-11-handlungskonzept-quantentechnologie-en.pdf?__blob=publicationFile&v=2

[73] D. Crouch, 'ITIL Maturity Model', August 25, 2023 https://www.axelos.com/resource-hub/blog/itil_maturity_model

[74] DigiCert, *Post-Quantum Cryptography (PQC) Maturity Model*, 2020 https://www.digicert.com/resources/post-quantum-cryptography-maturity-model.pdf

[75] T. Patterson, 'Moving toward a Quantum Security Maturity Index', Accenture Quantum Security, PKI Consortium Amsterdam, Netherlands, 8 November 2023 https://pkic.org/events/2023/pqc-conference-amsterdam-nl/pkic-pqcc_tom-patterson_accenture_moving-toward-a-quantum-security-maturity-index.pdf

[76] PKI 2023 – see [75]

[77] J. Hohm, A. Heinemann, A. Wiesmaier (2023), 'Towards a Maturity Model for Crypto-Agility Assessment', in G-V. Jourdan et al. (Eds.): *Foundations and Practice of Security*, vol. 13877. Cham: Springer Nature Switzerland (Lecture Notes in Computer Science), pp. 104–119 https://arxiv.org/html/2202.07645v3#S4

[78] CAMM – see [77]

[79] *The NIST Cybersecurity Framework (CSF) 2.0*, February 26, 2024 https://doi.org/10.6028/NIST.CSWP.29, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[80] A. Purohit et al. (2024), 'Building a quantum-ready ecosystem', in *IET Quantum Communication 5 (1)*, pp. 1–18. DOI: 10.1049/qtc2.12072 https://doi.org/10.1049/qtc2.12072

[81] Z. Li et al. (2023), 'Entanglement-Assisted Quantum Networks: Mechanics, Enabling Technologies, Challenges, and Research Directions', in *IEEE Communications Surveys & Tutorials 2023*, DOI: 10.48550/arXiv.2307.12490 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10177948

[82] Li et al. – see [81]

[83] S. Wehner, D. Elkouss, R. Hanson, 'Quantum Internet: A Vision for the Road Ahead', *Science*, 2018. https://www.science.org/doi/10.1126/science.aam9288