

ITU-T Technical Report

(06/2026)

XSTR.hyb-qsafe

**Overview of key management of hybrid
approaches for quantum-safe communications**

Technical Report ITU-T XSTR.hyb-qsafe

Overview of key management of hybrid approaches for quantum-safe communications

Summary

This Technical Report addresses key management of hybrid approaches using quantum key distribution (QKD) and post-quantum cryptography (PQC) for quantum-safe communications.

Keywords

Hybrid approaches, key management, PQC (post-quantum cryptography), QKD (quantum key distribution), QKDN (QKD network), quantum-safe communications.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

© ITU 2026

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope.....	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Technical Report	2
4 Abbreviations and acronyms	2
5 Introduction.....	2
6 Key management of hybrid approaches for quantum-safe communications and service scenarios	3
6.1 Review of documents on key management in QKDN in ITU-T SG 17.....	3
6.2 Concepts of key management of hybrid approaches	5
7 Overview of activities and use cases of key management of hybrid approaches for quantum-safe communications	6
7.1 Combination of QKD and PQC to realize end to end quantum-safe communication	6
7.2 Combining multiple key exchange systems	7
7.3 Mixing pre-shared keys	8
8 Security considerations for QKD-PQC integration	8
8.1 Preservation of security properties	8
8.2 Authentication	8
8.3 Protection of key forwarding and trusted nodes.....	9
8.4 Security aspects of hybrid architectures	9
9 Coordination with other SDOs	9
10 Role of SG17	9
11 Implications	9
Annex A – PQC authentication.....	10
A.1 Overview of PQC authentication.....	10
A.2 Motivation for PQC authentication	10
A.3 Representative PQC authentication algorithms.....	10
A.4 Use of PQC authentication in practical systems.....	10
A.5 Hybrid authentication approaches	11
A.6 Technical and operational considerations	11
Bibliography.....	12

Overview of key management of hybrid approaches for quantum-safe communications

1 Scope

This Technical Report studies case studies and use cases, service scenarios; and technical and security considerations of key management for hybrid approaches using quantum key distribution (QKD) and post-quantum cryptography (PQC) for quantum-safe communications.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 key manager (KM) [b-ITU-T Y.3800]: A functional module located in a quantum key distribution (QKD) node to perform key management in the key management layer.

3.1.2 key management [b-ITU-T Y.3800]: All activities performed on keys during their life cycle starting from their reception from the quantum layer, the storage, formatting, relay, synchronization, authentication, to supply to cryptographic application and delete or preserve depending on the key management policy.

3.1.3 quantum key distribution (QKD) [b-ETSI GR QKD 007]: Procedure involving the transport of quantum states to agree shared secret bit strings between remote parties using a protocol with security based on quantum entanglement or the impossibility of perfectly cloning or measuring the unknown transported quantum states.

3.1.4 quantum key distribution link (QKD link) [b-ITU-T Y.3800]: A communication link between two quantum key distribution (QKD) modules to operate the QKD.

NOTE – A QKD link consists of a quantum channel for the transmission of quantum signals, and a classical channel used to exchange information for synchronization and key distillation.

3.1.5 quantum key distribution module (QKD module) [b-ITU-T Y.3800]: A set of hardware and software components that implements cryptographic functions and quantum optical processes, including quantum key distribution (QKD) protocols, synchronization, distillation for key generation, and is contained within a defined cryptographic boundary.

NOTE – A QKD module is connected to a QKD link, acting as an endpoint module in which a key is generated. These are two types of QKD modules, namely, the transmitters (QKD-Tx) and the receivers (QKD-Rx).

3.1.6 quantum key distribution network (QKDN) [b-ITU-T Y.3800]: A network comprised of two or more quantum key distribution (QKD) nodes connected through QKD links.

NOTE – A QKDN allows sharing keys between the QKD nodes by key relay when they are not directly connected by a QKD link.

3.1.7 quantum key distribution network controller (QKDN controller) [b-ITU-T Y.3800]: A functional module, which is located in a quantum key distribution (QKD) network control layer to control a QKD network.

3.1.8 quantum key distribution network manager (QKDN manager) [b-ITU-T Y.3800]: A functional module, which is located in a quantum key distribution (QKD) network management layer to monitor and manage a QKD network.

3.1.9 quantum key distribution node (QKD node) [b-ITU-T Y.3800]: A node that contains one or more quantum key distribution (QKD) modules protected against intrusion and attacks by unauthorized parties.

NOTE – A QKD node can contain a key manager (KM).

3.2 Terms defined in this Technical Report

This Technical Report uses the following term:

3.2.1 quantum-safe communication: Communication that uses methods designed to resist attacks by quantum computers in order to protect information assets, including after the availability of large-scale quantum computers.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

IKE	Internet Key Exchange
IT-secure	Information-theoretically secure
KM	Key Manager
PKI	Public Key Infrastructure
PQC	Post-Quantum Cryptography
QKD	Quantum Key Distribution
QKDN	QKD Network

5 Introduction

In a quantum key distribution network (QKDN), the key management layer is the middle layer between the quantum layer and the service layer and is also connected to the QKDN control and management layer. It mainly handles the key-related tasks and plays a central role in interacting with different elements in a QKDN.

Several documents have been published in ITU-T SG17 for key management in QKDNs. These documents primarily focus on key management inside QKDNs, including key generation using quantum key distribution (QKD) and key relay based on trusted nodes.

In parallel, other approaches for achieving quantum-safe communications have been actively developed, most notably post-quantum cryptography (PQC). Quantum-safe methods are intended to resist attacks by quantum computers, with the objective of protecting information assets even after large-scale quantum computers become practical. Both QKD and PQC are candidate technologies for quantum-safe communications, but they rely on different assumptions, deployment models, and operational constraints.

While SG17 has developed multiple documents addressing key management within QKDNs, there has been limited discussion on how QKD-generated keys can be used to achieve end-to-end quantum-safe communications in conjunction with other approaches such as PQC.

QKD protocols can provide information-theoretic security for key establishment under their applicable security assumptions, because their security does not rely on the computational difficulty of mathematical problems. However, QKD requires specialized devices, i.e., QKD modules, and dedicated quantum and classical channels. In contrast, PQC algorithms are designed to resist known

quantum-computer attacks while operating on conventional communication and computing infrastructure. PQC security remains computational and relies on the assumed hardness of underlying mathematical problems; therefore, future cryptanalytic advances cannot be completely ruled out.

NIST has made significant progress in the standardization of PQC. In August 2024, NIST approved its first set of finalized PQC federal information processing standards (FIPS), including:

- [b-NIST FIPS 203]: Module-lattice-based key-encapsulation mechanism (ML-KEM);
- [b-NIST FIPS 204]: Module-lattice-based digital signature algorithm (ML-DSA);
- [b-NIST FIPS 205]: Stateless hash-based digital signature algorithm (SLH-DSA);
- [b-NIST IR 8545]: Status report on the fourth round of the NIST post-quantum cryptography standardization process.

With the publication of these standards, NIST has formally initiated the migration phase toward post-quantum cryptography and recommends that organizations begin transitioning their systems accordingly. However, the integration of these algorithms into widely deployed security protocols, operational networks, and commercial products is still ongoing. Additional standardization activities by other standards development organizations (SDOs) are expected to be necessary to ensure interoperability, operational consistency, and deployment guidance across diverse communication environments. For example, ITU-T SG17 has also started work items on PQC migration for PKI-related Recommendations in the X.500 series.

During this transition period, hybrid approaches combining multiple cryptographic techniques have been widely discussed and recommended within the cryptographic community, including by NIST. Such approaches may combine classical cryptography and PQC, or combine QKD with PQC, in order to mitigate uncertainties associated with individual technologies and to provide defence-in-depth for quantum-safe communications.

In existing ITU-T documents, QKDN specifications focus on key management functions within QKDNs to supply keys to cryptographic applications. To realize quantum-safe communications using hybrid approaches that involve both QKD and PQC, it is important for service providers and network operators to be able to consider all available technologies and select appropriate combinations depending on use cases, operational assumptions, and deployment constraints.

Given the current situation, where each candidate technology (QKD, PQC, and classical cryptography) has been developed based on different assumptions and target scenarios, it is beneficial to study key management architectures that support hybrid approaches combining QKD and PQC in comparison with the current key management mechanisms defined for QKDNs. Such a study can help identify representative use cases and deployment scenarios, clarify roles and interactions among different technologies, and derive additional requirements and gaps that need to be addressed to enable practical and interoperable quantum-safe communications.

6 Key management of hybrid approaches for quantum-safe communications and service scenarios

6.1 Review of documents on key management in QKDN in ITU-T SG 17

ITU-T SG17 has published several documents related to key management in QKDNs, as follows:

- 1) Recommendation ITU-T X.1712 'Security requirements and measures for quantum key distribution networks – key management'.

[b-ITU-T X.1712] specifies security threats and security requirements for key management in QKDNs, and security measures for key management to meet those security requirements. This Recommendation also provides support for the design, implementation, and operation of key management in QKDNs. This Recommendation addresses key management inside QKDNs, which is all the activities performed on keys during their life cycle starting from their reception from the

quantum layer, the storage, formatting, relay, synchronization, authentication, to supply to cryptographic application and delete or preserve depending on the key management policy.

- 2) Recommendation ITU-T X.1714 'Key combination and confidential key supply for quantum key distribution networks'.

[b-ITU-T X.1714] describes key combination methods for QKDN and specifies security requirements for both key combination and key supply from QKDNs to cryptographic applications. In particular, this Recommendation addresses the following points:

- The security of the combination of keys exchanged through a QKDN and keys exchanged through other key exchange methods;
- The security of the key supply from a QKDN to cryptographic applications.

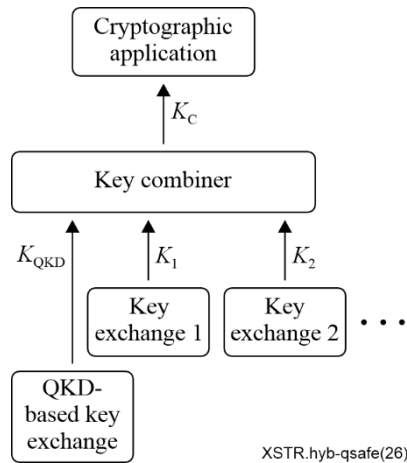


Figure 1 – Key combination method for QKDN

Figure 1 in [b-ITU-T X.1714] shows a general description of the key combination considered in this Recommendation. It consists of a key combiner that transforms two or more input keys supplied by different key exchange methods into a combined key. One of the input keys is supplied by a QKD-based key exchange.

When the key combiner is located outside the QKDN and is used in the service layer, the QKD-based key exchange is a key exchange performed by the QKDN. When the key combiner is located in the QKDN, the QKD-based key exchange is a key exchange between QKD modules, with or without key relays. The other input keys can be provided by any kind of method allowing the exchange of symmetric keys between two nodes, including cryptographic means and physical means (e.g., subscriber identity module (SIM) card).

If the key combiner is located outside the QKDN and is used as a cryptographic application, the requirements fully depend on the policy of the user of the application. Specification of the security requirements in this case is outside the scope of [b-ITU-T X.1714].

- 3) XSTR-HYB-QKD "Overview of hybrid approaches for key exchange with quantum key distributions".

This Technical Report provides a landscape of standardization activities on hybrid approaches for migration towards quantum-safe algorithms or protocols within international, regional, and national organizations. The hybrid approaches covered by this Technical Report focus on key exchange.

Hybrid approaches for key exchange consist of combining at least two different key exchange methods to establish keying material. This Technical Report studies possible ways to accommodate QKD protocols in the context of hybrid approaches for key exchange. This compatibility is studied for both generic hybrid key exchange methods and hybrid key exchange methods specific to certain communication protocols. The scope and objective of this Technical Report are to study how QKD-

7 Overview of activities and use cases of key management of hybrid approaches for quantum-safe communications

The introduction highlighted that every technology discussed in this TR claiming to provide quantum-safe communication has its own limitations. These limitations include the absence of security proofs, flaws in implementation, or potential technical vulnerabilities. By combining these technologies, the drawbacks of each individual solution can be mitigated, resulting in a significantly stronger security system. In order to compromise multiple quantum-safe communication technologies, an attacker would need to gain access to multiple solutions simultaneously. The subsequent subclauses outline various use cases and applications of hybrid solutions.

7.1 Combination of QKD and PQC to realize end to end quantum-safe communication

This clause provides a summary of multiple use cases that have been identified for combining QKD and PQC in order to achieve quantum-safe communication. It addresses solutions aimed at transitioning government and industry infrastructure to a quantum-safe state, which encompass the implementation of both QKD and PQC methodologies.

In the study [b-QED-C2024], an analysis of the advantages and disadvantages of adopting PQC and QKD for Internet security is conducted. The authors emphasize in their summary that the architecture of both QKD and PQC solutions plays a crucial role in determining the speed of deployment and the ability to adapt over time. They propose a hybrid PQC/QKD solution that considers the nature of the content to be protected, as illustrated in Figure 3. The figure demonstrates the feasibility of a hybrid approach in which PQC can be employed for a large number of endpoints where the likelihood of quantum computer attacks is relatively low, while QKD can be utilized by sites involved in the transmission of highly sensitive content that demands exceptional security measures.

EXAMPLE HYBRID IMPLEMENTATION

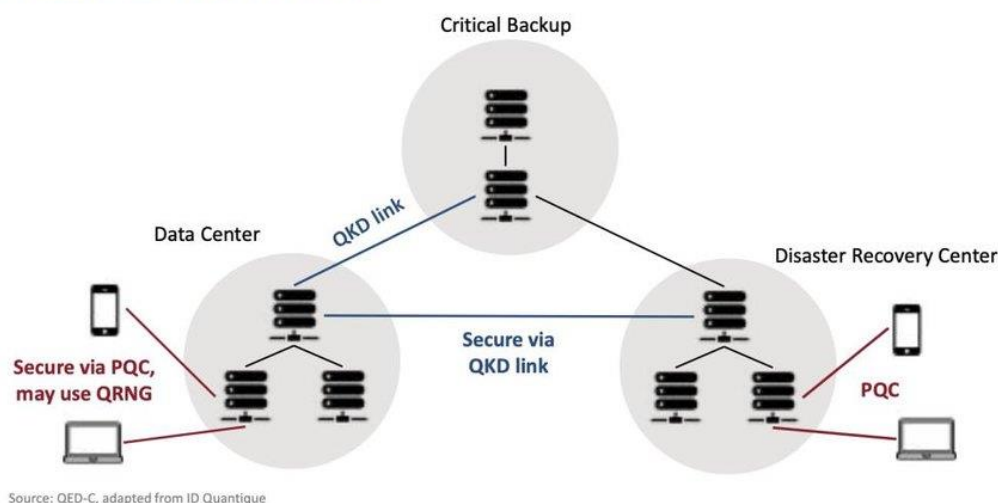


Figure 3 – PQC/QKD hybrid architecture

The white paper [b-QED-C2022] presents an illustrative example of a hybrid solution incorporating both QKD and PQC. It underscores the notion that QKD and PQC are complementary technologies that can and should be integrated in a hybrid fashion to achieve optimal effectiveness. In the example outlined in the white paper, QKD is employed for establishing secure links between a data centre, a critical backup site, and a disaster recovery centre. On the other hand, PQC is utilized for securing wireless connections between the data centre and various devices. This combination of QKD and PQC leverages their respective strengths and enhances overall security.

[b-ITU-T Y Supp. 79] provides the overview for integration of QKDN with mathematics-based cryptographic applications and recommends that the integration of QKDNs and PKI with PQC

algorithm should be studied for the extension of QKD service availability and market penetration for QKD service provider.

In the context of the integration, three use cases are introduced as follows;

- Use case 1: KSA-keys generated from QKDN are supplied to transport layer security (TLS) client and server symmetrically.
- Use case 2: KSA-keys generated from QKDN are supplied only to the corresponding portion for encryption by KSA-keys. The other end portions are encrypted by the cryptographic keys derived from modern cryptography, i.e., Internet key exchange (IKE) protocol.
- Use case 3: KSA-keys generated from QKDN are supplied to the corresponding portion. Then the keys are delivered to both ends of connectivity through key exchange function.

The follow-up standardization topics related to the implementation of the three use cases defined above include: [b-ITU-T Y.3826], which specifies the framework for the integration, and [b-ITU-T Y.3828], which defines the quality of service requirements for the integration.

7.2 Combining multiple key exchange systems

The research article [b-Geitz] presents various hybrid approaches that combine QKD and PQC to enhance the security of QKD nodes. These approaches have been implemented and tested in the OpenQKD testbed located in Berlin. The work presented in this paper is part of the OpenQKD project, which is a quantum flagship project under the EU Horizon 2020 program. The primary objective of OpenQKD is to facilitate the adoption of QKD technology in industry and demonstrate its practicality and effectiveness in real-world use cases.

Within the Berlin testbed, a telecommunications company in Germany has established one of the major QKD testbeds as part of the OpenQKD project, specifically in the metropolitan area of Berlin. The focus of their efforts lies in integrating QKD into provider networks. In addition to QKD key exchange, the Berlin testbed incorporates a key exchange mechanism based on post-quantum cryptography. This integration has led to intriguing use cases such as key exchange via mobile 5G networks and the inclusion of mobile clients in the security platform. Moreover, the paper introduces a PQC trust chain that relies on PQC algorithms. This trust chain enables secure communication between all applications within a QKD node and between adjacent QKD nodes. By leveraging PQC-based algorithms, communication within and between QKD nodes can be established with a high level of trust and security.

One of the use cases demonstrates the application of PQC to secure communication between QKD nodes as part of a key forwarding process. This approach ensures that encryption artifacts remain protected and inaccessible at intermediate QKD nodes. To achieve this, PQC encryption has been implemented to secure communication on all links within a QKD node.

It is important to note that QKD has distance limitations of a few hundred kilometres due to optical attenuation in optical fibres. Extending the range of quantum optical key exchange would require the involvement of trusted network nodes, which are network operating centres that adhere to high security standards. From a commercial standpoint, this implies that customers must rely on the network operator to safeguard the quantum key exchange process, resulting in a lack of end-to-end security for key exchange. To address this limitation, PQC encryption and authentication are integrated into the QKD key forwarding process to provide end-to-end security.

The key forwarding scheme enhances security by incorporating an additional layer of PQC encryption, ensuring that encryption keys remain concealed at intermediate nodes. Moreover, PQC key exchange can be routed through alternative network paths that bypass intermediate nodes entirely, preventing local adversaries from accessing the PQC key exchange. It is also possible to transmit the PQC key exchange over different types of networks, such as mobile networks or space networks. Each of these approaches contributes to improving the security of the key forwarding process.

By employing a key management system, a hybrid key exchange is facilitated by abstracting the interactions between QKD and PQC. This allows applications to select any desired combination of QKD keys, PQC keys, or hybrid keys, providing flexibility and versatility in the key exchange process.

7.3 Mixing pre-shared keys

[b-IETF RFC 8784] specifies a method for mixing pre-shared keys in the Internet key exchange protocol version 2 (IKEv2) to support post-quantum security. This Technical Report describes an extension to IKEv2 that allows the use of alternative key exchange mechanisms through pre-shared keys.

[b-IETF RFC 8784] assumes that each IKE peer maintains a list of pre-shared keys along with their associated identifiers, which may be exchanged using any post-quantum key exchange method. The specification also introduces notification messages that allow the initiator and the responder to decide whether pre-shared keys are used in an IKEv2 exchange. The decision not to use pre-shared keys can be taken by either of the parties during the various steps of the protocol. In this case, the initiator and the responder use the standard IKEv2 protocol.

When a pre-shared key is used, it is combined with the three sub-keys generated from the conventional IKEv2 protocol specified in [b-IETF RFC 7296]. The combination of these sub-keys with the pre-shared keys is performed using a pseudo-random function.

Clause 3 of [b-IETF RFC 8784] specifies notification messages related to the use of post-quantum pre-shared keys. These notifications are exchanged between the initiator and the responder. Depending on the responder's notification, applications may decide to abort the exchange, use the standard IKEv2 protocol, or use the variation of IKEv2 with post-quantum pre-shared keys. In the latter case, the initiator sends a notification containing the identifier of the post-quantum pre-shared key to the responder. The method for mixing post-quantum pre-shared keys with the secret exchanged using Diffie-Hellman, as specified in [b-IETF RFC 7296], is also defined in clause 3.

The methods for exchanging these pre-shared keys are not defined. Therefore, QKD is one option that may be used in this context. However, the approach defined in [b-IETF RFC 8784] is limited to initiators and responders that are configured with fixed lists of pre-shared keys and pre-shared key identifiers and does not support dynamic updates of pre-shared keys.

8 Security considerations for QKD-PQC integration

8.1 Preservation of security properties

The integration of QKD and PQC should preserve the security properties of each individual technology under clearly defined assumptions. It is essential that the integration does not weaken the security of either QKD or PQC, nor introduce additional vulnerabilities. The overall security claim of the combined system should be explicitly stated and supported by analysis of the key-combining method, authentication mechanism, implementation assumptions, and operational environment.

8.2 Authentication

From an authentication perspective, it is important to recognize that QKD does not inherently provide entity authentication. Therefore, QKD-based systems depend on external mechanisms for identity verification and protection against man-in-the-middle attacks. In this context, PQC-based authentication mechanisms, such as quantum-resistant digital signatures and PQC-enabled PKI, may be employed to support quantum-safe authentication and to protect against impersonation and unauthorized key injection.

8.3 Protection of key forwarding and trusted nodes

In practical deployments, QKD systems often rely on trusted nodes and key relay mechanisms. This introduces additional security considerations, including the need to protect key material at intermediate nodes and to clarify whether end-to-end protection is provided by QKD alone, by PQC mechanisms, or by a hybrid construction. PQC-based encryption and authentication mechanisms may be used to enhance protection of key forwarding and to limit the impact of potential node compromise on the overall system.

8.4 Security aspects of hybrid architectures

Hybrid QKD-PQC architectures introduce additional complexity that needs careful analysis. This includes interactions between QKD and PQC components, potential attack surfaces introduced by their integration, and operational as well as management-related risks. A comprehensive security analysis is therefore needed to ensure the robustness of such hybrid systems.

9 Coordination with other SDOs

Protocols such as TLS and IKEv2 are standardized within the IETF. As a result, security mechanisms involving these protocols should remain aligned with existing IETF specifications. ITU-T should, as far as possible, maintain alignment with relevant specifications while avoiding conflicts or overlaps in protocol behaviour. Close coordination with the IETF and other standards development organizations (SDOs), including through liaison activities where appropriate, is therefore essential.

10 Role of SG17

Within ITU-T, SG17 is well positioned to address security aspects of QKD-PQC integration. This includes the development of security requirements, threat models, and risk analysis, as well as authentication and trust frameworks and security considerations for hybrid key management.

11 Implications

The integration of QKD and PQC presents both opportunities and challenges from a security perspective.

To ensure secure deployment:

- Clear separation of roles between QKD(N) and PQC should be maintained.
- Security requirements for hybrid systems should be explicitly defined.
- Integration should not weaken existing security guarantees.
- Coordination with the IETF and other relevant organizations is essential.

SG17 may play a key role in defining the security framework, threat model, authentication considerations, and key-management requirements for such integration.

Annex A

PQC authentication

A.1 Overview of PQC authentication

Post-quantum cryptography (PQC) authentication refers to authentication mechanisms that employ cryptographic algorithms designed to remain secure against attacks by quantum computers. In contrast with classical public-key authentication mechanisms based on RSA or elliptic-curve cryptography (ECC), PQC authentication relies on mathematical problems for which no efficient quantum algorithms are currently known. PQC authentication primarily provides entity authentication, message authentication, and integrity protection through quantum-resistant digital signatures and related cryptographic primitives. It plays a critical role in establishing trust relationships in quantum-safe communication systems, including hybrid architectures that combine QKD and PQC.

A.2 Motivation for PQC authentication

Authentication mechanisms based on RSA and ECC are vulnerable to large-scale quantum computers due to Shor's algorithm, which can efficiently solve the underlying mathematical problems. This creates a risk not only for future communications, but also for long-term credentials such as certificates, device identities, firmware signatures, and trust anchors that may be captured today and exploited later. This risk is commonly referred to as "harvest now, decrypt later" or, in the case of authentication artefacts, "harvest now, forge later". PQC authentication is therefore required to preserve the long-term security and trustworthiness of communication infrastructures, particularly for systems with long service lifetimes, critical infrastructure, and regulatory or compliance requirements. In hybrid quantum-safe communications, PQC authentication is essential to securely bind identities, protect control signalling, and authenticate key management operations.

A.3 Representative PQC authentication algorithms

PQC authentication is mainly realized using quantum-resistant digital signature schemes. Representative algorithms include lattice-based, hash-based, and other constructions. Lattice-based digital signature schemes provide a practical balance between security, performance, and implementation cost, and are suitable for protocols such as TLS, IPsec, and software signing. Hash-based signature schemes offer strong security assurances based on well-studied hash functions, at the cost of larger signature sizes. These signature algorithms can be used in a variety of authentication contexts, including certificate-based authentication, device authentication, and code signing.

A.4 Use of PQC authentication in practical systems

PQC authentication can be deployed in various practical systems to provide quantum-resistant trust establishment and long-term security. Typical application areas include secure transport protocols, device and IoT authentication, and software or firmware signing.

A.4.1 Use in TLS / HTTPS

In transport layer security (TLS) and HTTPS, PQC authentication can be applied to server and client authentication by replacing or augmenting classical digital signatures in ITU-T X.509 certificates with PQC-based digital signature algorithms. For example, a TLS server may use a certificate signed with a PQC digital signature algorithm to prove its identity to a client during the TLS handshake. During the migration phase, hybrid authentication approaches are commonly adopted, where both a classical signature algorithm (such as ECDSA) and a PQC signature algorithm are used in parallel within certificates or protocol messages. This enables compatibility with legacy implementations while providing protection against future quantum adversaries. In such deployments, PQC

authentication is typically combined with PQC or hybrid key establishment mechanisms to achieve end-to-end quantum-safe secure communication.

A.4.2 Use in device and IoT authentication

PQC authentication is particularly relevant for device and IoT environments, where devices often have long operational lifetimes and limited opportunities for cryptographic upgrades. PQC digital signatures can be used to establish secure device identities, authenticate devices during network onboarding, and protect device-to-device or device-to-cloud communications. For example, a device may be provisioned at manufacturing time with a PQC public-private key pair and a corresponding PQC-signed certificate or credential. During authentication, the device proves possession of the private key using a PQC signature, allowing the verifier to authenticate the device in a quantum-resistant manner. In hybrid architectures, PQC authentication can be combined with classical credentials to ensure interoperability and gradual migration.

A.4.3 Use in software and firmware signing

Software and firmware signing is a critical use case for PQC authentication, as signed software artifacts may remain valid and trusted for many years. PQC digital signature algorithms can be used to sign software updates, firmware images, and configuration files to ensure authenticity and integrity over their entire lifecycle. This prevents adversaries from forging valid signatures in the future using quantum computers. In practical deployments, PQC-signed software or firmware can be verified by operating systems, bootloaders, or embedded devices before installation or execution. Hybrid signing approaches, where both classical and PQC signatures are applied to the same software artifact, are often used during the transition period to maintain compatibility with existing verification mechanisms while introducing quantum-resistant assurance.

A.5 Hybrid authentication approaches

Given the ongoing transition toward PQC, hybrid authentication approaches are widely regarded as a practical and risk-mitigating solution. Hybrid authentication combines classical authentication algorithms (e.g., RSA or ECDSA) with PQC authentication algorithms within a single protocol or trust framework. This ensures security against both classical and quantum adversaries, even if weaknesses are later discovered in one class of algorithms. Hybrid authentication can be realized through parallel signatures, composite certificates, or protocol extensions that support multiple authentication algorithms. Such approaches are particularly relevant for large-scale deployments and for maintaining backward compatibility during migration.

A.6 Technical and operational considerations

The deployment of PQC authentication introduces several technical and operational challenges. PQC public keys and signatures are generally larger than their classical counterparts, which may affect bandwidth usage, latency, and storage requirements. Efficient and secure implementation, including resistance to side-channel attacks, remains a critical consideration [b-SC 27 Journal]. Integration with existing PKI infrastructures, hardware security modules, and management systems may require updates or extensions. Operational aspects such as algorithm agility, certificate lifecycle management, and interoperability across different vendors and networks should also be addressed to ensure robust and scalable adoption of PQC authentication.

Bibliography

- [[b-ITU-T X.1712](#)] Recommendation ITU-T X.1712 (2021), *Security requirements and measures for quantum key distribution networks – key management*.
- [[b-ITU-T X.1714](#)] Recommendation ITU-T X.1714 (2020), *Key combination and confidential key supply for quantum key distribution networks*.
- [[b-ITU-T Y Supp. 79](#)] Supplement 79 to ITU-T Y-series Recommendations (2023), ITU-T Y.3800 series – Quantum key distribution networks – *Role in end-to-end cryptographic services with non-quantum cryptography*.
- [[b-ITU-T Y.3800](#)] Recommendation ITU-T Y.3800 (2019), *Overview on networks supporting quantum key distribution*.
- [[b-ITU-T Y.3826](#)] Recommendation ITU-T Y.3826 (2024), *Integration of quantum key distribution network and user network supporting end-to-end modern cryptography services – Framework*.
- [[b-ITU-T Y.3828](#)] Recommendation ITU-T Y.3828 (2025), *Integration of quantum key distribution network and user network supporting end-to-end modern cryptography services – Requirements for quality of service assurance*.
- [[b-ITU-T XSTR-HYB-QKD](#)] Technical Report ITU-T XSTR-HYB-QKD (2022), *Overview of hybrid approaches for key exchange with quantum key distribution*.
- [b-ETSI GR QKD 007] ETSI GR QKD 007 V1.2.1 (2026), *Quantum Key Distribution (QKD); Vocabulary*.
<https://www.etsi.org/deliver/etsi_gr/QKD/001_099/007/01.02.01_60/gr_QKD007v010201p.pdf>
- [b-Geitz] Geitz, M., Döring, R., & Braun, R-P. (2023), *Hybrid QKD & PQC protocols implemented in the Berlin OpenQKD testbed*. IEEE.
<<https://ieeexplore.ieee.org/document/10372894>>
- [b-IETF RFC 7296] IETF Standard RFC 7296 (2014), *Internet Key Exchange Protocol Version 2 (IKEv2)*.
<<https://www.rfc-editor.org/info/rfc7296/>>
- [b-IETF RFC 8784] IETF Standard RFC 8784 (2020), *Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security*.
<<https://www.rfc-editor.org/info/rfc8784/>>
- [b-SC 27 Journal] JTC 1/SC 27 Journal (2024), *Technology, Security and Privacy*. Volume 4, Issue 2.
<https://committee.iso.org/files/live/sites/jtc1sc27/files/resources/SC27%20Journal%20Vol%204%20Issue%202%20%28rev2%29.pdf?utm_source=chatgpt.com>
- [b-NIST FIPS 203] FIPS 203 (2024), *Module-Lattice-Based Key-Encapsulation Mechanism Standard*.
<<https://csrc.nist.gov/pubs/fips/203/final>>
- [b-NIST FIPS 204] FIPS 204 (2026), *Module-Lattice-Based Digital Signature Standard*.
<<https://csrc.nist.gov/pubs/fips/204/final>>

- [b-NIST FIPS 205] FIPS 205 (2024), *Stateless Hash-Based Digital Signature Standard*.
<<https://csrc.nist.gov/pubs/fips/205/final>>
- [b-NIST IR 8545] NIST IR 8545 (2025), Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process.
<<https://csrc.nist.gov/pubs/ir/8545/final>>
- [b-QED-C2022] QED-C (2022), *A Guide to a Quantum-Safe Organization*.
<<https://quantumconsortium.org/publication/a-guide-to-a-quantum-safe-organization/>>
- [b-QED-C2024] QED-C (2024), *QKD: Part of a Defense-In-Depth Security Strategy*.
<<https://quantumconsortium.org/publication/qkd-part-of-a-defense-in-depth-security-strategy/>>
-