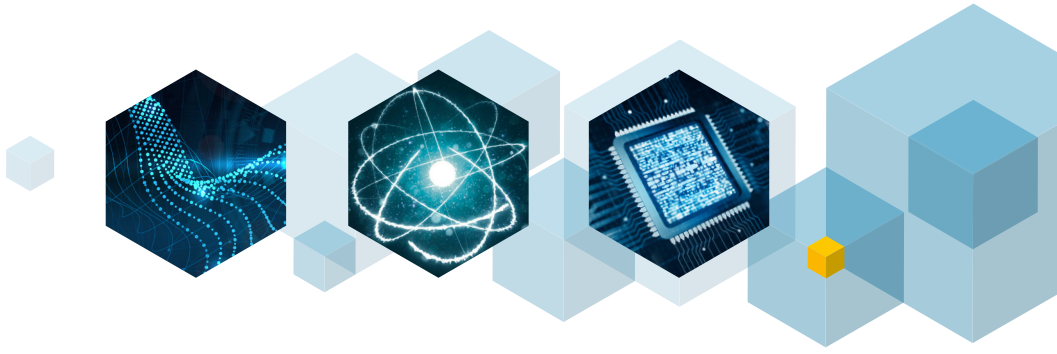
ILNAS

TECHNICAL STANDARDIZATION

TECHNICAL STANDARDIZATION

QUANTUM COMMUNICATION AND TECHNICAL STANDARDIZATION

Version 1.0 · November 2024
ISBN 978-99987-734-5-5



ANEC

TECHNICAL STANDARDIZATION

QUANTUM COMMUNICATION AND TECHNICAL STANDARDIZATION

Version 1.0 · November 2024

ILNAS
Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services

ANEC
Agence pour la Normalisation et l'Economie de la Connaissance

Foreword

Technical standardization plays an important role in the support of economic development. Nowadays, almost every sector relies on standards to provide services in an efficient manner. Standards are therefore considered as a major source of benefits, and this is particularly true for Information and Communication Technology (ICT), which supports all other economic developments.

The Grand Duchy of Luxembourg has understood the importance of the digital economy and has engaged since several years in an ambitious innovation strategy for the ICT sector. The "Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services" (ILNAS) supports this development through the "Luxembourg Standardization Strategy 2024-2030", signed by the Minister of the Economy, which identifies the ICT sector as one of the most relevant for national economic growth, along with the Construction and Aerospace sectors.

In addition to the strategy, ILNAS has also developed the "Luxembourg's policy on ICT technical standardization 2022-2025", which it carries out with the support of the Economic Interest Group "Agence pour la Normalisation et l'économie de la Connaissance" (ANEC GIE – Standardization Department). The policy aims to promote and strengthen the use of technical standards by the national market, to reinforce the positioning of Luxembourg in the global ICT standardization landscape, particularly through a stronger involvement of national stakeholders in the relevant standardization technical committees, and to pursue the development of research and education programs. In the frame of this policy, ILNAS has notably launched different research activities in the ICT domain.

As a result of these research activities, a series of White Papers and reports, that aim to inform the market about technical standardization developments in certain ICT subtopics have been published. Moreover, a Standards Analysis of the ICT Sector - Luxembourg consisting in a practical tool to discover the latest standardization developments in the overall landscape of ICT related technologies is regularly published by ILNAS, with the support of the ANEC GIE.

Within this global framework, the current document is intended to present current standardization developments in the area of Quantum Communication, with a view towards informing the national stakeholders and encouraging their involvement in the standards development process, for the benefit of Luxembourg's economy.

Jean-Marie REIFF
Director
ILNAS

Jean-Philippe HUMBERT
Deputy Director
ILNAS

Abstract

Quantum communication is emerging as a transformative field within quantum technologies, offering unprecedented levels of security and efficiency in data transmission. This report aims to provide a comprehensive understanding of quantum communication and the associated standardization efforts that are crucial to its advancement and widespread adoption.

The report begins with an overview of quantum technologies, focusing on quantum computing and its risks and opportunities. As quantum computing advances, it poses a significant threat to traditional cryptographic systems, including those used in communication, due to its ability to solve complex mathematical problems much faster than classical computers. This makes the development of quantum communication technologies crucial, as they offer solutions like Quantum Key Distribution (QKD) to protect information against quantum attacks. The report further explores quantum communication, outlining its three main generations, starting with Prepare & Measure QKD in the first generation, progressing through entanglement-based QKD in the second, and concluding with quantum repeaters in the third generation.

Following this, the document delves into the challenges of quantum communication and underscores the importance of technical standardization in overcoming these barriers. The report highlights the role of leading standardization bodies such as ISO, IEC, ITU-T, CEN, CENELEC and ETSI, detailing their contributions to the development of standards that ensure the security, interoperability, and scalability of quantum communication systems. Additionally, the report identifies key documents and ongoing projects related to quantum communication developed by these organizations.

Finally, the document explores standardization opportunities specific to Luxembourg, offering practical guidance on how stakeholders can engage with ongoing projects and participate in standards development processes. With their involvement, organizations can help shape the future of quantum technologies, driving innovation and technological progress on a national and global scale.

Table of contents

1

Introduction to quantum technologies

1. Introduction to quantum technologies

Quantum technologies represent a rapidly expanding field that delves into the fundamental principles of quantum mechanics. This interdisciplinary domain brings together the expertise of physicists, computer scientists, mathematicians, and engineers to pioneer innovations that leverage the unique properties of quantum systems. These properties, such as superposition and entanglement, unlock new possibilities in computation, communication, and sensing, pushing the boundaries of technological advancement.

Figure 1 illustrates the key concepts of superposition and entanglement in quantum systems. These fundamental properties enable the unique behaviors of quantum particles and are essential in understanding the mechanics that drive quantum technologies.

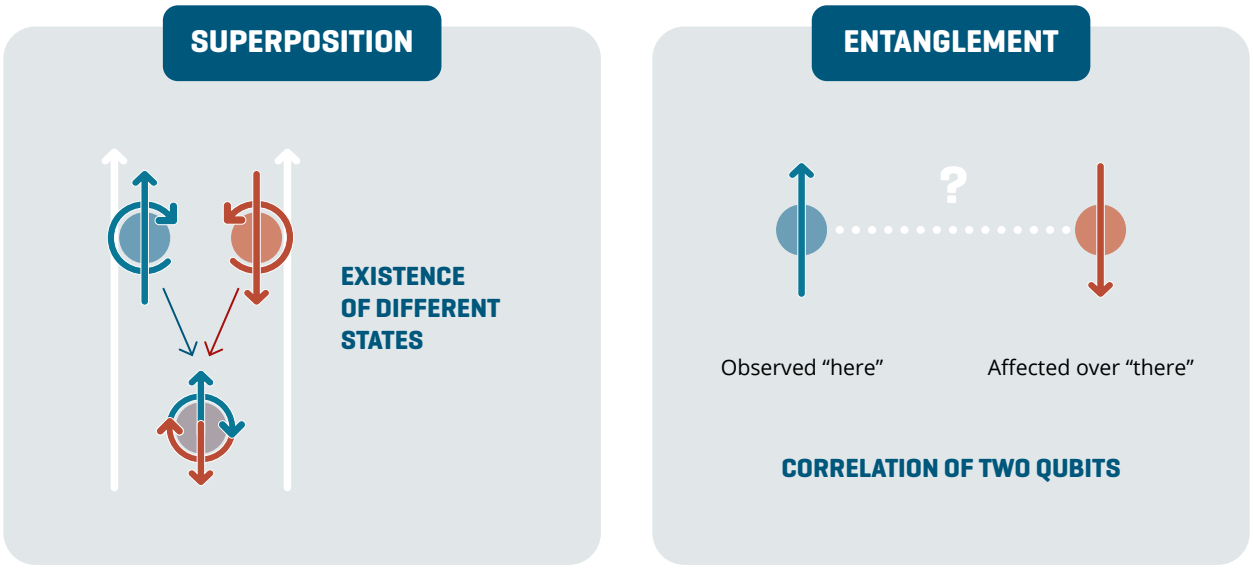


Figure 1: Properties of Quantum Behavior – Superposition and Entanglement

Superposition represents one of the fundamental features of quantum systems, allowing these systems to exist in multiple states simultaneously [1]. For instance, a photon can occupy various potential states at once. Until an observation or a measurement is made, the photon remains in a superposition of all these possible states. However, once measured, the superposition collapses, and the photon assumes a specific, well-defined state.

Entanglement is another cornerstone of quantum mechanics, famously referred by Einstein as “spooky action at a distance” [2]. Quantum entanglement occurs when two systems become so strongly correlated that information obtained from one immediately reveals information about the other, no matter the distance separating them [3]. This phenomenon underpins many emerging quantum technologies and fuels ongoing innovation across diverse scientific disciplines.

By harnessing these properties, quantum technologies can overcome the limitations of classical systems by enabling more secure communication networks, ultra-precise measurement tools, and exponentially increased computing power.

2 Quantum computing

2. Quantum computing

At the forefront of quantum technologies is quantum computing, which promises to exponentially increase computing power compared to classical systems. Classical computers use bits to represent data in binary form, either as a 0 or a 1. However, quantum computers leverage quantum bits or qubits, which can exist in multiple states simultaneously using quantum properties. This unique feature enables quantum computers to perform many calculations at once, which leads to the reduction of the computation time for certain problems.

The primary goal of quantum computing is to tackle highly complex problems that are currently beyond the reach of classical computers. For instance, quantum computing has the potential to revolutionize fields such as machine learning by improving pattern recognition in vast datasets. With quantum algorithms, quantum computers can analyze and identify patterns much faster and more accurately than classical algorithms, benefiting areas such as image recognition, language processing, and data mining [4].

However, while quantum computing offers significant opportunities, it also presents serious risks, especially for modern data security. The immense processing power of quantum computers poses a threat to current cryptographic methods that protect online communications and sensitive data. Most encryption techniques today rely on the difficulty of solving complex mathematical problems, such as factorizing large numbers. Quantum computers, using algorithms like Shor's algorithm, could potentially break these cryptographic systems in a fraction of the time it would take classical computers [5]. This could expose sensitive information in fields such as finance, healthcare, and government, rendering traditional encryption obsolete.

Classical encryption systems, including widely used techniques such as RSA (Rivest-Shamir-Adleman cryptosystem) and elliptic-curve cryptography, rely heavily on mathematical algorithms to secure communications. These encryption methods are considered secure because classical computers lack the computational power to solve the complex mathematical challenges they present within a practical timeframe.

However, with the anticipated rise of quantum computing, these cryptographic methods become increasingly vulnerable. A sufficiently powerful quantum computer could solve these mathematical problems exponentially faster than classical computers, making it possible to decrypt encrypted communications and compromising sensitive information. This poses a significant challenge for sectors reliant on secure key distribution, such as the Internet of Things and cloud-based systems.

As cyberattacks and data breaches get more sophisticated, the limitations of traditional encryption methods have become more apparent [6]. The urgent need for more resilient security solutions has driven research and development into next-generation technologies. Quantum communication, in particular, offers a promising path forward.

The following section provides an overview of quantum communication, with a particular focus on Quantum Key Distribution (QKD). This section will also explore the generations of quantum communication, outlining the key advancements and innovations that have shaped its development.

3

Quantum communication

3. Quantum communication

3.1. Overview

Quantum communication represents a new era for securing data transmission [7]. It offers a transformative approach by leveraging the principles of quantum mechanics to create inherently secure communication channels. Unlike classical systems that rely on mathematical algorithms to encrypt data, quantum communication uses the physical properties of quantum systems to guarantee security.

The key feature of quantum communication lies in the use of qubits that can exist in multiple states simultaneously due to superposition. Additionally, entanglement allows qubits that are spatially separated to remain interconnected, so that the state of one qubit directly influences the state of another, no matter the distance between them. These properties enable secure communication networks where any attempt to eavesdrop is immediately detectable.

Quantum communication also relies on principles like the no-cloning theorem, which makes it impossible to copy an unknown quantum state without causing changes [8]. Any attempt to intercept quantum-encoded information will always introduce errors into the system, because measuring or copying the quantum states disturbs them. These errors are what notify the communicating parties of an interception. Therefore, while interception is possible, it always leads to detectable errors, making it clear that the communication has been compromised.

As the computational capabilities of quantum systems continue to advance, the risks to classical cryptographic systems are becoming increasingly evident. Quantum communication, however, offers a robust solution to this threat by ensuring that any interception attempt is immediately detected.

One of the most promising applications of quantum communication is QKD. In QKD, the security of data transmission is based on the fundamental laws of quantum mechanics rather than mathematical algorithms. The most well-known QKD protocol, BB84, allows two parties to establish a shared secret key that is provably secure, even against quantum computer attacks [9]. If an eavesdropper tries to intercept the communication, the quantum states will be disturbed, immediately revealing the intrusion.

The evolution of quantum communication has progressed through three main generations [10], each representing significant advancements in technology and a deeper understanding of quantum mechanics, pushing the limits of secure communication even further.

3.2. Main generations of quantum communication

3.2.1. First generation: quantum key distribution (prepare & measure)

3.2.1.1. Definition

The first generation of quantum communication is primarily centered on QKD using the Prepare & Measure approach. This method is most famously exemplified by the BB84 protocol, developed by Charles Bennett and Gilles Brassard in 1984. BB84 marked a significant breakthrough in cryptography, offering a new way to securely distribute cryptographic keys between two parties, typically referred to as Alice and Bob, over a quantum channel [10].

The security of QKD relies on several key principles of quantum mechanics:

- No-cloning theorem: This principle asserts that it is impossible to create an identical copy of an arbitrary unknown quantum state. This ensures that no eavesdropper cannot copy the transmitted qubits without introducing detectable errors.
- Heisenberg uncertainty principle: According to this principle, any attempt to measure or observe a quantum state disturbs that state. In the context of QKD, if an eavesdropper tries to intercept and measure the qubits, this will cause detectable disturbances in the quantum states, alerting Alice and Bob of the presence of an intrusion.

These principles together ensure that any attempt at eavesdropping on the quantum channel will introduce detectable disturbances, thus preserving the integrity of the key exchange process.

3.2.1.2. Architecture

The architecture of first-generation QKD systems follows a straightforward yet highly effective design. It involves:

- Quantum channel: This is the channel used for transmitting quantum information in the form of qubits, typically photons. The quantum channel can be either an optical fiber or free-space link. Photons, as carriers of quantum information, are sent from Alice to Bob.
- Classical channel: Alongside the quantum channel, a classical communication channel is used for the coordination of the key exchange. Importantly, while the classical channel is not required to be secure, any attempt to eavesdrop on the quantum channel will be detected through disturbances in the transmitted qubits.

The process works as follows:

- Preparation: Alice prepares qubits in one of two possible bases, either the rectilinear basis (horizontal and vertical polarizations) or the diagonal basis (45° and 135° polarizations). She randomly assigns a value of 0 or 1 to each qubit depending on the basis used.
- Measurement: Bob receives these qubits and measures them using randomly chosen bases. If Bob chooses the same basis as Alice, the measurement will match the value Alice assigned (0 or 1). If the bases are different, the measurement will be random.
- Eavesdropping detection: After the transmission, Alice and Bob compare a subset of their results through the classical channel. If an eavesdropper has interfered with the qubits during transmission, discrepancies will appear in the results, indicating the presence of eavesdropping. If no eavesdropping is detected, the matching results from Alice and Bob form the shared secret key.

This simple yet effective architecture allows for practical implementation in both fiber-optic networks and free-space communication [5], enabling secure quantum communication. The use of standard optical components makes QKD highly adaptable for integration into existing communication infrastructures.

3.2.1.3. Standardization related developments

To support the development and secure deployment of first-generation quantum communication technologies, particularly the Prepare & Measure QKD protocols like BB84, several specifications and reports have been established. ETSI GS QKD 002 "Quantum Key Distibution – Use Cases" outlines a variety of potential use cases where QKD systems in general can be applied, demonstrating their practical utility in secure communications across different implementations, including first-generation technologies. Additionally, ETSI GR QKD 003 "QKD - Components and Internal Interfaces" provides guidelines for the components and internal interfaces required to build interoperable QKD systems, ensuring that the various hardware and software elements in these systems work together seamlessly. Moreover, ETSI GS QKD 016 "QKD - Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules" introduces a protection profile for QKD modules, ensuring that the physical implementation of QKD systems meets strict security requirements, particularly for first-generation QKD systems. Together, these documents help establish a solid foundation for the secure implementation of first-generation QKD systems in various environments.

3.2.2. Second generation: quantum key distribution (photonic entanglement sources)

3.2.2.1. Definition

The second generation of quantum communication introduces advancements over the first generation by utilizing entangled photon pairs for QKD. This approach builds on the unique properties of quantum entanglement, where two photons are produced in such a way that their quantum states remain intrinsically linked, regardless of the distance separating them.

One of the foundational protocols in this category is the E91 protocol, developed by Artur Ekert in 1991 [10]. Unlike the Prepare & Measure schemes, where qubits are prepared and measured independently, entanglement-based QKD leverages the fact that measuring the state of one photon in an entangled pair will instantly determine the state of the other, even if the two photons are separated by vast distances. This correlation makes entanglement-based QKD highly resistant to eavesdropping, as any attempt to intercept the entangled photons will disturb the system and be immediately detectable.

Entanglement-based QKD also benefits from stronger security guarantees based on Bell's theorem, which demonstrates that quantum correlations cannot be explained by classical physics. This provides an additional layer of security for key exchange, as any third-party interference would break these correlations.

3.2.2.2. Architecture

The architecture of second-generation quantum communication systems involves the generation of entangled photon pairs, typically through nonlinear crystals or specialized photonic sources. These photon pairs are then distributed to two parties, Alice and Bob, who each receive one photon from the pair. The process works as follows:

- Generation of Entangled Photons: A photonic source generates pairs of entangled photons. The entanglement ensures that when Alice measures her photon's state, Bob's photon will instantly adopt the correlated state, regardless of the distance between them.
- Measurement: Both Alice and Bob independently measure their photons in randomly chosen bases. Since the photon pairs are entangled, their measurement results will be correlated. The bases they use for measurement are compared over a classical communication channel.
- Key Generation: If their measurement bases match, Alice and Bob will generate identical results that can be used to establish a shared secret key. Any external interference would disturb the quantum correlations, making it detectable and thus ensuring the security of the key distribution.
- Eavesdropping Detection: Any attempt to intercept the photons would disturb the entanglement between the photon pairs, introducing detectable errors in the measurements. This guarantees the security of the communication by alerting Alice and Bob to any potential interference.

Entanglement-based QKD systems offer significant advantages over first-generation. One key benefit is the ability to operate over longer distances without requiring direct line-of-sight between the communicating parties. However, one of the main challenges lies in maintaining the entanglement over long distances. Entangled states are highly susceptible to environmental disturbances, such as losses in optical fibers, which degrade the entanglement. To address this, quantum repeaters (third generation) are being developed to preserve the quantum correlations over extended distances [11], ensuring the reliability and security of second-generation QKD systems. These technological advancements are crucial for the scalability of secure quantum communication networks.

3.2.2.3. Standardization related developments

To support the development and secure deployment of second-generation quantum communication technologies, which focus on entanglement-based QKD systems, several important specifications and reports have been developed. ETSI GS QKD 011 "QKD - Component characterization: characterizing optical components for QKD systems" plays a crucial role by providing the necessary guidelines for the characterization of components, particularly optical components, used in entanglement-based QKD systems. This ensures that the quantum states between entangled photons are reliably distributed across different nodes. ETSI GR QKD 003 "QKD - Components and Internal Interfaces" covers the properties of the components and interfaces needed for interoperable QKD systems, which is critical for ensuring that the hardware and software elements function seamlessly across different QKD implementations. This report is of paramount importance for both first- and second-generation QKD technologies.

3.2.3. Third generation: quantum repeater (entanglement distribution)

3.2.3.1. Definition

The third generation of quantum communication introduces the concept of quantum repeaters, a critical technology designed to overcome the limitations imposed by signal loss and decoherence in transmission channels over long distances. Decoherence refers to the process by which a quantum system loses its quantum properties (such as superposition and entanglement) due to interactions with its environment [12]. Quantum repeaters enable entanglement distribution across greater distances by dividing the communication path into shorter, more manageable segments. In each segment, local entanglement is generated, and entanglement swapping is employed to extend the entanglement between distant nodes by linking these segments together [10].

Quantum repeaters are essential for realizing long-distance quantum networks, such as the proposed quantum internet, which envisions a global network of quantum computers and communication devices connected by entangled qubits. Without quantum repeaters, the exponential loss of photons and signal degradation over long distances (especially in optical fibers) makes direct quantum communication over distances exceeding a few hundred kilometers infeasible.

3.2.3.2. Architecture

The architecture of quantum repeater systems is significantly more complex than that of first and second-generation quantum communication systems. It generally involves three critical components:

- Entanglement Generation: Local pairs of entangled qubits are generated at intermediate nodes (repeater stations) along the communication path. These nodes act as relay points for entanglement distribution across the network.
- Entanglement Swapping: Entanglement swapping is a process used to extend entanglement between distant nodes. By performing a Bell-state measurement on one qubit from each of two entangled pairs, the entanglement is "swapped" to the remaining qubits, effectively linking the segments. This allows for entanglement to be distributed across multiple nodes without requiring direct interaction between the distant endpoints.
- Quantum Memory: Quantum memories are employed at each node to temporarily store the entangled states of particles until entanglement is successfully established across the entire communication path. This is crucial because the transmission of photons and the measurements taken at different nodes might not happen simultaneously, especially over long distances. The quantum memory ensures that entanglement can be synchronized and maintained across distant nodes, allowing for efficient entanglement distribution.

Quantum repeaters hold the potential to enable quantum communication over thousands of kilometers, overcoming the signal losses and decoherence that currently limit the range of quantum communication through fiber optics and free-space transmission. However, the practical implementation of quantum repeaters remains a significant technical challenge, requiring ongoing advances in quantum memory, error correction, and entanglement purification techniques.

3.2.3.3. Standardization related developments

In terms of supporting the development of third-generation quantum communication, several ITU-T Y-series standards are highly relevant. For example, Y.3800 "Overview on networks supporting quantum key distribution" provides an overview of networks that support QKD, helping to establish a foundational framework for such technologies. Similarly, Y.3802 "Quantum key distribution networks – Functional architecture" defines the functional architecture of QKD networks, which is crucial for the integration of quantum repeaters and long-distance communication. These standards are essential as third-generation quantum technologies, such as quantum repeaters, are still under development and require clear architectural guidance for their full realization.

3.3. Challenges of quantum communication

Quantum communication is set to bring transformative advancements in secure data transmission, offering new possibilities for privacy and security in various sectors. However, the development and integration of this technology come with a unique set of challenges that must be overcome to fully realize its potential. Some of these challenges are highlighted in Figure 2:

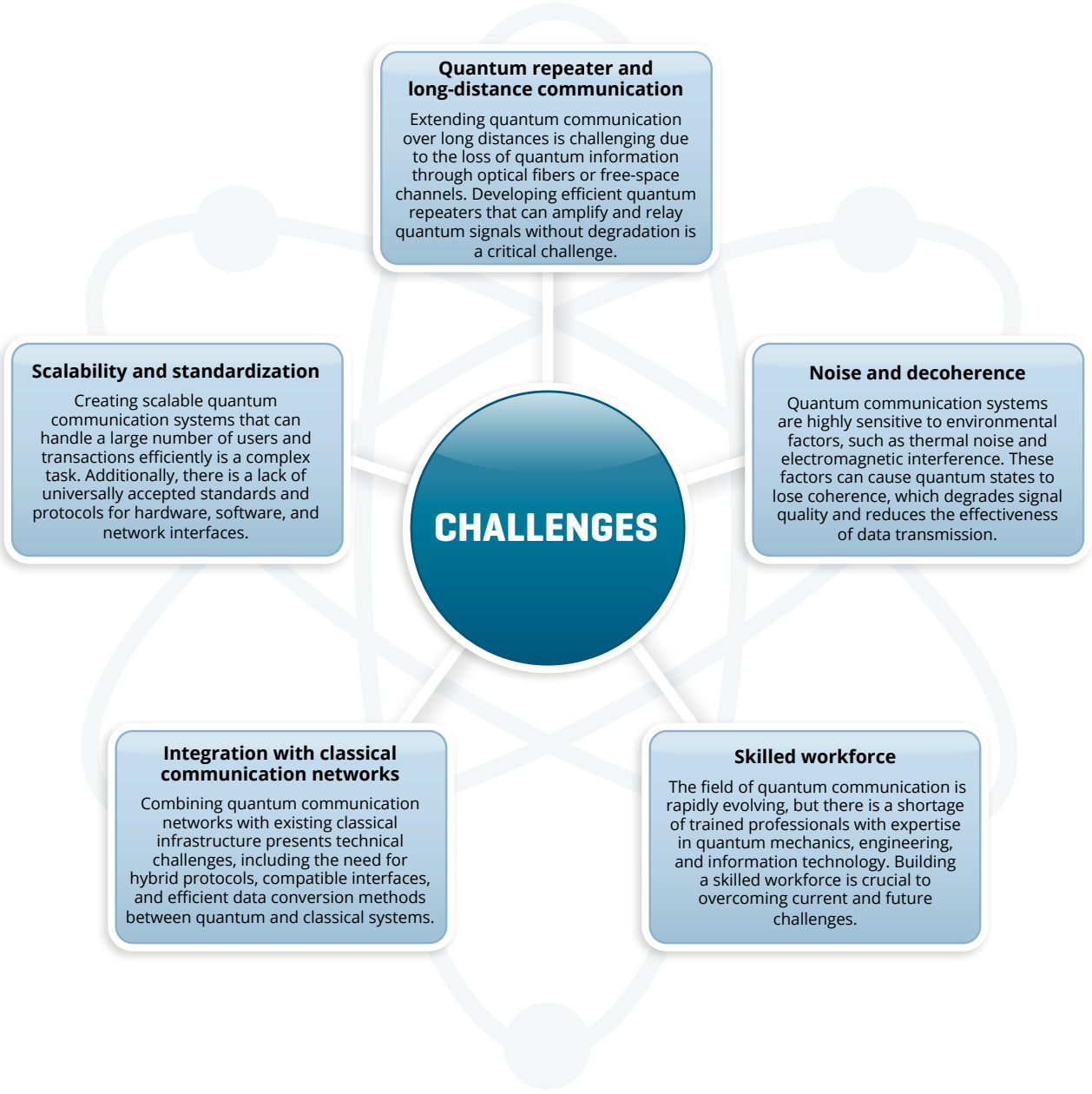


Figure 2: Some Challenges of Quantum Communication

The challenges facing quantum communication are diverse and complex, ranging from technical hurdles in maintaining quantum coherence over long distances to the integration with existing communication frameworks. These challenges highlight the nascent stage of this technology and underscore the critical need for focused research and collaborative efforts to address these barriers. Overcoming these obstacles is essential for enabling the widespread adoption of quantum communication and unlocking its full potential in secure communications.

As we look towards solutions to these challenges, one pivotal area that holds the potential to accelerate the development and adoption of quantum communication is standardization. Establishing universally accepted standards and protocols is crucial for ensuring compatibility across different systems and technologies, enhancing security measures, and facilitating global cooperation in the quantum field.

4

Quantum communication and technical standardization

4. Quantum communication and technical standardization

4.1. Definition of a standard

As defined by CEN, CENELEC and ETSI [13], a standard is *"a document, established by consensus and approved by a recognized body that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context. Standards should be based on consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits."*

4.2. Benefits of standardization

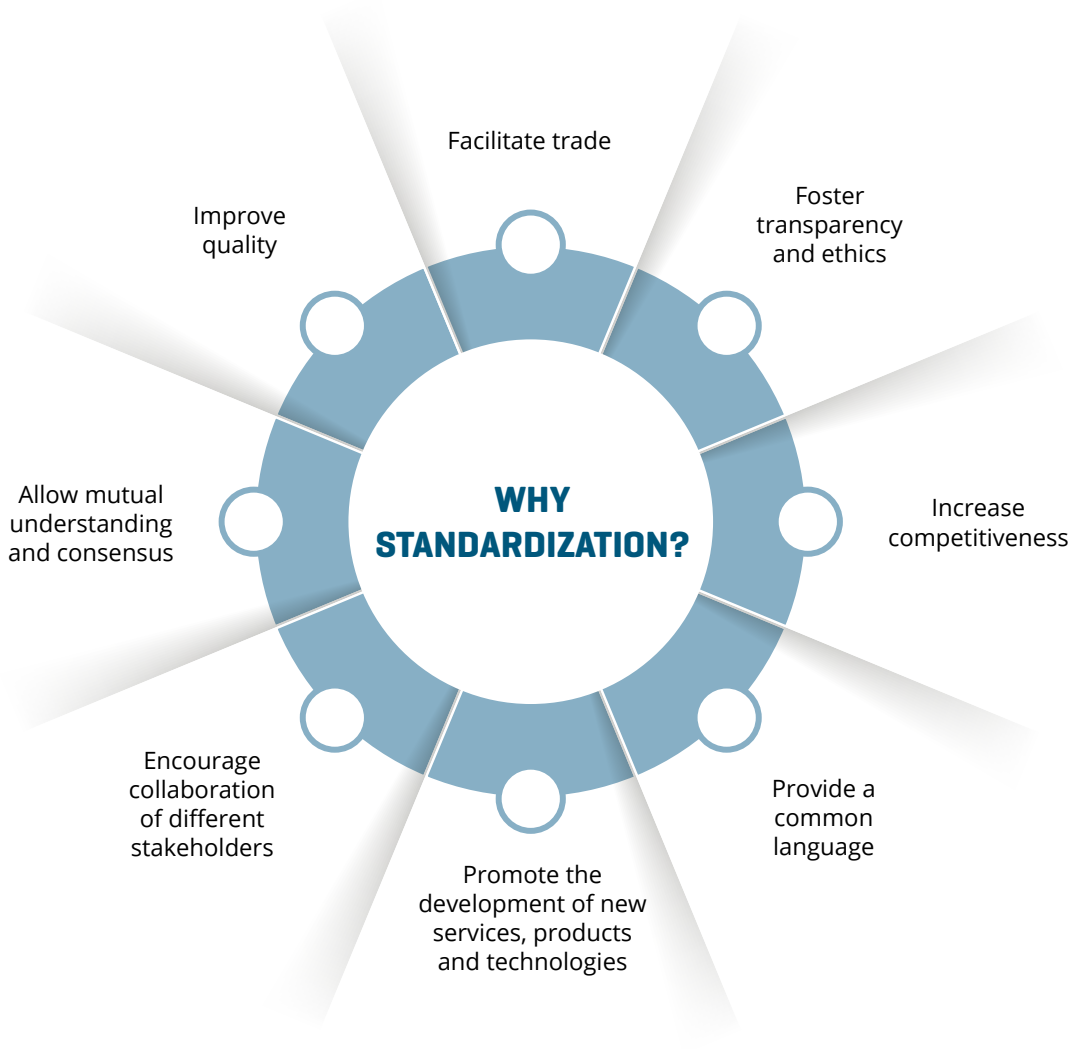


Figure 3: Benefits of standardization

4.3. Standards development organizations

Technical standards are developed by organizations that bring all interested stakeholders together and follow well-accepted principles (e.g., defined by the World Trade Organization[1]). In the European Union, Regulation (EU) No 1025/2012[2] recognizes the following standardization organizations:

At the international level:

- International Organization for Standardization (ISO).
- International Electrotechnical Commission (IEC).
- International Telecommunication Union's Telecommunication Standardization Sector (ITU-T).

At the EU level:

- European Committee for Standardization (CEN).
- European Committee for Electrotechnical Standardization (CENELEC).
- European Telecommunications Standards Institute (ETSI).

Finally, at national level, the *Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services* (ILNAS) is the national standards body representing Luxembourg in international and European standardization organizations. As such, ILNAS is a member of the six recognized standardization organizations.

4.4. Standardization activities related to quantum communication and security

Standardization efforts related to quantum communication have been established, with many others currently underway through various prominent standardization organizations.

1 https://www.wto.org/english/tratop_e/tbt_e/principles_standards_tbt_e.htm

2 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012R1025

4.4.1. ETSI

Groups active in quantum standardization

Groups	Description
ETSI ISG-QKD	Industry Specification Group[3] (ISG) on Quantum Key Distribution was established in 2008. It aims to connect stakeholders from commerce, industry and science to develop ETSI Group Specifications (GSs) describing quantum cryptography for ICT [14]. QKD is the essential credential in order to use quantum cryptography on a broad basis. It is the main task of the QKD ISG to specify a system for QKD and its environment.
ETSI TC CYBER WG QSC	ETSI TC CYBER WG QSC is a working group for Quantum-Safe Cryptography. The primary responsibilities of this working group are to make assessments and recommendations on the various proposals from industry and academia regarding real-world deployments of quantum-safe cryptography, including practical properties, (such as efficiency, functionality, agility, etc.), security properties, appropriateness of certain quantum-safe cryptographic primitives to various application domains (Internet protocols, wireless systems, resource constrained environments, cloud deployments, big data, etc.). Note: before operating as a WG in TC CYBER, QSC was initially created as an ISG in ETSI. In order to produce normative ETSI deliverables, such as technical reports or technical specifications, it was necessary to promote the ISG as a WG within an ETSI Technical Committee.

Relevant documents developed by ETSI

Committees	Document reference	Title	Date of publication
ETSI ISG-QKD	ETSI GS QKD 002	Quantum Key Distribution; Use Cases	06/2010
	ETSI GR QKD 003	Quantum Key Distribution (QKD); Components and Internal Interfaces	03/2018
	ETSI GS QKD 004	Quantum Key Distribution (QKD); Application Interface	08/2020 *(under revision)*
	ETSI GS QKD 005	Quantum Key Distribution (QKD); Security Proofs	12/2010 *(under revision)*
	ETSI GR QKD 007	Quantum Key Distribution (QKD); Vocabulary	12/2018 *(under revision)*
	ETSI GS QKD 008	Quantum Key Distribution (QKD); QKD Module Security Specification	12/2010
	ETSI GS QKD 011	Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems	05/2016
	ETSI GS QKD 012	Quantum Key Distribution (QKD); Device and Communication Channel Parameters for QKD Deployment	02/2019
	ETSI GS QKD 014	Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API	02/2019 *(under revision)*
	ETSI GS QKD 015	Quantum Key Distribution (QKD); Control Interface for Software Defined Networks	04/2022
	ETSI GS QKD 016	Quantum Key Distribution (QKD); Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules	01/2024 *(under revision)*
	ETSI GS QKD 018	Quantum Key Distribution (QKD); Orchestration Interface for Software Defined Networks	04/2022

3 Industry Specification Groups operate alongside traditional standards-making committees in a specific technology area. They are designed to be quick and easy to set up. They provide an effective alternative to the creation of industry fora. (source ETSI)

ETSI TC CYBER WG QSC	ETSI GR QSC 001	Quantum-Safe Cryptography (QSC); Quantum-safe algorithmic framework	07/2016
	ETSI GR QSC 003	Quantum Safe Cryptography; Case Studies and Deployment Scenarios	02/2017
	ETSI GR QSC 004	Quantum-Safe Cryptography; Quantum-Safe threat assessment	03/2017
	ETSI GR QSC 006	Quantum-Safe Cryptography (QSC); Limits to Quantum Computing applied to symmetric key sizes	02/2017
	ETSI TR 103 570	CYBER; Quantum-Safe Key Exchanges	10/2017
	ETSI TR 103 616	CYBER; Quantum-Safe Signatures	09/2021
	ETSI TR 103 617	Quantum-Safe Virtual Private Networks	09/2018
	ETSI TR 103 618	CYBER; Quantum-Safe Identity-Based Encryption	12/2019
	ETSI TR 103 619	CYBER; Migration strategies and recommendations to Quantum Safe schemes	07/2020
	ETSI TR 103 692	CYBER; State management for stateful authentication mechanisms	11/2021
	ETSI TS 103 744	CYBER; Quantum-safe Hybrid Key Exchanges	12/2020 *(under revision)*
	ETSI TR 103 823	CYBER; Quantum-Safe Public-Key Encryption and Key Encapsulation	10/2021
	ETSI TR 103 949	Quantum-Safe Cryptography (QSC) Migration; ITS and C-ITS migration study	05/2023
	ETSI TR 103 965	CYBER; Quantum-Safe Cryptography (QSC); Impact of Quantum Computing on Cryptographic Security Proofs	10/2024
	ETSI TR 103 966	CYBER; Quantum-Safe Cryptography (QSC); Deployment Considerations for Hybrid Scheme	10/2024

Examples of projects under development

Groups	Document reference	Title
ETSI ISG-QKD	ETSI GS QKD 010	Quantum Key Distribution (QKD); Implementation security: protection against Trojan horse attacks in one-way QKD systems
	ETSI GS QKD 013	Quantum Key Distribution (QKD); Characterisation of Optical Output of QKD transmitter modules
	ETSI GR QKD 017	Quantum Key Distribution (QKD); Network architectures
	ETSI GR QKD 019	Quantum Key Distribution (QKD); Design of QKD interfaces with Authentication
	ETSI GS QKD 020	Quantum Key Distribution (QKD); Protocol and data format of REST-based Interoperable Key Management System API
	ETSI GS QKD 021	Quantum Key Distribution (QKD); Orchestration Interface of Software Defined Nsetworks for Interoperable key management system
	ETSI GS QKD 022	Quantum Key Distribution (QKD); Network Architecture
	ETSI GS QKD 023	Quantum Key Distribution (QKD); Monitoring Interface and Data Model
ETSI TC CYBER WG QSC	ETSI TR 103 967	Quantum-Safe Cryptography (CYBER); Impact of Quantum Computing on Symmetric Cryptography
	ETSI TS 104 015	Quantum-Safe Cryptography (CYBER); Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies
	ETSI TR 104 016	Quantum-Safe Cryptography (CYBER); A Repeatable Framework for Quantum-safe Migrations
	ETSI TR 104 017	Quantum-Safe Cryptography (CYBER); QSC Protocol Inventory

4.4.2. ITU-T

Groups active in quantum standardization

Groups	Description
ITU-T Study Group 11	ITU-T Study Group 11 'Signalling requirements, protocols, test specifications and combating counterfeit telecommunication/ICT devices', focuses on the standardization of protocols and test specifications for next-generation network technologies, including quantum communication.
ITU-T Study Group 13	The Study Group 13, 'Future networks' focuses on general functional requirements for QKD networks. Their ongoing work involves the exploration of a functional framework, the development of a generic functional architecture, and a specific emphasis on key management functions.
ITU-T Study Group 17	The activities of the Study Group 17 'Security' focuses on cybersecurity, security management, service and application security, fundamental security technologies, and security strategy and coordination which include quantum-based security.

Relevant documents developed by ITU-T

Groups	Document reference	Title	Date of publication
ITU-T Study Group 13	Y.3800	Overview on networks supporting quantum key distribution	10/2019
	Y.3801	Functional requirements for quantum key distribution networks	04/2020
	Y.3802	Quantum key distribution networks – Functional architecture	11/2023
	Y.3803	Quantum key distribution networks – Key management	11/2023
	Y.3804	Quantum key distribution networks – Control and management	11/2023
	Y.3805	Quantum key distribution networks – Software-defined networking control	11/2023
	Y.3806	Quantum key distribution networks – Requirements for quality of service assurance	09/2021
	Y.3807	Quantum key distribution networks – Quality of service parameters	02/2022
	Y.3808	Framework for integration of quantum key distribution network and secure storage network	02/2022
	Y.3809	A role-based model in quantum key distribution networks deployment	02/2022
	Y.3810	Quantum key distribution network interworking – Framework	09/2022
	Y.3811	Quantum key distribution networks – Functional architecture for quality of service assurance	11/2023
	Y.3812	Quantum key distribution networks – Requirements for machine learning based quality of service assurance	09/2022
	Y.3813	Quantum key distribution networks – functional requirements	01/2023
	Y.3814	Quantum key distribution networks – functional requirements and architecture for machine learning enablement	11/2023

Groups	Document reference	Title	Date of publication
ITU-T Study Group 13	Y.3815	Quantum key distribution networks – Overview of resilience	09/2023
	Y.3816	Quantum key distribution networks – Functional architecture enhancement of machine learning based quality of service assurance	09/2023
	Y.3817	Quantum key distribution networks interworking – Requirements of quality of service assurance	09/2023
	Y.3818	Quantum key distribution networks interworking – Architecture	09/2023
	Y.3819	Quantum key distribution networks - Requirements and architectural model for autonomic management and control	12/2023
	Y.3820	Quantum Key Distribution Network Interworking – Software Defined Networking Control	09/2024
	Y.3821	Requirements for quantum key distribution network resilience	04/2024
	Y.3822	Quantum key distribution networks – Requirements for autonomic quality of service assurance	09/2024
	Y.3824	Quantum key distribution network federation - Reference models	09/2024
	Y.3825	Framework for integration of quantum key distribution network and time sensitive network	09/2024
	Y.3826	Integration of quantum key distribution network and user network supporting end-to-end modern cryptography services – Framework	09/2024
	Y Suppl. 70	ITU-T Y.3800-series – Quantum key distribution networks - Applications of machine learning	07/2021
	Y Suppl. 74	ITU-T Y.3800-series – Standardization roadmap on quantum key distribution networks	03/2023
	Y Suppl. 75	ITU-T Y.3000 series – Quantum key distribution networks – Quantum-enabled future networks	03/2023
	Y Suppl. 79	ITU-T Y.3800 series – Quantum key distribution networks – Role in end-to-end cryptographic services with non-quantum cryptography	11/2023
	Y Suppl. 80	Quantum key distribution networks use cases	11/2023
ITU-T Study Group 17	X.1702	Quantum noise random number generator architecture	11/2019
	X.1710	Security framework for quantum key distribution networks	10/2020
	X.1712	Security requirements and measures for quantum key distribution networks – key management	10/2021
	X.1713	Security requirements and designs for quantum key distribution networks node	04/2024
	X.1714	Key combination and confidential key supply for quantum key distribution networks	10/2020
	X.1715	Security requirements and measures for integration of quantum key distribution network and secure storage network	04/2024
	X.1716	Authentication and authorization in quantum key distribution network (QKDN)	10/2024
	X.1717	Security requirements and measures for quantum key distribution network (QKDN) - control and management	10/2024
	X.1811	Security guidelines for applying quantum-safe algorithms in IMT-2020 systems	04/2021

ITU-T Study Group 11	Q.4160	Quantum key distribution networks - Protocol framework	12/2023
	Q.4161	Protocols for Ak interface for quantum key distribution network	12/2023
	Q.4162	Protocols for Kq-1 interface for quantum key distribution network	12/2023
	Q.4163	Protocols for Kx interface for quantum key distribution network	12/2023
	Q.4164	Protocols for Ck interface for quantum key distribution network	12/2023

Examples of projects under development

Groups	Document reference	Title
ITU-T Study Group 13	Y.QKDN-qos-mmq	Quantum key distribution Networks - Measurement methodology for QoS parameters
	Y.supp. QKDN_sync	Analysis of Time Synchronization in Quantum Key Distribution Networks
	Y.QKDNi-qos-fa	Quantum key distribution networks interworking - Functional architecture for quality of service assurance
	Y.QKDN-nq-qos-rf	Framework of quality of service assurance for integrated quantum key distribution network and user network supporting end-to-end modern cryptography services
	Y.QKDN-QoS-Allo	Quantum key distribution networks - Allocation of the end-to-end quality of service
	Y.QKDN-qos-au-to-fa	Quantum key distribution networks - Functional architecture enhancement for autonomic quality of service assurance
	Y.QKD-IPSec-fr	Framework for integration of quantum key distribution and IPSec
	Y.QKDN-GQT	Generic Quantum Key Distribution Network Template
	Y.QKD-TLS	Quantum Key Distribution integration with Transport Layer Security 1.3
	Y.QKDN-da	Quantum key distribution networks - Dependability assessment
	Y.QKDN-qos-sdnc	QoS assurance requirements for quantum key distribution networks enabled by software defined networking control
	Y.QKDN-orfr	Framework for quantum key distribution network orchestration
	Y.QKDN-rsff	Quantum key distribution networks - functional framework of resilience
	Y.QKDN-safr	Quantum key distribution networks - Framework for service awareness
	Y.QKDN-slicing	Requirements and framework of quantum key distribution network slicing
ITU-T Study Group 17	TR.hyb_qsafe	Overview of key management of hybrid approaches for quantum-safe communications
	X.qsdlt-ca	Guidelines for building crypto-agility and migration for quantum-safe DLT systems
	TR.QKDN-SP	Technical Report: Overview of security profile for Quantum Key Distribution Networks in hybrid mode
	X.sec_QKD_profr	Framework of quantum key distribution (QKD) protocols in QKD network
	X.sec_QKDNi	Security requirements for Quantum Key Distribution Network interworking (QKDNi)

ITU-T Study Group 11	Q.4164_rev	Protocols for Ck interfaces for quantum key distribution networks
	Q.QKDN_Cq	Protocols for Cq interfaces for quantum key distribution networks
	Q.QKDN_GC	General control protocols for interfaces on quantum key distribution network controller for quantum key distribution networks
	Q.QKDN_Mk	Protocols for interfaces on quantum key distribution network manager for quantum key distribution networks
	Q.QKDNi_KM	Protocols for interfaces between key managers for quantum key distribution network interworking
	Q.QKDNi_profr	Quantum key distribution networks Interworking - Protocol framework

4.4.3. IEC and ISO/IEC

Groups active in quantum standardization

Groups	Description
ISO/IEC JTC 3	ISO/IEC JTC 3 "Quantum technologies" develops standards in the field of quantum technologies including quantum information technologies (quantum computing and quantum simulation), quantum metrology, quantum sources, quantum detectors, quantum communications, and fundamental quantum technologies.
ISO/IEC JTC 1/SC 27	ISO/IEC JTC 1/SC 27 "Information security, cybersecurity and privacy protection", has started to develop standards related to the security requirements, test and evaluation methods for QKD products, through its working group 3 "Security evaluation, testing and specification".

Relevant documents developed by ISO/IEC

Groups	Document reference	Title	Date of publication
ISO/IEC JTC 1/ SC 27	ISO/IEC 23837-1	Information security – Security requirements, test and evaluation methods for quantum key distribution – Part 1: Requirements	08/2023
	ISO/IEC 23837-2	Information security – Security requirements, test and evaluation methods for quantum key distribution – Part 2: Evaluation and testing methods	09/2023

Examples of projects under development

ISO/IEC JTC 3 is currently working to initiate new projects in various areas of quantum technologies including quantum communication. These efforts are aimed at addressing emerging challenges in quantum communication by developing international standards that can guide the secure deployment and interoperability of quantum systems. The committee is assessing the feasibility of these projects and ensuring alignment with the growing global needs for quantum-based innovations.

4.4.4. CEN/CENELEC

Groups active in quantum standardization

Groups	Description
CEN/CLC JTC 13	CEN/CLC JTC 13 "Cybersecurity and Data Protection", is a joint technical committee between CEN and CENELEC dedicated to the development of standards for cybersecurity and data protection covering all aspects of the evolving information society. The JTC 13 has recently approved the creation of a new WG 10 "Cryptography", which includes post-quantum cryptography in its scope.
CEN/CLC JTC 22	CEN/CLC JTC 22 "Quantum Technologies", is a joint technical committee between CEN and CENELEC dedicated to QT standardization. It has been created based on the work performed by the CEN/CLC FGQT, which led to the publication of two key documents: Standardization Roadmap on Quantum Technologies and Quantum technologies Use Cases. CEN/CLC JTC 22 shall produce standardization deliverables in the field of QT. This field includes quantum enabling technologies, quantum sub-systems, quantum platforms & systems, quantum composite systems and applications. CEN/CLC JTC 22 is composed of 4 WGs: WG 1 "Strategic Advisory Group"; WG 2 "Quantum Metrology, Sensing and Enhanced Imaging, and Quantum Enabling Technologies"; WG 3 "Quantum Computing and Simulation"; WG 4 "Quantum Communication and Quantum Cryptography".

Examples of projects under development

Groups	Document reference	Title
CEN/CLC JTC 22	/	Gap analysis of current quantum communication and quantum cryptography standards
	/	QKD and PQC – An equitable analysis and comparison of both technologies
	/	Quantum network best practices

4.5. Standardization activities related to other quantum technologies

Relevant published documents

Groups	Document reference	Title	Date of publication
ISO/IEC JTC 3	ISO/IEC 4879	Information technology – Quantum computing – Vocabulary	05/2024

Examples of projects under development

Groups	Document reference	Title
ISO/IEC JTC 3	ISO/IEC AWI TR 18157	Information technology — Introduction to quantum computing
CEN/CLC JTC 22	/	Layer model of Quantum Computing
	/	Hybridization of Quantum Computing
	/	Cryogenic Solid-State Quantum Computing; Part 1: Descriptions and functional requirements of modules
	/	Quantum technologies - Characterization of quantum technologies – Metrics and terminology
	/	Traveling-wave parametric amplifiers (TWPA) - Parameters and test methods
	/	Performance benchmarks of quantum computing applications

5

Standardization opportunities in Luxembourg

5. Standardization opportunities in Luxembourg

A proper understanding of the stakes associated with technical standardization, including quantum communication, is key to adopting the appropriate position across the standardization landscape and benefit from all the related opportunities. In this context, ILNAS aims to facilitate the adoption of technical standards by national stakeholders and promote their active participation in the standardization process to benefit the national economy.

5.1. National standardization commission for quantum technologies

At the beginning of 2024, ILNAS established a new national standardization commission (NSC 03) "Quantum technologies" to provide Luxembourgish market players with a unique platform to monitor and engage in standardization work in the field of quantum technologies. Members of the commission gain privileged access to European and international standardization activities, allowing them to contribute to the global development of quantum technology standards. Through the commission, national organizations can engage in the work of CEN/CLC JTC 22 and ISO/IEC JTC 3. This commission currently consists of 7 experts, who actively contribute to the European and international standardization efforts in quantum technologies.

5.2. Who can participate in standards development in Luxembourg?

ILNAS, with the support of ANEC GIE, encourages companies, institutions, researchers, etc. to participate in the standardization ecosystem. Any interested party can become an active national standardization delegate through ILNAS, free of charge, by joining the NSC 03 "Quantum Technologies" or other technical committees of ISO, IEC, CEN, and CENELEC. Interested experts can request to ILNAS their registration using a dedicated form.

5.3. How to access the standards?

The application and uptake of standards is a key opportunity that the market can take advantage of. In order to encourage this, ILNAS allows the consultation of published standards for free and their purchase for further use.

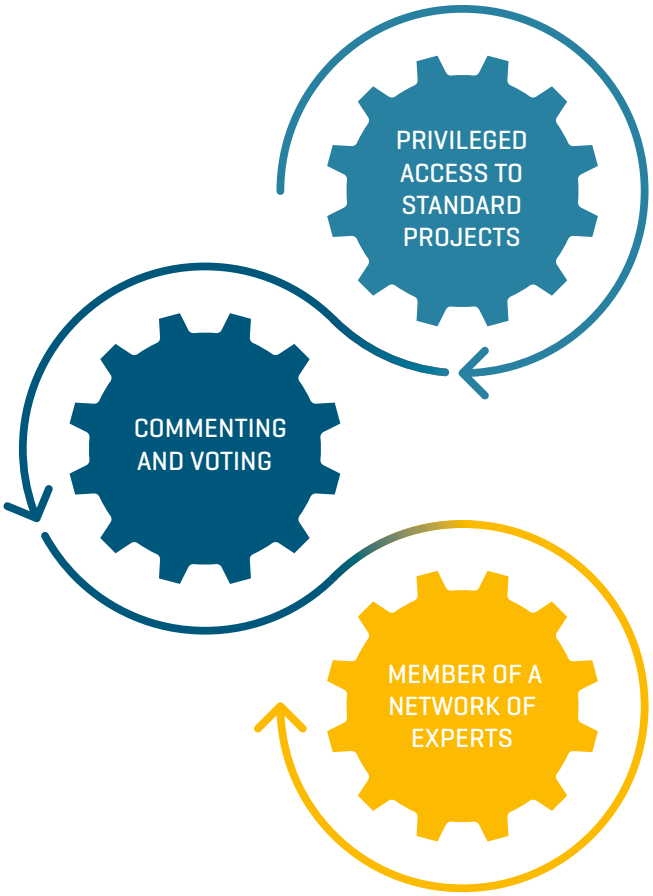
The ILNAS e-Shop is a catalog of more than 210,000 normative documents. It offers the possibility to purchase national (ILNAS and DIN), European (CEN, CENELEC and ETSI[4]) and international (ISO and IEC) standards in electronic format at competitive prices.

In addition, ILNAS offers the possibility to consult its entire standards' catalog free of charge through dedicated reading stations located in different places in Luxembourg. This service allows, for example, interested organizations or individuals to consult a standard before its purchase on the ILNAS e-Shop.

4 Generally, standards published by the ETSI are available for free to the public, except in some exceptional cases where fees may apply to access specific standards or detailed versions.

5.4. Good reasons to participate in standards development

- Access drafts standards and influence their content based on your know-how
- Increase your knowledge regarding the state of the art in standardization of your core business
- Propose new standards projects
- Anticipate the evolution of your activity sector's good practices
- Integrate strategic network of national, European or international experts
- Collaborate to defend common interests
- Learn about your competitors and their positions in meetings
- Promote your organization and your skills at national, European and international levels



Conclusion

This report aims to inform national stakeholders about the opportunities available through the use of technical standards and participation in the standards development process within the fast-evolving field of quantum communication technology. The document provides a comprehensive overview of quantum technologies, explaining how the advancement of quantum computing can threaten current communication and security systems. The report also offers an overview of quantum communication and its three main generations.

Moreover, the report highlights the challenges associated with the development of quantum communication and underscores the critical need for technical standardization to ensure the secure and scalable deployment of these technologies. The role of standards is explained, emphasizing how they promote innovation, ensure interoperability, and support the development of new technologies in this rapidly advancing field.

Additionally, the document provides national stakeholders with an overview of the major standardization organizations active in the field, both at the European and international levels, and details the published standards and ongoing projects aimed at advancing quantum communication.

Indeed, one of ILNAS' missions, as stated in the Luxembourg Standardization Strategy 2024-2030, is to actively promote the use of standards as they are published, to benefit from these effects as early as possible. To this end, ILNAS communicates regularly on standardization updates, disseminating the information of the publication of new standards and technical committee activities. This is done through different channels, such as news items available on the Portail-Qualite.lu, reports and white papers, or national standards analyses (such as the Standards Analysis of the ICT sector), developed with the support of ANEC GIE.

Finally, the report details valuable insights into the standardization landscape specific to Luxembourg, outlining the opportunities for individuals and organizations to actively participate in standards development. ILNAS can indeed register national delegates in standardization, in the technical committees of ISO, IEC, CEN, and CENELEC free of charge, so that they may make their voices heard and their ideas accepted in upcoming normative documents. In addition, ILNAS, as the National Standards Body representing Luxembourg in ETSI, strongly encourages any interested national organization to become a member of ETSI in order to take part in the development of important ICT standards that will participate in designing the future of new technologies. Since quantum technologies are still at an early stage, notably in terms of standardization, now is the best time to take part in these opportunities.

References

[1] "Azure Quantum | Superposition." Accessed: Oct. 10, 2024. [Online]. Available: https://quantum.microsoft.com/en-us/insights/education/concepts/superposition

[2] A. Muller, "What is quantum entanglement? A physicist explains Einstein's "spooky action at a distance,"" Astronomy Magazine. Accessed: Jul. 12, 2023. [Online]. Available: https://www.astronomy.com/science/what-is-quantum-entanglement-a-physicist-explains-einsteins-spooky-action-at-a-distance/

[3] "Quantum Entanglement: What is it & Why is it Important in 2023?" Accessed: Aug. 25, 2023. [Online]. Available: https://research.aimultiple.com/quantum-computing-entanglement/

[4] B. Martin, "Quantum Computing: Revolutionizing the Future of AI," Medium. Accessed: Oct. 12, 2023. [Online]. Available: https://medium.com/@BobMartin89/quantum-computing-revolutionizing-the-future-of-ai-13f6a9cbf254

[5] A. Ahmed, "Shor's Algorithm deepdive: Revolutionizing Factorization in Quantum Computing — Part 5," Medium. Accessed: Oct. 10, 2024. [Online]. Available: https://medium.com/@ashfaqe.sa12/shors-algorithm-deepdive-revolutionizing-factorization-in-quantum-computing-part-5-bdff7467d72b

[6] N. A. of S. Medicine Engineering, and, D. on E. and P. Sciences, I. C. S. Board, C. S. and T. Board, and C. on T. A. of the F. and I. of Q. Computing, "Quantum Computing: Progress and Prospects". National Academies Press, 2019.

[7] "Dive into the Quantum Realm: Promise of Quantum Communication and What's Next! | IEEE Communications Society." Accessed: Sep. 16, 2024. [Online]. Available: https://www.comsoc.org/publications/ctn/dive-quantum-realm-promise-quantum-communication-and-whats-next

[8] "What is No-Cloning Theorem." Accessed: Oct. 28, 2024. [Online]. Available: https://www.quera.com/glossary/no-cloning-theorem

[9] S. R. M and C. M. B, "Comprehensive Analysis of BB84, A Quantum Key Distribution Protocol," Dec. 09, 2023, arXiv: arXiv:2312.05609. Accessed: Oct. 28, 2024. [Online]. Available: http://arxiv.org/abs/2312.05609

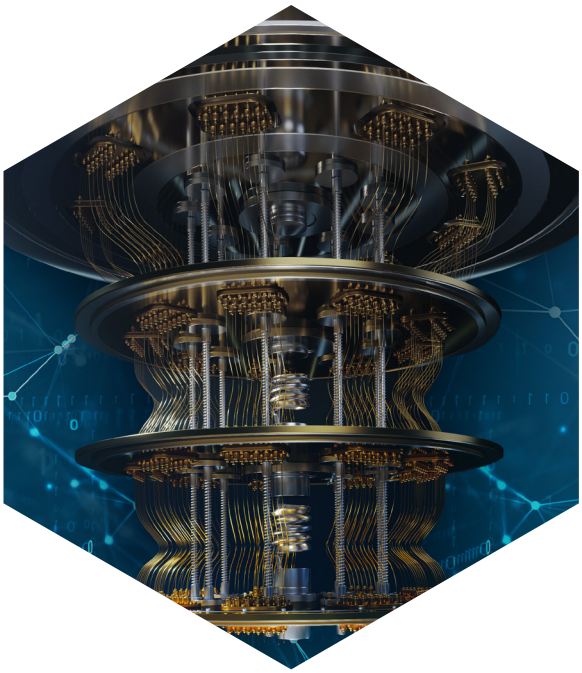
[10] T. Schmaltz et al., "Monitoring Report 1 - Quantum Communication," Fraunhofer ISI, 2024. doi: 10.24406/PUBLICA-3285.

[11] "Quantum Key Distribution (QKD): Safeguarding for the Future | IEEE Communications Society." Accessed: Oct. 28, 2024. [Online]. Available: https://www.comsoc.org/publications/ctn/quantum-key-distribution-qkd-safeguarding-future

[12] "Quantum Decoherence: The Loss of Quantum Information and Its Impact on Quantum Computing," SolveForce Fiber Internet, Cloud Computing & Telecommunications. Accessed: Oct. 22, 2024. [Online]. Available: https://solveforce.com/quantum-decoherence-the-loss-of-quantum-information-and-its-impact-on-quantum-computing/

[13] "European Standards," CEN-CENELEC. Accessed: Oct. 18, 2023. [Online]. Available: https://www.cencenelec.eu/european-standardization/european-standards/

[14] CEN-CENELEC Focus Group and on Quantum Technologies (FGQT), "Standardization Roadmap on Quantum Technologies." CEN-CENELEC Focus Group on Quantum Technologies (FGQT), 2023.



Please fill out the satisfaction survey

https://gd.lu/bJ6RbB

November 2024 · TECHNICAL STANDARDIZATION · QUANTUM COMMUNICATION AND TECHNICAL STANDARDIZATION · VERSION 1.0 · © ILNAS/ANEC · ISBN 978-99987-734-5-5

ILNAS
Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services

ANEC
Agence pour la Normalisation et l'Economie de la Connaissance

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux · Tel. : (+352) 24 77 43 -70 · Fax : (+352) 24 79 43 -70 · E-mail : normalisation@ilnas.etat.lu

www.portail-qualite.lu