Norm / Standard	Title	Institute	Focus Group	Source (File)	Most recent version	(upcoming) Release	Scope	Comment
FGQT Q01	Terms of Reference (ToR)	**CEN-CENELEC**	CEN/CLC/JTC 22 – FGQT	https://www.cen	(Jul 2020)	Latest	The purpose of the FGQT is be to ensure interaction, such as workshops, between all relevant European stakeholders interested in potential standardization in the field of QT to map ongoing standardization activities, define needs and opportunities and recommend further action to ensure that standards support the deployment of QT in industry. The FGQT does not develop standardization deliverables.	
FGQT Q02	Work Programme - Call for Participation	**CEN-CENELEC**	CEN/CLC/JTC 22 – FGQT	https://www.cen	–	Latest	One-pager to call for participation	
FGQT Q03	Towards Standardization for Quantum Technologies	**CEN-CENELEC**	CEN/CLC/JTC 22 – FGQT	https://www.cen	–	Latest	This text provides some of the central ideas underlying the FGQT Standardization Roadmap. It gives a more detailed insight and accompanies the FGQT Work Programme (FGQT Q02). Its purpose is to encourage people to read, comment, and further improve the FGQT Standardization Roadmap (FGQT Q04).	
FGQT Q04	Standardization Roadmap on Quantum Technologies	**CEN-CENELEC**	CEN/CLC/JTC 22 – FGQT	https://www.cen	(Mar 2023)	Latest	This document outlines the activities of the Focus Group on Quantum Technologies (FGQT) established by the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC). Over 100 experts initially joined, with around 200 experts participating in 30 meetings, covering various doMayns of quantum technologies. The document aims to inform about standardization needs, opportunities, and ongoing activities related to quantum technologies, encouraging participation from National Standardization Bodies. The roadmap document is structured into chapters: historical milestones and challenges, the role of quantum technologies in the economy, and the ecosystem of standardization. It delves into broad classes of quantum technologies, types of standards, ongoing standardization platforms, and examples of standardization areas. Enabling technologies like nanodiamond color centers and superconducting quantum circuits are discussed, along with quantum technology components and subsystems. Specific analysis is provided for quantum communication, computing, simulation systems, and quantum metrology. The document concludes with a description of the composite system of the quantum internet and an outlook on future steps.	
FGQT Q05	Quantum Technologies Use Cases	**CEN-CENELEC**	CEN/CLC/JTC 22 – FGQT	https://www.cen	(Mar 2023)	Latest	The use cases presented in this document are unstructured, both in topic and in the readiness or impli- cation on standardization. Each subsection contains a separate use case and starts with a description, enabling technologies and standardization needs. Some use cases follow with a deeper discussion of the aspects where standards are needed or might be beneficial.	
FG QIT4N D1.1	QIT4N terminology: Network aspects of QITs	**ITU-T**	FG-QIT4N	https://www.itu.i	(Nov 2021)	Latest	This technical report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N). Based on existing work of various Standards Development Organizations (SDOs) and academic literature, it surveys terminology on network aspects of quantum information technology, studies their overlap and divergence and provides a list of terms that are required but are yet to be standardized. Future efforts to standardize terminology on network aspects of quantum information technology could be informed by this technical report.	
FG QIT4N D1.2	QIT4N use cases: Network aspects of QITs	**ITU-T**	FG-QIT4N	https://www.itu.i	(Nov 2021)	Latest	This technical report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N). It sorts and analyses QIT for network use cases gathered during the lifetime of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N). The uses cases which are only applied by QITs are collected, investigated and summarized; all use cases are analysed by current bottlenecks, application scenarios, technical requirements and solutions. This Technical Report also provides analyses and suggestions for future applications and potential standardization requirements.	
FG QIT4N D1.4	Standardization outlook and technology maturity: Network aspects of QITs	**ITU-T**	FG-QIT4N	https://www.itu.i	(Nov 2021)	Latest	This technical report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N). It provides: • a snapshot of the standardization landscape of quantum information technology (QIT) for networks; • prospects and barriers to the development and adoption of standards for QIT for networks; • a review of methodologies for assessing technology maturity and standardization readiness of QIT for networks. This document studies the standardization outlook and technology maturity of quantum information technologies which either comprise or impact the requirements for a quantum information network (QIN), at the period of performance of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N).	
FG QIT4N D2.1	QIT4N terminology: QKDN	**ITU-T**	FG-QIT4N	https://www.itu.i	(Nov 2021)	Latest	This technical report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N). This technical report provides a survey of terminology relevant to QKDN currently published or under development by SDOs including ETSI ISG QKD, ISO/IEC JTC1 SC27 WG3 and ITU-T SG13/17. Based on the survey, the terms are categorized according to the specific technical directions they fall under.	
FG QIT4N D2.2	QIT4N use cases: QKDN	**ITU-T**	FG-QIT4N	https://www.itu.i	(Nov 2021)	Latest	This Technical Report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N). It consolidates the QKDN use cases gathered during the lifetime of the ITU-T FG QIT4N. The QKDN uses cases are classified into 6 classes and the report highlights the competitive advantage of the use cases brought by QKDN and provides suggestions for future standardization efforts.	
FG QIT4N D2.3	QKDN protocols: Key management layer, QKDN control layer and QKDN mai	**ITU-T**	FG-QIT4N	https://www.itu.i	(Nov 2021)	Latest	This technical report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N) which studies and reviews protocols in the quantum layer of a quantum key distribution network (QKDN). It mainly focuses on quantum key distribution (QKD) protocols in the quantum layer, where QKD is an essential part of the QKDN and is an emerging technology expected to strengthen the security of the current communication network. This technical report endeavours to give an overall review of the QKD protocols, including different types of QKD protocols, their workflows, protocol features, parameters, commercialization status. For this reason, it briefly discusses the security of QKD, specifically the security of protocols in their relation to real world QKD systems. More generally, this technical report discusses the potential of integration of QKD in future networks and provides an overview of considerations and suggestions for future work on QKDN protocols.	
FG QIT4N D2.3-part 1	QKDN protocols: Quantum layer	**ITU-T**	FG-QIT4N	https://www.itu.i	(Nov 2021)	Latest	This technical report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N) which studies classical communication protocols in the quantum key distribution network (QKDN) which include protocols with respect to the key management layer, QKDN control layer, and QKDN management layer. The QKDN protocols are classified into different layers according to main functions of each layer. Representative operational procedures and corresponding message parameters are given for some protocols.	
FG QIT4N D2.4	QKDN transport technologies	**ITU-T**	FG-QIT4N	https://www.itu.i	(Nov 2021)	Latest	This technical report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N) which discusses QKDN transport technologies such as transport system components, technical solutions, the typical scenarios of the co-existence of quantum and classical signals in a common fibre (CEQC). Analysis about the impact of the classic optical light on the quantum signals is given. Furthermore, some CEQC schemes are shown in the document, both for DV-QKD system and CV-QKD.	
FG QIT4N D2.5	QKDN standardization outlook and technology maturity	**ITU-T**	FG-QIT4N	https://www.itu.i	(Nov 2021)	Latest	This Technical Report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N). It provides an overview of quantum key distribution (QKD) technology, including frontier research, system experiment, field trial, and commercialized product. It conducts a summary of QKD industry status, including market players such as system vendor, network provider, and end user, project and opinions from different country and region, and other aspects. It contains QKD network standardization landscape, conducts gap analysis, and provides future standardization suggestions.	
TR.qs-dlt	Guidelines for quantum-safe distributed ledger technology systems	**ITU-T**	ICT Security	https://www.itu.i	V1.0 (Sep 2023)	Latest	This Technical Report provides guidelines for quantum-safe distributed ledger technology (DLT) systems, including: – security assessments of cryptographic algorithms used in current DLT systems when large-scale quantum computers are available; – construction requirements and guidelines for a quantum-safe DLT system; and – measures for migration at the cryptographic algorithm level from the current to a quantum-safe DLT system.	
XSTR-HYB-QKD	Overview of hybrid approaches for key exchange with QKD	**ITU-T**	ICT Security	https://www.itu.i	V1.0 (May 2022)	Latest	This Technical Report provides a landscape of the standardization activities on hybrid approaches for migration towards quantum-safe algorithms or protocols within international, regional and national organizations. The hybrid approach that is covered by this Technical Report is for key exchange. Hybrid approaches for key exchange consist of generating a key exchange functionality by combining at least two different key exchange methods. This Technical Report studies the possible way forward to accommodate quantum key distribution protocols in the context of hybrid approaches for key exchange. This compatibility is studied for generic hybrid key exchange and hybrid key exchange that is specific to certain communication protocols.	
FIPS 203	Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)	**NIST**	Information Technology Labor	https://doi.org/10	Published (Aug 2024)	Latest	A key-encapsulation mechanism (KEM) is a set of algorithms that, under certain conditions, can be used by two parties to establish a shared secret key over a public channel. A shared secret key that is securely established using a KEM can then be used with symmetric-key cryptographic algorithms to perform basic tasks in secure communications, such as encryption and authentication. This standard specifies a key-encapsulation mechanism called ML-KEM. The security of ML-KEM is related to the computational difficulty of the Module Learning with Errors problem. At present, ML-KEM is believed to be secure, even against adversaries who possess a quantum computer. This standard specifies three parameter sets for ML-KEM. In order of increasing security strength and decreasing performance, these are ML-KEM-512, ML-KEM-768, and ML-KEM-1024.	
FIPS 204	Module-Lattice-Based Digital Signature Standard (ML-DSA)	**NIST**	Information Technology Labor	https://doi.org/10	Published (Aug 2024)	Latest	Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation since the signatory cannot easily repudiate the signature at a later time. This standard specifies ML-DSA, a set of algorithms that can be used to generate and verify digital signatures. ML-DSA is believed to be secure, even against adversaries in possession of a large-scale quantum computer.	
FIPS 205	Stateless Hash-Based Digital Signature Standard (SLH-DSA)	**NIST**	Information Technology Labor	https://doi.org/10	Published (Aug 2024)	Latest	This standard specifies the stateless hash-based digital signature algorithm (SLH-DSA). Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation since the signatory cannot easily repudiate the signature at a later time. SLH-DSA is based on SPHINCS+, which was selected for standardization as part of the NIST Post-Quantum Cryptography Standardization process.	
ETSI GR QKD 003	QKD – Components and Internal Interfaces	**ETSI**	ISG on QKD	https://portal.ets	V2.1.1 (Mar 2018)	Latest	The present document is a preparatory action for the definition of properties of components and internal interfaces of QKD Systems. Irrespective of the underlying technologies, there are certain devices that appear in most QKD Systems. These are e.g. quantum physical devices such as photon sources and detectors, or classical equipment such as protocol processing computer hardware and operating systems. For these components, relevant properties should be identified that will subsequently be subject to standardization. Furthermore, a catalogue of relevant requirements for interfaces between components should be established, to support the upcoming definition of internal interfaces.	
ETSI GR QKD 007	QKD – Vocabulary	**ETSI**	ISG on QKD	https://www.etsi.	V1.1.1 (Dec 2018)	**Drafting - V2.1.1 (TBA 01.12.2024)**	The present document collects together definitions and abbreviations used in relation to Quantum Key Distribution (QKD) and ETSI ISG-QKD documents. QKD introduces new concepts and technologies to the field of telecommunications and considerable related vocabulary. Many terms derive from the wider fields of quantum physics and classical cryptography but in some cases terms assume a modified or more specific meaning when applied to QKD. The Mayn objectives of the present document are: • to improve the consistency with which terminology and abbreviations are used within ISG-QKD documents; • to provide a reference document to reduce confusion by readers who may not be familiar with QKD. Most definitions and abbreviations come from ISG-QKD Group Specifications and Group Reports or are expected to be used in future documents. The terms included have been selected to focus the present document on those that are expected to be of widespread use or where consistency is felt to be particularly important, e.g. due to a specific risk of confusion. Terms introduced in a single ISG-QKD document for a specific purpose that is local to that document are excluded unless of particular importance.	
ETSI GS QKD 002	QKD – Use Cases	**ETSI**	ISG on QKD	https://portal.ets	V1.1.1 (Jun 2010)	Latest	The Use Cases Document shall provide an overview of possible application scenarios in which Quantum Key Distribution (QKD) systems can be used as building blocks for high security information and communication technology (ICT) systems.	

ETSI GS QKD 004	QKD – Application Interface	ETSI	ISG on QKD	https://www.etsi. V2.1.1 (Aug 2020)	Drafting - V3.1.1 (TBA 11.08.2025)	The present document is intended to specify an Application Programming Interface (API) between a QKD key manager and applications. The function of a QKD key manager is to manage the secure keys produced by an implementation of a QKD protocol and to deliver the identical set of keys, via this API, to the associated applications at the communication end points.	
ETSI GS QKD 005	QKD – Security Proofs	ETSI	ISG on QKD	https://www.etsi. V1.1.1 (Dec 2010)	Drafting - V2.1.1 (TBA 15.01.2025)	The goals of the present document are as follows: • to make precise the nature of the security claim, including its statistical component; • to list meaningful restrictions of adversarial action; • to clarify the difference between security claim of a protocol (based on models) and the security claim of its implementation; • to carefully list all the usual components of a QKD protocol with their critical characterizations. The present document is developed by the QKD ISG group in which participate experts of QKD theory and practice. With the goals identified above, the present document shall help to: • clarify the role QKD devices can play in a security infrastructure given the exact nature of their security claim; • classify QKD devices regarding the security level they can achieve; • clarify which parameters need to be monitored continuously or periodically to assure the generation of a secret key for the different security levels. On the other hand, the present document will not try to do the following: • to give specific parameters for successful QKD as these numbers change with time; • to endorse particular security proofs.	
ETSI GS QKD 008	QKD – QKD Module Security Specification	ETSI	ISG on QKD	https://portal.ets V1.1.1 (Dec 2010)	Latest	The present document aims to establish the necessary requirements for a QKD module to have a high probability of detecting and responding precisely and timely to attempts of direct physical access, and use or modification of modules inside. The principal objective is to detect any possible penetration with high probability, and resulting in the immediate zeroization of all Critical Security Parameters in plain text.	
ETSI GS QKD 010	QKD – Implementation security: protection against Trojan horse attacks	ETSI	ISG on QKD	https://docbox.et V0.4.1 (Jun 2021)	Drafting - V1.1.1 (TBA 11.12.2024)	The present document specifies protection of QKD modules against Trojan horse attacks launched against a time-varying phase, polarisation or intensity modulator that encodes or decodes at least one of bit values, basis values or the intensities of signal, decoy or vacuum states from the quantum channel.	
ETSI GS QKD 011	QKD – Component characterization: characterizing optical components for	ETSI	ISG on QKD	https://portal.ets V1.1.1 (May 2016)	Latest	The present document gives specifications and procedures for the characterization of optical components for use in QKD systems. Examples of specific tests and procedures for performing such tests are given. Due to their importance in the security of a QKD system, particular attention is given to active optical components such as optical sources and single photon detectors.	
ETSI GS QKD 012	QKD – Device and Communication Channel Parameters for QKD Deploymer	ETSI	ISG on QKD	https://portal.ets V1.1.1 (Feb 2019)	Latest	The present document describes the Mayn communication resources involved in a QKD system and the possible architectures that can be adopted when performing a QKD deployment over an optical network infrastructure. The scope of the present document is restricted to QKD deployments over fibre optical networks. Architectural options are also restricted to point-to-point communication. The different entities that can take part in a QKD deployment and the possible contexts of deployment capturing the roles played by the different entities are defined. One specific context (context1) is then addressed where one entity (QKD_O), operating QKD Modules, plans a QKD deployment over an optical network infrastructure, operated by another entity (NET_O). The information regarding the QKD system parameters and the network parameters to be exchanged (in context1) are listed and prioritized. The corresponding tables, placed at the end of the present document, can be used as a standard template for the exchange of information between QKD_O entities and NET_O entities involved in the QKD deployment.	
ETSI GS QKD 013	QKD – Characterisation of Optical Output of QKD transmitter modules	ETSI	ISG on QKD	https://portal.ets V0.1.4 (May 2024)	Drafting - V1.1.1 (TBA 22.01.2025)	The present document defines procedures for characterising specific properties of complete QKD transmitter modules. These procedures shall be limited to characterising the signals emitted by the transmitter under operational conditions.	Standard not ready for download
ETSI GS QKD 014	QKD – Protocol and data format of REST-based key delivery API	ETSI	ISG on QKD	https://www.etsi. V1.1.1 (Feb 2019)	Drafting - V2.1.1 (TBA 01.12.2024)	The present document specifies a communication protocol and data format for a quantum key distribution (QKD) network to supply cryptographic keys to an application. It is in the form of an API (Application Programming Interface) that allows application developers to make simple method calls to a QKD network and to be delivered key material. It is intended to allow interoperability of equipment from different vendors. The QKD network can consist of a single link between a single QKD transmitter and a single QKD receiver, or it can be an extended network involving many such QKD links. The API defines a single interface for the delivery of key material to applications in both scenarios. It is beyond the scope of the present document to describe how a QKD network generates key material shared between distant nodes.	
ETSI GS QKD 015	QKD – Control Interface for Software Defined Networks	ETSI	ISG on QKD	https://www.etsi. V2.1.1 (Apr 2022)	Drafting - V3.1.1 (TBA 26.08.2025)	The present document provides a definition of management interfaces for the integration of QKD in disaggregated network control plane architectures, in particular with Software-Defined Networking (SDN). It defines abstraction models and workflows between an SDN-enabled QKD node and the SDN controller, including resource discovery, capabilities dissemination and system configuration operations. Application layer interfaces and quantum-channel interfaces are out of scope.	
ETSI GS QKD 016	QKD – Common Criteria Protection Profile - Pair of Prepare and Measure QK	ETSI	ISG on QKD	https://www.etsi. V2.1.1 (Jan 2024)	Latest	The present document specifies a Protection Profile (PP) for the security evaluation of pairs of Quantum Key Distribution (QKD) modules under the Common Criteria for Information Technology Security Evaluation (CC v3.1 rev5). The present document is applicable to a pair of QKD modules operating a prepare and measure QKD protocol that can form a complete QKD system when connected by an appropriate point-to-point QKD link. The PP specifies high-level requirements for the physical implementation through to the output of final secret keys.	
ETSI GS QKD 017	QKD – Network architectures	ETSI	ISG on QKD	https://portal.ets V0.1.12 (Nov 2023)	Drafting - V1.1.1 (vrsl. 15.01.2025)	This work item will review the variety of architectures that have been proposed for QKD networking. It will further aim to reveal the basic functionalities that the mentioned architectures implement as well as the commonalities between the architectures.	Standard not ready for download
ETSI GS QKD 018	QKD – Orchestration Interface for Software Defined Networks	ETSI	ISG on QKD	https://portal.ets V1.1.1 (Apr 2022)	Latest	The present document provides a definition of an orchestration interface between an SDN orchestrator and an SDN controller of a QKD network. This orchestration interface defines the abstract information models and workflows for QKD network resource management, configuration management, performance management, service provisioning, notifications and management of multi-doMayn QKD networks. Interfaces between an SDN orchestrator and SDN controllers of classical optical transport networks are out of scope.	
ETSI GS QKD 019	QKD – Design of QKD interfaces with Authentication	ETSI	ISG on QKD	https://portal.ets V0.1.6 (Aug 2024)	Drafting - V1.1.1 (TBA 05.11.2024)	This work item will be a technical report on the design of classical interfaces for QKD systems that include authentication, including protocols used in discussion channels, auxiliary channels, management interfaces and key delivery interfaces. Assumptions on long-term or physical security will be discussed. Research on information-theoretic secure (e.g. Wegman Carter) and symmetric authentication for QKD discussion channels will be reviewed as well as the use of other cryptographic algorithms (including public key) to augment protocols. Standard principles, frameworks and analytical tools from the cryptographic doMayn will be considered. Design principles specific to authenticated QKD, including protection of authentication keys against denial of service attacks, will be discussed citing existing literature.	Standard not ready for download
ETSI GS QKD 020	QKD – Protocol and data format of REST-based Interoperable Key Manageme	ETSI	ISG on QKD	https://portal.ets V0.4.1 (Aug 2024)	Drafting - V1.1.1 (TBA 01.12.2024)	This work item will specify a REST API that allows key management systems to interoperate to pass keys horizontally between two systems located in a common trusted node. The API will enable QKD networks to serve applications that request shared secret keys from key management systems that are not linked by a contiguous chain of systems from the same vendor. It is beyond the scope of the document to describe how the underlying QKD network agrees key material between nodes. URI formats, communication protocols (HTTPS), and the JSON data format encoding of posted parameters and responses (including key material) will be described. An OpenAPI description of the API will be included.	Standard not ready for download
ETSI GS QKD 021	QKD – Orchestration Interface of Software Defined Networks for Interoperat	ETSI	ISG on QKD	https://portal.ets V0.0.1 (May 2023)	Drafting - V1.1.1 (TBA 12.05.2025)	This work item deals with the interface between the SDN Orchestrator and the SDN Controller of QKD networks for cooperating key management systems. It defines abstraction models and workflows between the SDN Orchestrator and SDN Controller of QKD networks, including resource management, system configuration management, performance management, alarm, service provisioning, and management of multi-doMayn QKD networks to allow for the operation and management of multi-doMayn E2E key usage patterns.	Standard not ready for download
ETSI GS QKD 022	QKD – Network Architecture	ETSI	ISG on QKD	https://portal.ets V0.0.1 (May 2023)	Drafting - V1.1.1 (TBA 11.09.2025)	This work item will specify a QKD network architecture building on analysis in DGR/QKD-017NwkArch (GR QKD 017). It will identify network functionalities and interfaces aligned with modern communication networking paradigms suitable for both stand-alone critical infrastructures and integration with general telecommunications networks.	Standard not ready for download
ETSI GS QKD 023	QKD – Monitoring Interface and Data Model	ETSI	ISG on QKD	https://portal.ets V0.0.2 (May 2023)	Drafting - V1.1.1 (TBA 14.03.2025)	This work item will provide an interface and data model definition for QKD monitoring, consistent with the existing approved interfaces. It will define monitoring and telemetry interactions with QKD modules, covering information about the modules and the link(s) attached to them.	Standard not ready for download
ETSI GR QSC 001	QSC – Quantum-safe algorithmic framework	ETSI	ISG on QSC	https://portal.ets V1.1.1 (Jul 2016)	Latest	The present document gives an overview of the current understanding and best practice in academia and industry about quantum-safe cryptography (QSC). It focuses on identifying and assessing cryptographic primitives that have been proposed for efficient key establishment and authentication applications, and which may be suitable for standardization by ETSI and subsequent use by industry to develop quantum-safe solutions for real-world applications.	
ETSI GR QSC 003	QSC – Case Studies and Deployment Scenarios	ETSI	ISG on QSC	https://portal.ets V1.1.1 (Feb 2017)	Latest	The present document examines a number of real-world uses cases for the deployment of quantum-safe cryptography (QSC). Specifically, it examines some typical applications where cryptographic primitives are deployed today and discusses some points for consideration by developers, highlighting features that may need change to accommodate quantum-safe cryptography. The Mayn focus of the document is on options for upgrading public-key primitives for key establishment and authentication, although several alternative, non-public-key options are also discussed.	
ETSI GR QSC 004	QSC – Quantum-Safe threat assessment	ETSI	ISG on QSC	https://portal.ets V1.1.1 (Mar 2017)	Latest	The present document presents the results of a simplified threat assessment following the guidelines of ETSI TS 102 165-1 [i.3] for a number of use cases. The method and key results of the analysis is described in clause 4.	
ETSI GR QSC 006	QSC – Limits to Quantum Computing applied to symmetric key sizes	ETSI	ISG on QSC	https://portal.ets V1.1.1 (Feb 2017)	Latest	The present document concludes that there are existing and widely used symmetric (AES-256) and hash primitives (SHA-2 and SHA-3 with an output length of at least 256 bits) that will withstand quantum computer attacks until way after 2050.	
ISO / IEC 23837-1:2023	Information security – Security requirements, test and evaluation methods f	ISO / IEC	JTC 1 SC 27	https://www.iso.c Edt 1 (Aug 2023)	Latest	The ISO/IEC 23837 series specifies the security requirements, test and evaluation methods for quantum key distribution (QKD) under the framework of the ISO/IEC 15408 series. This document focuses on specifying the common baseline set of security functional requirements (SFRs) of QKD modules.	Behind paywall
ISO / IEC 23837-2:2023	Information security – Security requirements, test and evaluation methods f	ISO / IEC	JTC 1 SC 27	https://www.iso.c Edt 1 (Sep 2023)	Latest	The ISO/IEC 23837 series specifies security requirements, test and evaluation methods for quantum key distribution (QKD) modules under the framework of the ISO/IEC 15408 series. This document specifies an evaluation method and relevant evaluation activities for the security evaluation of QKD modules in a relatively general way. The evaluation activities that are necessary for the security evaluation of QKD modules include supplementary evaluation activities for the QKD-related security functional requirements (SFRs) specified in ISO/IEC 23837-1 and the supplementary evaluation activities for security assurance requirements (SARs) with security assurance levels ranging from evaluation assurance level (EAL) 1 to EAL 5+.	Behind paywall
ISO / IEC 4879:2024	Information technology — Quantum computing — Vocabulary	ISO / IEC	JTC 1 WG 14	https://www.iso.c Edt 1 (May 2024)	Latest		Behind paywall
P7131	Standard for Quantum Computing Performance Metrics & Performance Ben	IEEE	QCB-WG - Quantum Computi	https://standards –	Drafting (PAR Approval Sep 2023)	The standard covers quantum computing performance metrics for standardizing performance benchmarking of quantum computing hardware and software. These metrics and performance tests include everything necessary to benchmark quantum computers (stand alone and by/for comparison) and to benchmark quantum computers against classical computers using a methodology that accounts for factors such as dedicated solvers.	

P7130	Standard for Quantum Computing Definitions	IEEE	QCN-WG - Quantum Comput	https://standards	–	Drafting (PAR Approval Sep 2023)	This standard addresses quantum technologies specific terminology and establishes definitions necessary to facilitate clarity of understanding to enable compatibility and interoperability.	
P1913	YANG Model for Software-Defined Quantum Communication	IEEE	QuantumComm - Software-D	https://standards	–	Drafting (PAR Approval Dec 2022)	This standard defines the Software-Defined Quantum Communication (SDQC) protocol that enables configuration of quantum endpoints in a communication network in order to dynamically create, modify, or remove quantum protocols or applications.	
P1943	Standard for Post-Quantum Network Security	IEEE	QuNET/WG - Post-Quantum N	https://standards	–	Drafting (PAR Approval Jun 2021)	This standard defines a post-quantum optimized version of network security protocols. It is based on a multi-layer protocols approach and allows data packets to be quantum resistant to future cryptographically relevant quantum computers (CRQCs).	
P3172	Recommended Practice for Post-Quantum Cryptography Migration	IEEE	QuSEC/WG - Quantum Securi	https://standards	–	Drafting (PAR Approval May 2022)	This recommended practice describes multi-step processes that can be used to implement hybrid mechanisms (combinations of classical quantum-vulnerable and quantum-resistant public-key algorithms). Existing post-quantum cryptography (PQC) systems are described. Desired characteristics of the hybrid mechanisms, such as crypto agility are also described.	
Q.4160	QKD networks - Protocol framework	ITU-T	SG 11	https://www.itu.i	V1.0 (Dec 2023)	Latest	Recommendation ITU-T Q.4160 specifies a framework for signalling and protocols for quantum key distribution network (QKDN).	
Q.4161	Protocols for Ak interface for QKD network	ITU-T	SG 11	https://www.itu.i	V1.0 (Dec 2023)	Latest	Recommendation ITU-T Q.4161 specifies protocols for Ak interfaces in quantum key distribution networks.	
Q.4162	Protocols for Kq-1 interface for QKD network	ITU-T	SG 11	https://www.itu.i	V1.0 (Dec 2023)	Latest	Recommendation ITU-T Q.4162 specifies protocols for Kq-1 interfaces in quantum key distribution networks.	
Q.4163	Protocols for Kx interface for QKD network	ITU-T	SG 11	https://www.itu.i	V1.0 (Dec 2023)	Latest	Recommendation ITU-T Q.4163 specifies protocols for Kx interfaces for quantum key distribution networks.	
Q.4164	Protocols for Ck interface for QKD network	ITU-T	SG 11	https://www.itu.i	V1.0 (Dec 2023)	Latest	Recommendation ITU-T Q.4164 specifies protocols for Ck interfaces in quantum key distribution networks.	
Y.3800	Overview on networks supporting QKD	ITU-T	SG 13	https://www.itu.i	V1.1 (Apr 2020)	Latest	This Recommendation is an overview that provides basic QKDN conceptual structures with a clear security boundary. This is the first Recommendation of a series of QKDN Recommendations that cover various aspects such as network architectures and network security. Requirements will be for further study.	
Y.3801	Functional requirements for QKD networks	ITU-T	SG 13	https://www.itu.i	V1.1 (Apr 2020)	Latest	In the context of quantum key distribution networks (QKDNs), Recommendation ITU-T Y.3801 specifies the functional requirements for quantum layer, the key management layer, the QKDN control layer and the QKDN management layer.	
Y.3802	QKD networks – Functional architecture	ITU-T	SG 13	https://www.itu.i	V1.2 (Nov 2023)	Latest	Recommendation ITU-T Y.3802 defines a functional architecture model of quantum key distribution (QKD) networks. In order to realize this model, it specifies detailed functional elements and reference points, architectural configurations and basic operational procedures of QKD networks (QKDN).	
Y.3803	QKD networks – Key management	ITU-T	SG 13	https://www.itu.i	V1.1 (Nov 2023)	Latest	Recommendation ITU-T Y.3803 provides help for the design, deployment, and operation of key management of a quantum key distribution network (QKDN).	
Y.3804	QKD networks – Control and management	ITU-T	SG 13	https://www.itu.i	V1.1 (Nov 2023)	Latest	To realize secure, stable, efficient, and robust operations of and services by a quantum key distribution (QKD) network as well as to manage a QKD network (QKDN) as a whole and support user network management, Recommendation ITU-T Y.3804 specifies functions and procedures for QKDN control and management based on the requirements specified in Recommendation ITU-T Y.3801.	
Y.3805	QKD networks – Software-defined networking control	ITU-T	SG 13	https://www.itu.i	V1.1 (Nov 2023)	Latest	Recommendation ITU-T Y.3805 specifies the requirements, functional architecture, reference points, hierarchical SDN controller and overall operational procedures of SDN control.	
Y.3806	QKD networks – Requirements for quality of service assurance	ITU-T	SG 13	https://www.itu.i	V1.0 (Sep 2021)	Latest	Recommendation ITU-T Y.3806 specifies the high-level and functional requirements of quality of service (QoS) assurance for quantum key distribution networks (QKDN). The functional requirements include QoS planning, QoS monitoring, QoS optimization, QoS provisioning, QoS protection and recovery.	
Y.3807	QKD networks – Quality of service parameters	ITU-T	SG 13	https://www.itu.i	V1.0 (Feb 2022)	Latest	Recommendation ITU-T Y.3807 describes QoS and network performance (NP) on QKDN and specifies the associated relative parameters for QoS and their definitions. This Recommendation helps to quantify what kind of QoS requirements should be monitored and measured for this purpose; QoS parameters.	
Y.3808	Framework for integration of QKD network and secure storage network	ITU-T	SG 13	https://www.itu.i	V1.0 (Feb 2022)	Latest	Recommendation ITU-T Y.3808 provides an overview of secure storage networks (SSNs) for quantum key distribution networks (QKDNs). It specifies the functional requirements, functional architecture model, reference points and operational procedures for SSNs.	
Y.3809	A role-based model in QKD networks deployment	ITU-T	SG 13	https://www.itu.i	V1.0 (Feb 2022)	Latest	Recommendation ITU-T Y.3809 describes roles, a role-based model and service scenarios in quantum key distribution networks (QKDN) from different deployment and operation perspectives within existing user networks for supporting security applications services. This Recommendation can be used as a guideline for applying QKDN from a role point of view as well as for deployment and operation of QKDN from a telecom operators' point of view.	
Y.3810	QKD network interworking – Framework	ITU-T	SG 13	https://www.itu.i	V1.0 (Sep 2022)	Latest	For quantum key distribution networks (QKDN), Recommendation ITU-T Y.3810 specifies the framework of QKDN interworking (QKDNi). This Recommendation describes the overview of interworking QKDNs, the reference models, and the functional models of gateway functions (GWFs) and interworking functions (IWFs). The configurations for QKDNi are specified. Appendix I includes QKDNi with different key relay schemes.	
Y.3811	QKD networks – Functional architecture for quality of service assurance	ITU-T	SG 13	https://www.itu.i	V1.1 (Nov 2023)	Latest	Recommendation ITU-T Y.3811 specifies the functional architecture of quality of service (QoS) assurance for the quantum key distribution networks (QKDNs). This Recommendation first provides an overview of the functional architecture of QoS assurance for the QKDN. It then describes the functional architecture of QoS assurance which includes functional entities such as QoS data collection, data processing, data storage, data analytics, QoS anomaly detection and prediction, QoS policy decision making, and enforcement and reporting. Based on the functional entities described in the functional architecture, this Recommendation specifies a basic operational procedure of QoS assurance for the QKDN.	
Y.3812	QKD networks – Requirements for machine learning based quality of service	ITU-T	SG 13	https://www.itu.i	V1.0 (Sep 2022)	Latest	Recommendation ITU-T Y.3812 specifies high-level and functional requirements of machine learning (ML) based quality of service (QoS) assurance for quantum key distribution networks (QKDNs). This Recommendation first provides an overview of requirements of ML based QoS assurance for the QKDN. It describes a functional model of ML based QoS assurance which is followed by associated high-level and functional requirements of ML based QoS assurance. Additionally, some use cases are described.	
Y.3813	QKD network interworking – Functional requirements	ITU-T	SG 13	https://www.itu.i	V1.0 (Jan 2023)	Latest	For quantum key distribution networks (QKDNs), Recommendation ITU-T Y.3813 specifies functional requirements for QKDN interworking (QKDNi). This Recommendation describes the functional requirements for the key management layer, QKDN control layer and QKDN management layer, for interworking using gateway nodes (GWNs) and/or interworking nodes (IWNs).	
Y.3814	QKD networks – Functional requirements and architecture for machine lear	ITU-T	SG 13	https://www.itu.i	V1.1 (Nov 2023)	Latest	A quantum key distribution network (QKDN) is expected to maintain stable operations and meet the requirements of various cryptographic applications efficiently. Due to the advantages of machine learning (ML) related to autonomous learning, it can help to overcome the challenges of QKDN in terms of quantum layer performances, key management layer performances and QKDN control and management efficiency. Based on the functional requirements and architecture of QKDN stated in Recommendations ITU-T Y.3801 and ITU-T Y.3802, this Recommendation specifies one possible set of functional requirements and a possible architecture for an ML-enabled QKDN (QKDNml), including an overview and the functional requirements, architecture and operational procedures of QKDNml.	
Y.3815	QKD networks – Overview of resilience	ITU-T	SG 13	https://www.itu.i	V1.0 (Sep 2023)	Latest	Recommendation ITU-T Y.3815 gives an overview of resilience and conceptual models of protection and recovery for quantum key distribution networks for seamless key supply even in the case of network failure.	
Y.3816	QKD networks – Functional architecture enhancement of machine learning	ITU-T	SG 13	https://www.itu.i	V1.0 (Sep 2023)	Latest	Recommendation ITU-T Y.3816 specifies functional architecture enhancement of quality of service (QoS) assurance based on machine learning (ML) for quantum key distribution networks (QKDNs). Recommendation ITU-T Y.3816 first provides an overview of functional architecture enhancement of ML-based QoS assurance for QKDNs. It then describes a functional architecture enhancement of QoS assurance that includes functional components such as QoS data collection, data processing, data storage, data analytics, QoS anomaly detection and prediction, QoS policy decision making, enforcement and reporting. Based on the capabilities described in the functional architecture enhancement, Recommendation ITU-T Y.3816 specifies an operational procedure of QoS assurance for QKDNs.	
Y.3817	QKD network interworking – Requirements for quality of service assurance	ITU-T	SG 13	https://www.itu.i	V1.0 (Sep 2023)	Latest	Recommendation ITU-T Y.3817 specifies high-level and functional requirements for quality of service (QoS) assurance for quantum key distribution network interworking. The functional requirements include QoS information transfer, QoS negotiation, QoS management and QoS routing.	
Y.3818	QKD network interworking – Architecture	ITU-T	SG 13	https://www.itu.i	V1.0 (Sep 2023)	Latest	Recommendation ITU-T Y.3818 specifies functional architecture models for quantum key distribution network interworking (QKDNi), i.e., functional architectures with gateway and interworking nodes. In order to realize these two models, Recommendation ITU-T Y.3818 specifies detailed functional elements, basic operational procedures and architectural configurations for QKDNi.	
Y.3819	QKD networks – Requirements and architectural model for autonomic mana	ITU-T	SG 13	https://www.itu.i	V1.0 (Dec 2023)	Latest	This Recommendation specifies one possible set of functional requirements and a possible architectural model for autonomic management and control (AMC)-enabled QKDN (QKDNamc). In particular, the scope of this Recommendation includes: – Overview of QKDNamc; – Requirements for QKDNamc; – Consideration for the cognition process of QKDNamc; – Architectural model for QKDNamc; – Example operational procedures of QKDNamc.	
Y.3820	QKD network interworking – Software-defined networking control	ITU-T	SG 13	https://www.itu.i	V1.0 (Apr 2024)	Latest	Recommendation ITU-T Y.3820 specifies the software-defined networking (SDN)-based quantum key distribution network (QKDN) interworking control between QKDN providers. It provides an overview of the role of SDN control for the interworking between QKDN providers, the functional requirements for an SDN controller for interworking, the functional entities of an SDN controller for interworking, the interfaces of an SDN controller for interworking, the operational procedures of an SDN controller for interworking, as well as any security considerations.	
Y.3821	QKD networks – Requirements for resilience	ITU-T	SG 13	https://www.itu.i	V1.0 (Apr 2024)	Latest	For quantum key distribution networks (QKDN), Recommendation ITU-T Y.3821 specifies the general requirements for resilience, and separately specifies the requirements for supporting protection and recovery.	
X.1702	Quantum noise random number generator architecture	ITU-T	SG 17	https://www.itu.i	V1.0 (Nov 2019)	Latest	Recommendation ITU-T X.1702 defines a generic functional architecture of a quantum entropy source, a common method to estimate and validate the entropy of a noise source under evaluation, and a common method to specify randomness extractors when they are part of the implemented system.	
X.1710	Security framework for QKD networks	ITU-T	SG 17	https://www.itu.i	V1.0 (Oct 2020)	Latest	Recommendation ITU-T X.1710 specifies a framework including requirements and measures to combat security threats for quantum key distribution networks (QKDNs). It specifies a simplified QKDN structure for analysis of the relevant security threats. Security requirements and corresponding security measures are then specified on that basis.	
X.1712	Security requirements and measures for QKD networks – key management	ITU-T	SG 17	https://www.itu.i	V1.1 (Feb 2022)	Latest	Recommendation ITU-T X.1712 specifies security threats and security requirements for key management in quantum key distribution networks (QKDNs), and security measures of key management to meet the security requirements. This Recommendation also provides support for the design, implementation, and operation of key management in QKDNs with approved security.	
X.1713	Security requirements for the protection of QKD nodes	ITU-T	SG 17	https://www.itu.i	V1.0 (Apr 2024)	Latest	Quantum key distribution (QKD) enables two remote parties to share a common random binary key that is unknown to a potential eavesdropper. QKD networks based on trusted nodes (QKD nodes) have been widely adopted to enlarge the key distribution distance and enrich QKD-based applications. The trustworthiness of a QKD node is fundamental to ensure the overall security in a QKD network. Recommendation ITU-T X.1713 provides guidance for the secure implementation and operation of QKD nodes in QKD networks. The Recommendation identifies security threats, provides security requirements for QKD nodes and provides specific techniques to meet the requirements.	
X.1714	Key combination and confidential key supply for quantum key distri-bution n	ITU-T	SG 17	https://www.itu.i	V1.0 (Oct 2020)	Latest	Recommendation ITU-T X.1714 describes key combination methods for quantum key distribution network (QKDN) and specifies security requirements for both the key combination and the key supply from QKDN to cryptographic applications.	
X.1715	Security requirements and measures for integration of QKD network and sec	ITU-T	SG 17	https://www.itu.i	V1.0 (Apr 2024)	Latest	Recommendation ITU-T X.1715 specifies security requirements and measures for integrating a quantum key distribution network (QKDN) with a secure storage network (SSN) in the service layer (Recommendation ITU-T Y.3800) and public key infrastructure (PKI) (Recommendation ITU-T X.509).	
XSTR-SEC-QKD	Security considerations for QKD network (Corrigendum)	ITU-T	SG 17	https://www.itu.i	V1.0 (Apr 2021)	Latest	This Technical Report only studies the perspective of QKD. Although QKD technologies have been developed for several decades, there is a need to develop a QKD framework to satisfy requirements from the telecom network's perspective.	Restricted to TIES users
ETSI EG 203 310	CYBER – Quantum Computing Impact on security of ICT Systems; Recomme	ETSI	TC CYBER QSC	https://portal.ets	V1.1.1 (Jun 2016)	Latest	The present document addresses business continuity arising from the concern that Quantum Computing (QC) is likely to invalidate the problems that lie at the heart of both RSA and ECC asymmetric cryptography. The present document considers the transition to the post-quantum era of how to re-assert CAs in a PKI, the distribution of new algorithms, and the distribution of new keys, and advises that business continuity planning addresses the impact of QC on ICT.	

ETSI TR 103 570	CYBER – Quantum-Safe Key Exchanges	**ETSI**	TC CYBER QSC	https://portal.ets V1.1.1 (Oct 2017)	Latest	The present document compares a selection of proposals for quantum-safe key exchanges taken from the academic literature. In particular, it includes key exchanges based on the Learning with Errors (LWE), Ring-LWE and Supersingular Isogeny Diffie-Hellman (SIDH) problems, as well as key exchanges constructed from the Niederreiter and NTRU key transport schemes.
ETSI TR 103 616	CYBER – Quantum-Safe Signatures	**ETSI**	TC CYBER QSC	https://www.etsi. V1.1.1 (Sep 2021)	Latest	The present document provides technical descriptions of the digital signature schemes submitted to the National Institute of Standards and Technology (NIST) for the third round of their post-quantum cryptography standardization process.
ETSI TR 103 617	Quantum-Safe Virtual Private Networks	**ETSI**	TC CYBER QSC	https://www.etsi. V1.1.1 (Sep 2018)	Latest	The present document explores protocol requirements necessary to add quantum resistance to VPN technologies, including client, server and architectural considerations. Specifically, requirements around protocols and key establishment are considered, based on the multitude of systems that are at risk and require security updates before quantum computers that can attack commercial cryptography are developed.
ETSI TR 103 618	CYBER – Quantum-Safe Identity-Based Encryption	**ETSI**	TC CYBER QSC	https://portal.ets V1.1.1 (Dec 2019)	Latest	The present document describes a proposal for a quantum-safe hierarchical identity-based encryption scheme. It gives an overview of the functionality provided by hierarchical identity-based encryption, outlines some example uses cases and provides a high-level description of a potential solution based on structured lattices. The description includes concrete proposals for parameter sets, estimates for performance in software and a practical security analysis.
ETSI TR 103 619	CYBER – Migration strategies and recommendations to Quantum Safe scher	**ETSI**	TC CYBER QSC	https://www.etsi. V1.1.1 (Jul 2020)	Latest	The present document addresses the problem of migration to an environment in a Fully Quantum Safe Cryptographic State (FQSCS) from a non-Quantum Safe Cryptographic State. The present document provides recommendations and guidance to ensure safe transition between the two (2) states.
ETSI TR 103 692	CYBER – State management for stateful authentication mechanisms	**ETSI**	TC CYBER QSC	https://portal.ets V1.1.1 (Nov 2021)	Latest	The present document is limited to discussion of the characteristics of the state object, the reuse of the state index, and of architectural and operational considerations for deploying stateful hash-based signatures. First, it discusses characteristics of the state object for S-HBS schemes and identifies potential security vulnerabilities and operational problems associated with its management. Second, it gives guidance on mitigating the issues identified. And third, it helps a prospective implementor determine if a S-HBS solution is suitable for their given application; examples of suitable and non-suitable applications are given.
ETSI TR 103 744	CYBER – Quantum-safe Hybrid Key Exchanges	**ETSI**	TC CYBER QSC	https://portal.ets V1.1.1 (Dec 2020)	Latest	The present document specifies several methods for deriving cryptographic keys from multiple shared secrets. The shared secrets are established using existing classical key agreement schemes, like elliptic curve Diffie-Hellman (ECDH) in NIST SP800-56Ar3 [1], and new quantum-safe key encapsulation mechanisms (KEMs).
ETSI TR 103 823	CYBER – Quantum-Safe Public-Key Encryption and Key Encapsulation	**ETSI**	TC CYBER QSC	https://portal.ets V1.1.2 (Oct 2021)	Latest	The present document provides technical descriptions of the Public-Key Encryption (PKE) and Key Encapsulation Mechanisms (KEMs) submitted to the National Institute for Standards and Technology (NIST) for the third round of their Post-Quantum Cryptography (PQC) standardization process.
ETSI TR 103 949	QSC – QSC Migration; ITS and C-ITS migration study	**ETSI**	TC CYBER QSC	https://portal.ets V1.1.1 (May 2023)	Latest	The present document reviews the state of deployment of cryptographic security mechanisms in Intelligent Transport Systems (ITS) and Cooperative Intelligent Transport Systems (C-ITS) and their susceptibility to attack by a quantum computer. The present document makes a number of recommendations regarding the adoption of Quantum Safe Cryptography in order to minimize the exposure of ITS and C-ITS to attack.