Norm / Standard

FGQT Q01

FGQT Q02

FGQT Q03

FGQT Q04

FGQT Q05

FG QIT4N D1.1

FG QIT4N D1.2

FG QIT4N D1.4

FG QIT4N D2.1

FG QIT4N D2.2

FG QIT4N D2.3

FG QIT4N D2.3-part 1

FG QIT4N D2.4

FG QIT4N D2.5

TR.qs-dlt

XSTR-HYB-QKD

FIPS 203
FIPS 204
FIPS 205

ETSI GR QKD 003

ETSI GR QKD 007

ETSI GS QKD 002

ETSI GS QKD 004

ETSI GS QKD 005

ETSI GS QKD 008

ETSI GS QKD 010

ETSI GS QKD 011

ETSI GS QKD 012

ETSI GS QKD 013

ETSI GS QKD 014

ETSI GS QKD 015

ETSI GS QKD 016

ETSI GS QKD 017

ETSI GS QKD 018

ETSI GS QKD 019

ETSI GS QKD 020

ETSI GS QKD 021

ETSI GS QKD 022

ETSI GS QKD 023

ETSI GR QSC 001

ETSI GR QSC 003

ETSI GR QSC 004

ETSI GR QSC 006

ISO / IEC 23837-1:2023

ISO / IEC 23837-2:2023

ISO / IEC 4879:2024

P7131

P7130

P1913

P1943

P3172

Q.4160

Q.4161
Q.4162
Q.4163
Q.4164

Y.3800

Y.3801

Y.3802

Y.3803

Y.3804

Y.3805

Y.3806

Y.3807

Y.3808

Y.3809

Y.3810

Y.3811

Y.3812

Y.3813

Y.3814

Y.3815

Y.3816

Y.3817

Y.3818

Y.3819

Y.3820

Y.3821

X.1702

X.1710

X.1712

X.1713

X.1714

X.1715

XSTR-SEC-QKD

ETSI EG 203 310

ETSI TR 103 570

ETSI TR 103 616

ETSI TR 103 617

ETSI TR 103 618

ETSI TR 103 619

ETSI TR 103 692

ETSI TR 103 744

ETSI TR 103 823

ETSI TR 103 949

Title

Terms of Reference (ToR)

Work Programme - Call for Participation

Towards Standardization for Quantum Technologies

Standardization Roadmap on Quantum Technologies

Quantum Technologies Use Cases

QIT4N terminology: Network aspects of QITs

QIT4N use cases: Network aspects of QITs

Standardization outlook and technology maturity: Network aspects of QIT

QIT4N terminology: QKDN

QIT4N use cases: QKDN

QKDN protocols: Key management layer, QKDN control layer and QKDN n

QKDN protocols: Quantum layer

QKDN transport technologies

QKDN standardization outlook and technology maturity

Guidelines for quantum-safe distributed ledger technology systems

Overview of hybrid approaches for key exchange with QKD

Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)
Module-Lattice-Based Digital Signature Standard (ML-DSA)
Stateless Hash-Based Digital Signature Standard (SLH-DSA)

QKD – Components and Internal Interfaces

QKD – Vocabulary

QKD – Use Cases

QKD – Application Interface

QKD – Security Proofs

QKD – QKD Module Security Specification

QKD – Implementation security: protection against Trojan horse attacks

QKD – Component characterization: characterizing optical components fo

QKD – Device and Communication Channel Parameters for QKD Deploym

QKD – Characterisation of Optical Output of QKD transmitter modules

QKD – Protocol and data format of REST-based key delivery API

QKD – Control Interface for Software Defined Networks

QKD – Common Criteria Protection Profile - Pair of Prepare and Measure (

QKD – Network architectures

QKD – Orchestration Interface for Software Defined Networks

QKD – Design of QKD interfaces with Authentication

QKD – Protocol and data format of REST-based Interoperable Key Manage

QKD – Orchestration Interface of Software Defined Networks for Interope

QKD – Network Architecture

QKD – Monitoring Interface and Data Model

QSC – Quantum-safe algorithmic framework

QSC – Case Studies and Deployment Scenarios

QSC – Quantum-Safe threat assessment

QSC – Limits to Quantum Computing applied to symmetric key sizes

Information security – Security requirements, test and evaluation method

Information security – Security requirements, test and evaluation method

Information technology — Quantum computing — Vocabulary

Standard for Quantum Computing Performance Metrics & Performance B

Standard for Quantum Computing Definitions

YANG Model for Software-Defined Quantum Communication

Standard for Post-Quantum Network Security

Recommended Practice for Post-Quantum Cryptography Migration

QKD networks - Protocol framework

Protocols for Ak interface for QKD network
Protocols for Kq-1 interface for QKD network
Protocols for Kx interface for QKD network
Protocols for Ck interface for QKD network

Overview on networks supporting QKD

Functional requirements for QKD networks

QKD networks – Functional architecture

QKD networks – Key management

QKD networks – Control and management

QKD networks – Software-defined networking control

QKD networks – Requirements for quality of service assurance

QKD networks – Quality of service parameters

Framework for integration of QKD network and secure storage network

A role-based model in QKD networks deployment

QKD network interworking – Framework

QKD networks – Functional architecture for quality of service assurance

QKD networks – Requirements for machine learning based quality of serv

QKD network interworking – Functional requirements

QKD networks – Functional requirements and architecture for machine le

QKD networks – Overview of resilience

QKD networks – Functional architecture enhancement of machine learnin

QKD network interworking – Requirements for quality of service assuranc

QKD network interworking – Architecture

QKD networks – Requirements and architectural model for autonomic ma

QKD network interworking – Software-defined networking control

QKD networks – Requirements for resilience

Quantum noise random number generator architecture

Security framework for QKD networks

Security requirements and measures for QKD networks – key managemer

Security requirements for the protection of QKD nodes

Key combination and confidential key supply for quantum key distri-butio

Security requirements and measures for integration of QKD network and

Security considerations for QKD network (Corrigendum)

CYBER – Quantum Computing Impact on security of ICT Systems; Recomn

CYBER – Quantum-Safe Key Exchanges

CYBER – Quantum-Safe Signatures

Quantum-Safe Virtual Private Networks

CYBER – Quantum-Safe Identity-Based Encryption

CYBER – Migration strategies and recommendations to Quantum Safe sch

CYBER – State management for stateful authentication mechanisms

CYBER – Quantum-safe Hybrid Key Exchanges

CYBER – Quantum-Safe Public-Key Encryption and Key Encapsulation

QSC – QSC Migration; ITS and C-ITS migration study

Institute	Focus Group	Source (File)	Most recent version
CEN-CENELEC	CEN/CLC/JTC 22 – FGQT	https://www.cenc	(Jul 2020)
CEN-CENELEC	CEN/CLC/JTC 22 – FGQT	https://www.cenc	–
CEN-CENELEC	CEN/CLC/JTC 22 – FGQT	https://www.cenc	–
CEN-CENELEC	CEN/CLC/JTC 22 – FGQT	https://www.cenc	(Mar 2023)
CEN-CENELEC	CEN/CLC/JTC 22 – FGQT	https://www.cenc	(Mar 2023)
ITU-T	FG-QIT4N	https://www.itu.ir	(Nov 2021)
ITU-T	FG-QIT4N	https://www.itu.ir	(Nov 2021)
ITU-T	FG-QIT4N	https://www.itu.	(Nov 2021)

ITU-T	FG-QIT4N	https://www.itu.	(Nov 2021)
ITU-T	FG-QIT4N	https://www.itu.	(Nov 2021)
ITU-T	FG-QIT4N	https://www.itu.i	(Nov 2021)
ITU-T	FG-QIT4N	https://www.itu.i	(Nov 2021)
ITU-T	FG-QIT4N	https://www.itu.	(Nov 2021)
ITU-T	FG-QIT4N	https://www.itu.	(Nov 2021)
ITU-T	ICT Security	https://www.itu.ir	V1.0 (Sep 2023)

ITU-T	ICT Security	https://www.itu.ir	V1.0 (May 2022)
NIST	Information Technology Lab	https://doi.org/10	Published (Aug 2024)
NIST	Information Technology Lab	https://doi.org/10	Published (Aug 2024)
NIST	Information Technology Lab	https://doi.org/10	Published (Aug 2024)
ETSI	ISG on QKD	https://portal.etsi	V2.1.1 (Mar 2018)
ETSI	ISG on QKD	https://www.etsi.(	V1.1.1 (Dec 2018)
ETSI	ISG on QKD	https://portal.etsi	V1.1.1 (Jun 2010)

ETSI	ISG on QKD	https://www.etsi.(	V2.1.1 (Aug 2020)
ETSI	ISG on QKD	https://www.etsi.(	V1.1.1 (Dec 2010)
ETSI	ISG on QKD	https://portal.etsi	V1.1.1 (Dec 2010)
ETSI	ISG on QKD	https://docbox.et	V0.4.1 (Jun 2021)
ETSI	ISG on QKD	https://portal.e	V1.1.1 (May 2016)

ETSI	ISG on QKD	https://portal.e	V1.1.1 (Feb 2019)
ETSI	ISG on QKD	https://portal.etsi	V0.1.4 (May 2024)
ETSI	ISG on QKD	https://www.etsi.(	V1.1.1 (Feb 2019)
ETSI	ISG on QKD	https://www.etsi	V2.1.1 (Apr 2022)
ETSI	ISG on QKD	https://www.etsi.(	V2.1.1 (Jan 2024)

ETSI	ISG on QKD	https://portal.etsiV0.1.12 (Nov 2023)
ETSI	ISG on QKD	https://portal.etsiV1.1.1 (Apr 2022)
ETSI	ISG on QKD	https://portal.etsiV0.1.6 (Aug 2024)
ETSI	ISG on QKD	https://portal.etsiV0.4.1 (Aug 2024)
ETSI	ISG on QKD	https://portal.etsiV0.0.1 (May 2023)
ETSI	ISG on QKD	https://portal.etsiV0.0.1 (May 2023)
ETSI	ISG on QKD	https://portal.etsiV0.0.2 (May 2023)
ETSI	ISG on QSC	https://portal.etsiV1.1.1 (Jul 2016)

ETSI	ISG on QSC	https://portal.e	V1.1.1 (Feb 2017)
ETSI	ISG on QSC	https://portal.e	V1.1.1 (Mar 2017)
ETSI	ISG on QSC	https://portal.etsi	V1.1.1 (Feb 2017)
ISO / IEC	JTC 1 SC 27	https://www.iso.c	Edt 1 (Aug 2023)
ISO / IEC	JTC 1 SC 27	https://www.iso.c	Edt 1 (Sep 2023)
ISO / IEC	JTC 1 WG 14	https://www.iso.c	Edt 1 (May 2024)
IEEE	QCB-WG - Quantum Computi	https://standards	–
IEEE	QCN-WG - Quantum Comput	https://standards	–
IEEE	QuantumComm - Software-D	https://standards	–
IEEE	QuNET/WG - Post-Quantum N	https://standards	–
IEEE	QuSEC/WG - Quantum Securi	https://standards	–
ITU-T	SG 11	https://www.itu.ir	V1.0 (Dec 2023)
ITU-T	SG 11	https://www.itu.ir	V1.0 (Dec 2023)
ITU-T	SG 11	https://www.itu.ir	V1.0 (Dec 2023)
ITU-T	SG 11	https://www.itu.ir	V1.0 (Dec 2023)
ITU-T	SG 11	https://www.itu.ir	V1.0 (Dec 2023)

ITU-T	SG 13	https://www.itu.i	V1.1 (Apr 2020)
ITU-T	SG 13	https://www.itu.i	V1.1 (Apr 2020)
ITU-T	SG 13	https://www.itu.i	V1.2 (Nov 2023)
ITU-T	SG 13	https://www.itu.i	V1.1 (Nov 2023)
ITU-T	SG 13	https://www.itu.i	V1.1 (Nov 2023)
ITU-T	SG 13	https://www.itu.i	V1.1 (Nov 2023)
ITU-T	SG 13	https://www.itu.i	V1.0 (Sep 2021)
ITU-T	SG 13	https://www.itu.i	V1.0 (Feb 2022)
ITU-T	SG 13	https://www.itu.i	V1.0 (Feb 2022)
ITU-T	SG 13	https://www.itu.i	V1.0 (Feb 2022)
ITU-T	SG 13	https://www.itu.i	V1.0 (Sep 2022)
ITU-T	SG 13	https://www.itu.i	V1.1 (Nov 2023)

ITU-T	SG 13	https://www.itu.i	V1.0 (Sep 2022)
ITU-T	SG 13	https://www.itu.i	V1.0 (Jan 2023)
ITU-T	SG 13	https://www.itu.i	V1.1 (Nov 2023)
ITU-T	SG 13	https://www.itu.i	V1.0 (Sep 2023)
ITU-T	SG 13	https://www.itu.i	V1.0 (Sep 2023)
ITU-T	SG 13	https://www.itu.i	V1.0 (Sep 2023)
ITU-T	SG 13	https://www.itu.i	V1.0 (Sep 2023)
ITU-T	SG 13	https://www.itu.ir	V1.0 (Dec 2023)

ITU-T	SG 13	https://www.itu.ir	V1.0 (Apr 2024)
ITU-T	SG 13	https://www.itu.ir	V1.0 (Apr 2024)
ITU-T	SG 17	https://www.itu.i	V1.0 (Nov 2019)
ITU-T	SG 17	https://www.itu.ir	V1.0 (Oct 2020)
ITU-T	SG 17	https://www.itu.i	V1.1 (Feb 2022)
ITU-T	SG 17	https://www.itu.ir	V1.0 (Apr 2024)
ITU-T	SG 17	https://www.itu.i	V1.0 (Oct 2020)
ITU-T	SG 17	https://www.itu.ir	V1.0 (Apr 2024)
ITU-T	SG 17	https://www.itu.ir	V1.0 (Apr 2021)
ETSI	TC CYBER QSC	https://portal.etsi	V1.1.1 (Jun 2016)
ETSI	TC CYBER QSC	https://portal.etsi	V1.1.1 (Oct 2017)

ETSI	TC CYBER QSC	https://www.etsi.	V1.1.1 (Sep 2021)
ETSI	TC CYBER QSC	https://www.etsi.	V1.1.1 (Sep 2018)
ETSI	TC CYBER QSC	https://portal.etsi	V1.1.1 (Dec 2019)
ETSI	TC CYBER QSC	https://www.etsi.	V1.1.1 (Jul 2020)
ETSI	TC CYBER QSC	https://portal.e	V1.1.1 (Nov 2021)
ETSI	TC CYBER QSC	https://portal.e	V1.1.1 (Dec 2020)
ETSI	TC CYBER QSC	https://portal.etsi	V1.1.2 (Oct 2021)
ETSI	TC CYBER QSC	https://portal.etsi	V1.1.1 (May 2023)

(upcoming) Release

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest
Latest
Latest

Latest

Drafting - V2.1.1 (TBA 01.12.2024)

Latest

Drafting - V3.1.1 (TBA 11.08.2025)

Drafting - V2.1.1 (TBA 15.01.2025)

Latest

Drafting - V1.1.1 (TBA 11.12.2024)

Latest

Latest

Drafting - V1.1.1 (TBA 22.01.2025)

Drafting - V2.1.1 (TBA 01.12.2024)

Drafting - V3.1.1 (TBA 26.08.2025)

Latest

Drafting - V1.1.1 (vrsl. 15.01.2025)

Latest

Drafting - V1.1.1 (TBA 05.12.2024)

Drafting - V1.1.1 (TBA 01.12.2024)

Drafting - V1.1.1 (TBA 12.05.2025)

Drafting - V1.1.1 (TBA 11.09.2025)

Drafting - V1.1.1 (TBA 14.03.2025)

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Drafting (PAR Approval Sep 2023)

Drafting (PAR Approval Sep 2023)

Drafting (PAR Approval Dec 2022)

Drafting (PAR Approval Jun 2021)

Drafting (PAR Approval May 2022)

Latest

Latest
Latest
Latest
Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Latest

Scope

The purpose of the FGQT is be to ensure interaction, such as workshops, between all relevant European stakeho
potential standardization in the field of QT to map ongoing standardization activities, define needs and opportun
further action to ensure that standards support the deployment of QT in industry. The FGQT does not develop st
deliverables.

One-pager to call for participation

This text provides some of the central ideas underlying the FGQT Standardization Roadmap. It gives a more deta
accompanies the FGQT Work Programme (FGQT Q02). Its purpose is to encourage people to read, comment, an
FGQT Standardization Roadmap (FGQT Q04).

This document outlines the activities of the Focus Group on Quantum Technologies (FGQT) established by the Eu
for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC). Over 10
joined, with around 200 experts participating in 30 meetings, covering various doMayns of quantum technologie
aims to inform about standardization needs, opportunities, and ongoing activities related to quantum technolog
participation from National Standardization Bodies. The roadmap document is structured into chapters: historica
challenges, the role of quantum technologies in the economy, and the ecosystem of standardization. It delves in
quantum technologies, types of standards, ongoing standardization platforms, and examples of standardization
technologies like nanodiamond color centers and superconducting quantum circuits are discussed, along with qu
components and subsystems. Specific analysis is provided for quantum communication, computing, simulation s
metrology. The document concludes with a description of the composite system of the quantum internet and ar
steps.

The use cases presented in this document are unstructured, both in topic and in the readiness or impli- cation o
Each subsection contains a separate use case and starts with a description, enabling technologies and standardiz
use cases follow with a deeper discussion of the aspects where standards are needed or might be beneficial.

This technical report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Network
on existing work of various Standards Development Organizations (SDOs) and academic literature, it surveys ter
aspects of quantum information technology, studies their overlap and divergence and provides a list of terms th
are yet to be standardized. Future efforts to standardize terminology on network aspects of quantum informatio
be informed by this technical report.

This technical report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Network
and analyses QIT for network use cases gathered during the lifetime of the ITU-T Focus Group on Quantum Infor
for Networks (FG QIT4N). The uses cases which are only applied by QITs are collected, investigated and summari
analysed by current bottlenecks, application scenarios, technical requirements and solutions. This Technical Rep
analyses and suggestions for future applications and potential standardization requirements.

This technical report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Network
provides: • a snapshot of the standardization landscape of quantum information technology (QIT) for networks;
barriers to the development and adoption of standards for QIT for networks; • a review of methodologies for as
maturity and standardization readiness of QIT for networks. This document studies the standardization outlook
maturity of quantum information technologies which either comprise or impact the requirements for a quantum
network (QIN), at the period of performance of the ITU-T Focus Group on Quantum Information Technology for

This technical report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Network technical report provides a survey of terminology relevant to QKDN currently published or under development b ISG QKD, ISO/IEC JTC1 SC27 WG3 and ITU-T SG13/17. Based on the survey, the terms are categorized according t technical directions they fall under.

This Technical Report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Networ consolidates the QKDN use cases gathered during the lifetime of the ITU-T FG QIT4N. The QKDN uses cases are c classes and the report highlights the competitive advantage of the use cases brought by QKDN and provides sug standardization efforts.

This technical report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Network studies and reviews protocols in the quantum layer of a quantum key distribution network (QKDN). It mainly foc distribution (QKD) protocols in the quantum layer, where QKD is an essential part of the QKDN and is an emergi expected to strengthen the security of the current communication network. This technical report endeavours to review of the QKD protocols, including different types of QKD protocols, their workflows, protocol features, para commercialization status. For this reason, it briefly discusses the security of QKD, specifically the security of prot to real world QKD systems. More generally, this technical report discusses the potential of integration of QKD in provides an overview of considerations and suggestions for future work on QKDN protocols.

This technical report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Network studies classical communication protocols in the quantum key distribution network (QKDN) which include proto the key management layer, QKDN control layer, and QKDN management layer. The QKDN protocols are classifie according to main functions of each layer. Representative operational procedures and corresponding message p for some protocols.

This technical report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Network discusses QKDN transport technologies such as transport system components, technical solutions, the typical sc existence of quantum and classical signals in a common fibre (CEQC). Analysis about the impact of the classic op quantum signals is given. Furthermore, some CEQC schemes are shown in the document, both for DV-QKD syste

This Technical Report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Networ provides an overview of quantum key distribution (QKD) technology, including frontier research, system experim commercialized product. It conducts a summary of QKD industry status, including market players such as system provider, and end user, project and opinions from different country and region, and other aspects. It contains Q standardization landscape, conducts gap analysis, and provides future standardization suggestions.

This Technical Report provides guidelines for quantum-safe distributed ledger tech systems, including:

– security assessments of cryptographic algorithms used in current DLT systems wh 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 safe DLT system.

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.

The present document is a preparatory action for the definition of properties of components and internal interfa Irrespective of the underlying technologies, there are certain devices that appear in most QKD Systems. These a physical devices such as photon sources and detectors, or classical equipment such as protocol processing comp operating systems. For these components, relevant properties should be identified that will subsequently be sub standardization. Furthermore, a catalogue of relevant requirements for interfaces between components should support the upcoming definition of internal interfaces.

The present document collects together definitions and abbreviations used in relation to Quantum Key Distribut (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 and classical cryptography but in some cases terms assume a modified or more specific meaning when applied t
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 used in future documents. The terms included have been selected to focus the present document on those that expected to be of widespread use or where consistency is felt to be particularly important, e.g. due to a specific confusion. Terms introduced in a single ISG-QKD document for a specific purpose that is local to that document excluded unless of particular importance.

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.

The present document is intended to specify an Application Programming Interface (API) between a QKD key ma
and applications. The function of a QKD key manager is to manage the secure keys produced by an implementat
QKD protocol and to deliver the identical set of keys, via this API, to the associated applications at the communic
end points.

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 practi
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 secre
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.

The present document aims to establish the necessary requirements for a QKD module to have a high probabilit
detecting and responding precisely and timely to attempts of direct physical access, and use or modification of m
inside. The principal objective is to detect any possible penetration with high probability, and resulting in the im
zeroization of all Critical Security Parameters in plain text.

The present document specifies protection of QKD modules against Trojan horse attacks launched against a time
polarisation or intensity modulator that encodes or decodes at least one of bit values, basis values or the intensi
or vacuum states from the quantum channel.

The present document gives specifications and procedures for the characterization of optical components for us
QKD systems. Examples of specific tests and procedures for performing such tests are given. Due to their import
the security of a QKD system, particular attention is given to active optical components such as optical sources a
single photon detectors.

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 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 roles played by the different entities are defined. One specific context (context1) is then addressed where one e (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 contex listed and prioritized. The corresponding tables, placed at the end of the present document, can be used as a sta template for the exchange of information between QKD_O entities and NET_O entities involved in the QKD deployment.

The present document defines procedures for characterising specific properties of complete QKD transmitter m procedures shall be limited to characterising the signals emitted by the transmitter under operational conditions

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 equip from different vendors.
The QKD network can consist of a single link between a single QKD transmitter and a single QKD receiver, or it ca 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 QK network generates key material shared between distant nodes.

The present document provides a definition of management interfaces for the integration of QKD in disaggregat network control plane architectures, in particular with Software-Defined Networking (SDN). It defines abstractio 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-chann interfaces are out of scope.

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 proto that can form a complete QKD system when connected by an appropriate point-to-point QKD link. The PP specif high-level requirements for the physical implementation through to the output of final secret keys.

This work item will review the variety of architectures that have been proposed for QKD networking. It will furth
basic functionalities that the mentioned architectures implement as well as the commonalities between the arch

The present document provides a definition of an orchestration interface between an SDN orchestrator and an S
controller of a QKD network. This orchestration interface defines the abstract information models and workflow
QKD network resource management, configuration management, performance management, service provisioni
notifications and management of multi-doMayn QKD networks. Interfaces between an SDN orchestrator and SD
controllers of classical optical transport networks are out of scope.

This work item will be a technical report on the design of classical interfaces for QKD systems that include authe
protocols used in discussion channels, auxiliary channels, management interfaces and key delivery interfaces. As
term or physical security will be discussed. Research on information-theoretic secure (e.g. Wegman Carter) and
authentication for QKD discussion channels will be reviewed as well as the use of other cryptographic algorithms
key) to augment protocols. Standard principles, frameworks and analytical tools from the cryptographic doMayn
Design principles specific to authenticated QKD, including protection of authentication keys against denial of ser
discussed citing existing literature.

This work item will specify a REST API that allows key management systems to interoperate to pass keys horizon
systems located in a common trusted node. The API will enable QKD networks to serve applications that request
from key management systems that are not linked by a contiguous chain of systems from the same vendor. It is
the document to describe how the underlying QKD network agrees key material between nodes. URI formats, co
protocols (HTTPS), and the JSON data format encoding of posted parameters and responses (including key mate
An OpenAPI description of the API will be included.

This work item deals with the interface between the SDN Orchestrator and the SDN Controller of QKD networks
management systems. It defines abstraction models and workflows between the SDN Orchestrator and SDN Cor
networks, including resource management, system configuration management, performance management, alar
provisioning, and management of multi-doMayn QKD networks to allow for the operation and management of n
usage patterns.

This work item will specify a QKD network architecture building on analysis in DGR/QKD-017NwkArch (GR QKD 0
network functionalities and interfaces aligned with modern communication networking paradigms suitable for b
critical infrastructures and integration with general telecommunications networks.

This work item will provide an interface and data model definition for QKD monitoring, consistent with the exist
interfaces. It will define monitoring and telemetry interactions with QKD modules, covering information about th
link(s) attached to them.

The present document gives an overview of the current understanding and best practice in academia and indust
safe cryptography (QSC). It focuses on identifying and assessing cryptographic primitives that have been propose
establishment and authentication applications, and which may be suitable for standardization by ETSI and subse
to develop quantum-safe solutions for real-world applications.

The present document examines a number of real-world uses cases for the deployment of quantum-safe crypto
Specifically, it examines some typical applications where cryptographic primitives are deployed today and discus
consideration by developers, highlighting features that may need change to accommodate quantum-safe crypto
focus of the document is on options for upgrading public-key primitives for key establishment and authenticatio
alternative, non-public-key options are also discussed.

The present document presents the results of a simplified threat assessment following the guidelines of ETSI TS
number of use cases. The method and key results of the analysis is described in clause 4.

The present document concludes that there are existing and widely used symmetric (AES-256) and hash primitiv
with an output length of at least 256 bits) that will withstand quantum computer attacks until way after 2050.

The ISO/IEC 23837 series specifies the security requirements, test and evaluation methods for quantum key dist
the framework of the ISO/IEC 15408 series. This document focuses on specifying the common baseline set of se
requirements (SFRs) of QKD modules.

The ISO/IEC 23837 series specifies security requirements, test and evaluation methods for quantum key distribu
under the framework of the ISO/IEC 15408 series. This document specifies an evaluation method and relevant e
for the security evaluation of QKD modules in a relatively general way. The evaluation activities that are necessa
evaluation of QKD modules include supplementary evaluation activities for the QKD-related security functional r
specified in ISO/IEC 23837-1 and the supplementary evaluation activities for security assurance requirements (SA
assurance levels ranging from evaluation assurance level (EAL) 1 to EAL 5+.

The standard covers quantum computing performance metrics for standardizing performance benchmarking of
hardware and software. These metrics and performance tests include everything necessary to benchmark quant
alone and by/for comparison) and to benchmark quantum computers against classical computers using a metho
for factors such as dedicated solvers.

This standard addresses quantum technologies specific terminology and establishes definitions necessary to faci
understanding to enable compatibility and interoperability.

This standard defines the Software-Defined Quantum Communication (SDQC) protocol that enables configuratio
endpoints in a communication network in order to dynamically create, modify, or remove quantum protocols or

This standard defines a post-quantum optimized version of network security protocols. It is based on a multi-lay
and allows data packets to be quantum resistant to future cryptographically relevant quantum computers (CRQC

This recommended practice describes multi-step processes that can be used to implement hybrid mechanisms (
classical quantum-vulnerable and quantum-resistant public-key algorithms). Existing post-quantum cryptograph
described. Desired characteristics of the hybrid mechanisms, such as crypto agility are also described.

Recommendation ITU-T Q.4160 specifies a framework for signalling and protocols for quantum key distribution

Recommendation ITU-T Q.4161 specifies protocols for Ak interfaces in quantum key distribution networks.

Recommendation ITU-T Q.4162 specifies protocols for Kq-1 interfaces in quantum key distribution networks.

Recommendation ITU-T Q.4163 specifies protocols for Kx interfaces for quantum key distribution networks.

Recommendation ITU-T Q.4164 specifies protocols for Ck interfaces in quantum key distribution networks.

This Recommendation is an overview that provides basic QKDN conceptual structures with a clear security boun
Recommendation of a series of QKDN Recommendations that cover various aspects such as network architectur
security. Requirements will be for further study.

In the context of quantum key distribution networks (QKDNs), Recommendation ITU-T Y.3801 specifies the funct
for quantum layer, the key management layer, the QKDN control layer and the QKDN management layer.

Recommendation ITU-T Y.3802 defines a functional architecture model of quantum key distribution (QKD) netw
realize this model, it specifies detailed functional elements and reference points, architectural configurations an
procedures of QKD networks (QKDN).

Recommendation ITU-T Y.3803 provides help for the design, deployment, and operation of key management of
distribution network (QKDN).

To realize secure, stable, efficient, and robust operations of and services by a quantum key distribution (QKD) ne
manage a QKD network (QKDN) as a whole and support user network management, Recommendation ITU-T Y.3
functions and procedures for QKDN control and management based on the requirements specified in Recomme

Recommendation ITU-T Y.3805 specifies the requirements, functional architecture, reference points, hierarchica
overall operational procedures of SDN control.

Recommendation ITU-T Y.3806 specifies the high-level and functional requirements of quality of service (QoS) as
key distribution networks (QKDN). The functional requirements include QoS planning, QoS monitoring, QoS opti
provisioning, QoS protection and recovery.

Recommendation ITU-T Y.3807 describes QoS and network performance (NP) on QKDN and specifies the associa
parameters for QoS and their definitions.
This Recommendation helps to quantify what kind of QoS requirements should be monitored and measured for
parameters.

Recommendation ITU-T Y.3808 provides an overview of secure storage networks (SSNs) for quantum key distrib
(QKDNs). It specifies the functional requirements, functional architecture model, reference points and operation
SSNs.

Recommendation ITU-T Y.3809 describes roles, a role-based model and service scenarios in quantum key distrib
(QKDN) from different deployment and operation perspectives within existing user networks for supporting secu
services.
This Recommendation can be used as a guideline for applying QKDN from a role point of view as well as for depl
operation of QKDN from a telecom operators' point of view.

For quantum key distribution networks (QKDN), Recommendation ITU-T Y.3810 specifies the framework of QKD
(QKDNi). This Recommendation describes the overview of interworking QKDNs, the reference models, and the f
gateway functions (GWFs) and interworking functions (IWFs). The configurations for QKDNi are specified. Appen
with different key relay schemes.

Recommendation ITU-T Y.3811 specifies the functional architecture of quality of service (QoS) assurance for the
distribution networks (QKDNs).
This Recommendation first provides an overview of the functional architecture of QoS assurance for the QKDN.
functional architecture of QoS assurance which includes functional entities such as QoS data collection, data pro
data analytics, QoS anomaly detection and prediction, QoS policy decision making, and enforcement and reporti
functional entities described in the functional architecture, this Recommendation specifies a basic operational p
assurance for the QKDN.

Recommendation ITU-T Y.3812 specifies high-level and functional requirements of machine learning (ML) based
(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 d
model of ML based QoS assurance which is followed by associated high-level and functional requirements of ML
assurance. Additionally, some use cases are described.

For quantum key distribution networks (QKDNs), Recommendation ITU-T Y.3813 specifies functional requiremer
interworking (QKDNi). This Recommendation describes the functional requirements for the key management lay
layer and QKDN management layer, for interworking using gateway nodes (GWNs) and/or interworking nodes (I

A quantum key distribution network (QKDN) is expected to maintain stable operations and meet the requiremer
cryptographic applications efficiently. Due to the advantages of machine learning (ML) related to autonomous le
overcome the challenges of QKDN in terms of quantum layer performances, key management layer performanc
and management efficiency. Based on the functional requirements and architecture of QKDN stated in Recomm
Y.3801 and ITU-T Y.3802, this Recommendation specifies one possible set of functional requirements and a poss
an ML-enabled QKDN (QKDNml), including an overview and the functional requirements, architecture and opera
QKDNml.

Recommendation ITU-T Y.3815 gives an overview of resilience and conceptual models of protection and recover
distribution networks for seamless key supply even in the case of network failure.

Recommendation ITU-T Y.3816 specifies functional architecture enhancement of quality of service (QoS) assuran
learning (ML) for quantum key distribution networks (QKDNs).
Recommendation ITU-T Y.3816 first provides an overview of functional architecture enhancement of ML-based
QKDNs. It then describes a functional architecture enhancement of QoS assurance that includes functional comp
data collection, data processing, data storage, data analytics, QoS anomaly detection and prediction, QoS policy
enforcement and reporting. Based on the capabilities described in the functional architecture enhancement, Rec
Y.3816 specifies an operational procedure of QoS assurance for QKDNs.

Recommendation ITU-T Y.3817 specifies high-level and functional requirements for quality of service (QoS) assu
key distribution network interworking. The functional requirements include QoS information transfer, QoS nego
management and QoS routing.

Recommendation ITU-T Y.3818 specifies functional architecture models for quantum key distribution network in
i.e., functional architectures with gateway and interworking nodes. In order to realize these two models, Recom
Y.3818 specifies detailed functional elements, basic operational procedures and architectural configurations for

This Recommendation specifies one possible set of functional requirements and a possible architectural model f
management and control (AMC)-enabled QKDN (QKDNamc). In particular, the scope of this Recommendation in
– Overview of QKDNamc;
– Requirements for QKDNamc;
– Consideration for the cognition process of QKDNamc;
– Architectural model for QKDNamc;
– Example operational procedures of QKDNamc.

Recommendation ITU-T Y.3820 specifies the software-defined networking (SDN)-based quantum key distributio
interworking control between QKDN providers. It provides an overview of the role of SDN control for the interw
QKDN providers, the functional requirements for an SDN controller for interworking, the functional entities of a
interworking, the interfaces of an SDN controller for interworking, the operational procedures of an SDN contro
as well as any security considerations.

For quantum key distribution networks (QKDN), Recommendation ITU-T Y.3821 specifies the general requireme
separately specifies the requirements for supporting protection and recovery.

Recommendation ITU-T X.1702 defines a generic functional architecture of a quantum entropy source, a commo
estimate and validate the entropy of a noise source under evaluation, and a common method to specify random
they are part of the implemented system.

Recommendation ITU-T X.1710 specifies a framework including requirements and measures to combat security
key distribution networks (QKDNs).
It specifies a simplified QKDN structure for analysis of the relevant security threats. Security requirements and c
measures are then specified on that basis.

Recommendation ITU-T X.1712 specifies security threats and security requirements for key management in qua
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
approved security.

Quantum key distribution (QKD) enables two remote parties to share a common random binary key that is unkn
eavesdropper. QKD networks based on trusted nodes (QKD nodes) have been widely adopted to enlarge the key
and enrich QKD-based applications. The trustworthiness of a QKD node is fundamental to ensure the overall sec
network.
Recommendation ITU-T X.1713 provides guidance for the secure implementation and operation of QKD nodes in
Recommendation identifies security threats, provides security requirements for QKD nodes and provides specifi
the requirements.

Recommendation ITU-T X.1714 describes key combination methods for quantum key distribution network (QKD
security requirements for both the key combination and the key supply from QKDN to cryptographic application

Recommendation ITU-T X.1715 specifies security requirements and measures for integrating a quantum key dist
(QKDN) with a secure storage network (SSN) in the service layer (Recommendation ITU-T Y.3800) and public key
(Recommendation ITU-T X.509).

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.

The present document addresses business continuity arising from the concern that Quantum Computing (QC) is
the problems that lie at the heart of both RSA and ECC asymmetric cryptography. The present document conside
the post-quantum era of how to re-assert CAs in a PKI, the distribution of new algorithms, and the distribution o
advises that business continuity planning addresses the impact of QC on ICT.

The present document compares a selection of proposals for quantum-safe key exchanges taken from the acade
particular, it includes key exchanges based on the Learning with Errors (LWE), Ring-LWE and Supersingular Isoge
(SIDH) problems, as well as key exchanges constructed from the Niederreiter and NTRU key transport schemes.

The present document provides technical descriptions of the digital signature schemes submitted to the Nationa
Standards and Technology (NIST) for the third round of their post-quantum cryptography standardization proces

The present document explores protocol requirements necessary to add quantum resistance to VPN technologie
server and architectural considerations. Specifically, requirements around protocols and key establishment are c
the multitude of systems that are at risk and require security updates before quantum computers that can attac
cryptography are developed.

The present document describes a proposal for a quantum-safe hierarchical identity-based encryption scheme. I
of the functionality provided by hierarchical identity-based encryption, outlines some example uses cases and pr
description of a potential solution based on structured lattices. The description includes concrete proposals for p
estimates for performance in software and a practical security analysis.

The present document addresses the problem of migration to an environment in a Fully Quantum Safe Cryptogr
from a non-Quantum Safe Cryptographic State. The present document provides recommendations and guidance
transition between the two (2) states.

The present document is limited to discussion of the characteristics of the state object, the reuse of the state inc
architectural and operational considerations for deploying stateful hash-based signatures. First, it discusses char
state object for S-HBS schemes and identifies potential security vulnerabilities and operational problems associa
management. Second, it gives guidance on mitigating the issues identified. And third, it helps a prospective impl
a S-HBS solution is suitable for their given application; examples of suitable and non-suitable applications are giv

The present document specifies several methods for deriving cryptographic keys from multiple shared secrets. T
established using existing classical key agreement schemes, like elliptic curve Diffie-Hellman (ECDH) in NIST SP80
quantum-safe key encapsulation mechanisms (KEMs).

The present document provides technical descriptions of the Public-Key Encryption (PKE) and Key Encapsulation
submitted to the National Institute for Standards and Technology (NIST) for the third round of their Post-Quantu
(PQC) standardization process.

The present document reviews the state of deployment of cryptographic security mechanisms in Intelligent Tran
and Cooperative Intelligent Transport Systems (C-ITS) and their susceptibility to attack by a quantum computer.
document makes a number of recommendations regarding the adoption of Quantum Safe Cryptography in orde
exposure of ITS and C-ITS to attack.

Comment

Standard not ready for download

Standard not ready for download

Standard not ready for download

Standard not ready for download

Standard not ready for download

Standard not ready for download

Standard not ready for download

Behind paywall

Behind paywall

Behind paywall

Institute	Focus Group
CEN-CENELEC	CEN/CLC/JTC 22 – FGQT
ETSI	ISG on QKD ISG on QSC TC CYBER QSC
IEEE	QuantumComm
ISO / IEC	JTC 1 SC 27 JTC 1 WG 14
ITU-T	SG 11 SG 13 SG 17 ICT Security FG-QIT4N
NIST	Information Technology Laboratory

Source (FG)
FGQT
ISG QKD ISG QSC CYBER QSC
IEEEquantumstandards
SC 27 WG 14
Q series Y series X series ICTS QIT4N
FIPS