INTERNATIONAL STANDARD

ISO/IEC 23837-1

First edition
2023-08

Information security — Security requirements, test and evaluation methods for quantum key distribution —

Part 1: Requirements

Technologies de l'information — Exigences de sécurité, méthodes d'essais et d'évaluation relatives à la distribution quantique de clés —

Partie 1: Exigences

Reference number
ISO/IEC 23837-1:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 23837 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

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.

Theoretically, QKD provides a method to use a pre-shared key to establish a longer symmetric key with security that does not depend upon the computational power of an adversary; the established key can then be used for cryptographic purposes, such as for an encryption mechanism to create a secure communication channel.

Although the security of QKD protocols is proven through rigorous security models that assume the two communicating parties share a secret key beforehand, discrepancies between the models and practical implementations frequently occur during the life cycle phases of QKD modules. These imperfections or deviations from the security models can result in vulnerabilities that compromise the security of practical QKD systems. Among them, severe side channel attacks have been proposed and there have been some proof-of-principle demonstrations in QKD hacking experiments. Like conventional cryptographic modules or network devices, QKD modules are expected to have strict security testing and evaluation to avoid security attacks and then leakage of information before being deployed into real applications. Intensive and strict evaluation is an essential step before QKD is widely accepted by the industry.

For this purpose, the ISO/IEC 23837 series defines a set of rigorous and common security specifications for QKD modules manufacturers, so that manufacturers can follow the standard procedure to design and implement IT products that use QKD, and evaluators can follow the standard procedure to test and evaluate the security of QKD modules, reducing the risk of a failure of security in operation. This document uses the standardized model and language of the ISO/IEC 15408 series to define a common baseline set of SFRs for QKD modules. The entire implementation of QKD protocols is included, from conventional network components to quantum optical components. Annex A provides information to facilitate the development of protection profiles for QKD modules. ISO/IEC 23837-2 is intended to specify evaluation activities that are necessary for the security evaluation of QKD modules at the expected evaluation assurance levels.

NOTE In this document, the description of extended security functional components in 8.2 and SFRs in Clause 9 corresponds to the style of the description of security functional components in ISO/IEC 15408-2. This includes not only the structure of the security functional family and components, but also the font styles (i.e. bold and italics) of the text, which are described by following the convention of ISO/IEC 15408-2 to distinguish some terms from the rest of the text. In this case, users with a background in using the ISO/IEC 15408 series can easily apply the extended security functional components and the SFRs to write documents for the evaluation of QKD modules.

Information security — Security requirements, test and evaluation methods for quantum key distribution —

Part 1: Requirements

1 Scope

This document specifies a general framework for the security evaluation of quantum key distribution (QKD) according to the ISO/IEC 15408 series. Specifically, it specifies a baseline set of common security functional requirements (SFRs) for QKD modules, including SFRs on the conventional network components and the quantum optical components, and the entire implementation of QKD protocols. To facilitate the analysis of SFRs, security problems that QKD modules can face in their operational environment are analysed based on a structural analysis of the security functionality of QKD modules and the classification of QKD protocols.

The SFRs on conventional network components of QKD modules are mainly characterized under the framework of the ISO/IEC 15408 series and also refer to the methodology of ISO/IEC 19790 and relevant standards on testing of cryptographic modules and network devices.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-1:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15408-1 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
adversary
attacker
entity seeking to exploit potential vulnerabilities of a *quantum key distribution system* (3.28)

[SOURCE: ISO/IEC 19792:2009, 4.1.2, modified — “adversary” has been added as an admitted term; in the definition, “person” has been replaced by “entity”, and “biometric system” has been replaced by “quantum key distribution system”.]

3.2
authentication
provision of assurance of the claimed identity of an entity

[SOURCE: ISO/IEC 10181-2:1996, 3.3]

3.3
classical channel
communication channel that is used by two communicating parties for exchanging data encoded in a form which may be non-destructively read and fully reproduced

[SOURCE: ETSI GR QKD 003 V2.1.1:2018]

3.4
component
<QKD module> constituent part of a *quantum key distribution (QKD) module* (3.23)

EXAMPLE Conventional network components, quantum optical components in a QKD module.

Note 1 to entry: A term with the same name of component is defined in ISO/IEC 15408-1 for a security requirement element group. The user of this document can distinguish which term is referenced from the context.

3.5
cryptographic module
set of hardware, software, and/or firmware that implements security functions and are contained within the cryptographic boundary

[SOURCE: ISO/IEC 19790:2012, 3.25]

3.6
decoding
procedure of converting *quantum signals* (3.32) into classical information

3.7
detection efficiency
probability that a photon, of a specific energy (spectral frequency) or wavelength, incident at the optical input is detected within a detection gate, and produces an output signal

[SOURCE: ETSI GR QKD 007 V1.1.1:2018]

3.8
double-click event
event indicating simultaneous detection of two *single-photon detectors* (3.37)

3.9
encoding
procedure of converting classical information into *quantum signals* (3.32)

3.10
error corrected data
keying material obtained after correcting the bit errors in the *sifted data* (3.36)

3.11
error correction
process of correcting errors in data that may have been corrupted due to errors during transmission or in storage

[SOURCE: ETSI GR QKD 007 V1.1.1:2018]

3.12
final key
key generated by a complete run of a *quantum key distribution session* (3.27)

3.13
homodyne detection
method to detect quadrature of a weak signal through interfering the weak signal with a strong phase reference

3.14
keying material
data necessary to establish and maintain cryptographic keying relationships

[SOURCE: ISO/IEC 11770-1:2010, 2.27]

3.15
non-deterministic random bit generator
NRBG
random bit generator whose security depends upon sampling one or more entropy sources

[SOURCE: ISO/IEC 18031:2011, 3.23, modified — "an" has been replaced by "one or more", note 1 to entry has been removed.]

3.16
parameter adjustment procedure
procedure or function aiming to adjust specific parameter(s) of a system

3.17
post-processing
quantum key distribution protocol (3.24) procedure for converting *raw data* (3.33) into a *final key* (3.12)

3.18
pre-shared key
key pre-established in secure ways between the legitimate parties before initiating a *quantum key distribution* (*QKD*) *session* (3.27)

Note 1 to entry: A pre-shared key is used to authenticate messages sent over the *classical channel* (3.3) during the first QKD session.

3.19
privacy amplification
process of extracting keys from partially compromised data

[SOURCE: ETSI GR QKD 007 V1.1.1:2018, modified — "distilling secret keys" has been replaced by "extracting keys".]

3.20
quantum channel
communication channel for transmitting *quantum signals* (3.32)

[SOURCE: ETSI GR QKD 007 V1.1.1:2018]

3.21
quantum key distribution
QKD
procedure or method for two legitimate parties to agree on symmetric keys using a *pre-shared key* (3.18), whose security is based on quantum information theory

Note 1 to entry: In some *QKD protocols* (3.24), establishment of keys occurs jointly involving both legitimate parties, while in others one party generates keys that are eventually transported to the other party.

3.22
quantum key distribution authentication key
QKD authentication key
cryptographic key used to authenticate messages over the *classical channel* (3.3) of a *quantum key distribution system* (3.28)

3.23
quantum key distribution module
QKD module
set of hardware, software and/or firmware *components* (3.4) that implements the functions of a *quantum key distribution transmitter party* (3.30) or *receiver party* (3.26)

3.24
quantum key distribution protocol
QKD protocol
protocol that implements the function of *quantum key distribution* (3.21)

3.25
quantum key distribution receiver module
QKD receiver module
functional module in a *quantum key distribution* (*QKD*) *system* (3.28) corresponding to the *QKD receiver party* (3.26) of the implemented *QKD protocol* (3.24)

3.26
quantum key distribution receiver party
QKD receiver party
quantum signal (3.32) receiver in a *quantum key distribution* (*QKD*) *protocol* (3.24)

[SOURCE: ETSI GR QKD 007 V1.1.1:2018, modified — the term has been changed from "Bob" to "quantum key distribution receiver party"; in the definition, “information” has been replaced by “signal”.]

3.27
quantum key distribution session
QKD session
session comprising a series of operations defined in a *quantum key distribution protocol* (3.24) to generate a *final key* (3.12), which generally includes the stages of *raw data generation* (3.34) and *post-processing* (3.17)

3.28
quantum key distribution system
QKD system
system that implements *quantum key distribution* (*QKD*) *protocols* (3.24), including at least two *QKD modules* (3.23) as well as the interconnecting *quantum* (3.20) and *classical channels* (3.3)

3.29
quantum key distribution transmitter module
QKD transmitter module
functional module in a *quantum key distribution* (*QKD*) *system* (3.28) corresponding to the *QKD transmitter party* (3.30) of the implemented *QKD protocol* (3.24)

3.30
quantum key distribution transmitter party
QKD transmitter party
quantum signal (3.32) sender in a *quantum key distribution protocol* (3.24)

[SOURCE: ETSI GR QKD 007 V1.1.1:2018, modified — the term has been changed from "Alice" to "quantum key distribution transmitter party"; in the definition, “information” has been replaced by “signal”, "system" has been replaced with "protocol", and “transmitter” has been removed.]

3.31
quantum random bit generator
QRBG
random bit generator that generates random bits based on principles of quantum mechanics

3.32
quantum signal
signal described by a quantum mechanical state

[SOURCE: ETSI GR QKD 007 V1.1.1:2018]

3.33
raw data
keying material (3.14) generated by measuring quantum states of the signal pulse

3.34
raw data generation
quantum key distribution protocol (3.24) procedure of generating *raw data* (3.33) by transmitting and detecting *quantum signals* (3.32)

Note 1 to entry: This term is also known as “raw key exchange” in the quantum key distribution community.

3.35
sifting
procedure in the *post-processing* (3.17) of a *quantum key distribution protocol* (3.24) to generate *sifted data* (3.36) by processing *raw data* (3.33)

3.36
sifted data
data obtained by the legitimate users from sifting *raw data* (3.33) according to an agreed strategy

3.37
single-photon detector
device that transforms a single-photon into a detectable signal with non-zero probability

[SOURCE: ETSI GR QKD 007 V1.1.1:2018, modified — “finite probability” has been replaced by “non-zero probability”.]

4 Abbreviated terms

APD	avalanche photodiode
CV-QKD	continuous-variable quantum key distribution
DV-QKD	discrete-variable quantum key distribution
EB-QKD	entanglement-based quantum key distribution
FTP	trusted path/channels
FUN_QKD	quantum key distribution function
FUN_SCM	system control and management function
FUN_SP	self-protection function
IT	information technology
KM	key manager
MDI-QKD	measurement-device-independent quantum key distribution
NRBG	non-deterministic random bit generator
PM-QKD	prepare-and-measure quantum key distribution

PP	protection profile
QBER	quantum bit error rate
QKD	quantum key distribution
QRBG	quantum random bit generator
RBG	random bit generator
SFR	security functional requirement
ST	security target
TOE	target of evaluation
TSF	target of evaluation security functionality

5 Theoretical aspects of QKD protocols

5.1 General

This clause describes the idea of QKD in a theoretical model. The theoretical model is limited to discussion on the theoretical aspects of QKD protocols, without considering the implementation vulnerabilities that can be potentially introduced in reality. In other words, in the theoretical model all parts of the QKD implementation are assumed to conform to this model, and there is no possibility of attack by means of any implementation vulnerabilities. The attacks allowed in the theoretical model are restricted to those that are already considered in the security model of the protocols.

The basic concepts and principles of QKD protocols are discussed in 5.2. Then in 5.3 and 5.4 the classification of QKD protocols and their architectures are presented to facilitate the later analysis of QKD implementations.

5.2 Principle

Roughly speaking, a QKD protocol can be used to expand an existing pre-shared key between two parties into a longer secret key that is qualified for cryptographic use. Specifically, in a generic model of QKD protocols, two parties are connected by two communication channels. One of the channels is called the quantum channel, which is used for quantum signal transmission. The other channel is called the classical channel, which is used to transmit classical signals. In order to generate an arbitrary number of secret keys (up to the demand of specific applications), the two parties are expected to run a number of QKD sessions to exchange and process information according to a QKD protocol. Data sent over the classical channel is typically required to be authenticated. The key used for data authentication of the classical channel is called the QKD authentication key. For the first QKD session, the two parties require a pre-shared symmetric key to be used in QKD authentication keys. Since the consumed QKD authentication keys for each QKD session are typically much shorter than the key generated by that session, later QKD sessions can start to use QKD authentication keys from dedicated parts of the keys that were generated in prior QKD sessions. From this point of view, QKD functions as a two-party key expansion protocol, which ideally allows the two parties to expand a short pre-shared key to a longer shared secret key of near-arbitrary length (according to the demand of specific applications).

NOTE 1 The pre-shared key can be manually entered (or downloaded from an external key manager) to a QKD module during the development, pre-operation and maintenance phases of the module. In practice, a sequence of symmetric keys, rather than a single key only sufficient to derive QKD authentication keys for the first QKD session, is usually pre-shared before operating the QKD system.

Generally, a QKD protocol comprises two procedures.

a) Procedure one: raw data generation, in which quantum signals are transmitted over the quantum channel and detected by the legitimate parties to generate raw data. To aid the classification of QKD protocols, the parties are differentiated in QKD protocols by their role in this procedure. Specifically, a party who transmits quantum signals in a QKD protocol is called a QKD transmitter party (or transmitter party for short), and a party who detects quantum signals in the protocol is called a QKD receiver party (or receiver party for short).

b) Procedure two: post-processing. In this procedure, a post-processing protocol is implemented on the raw data to derive a symmetric key, which is (generally shorter than the raw data and) called the final key. The post-processing procedure generally includes four sub-procedures:

   - sifting: derive the sifted data from the raw data;
   - parameter estimation: estimate the parameters to be used in the error correction and privacy amplification;
   - error correction: correct the errors in the sifted data;
   - privacy amplification: generate a final key from the sifted data.

NOTE 2 A practical QKD system can include other auxiliary procedures to realize its functionality, such as the initialization procedure described in 6.5.

NOTE 3 In some cases, the procedures of QKD protocol cannot be clearly separated. For example, the QBER estimation for error correction can be executed during the error correction procedure rather than during the parameter estimation procedure.

5.3 Classification

The functionality of QKD can be realized via different types of protocols, which may be more complicated than the generic protocol discussed in 5.2. These protocols can be classified from different perspectives. The ISO/IEC 23837 series considers two different classification methods of QKD protocols. The first classification is based on the methods used to measure the quantum states, including discrete-variable QKD (DV-QKD) and continuous-variable QKD (CV-QKD) protocols, as shown in Table 1. For DV-QKD protocols, the receiver party typically measures optical pulses with single-photon detectors, while for CV-QKD protocols, the receiver party typically measures optical pulses with coherent detection techniques.

The second classification is based on the architecture of QKD protocols, as shown in Table 2. In prepare-and-measure QKD (PM-QKD) protocols, a transmitter party encodes information on quantum states and sends them through the quantum channel to an intended receiver party, who measures these quantum states to obtain raw data (see Figure 1). In measurement-device-independent QKD (MDI-QKD) protocols, there are two transmitter parties and one receiver party. Each transmitter party is connected to the receiver party with a quantum channel. The transmitter parties prepare and send quantum states to the receiver party, which performs a joint measurement on these quantum states (see Figure 2). In entanglement-based QKD (EB-QKD) protocols, there are two receiver parties and one transmitter party. Each receiver party is connected to the transmitter party with a quantum channel. The transmitter party prepares a bipartite entangled quantum state, and sends different parts of the state to the two receiver parties, respectively. The two receiver parties individually measure the quantum states to generate raw data (see Figure 3).

NOTE DV-QKD and CV-QKD can both include PM-QKD, MDI-QKD and EB-QKD protocols.

Table 1 — Classification of QKD protocols by the decoding method of quantum states

Type	DV-QKD	CV-QKD
Description	The transmitter party typically encodes information with discrete variables of finite dimension such as phase, polarization or time-bin. To decode information, the receiver party typically uses single-photon detectors.	The transmitter party typically encodes information using conjugate variables (quadratures) of a quantized electromagnetic field in an infinite dimensional Hilbert space. An example is coherent optical states. The receiver party typically uses a coherent detection technique, such as homodyne or heterodyne detection, to perform quadrature measurements on the quantum states.

Table 2 — Classification of QKD protocols by the architecture of the protocols

Type	PM-QKD	MDI-QKD	EB-QKD
Description	This protocol includes a QKD transmitter party and a QKD receiver party. The transmitter party prepares and sends quantum states to the receiver party through a quantum channel. The receiver party measures the quantum states. The result (after post-processing) is a common final key available to the transmitter party and the receiver party.	This protocol includes two QKD transmitter parties and a QKD receiver party. The transmitter parties prepare and send quantum states to the receiver party through a quantum channel. The receiver party performs a joint measurement on the quantum states received from the two transmitter parties. The result (after post-processing) is a common final key available to the two transmitter parties.	This protocol includes a QKD transmitter party and two QKD receiver parties. The transmitter party prepares a bipartite entangled quantum state and sends the two parts to the two receiver parties, respectively. The two receiver parties individually measure the quantum states. The result (after post-processing) is a common final key available to the two receiver parties.

5.4 Architecture

5.3 discussed three different architectures of QKD protocols, which are illustrated in Figure 1, Figure 2 and Figure 3 respectively. Generally, the scope of security evaluation is tightly related to the architecture of the implemented QKD protocol.

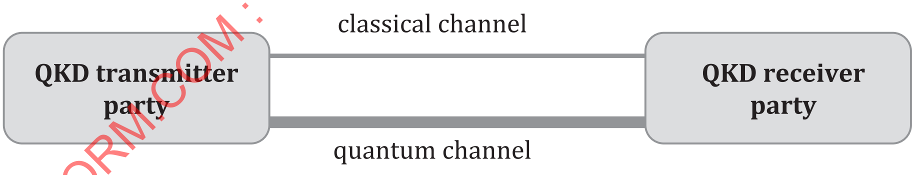

Figure 1 — Prepare-and-measure QKD protocol

The architecture corresponding to the PM-QKD protocol, illustrated in Figure 1, consists of a transmitter party and a receiver party connected by quantum and classical channels. The security of the practical QKD systems relies on the secure implementation of the functions of both parties, thus both of the implementation modules are required to be in the scope of security evaluation.

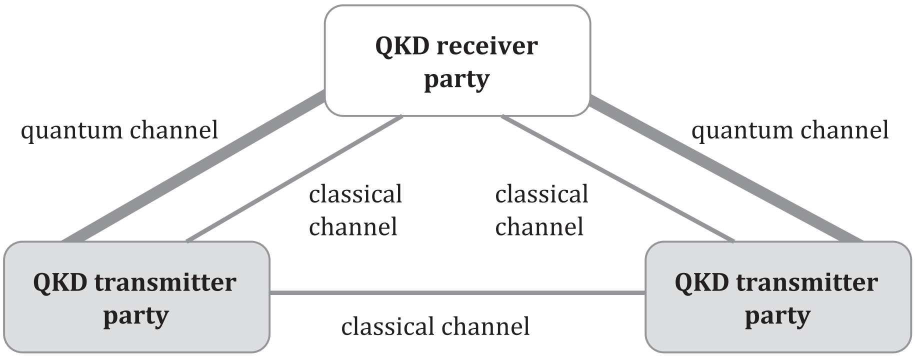

Figure 2 — MDI-QKD protocol

In the MDI-QKD protocol, a middle party assumes the role of receiver party who connects with the two transmitter parties through a quantum channel and a classical channel; the two transmitter parties are also connected via a classical channel (see Figure 2). After a successful QKD session, only the two transmitter parties know the final key. According to the characteristics of MDI-QKD protocols, the QKD receiver party in this case is only expected to follow the protocol specification for keys to be established correctly. However, no security assumptions are made on the receiver party when proving the security of MDI-QKD protocols. Therefore, the implementation module of the QKD receiver party is excluded from the scope of security evaluation, as described in 6.4.3.

NOTE There are two types of classical channels in MDI-QKD. One is the classical channel connecting the two QKD transmitter parties, where data over the channel are authenticated depending on the specific QKD protocols. The other type includes the two classical channels connecting each QKD transmitter party with the QKD receiver party. The latter type is used to transmit the measurement results of the QKD receiver party, but message authentication is not expected. In other words, it is assumed that the attacker can tamper with the measurement results sent from the QKD receiver party (via these classical channels) to the transmitter parties.

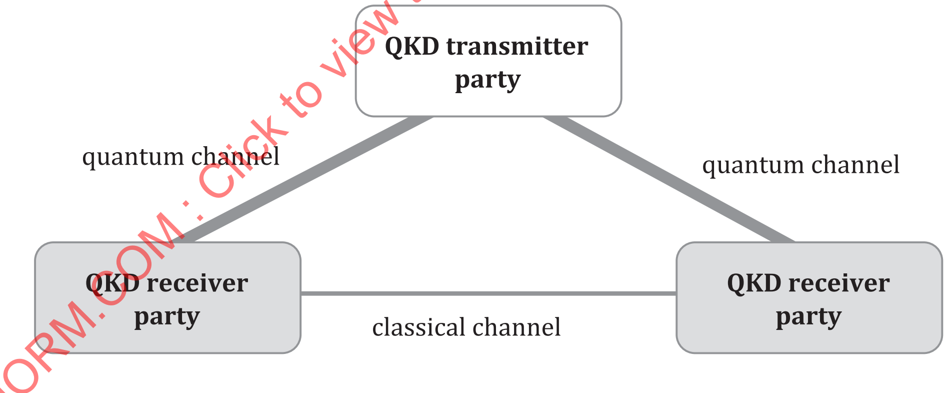

Figure 3 — EB-QKD protocol

In the EB-QKD protocol, a middle party assumes the role of QKD transmitter party, who connects with each of the two receiver parties via a quantum channel, and the two receiver parties are again connected via a classical channel (see Figure 3). After a successful QKD session, only the two QKD receiver parties know the final key. According to the characteristics of EB-QKD protocols, the transmitter party in this case is only expected to follow the protocol specification for keys to be established correctly. However, no security assumptions are made on the transmitter party when proving the security of EB-QKD protocols. Therefore, the implementation module of the transmitter party is excluded from the scope of security evaluation, as detailed in 6.4.3.

Moreover, in some implementations, the role of the middle party and one of the other two parties may be merged into a single party. In this case, the author of a PP or an ST shall take into account the level of integration to ensure that the overall security is ensured. Specially, where a component that requires evaluation is combined into a module with a component that does not normally require evaluation, the method of segregation shall be made clear and distinct in the PP or ST and TOE definition.

EXAMPLE For EB-QKD, the QKD transmitter party and one of the two QKD receiver parties can be implemented in the same module.

6 Implementation modules of QKD protocols

6.1 General

In this document, realizations of the modules of a QKD transmitter party and a QKD receiver party in a QKD protocol are hereinafter referred to as a QKD transmitter module (or transmitter module for short) and a QKD receiver module (or receiver module for short), respectively.

Generally, the security model of a QKD protocol assumes that the threat agents would only conduct adversarial actions over the quantum channel and the classical channel. In practice however, when threat agents are allowed to remotely access the computation devices via network interfaces, or even to physically approach the computation devices and invade into their hardware, critical information about the computation can potentially leak to the threat agents and render the security statement of the security model no longer valid.

NOTE For physical reasons, the operation of IT devices offers threat agents the possibility to extract data or information via side channels (for example, by measurements on power consumption, electromagnetic emanation etc.). These so-called side channel attacks are usually considered during the evaluation of cryptographic modules. The evaluation of side channel leakage of the QKD modules usually requires lots of efforts. These efforts can be reduced where environmental assumptions can remove some side channel considerations, as described in Clause 7 (especially 7.2 and 7.4.2) in detail.

From the perspective of practical security, the gap between the security model and the practice can be narrowed somewhat by introducing reasonable environmental assumptions or employing particular IT-related and non-IT related security controls. An evaluation of a QKD module according to the ISO/IEC 15408 series therefore aims to determine whether a practical security level has been achieved. It aims to demonstrate that there are no potential gaps between a QKD protocol and a practical implementation that can be exploited by an attacker with the strength assumed.

The ISO/IEC 23837 series aims to answer the following three questions:

a) Which assumptions on the operational environment should be made and what threats should be addressed from the perspective of practical security? (see Clause 7)

b) What IT-related security controls should be employed to address the identified threats and achieve the security objectives, or specifically what security requirements should be imposed upon QKD modules? (see Clause 9)

c) How is it possible to validate that the security controls and the core functionality of QKD modules have been implemented correctly in the product? (see ISO/IEC 23837-2)

To better understand these questions, the external interfaces of a typical QKD module are illustrated in 6.2, and then the internal components that make up a typical QKD system are analysed in 6.3. On the basis of this description, 6.4 describes a general definition of the scope of a TOE and its TSF. Finally, 6.5 describes a general working flow of the QKD system.

6.2 External interfaces of QKD modules

6.2.1 General

A generic description of the external interfaces of a QKD module is illustrated in Figure 4. The generalized QKD module shown in Figure 4 can be the instantiation of either a QKD transmitter party or a QKD receiver party, depending on the architecture of the specific protocol.

NOTE 1 A more complete description of QKD modules is shown in ETSI GS QKD 011[12].

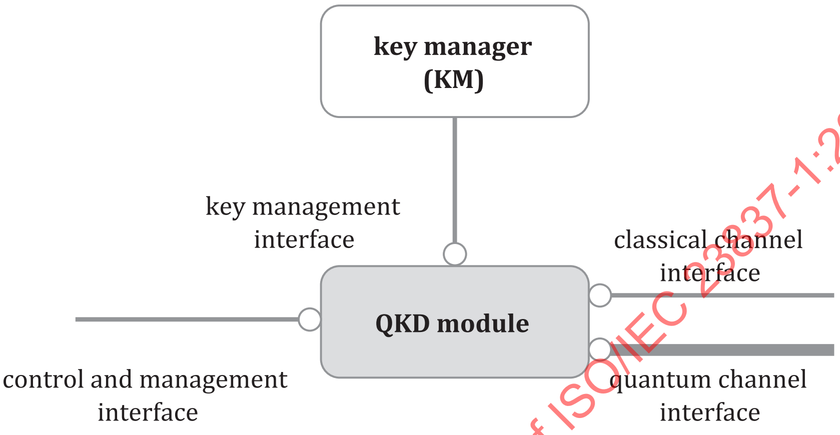
key manager
(KM)
key management interface
classical channel interface
QKD module
control and management interface
quantum channel interface

Figure 4 — The external interfaces of a generic QKD module

In addition to the interfaces connecting the quantum channel and classical channel, a QKD module is required to have some auxiliary interfaces to support the operation of QKD functions, including an interface for the operator to control and manage the functionality of the QKD module (i.e. the control and management interface), and an interface for the QKD module to interact with an external KM to upload final keys (i.e. the key management interface).

NOTE 2 Depending on the implementation strategy, the pre-shared key used for the QKD authentication key can be downloaded from the KM, or manually entered into the QKD module through the control and management interface directly.

The classical channel interface allows a QKD module to exchange messages with a counterpart module via classical signals and to perform post-processing procedure etc. From this point of view, the interface is not particularly unique compared to the case of conventional network devices, so 6.2.2 to 6.2.4 provide analysis of the quantum channel interface and the auxiliary interfaces.

6.2.2 The quantum channel interface

Although the quantum channel can be a single-mode fibre, a multi-mode optical fibre, or a free-space channel, the quantum channel interface is recommended only to propagate light entering the interface in a single lateral optical mode to components within the QKD module, to avoid potential attacks from exploiting any multi-mode characteristics of the QKD module. Therefore, in the ISO/IEC 23837 series, only single-mode optical fibre is considered in the implementation of quantum channel interface.

6.2.3 The control and management interface

a) Depending on the specific implementation, the control and management interface may be used by the operator to access the QKD module in order to:

   — configure system parameters;

   — manage audit information;

   — update software/hardware packages;

- monitor the operation status and handle exceptional events of the QKD module;
- enter the pre-shared key, applied in some specific implementations only.

NOTE For some implementations, the control and management interface can be accessed by the operator to collect audit information from the QKD module.

b) In practice, authentication-based access control is usually indispensable for QKD modules in order to manage the accessibility of the interface and protect it from unauthorized system access.

6.2.4 The key management interface

a) Depending on the specific implementation, the key management interface may be regularly invoked by the QKD module to communicate with the KM for:

- uploading a part of the newly generated final key;
- for some specific implementation strategies, optionally downloading the pre-shared key used for the QKD authentication keys of the first QKD session.

b) In practice, the interfacing path between the QKD module and the KM may span different internal networks. The communication over this channel is thus required to be protected from information leakage and tampering. See the security assumption in 7.2 a) and the exception under 7.2 a) 2) for more details.

6.3 Internal structure of QKD modules

6.3.1 General

In practice, implementations of specific QKD protocols can be very different. The differences between various implementations are mainly in the constituent components, such as photon sources, detectors and modulators as well as those implementing the post-processing procedure. Without loss of generality, the description on the internal structure of QKD modules emphasizes the general aspects of an abstracted high-level implementation of QKD protocols, and omits the subtle technical differences. Specifically, a generic structure about the internal functional elements within a typical PM-QKD module is described, as shown in Figure 5.

NOTE The description about the internal structure of QKD modules can be adjusted to suit QKD protocols with different architectures.

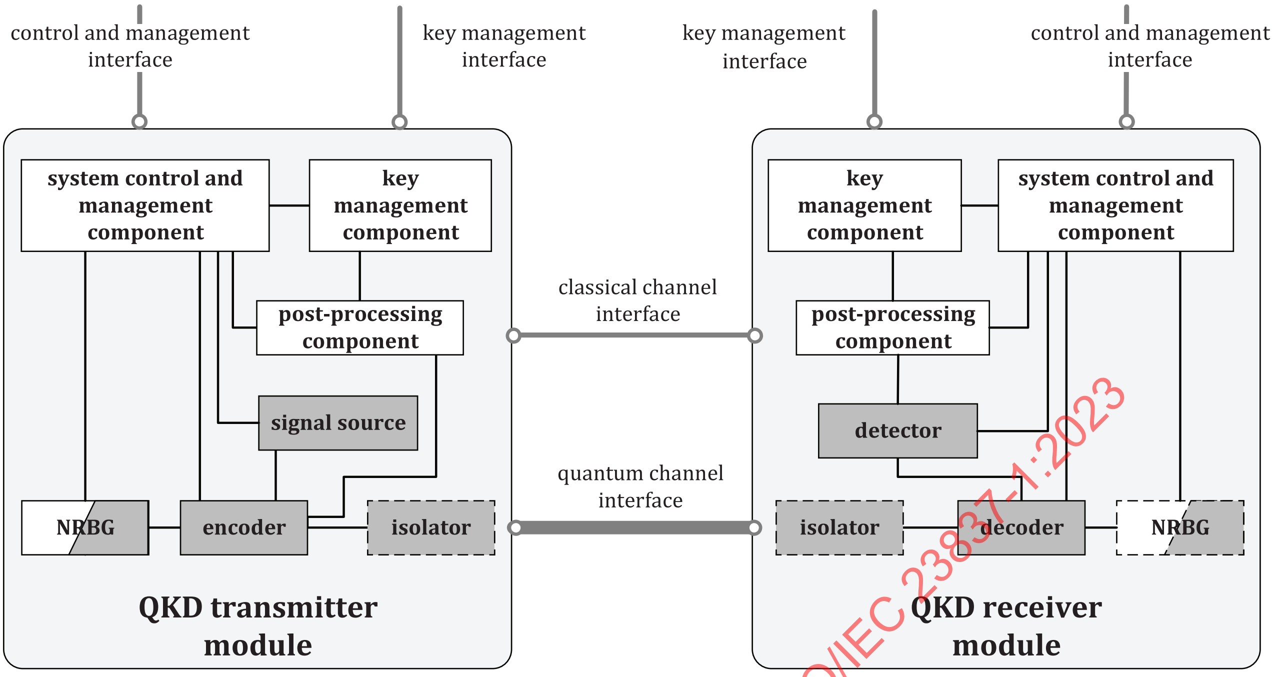
control and management interface
key management interface
key management interface
control and management interface
system control and management component
key management component
post-processing component
signal source
NRBG
encoder
isolator
QKD transmitter module
classical channel interface
quantum channel interface
key management component
system control and management component
post-processing component
detector
isolator
decoder
NRBG
QKD receiver module

Figure 5 — Generic internal structure of a PM-QKD protocol implementation

a) The internal structure of the QKD transmitter module and receiver module shown in Figure 5 corresponds to the PM-QKD scheme shown in Figure 1. The components shown in each module are typical of the functional components that make up such QKD transmitter or receiver modules.

b) The internal structure of the two transmitter modules of an MDI-QKD protocol is similar to the transmitter module shown in Figure 5. However, the internal structure of the receiver module is irrelevant from a security point of view and is therefore not considered in this document. See the analysis of the architecture of MDI-QKD protocols in 5.4.

c) The internal structure of the two receiver modules of an EB-QKD protocol is similar to the receiver module shown in Figure 5. However, the internal structure of the transmitter module is irrelevant from a security point of view and is therefore not considered in this document. See the analysis of the architecture of EB-QKD protocols in 5.4.

The division of components lays the foundation for the description of the threat analysis in Clause 7, the security functional requirements in Clause 9, and the evaluation activities in ISO/IEC 23837-2. In order to clearly understand the security problems of QKD modules, components in a QKD module are grouped as two types hereinafter. Specifically, the boxes shown in Figure 5 with a white background are identified as conventional network components, while the solid boxes are identified as quantum optical components. The characteristics of the NRBG component depend upon the implementation, as explained in 6.3.2 and 6.3.3, and it is represented by a half-solid box.

It is emphasized that the division of components is only instructive. The components in a QKD module can be subdivided into more specific elements, and the author of a PP or an ST may choose other ways to express the structure of the QKD modules.

6.3.2 Components in the QKD transmitter module

a) A generic QKD transmitter module includes a signal source component to produce photons as required by the implemented QKD protocol. The signal source component may include a functionality to modify the intensity of the optical signals it emits, and functionality to encode information.

b) The photon(s) are transmitted into the encoder component (for protocols in which information is encoded and where this functionality is not part of the signal source component) to adjust their state for information coding. The information is encoded on a set of the states of the photon(s), depending on the QKD protocol and the coding scheme, such as specified by the phase, polarization, or time-bin. The encoder component may include functionality to modify the intensity of the optical signals.

c) Some QKD transmitter modules may adopt an isolation component (i.e. isolator) in order to prevent optical pulses from injecting back into the transmitter module via the quantum channel. Therefore, the isolation component is depicted by a dashed box as an optional component. The isolation component may include a functionality to modify the intensity of the optical signals.

d) A non-deterministic random bit generator (NRBG) component is required to randomly choose, e.g. basis and bit values for signal coding and generating keying material. The NRBG can be realized with the conventional physical-noise-based schemes as specified in ISO/IEC 18031, or quantum-principle-based schemes (QRBG). It is regarded as a conventional network component if a conventional physical-noise-based design is used in the implementation, and a quantum optical component if a quantum-principle-based design is employed. Therefore, the NRBG component is depicted as a half-solid box in Figure 5.

e) The post-processing component handles the post-processing procedure related tasks including sifting, parameter estimation, error correction, and privacy amplification of a QKD session.

f) In general, coordination and management of the system is under the charge of the system control and management component. This component may rely upon a fundamental operating system (which usually is in the form of an embedded chip-based system) to support the control function (including flow control functions of raw data generation and post-processing procedures) and the following administrative services for the operation of the QKD module:

- audit of operational events;
- operator identification/authentication;
- access control of security-related information (as described in the description of assets in 7.3), which may rely upon the fundamental operating system to be effective;
- configuration and management of system parameters related to role management, access control, life cycle control of the QKD module etc., in which all configurations permitted by the system control and management component shall allow the module to produce secure final keys. A PP or an ST should provide a detailed description of the life cycle of the TOE and the different roles or users in each phase of it, such that the security requirements during each life cycle phase can be clearly understood. A PP or an ST should also describe the conditions and protection means that trigger or release the transition from one phase to the next;
- system debugging;
- firmware/software update.

NOTE 1 The life cycle of a QKD module, like a common IT product, is composed of a high-level of phases including for example the design phase, development phase, pre-operation phase, operation phase and maintenance phase, spanning the life of the QKD module from the definition of its requirements to the termination of its use. When shifting from one phase to a new phase, a QKD module is expected to be configured appropriately to ensure its security. This can be controlled by the manufacturer or operator.

g) The purpose of the key management component is to realize the key management interface of a QKD module to communicate with an external KM, and the key management function for keying material (as defined in 7.3) inside the QKD module. In detail, the key management component is expected to:

- upload a part of the newly generated final key from the QKD module to the external KM;
- optionally download the pre-shared key (from the external KM) used for the QKD authentication key of the first QKD session;

- store the pre-shared key and a part of the newly generated final keys for message authentication;
- ensure the confidentiality and integrity of the key uploading and downloading processes;
- destroy keying material that is no longer needed.

This document specifies key access and destruction functions inside the QKD module, but leaves other potentially required functions of the key management, such as key derivation and storage, to be specified in a PP or an ST. Moreover, the specification of the key management function of the external KM is out of the scope of this document.

NOTE 2 In practice, the security related to key access is mainly ensured by the access control mechanism of the QKD module. Specifically, the accessibility of the QKD authentication key can be restricted by the access control mechanism, such that only privileged processes (such as for post-processing procedure) can access or use it. The access to final key or keying material can also be restricted to only privileged processes by the access control mechanism. Furthermore, the access control mechanism related to key access can be realized by the system control and management component, or by the key management component itself.

6.3.3 Components in the QKD receiver module

The internal construction of the QKD receiver module is similar to that of the QKD transmitter module, with the main differences being:

a) The decoder and detector components in the receiver module shall decode signals encoded by the signal source and encoder components in the transmitter module to which it is connected. The isolation component in the receiver module strongly attenuates optical pulses inside the receiver module before they can exit the QKD receiver module to the quantum channel.

b) The NRBG block of the drawing in Figure 5 can be implemented by a passive beam splitter instead of a real NRBG. In either case, the implementation provides the function of random selection of the decoding basis, and evaluation activities should always be performed to check for any imperfections of the implementation. For that reason, the NRBG block is defined as optional and drawn with dashed lines.

6.4 TOE scope for QKD modules

6.4.1 General

Based on the structural analysis of a typical QKD module, it is possible to define a common TOE security functionality (TSF) and the scope of TOE for security evaluation of QKD modules, even if the QKD protocol architectures and implementation strategies are diverse in reality.

6.4.2 Definition of the TSF

Regarding the definition of the TSF, a set of common functions of QKD modules can be formalized by considering the role of the components described in 6.3. Generally, the TSF shall at least comprise the following three types of functions, and each type is composed of concrete functions as detailed below.

a) Quantum key distribution function (FUN_QKD), mainly includes the functions of raw data generation and post-processing procedures. In addition, the QKD modules of a QKD system may implement a parameter adjustment procedure in the raw data generation function.

b) System control and management function (FUN_SCM), implemented by the corresponding component of control and management of the QKD modules, mainly includes the flow control function and relevant management services listed in 6.3.

c) Key management function (FUN_KM), implemented by the key management component in the QKD modules to realize the functions of key uploading and downloading between the QKD modules and their relevant KMs, and key destruction as listed in 6.3.

Generally, the above listed three types of functions cover the most fundamental functionality of QKD modules. It means, without considering system exceptions and attacks, the QKD modules can be operated to generate the final key so long as those functions are correctly implemented. However, from the viewpoint of practical security, components within a QKD module can contain vulnerabilities, which can potentially be discovered after deployment as the attack methods evolve over the time. Attacks are conducted via the external interfaces of the QKD module, therefore the QKD module shall protect itself from intrusion and exploitation of vulnerabilities via its external interfaces, and it thus shall additionally include:

d) Self-protection function (FUN_SP), protects the TSF itself from attacks. This mainly involves the protection functions aiming to resist side channel attacks via the quantum channel, the self-testing function, information retention control, system recovery from failure, parameter adjustment etc.

It is noted that not all of the specific functions can be clearly listed in this document, since the concrete scope of TSF can only be well identified by considering the specific protocols and implementation strategy. Therefore, this document mainly provides a generic description of the definition of TSF. The author of a PP or an ST shall formalize the concrete definition of the TSF when more information is collected about the implementation.

NOTE The parameter adjustment function of QKD modules is assigned in this document as a part of the raw data generation procedure. Nevertheless, the adjustment is logically a part of the self-protection function, as it ensures the correct function of the QKD module. In addition, the parameter adjustment function is not a part of the self-testing function, as described in the security functional requirements of FPT_TST.1 in 9.2.22 and FTP_QKD.1 in 9.3.2.

6.4.3 Definition of the TOE

Although it is hard to give the concrete scope of the TOE for a QKD system in this document (which is in fact the role of a PP or an ST), a general scope of TOE for a QKD system can be established by considering all the necessary functions described in 6.4.2. In short, the TOE in this document shall in principle include all of the components that realize the functions of FUN_QKD, FUN_SCM, FUN_KM and FUN_SP. The TOE does not include the quantum channel and classic channel even if they are required by the QKD system for proper operation. However, the TOE includes the implementation components of the external interfaces that connect with the quantum channel and the classical channel.

In this way, the TOE defined above is a distributed one. Specifically, the definition of TOE is related to the architecture of the implemented protocols.

a) Regarding the case of PM-QKD protocols, the TOE incorporates the separated two modules corresponding to the QKD transmitter party and QKD receiver party respectively, and the relevant implementation components of external interfaces as shown in Figure 4. Therefore, a TOE defined to include only the individual QKD transmitter module or receiver module is not supported by the ISO/IEC 23837 series.

b) Regarding the case of MDI-QKD protocols, the TOE incorporates the two transmitter modules and the implementation components of the external interfaces of the two modules. The receiver module, in this case, is not included in the scope of the TOE. This is because the receiver module, though indispensable for the proper execution of the QKD functionality of MDI-QKD protocols, is not required to be trusted for the security of the QKD system.

c) Regarding the case of EB-QKD protocols, the TOE incorporates the two receiver modules and the implementation components of the external interfaces of the two modules. The transmitter module, in this case, is not included in the scope of the TOE. This is because the transmitter module, though indispensable for the proper execution of the QKD functionality of EB-QKD protocols, is not required to be trusted for the security of the QKD system.

NOTE 1 The above definition of TOE excludes the receiver module in MDI-QKD and the transmitter module in EB-QKD from the scope of security evaluation. Passing the security evaluation provides the simplification that the TOE can be deployed with any correctly functioning receiver module and transmitter module in MDI-QKD protocols and EB-QKD protocols, respectively. This definition does not deny other cases in which those modules are also expected incorporated into the TOE, e.g. the developer and evaluator can treat them as a non-TSF part of the TOE.

NOTE 2 For some specific implementation strategies, a few components shown in Figure 5 are claimed as optional. If those components are not implemented in the QKD module, they do not exist to be part of the TOE. For example, if there is no NRBG in the implementation of the QKD receiver module, e.g. a passive beam splitter is employed to realize the same function, an NRBG does not exist to be a part of the TOE.

6.5 General working flow of QKD modules

The working flow of a QKD module that participates in forming a QKD system may generally be described as comprising three stages:

a) Stage one: initialization stage. In this stage, each QKD module of the QKD system bootstraps, initializes itself, and performs start-up tests of its major functional components, such as the cryptographic component, its software and firmware integrity and, if part of the TOE, of the NRBG. Moreover, for some implementations, a mutual authentication procedure between the QKD modules of the QKD system can be required before proceeding to the raw data generation stage.

b) Stage two: raw data generation stage. In this stage, quantum signals are transmitted over the quantum channel and detected by the legitimate parties to generate raw data, i.e. correlated data with noise. The QKD modules of the QKD system may adjust certain parameters under appropriate restrictions during the raw data generation stage to ensure stable and secure operation.

c) Stage three: post-processing stage. In this stage, a post-processing protocol is implemented on the raw data to generate a shorter symmetric key, which is the final key. In detail, the post-processing stage generally includes four sub-stages: sifting, parameter estimation, error correction and privacy amplification, as described in 5.2 b).

NOTE Stage two and stage three correspond to the implementation of procedure one and procedure two of the generic QKD protocol shown in 5.2, respectively.

7 Security problems analysis of QKD modules

7.1 General

This clause intends to provide a basis for the development of a security problem definition in a PP or an ST for QKD modules. Due to the diversity of implementation strategies of QKD modules, this document mainly addresses those security problems which are common to various QKD implementations. Security problems going beyond the general cases are not addressed in this document.

7.2 and 7.3 form the basis for the subsequent threat analysis in 7.4 and 7.5. Specifically, the threats caused by the vulnerabilities of QKD modules are described as two types of threats, according to the component division method in 6.3; namely, threats related to conventional network components and threats related to quantum optical components.

NOTE The division does not remove the possibility that an actual attack upon QKD modules can attempt to leverage vulnerabilities across both types of components.

7.2 Security assumptions

Theoretically, a QKD protocol can establish keys with a security claim that does not depend upon the computational power of an adversary under the assumptions made by the security proof model of the QKD protocol. However, as far as practical security is concerned, those assumptions are expected to be translated accordingly. Specifically, some of the assumptions made in the security proof model can be translated into security functional requirements, which shall be realized with some mechanisms and validated during the evaluation of QKD modules. Some other assumptions made in the security proof model, however, shall be reserved and translated into assumptions on the operational environment, which are necessary for QKD modules to work properly in specific settings but will not be validated during the QKD security evaluation. In more detail, the assumptions on the operational environment of QKD modules include at least the following three aspects:

a) The QKD module is physically protected in its operational environment:

   1) The TOE is assumed to operate in a protected environment such that any threat agents cannot approach the QKD module, and a minimum geographical distance between them is enforced by the security and assurance measures of the operational environment. This assumption removes the possibility that the TOE is subject to physical security invasive and partial non-invasive attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. As such, the ISO/IEC 23837 series does not include the requirements on physical tampering protection and resistance to some kinds of side channel attacks. See 7.4.2 for those side channel attacks that are (or not) considered in this document.

      NOTE 1 In other words, the TOE itself is not expected to defend against physical access that allows unauthorized entities to extract data, bypass access controls, or manipulate the TOE.

   2) This assumption is not meant to remove the possible threats via the external interfaces to the QKD module. For example, in some use-cases, a QKD module and an external KM connected to it are located within a physically protected environment where the channel between them is protected at a same security level as well, so the environment can guarantee the security of communications over the channel. In other use-cases, however, the channel is not protected at the same security level, and internal adversaries (i.e. threat agents inside the organization) can eavesdrop upon or tamper with the communications over it. Consequently, countermeasures should be adopted to protect the communications over it. Though the first scenario is more common in practice, this document from a pragmatic view intends to relax the assumption on physical protection of the whole TOE. That is, only the QKD module (excluding its external interfaces) is assumed to be physically protected by the operational environment, but remote threat agents can connect to its external interfaces to conduct adverse actions. This strategy is logical since a TOE that is secure in an environment with weaker assumptions will also be secure in an environment with stronger assumptions, but the reverse is not always true. The starting point of this document is to state the security functional requirements on the protection of communications over the key management interface, as well as the control and management interface. See: SFRs FCS_COP.1, FDP_ITC.1, FIA_UAU.2, FPT_ITC.1 and FPT_ITI.1 for details. The author of a PP or an ST can strengthen the assumption by assuming that the QKD module and its external interfaces are both protected in a physically protected environment. In this case, some of the SFRs (on the protection of communications over the key management interface as well as the control and management interface) are not necessary anymore. This operation is supported by the conformance requirements in 10.2 a) 3).

      NOTE 2 By adoption of the weaker assumption on the environment, the tolerable computing power of the threat agents is analysed as follows. First, due to the security proof model of QKD protocols, the computing power of the threat agent over the quantum channel interface and the classical channel interface can be unbounded, meaning that it is only limited by the laws of quantum mechanics. On the other hand, the computing power of the threat agents over the key management interface as well as the control and management interface are assumed to be bounded, which means that the security mechanisms protected with the computational security can be applied to protect these interfaces when considering internal adversaries.

   3) The author of a PP or an ST shall not remove or reduce this assumption (or a part of it) unless specific mechanisms or components to address physical security attacks are implemented in the TOE. See 10.2 a) 1) for more information.

b) Operators are trusted. It is assumed that operators of the TOE (including system administrator, auditor or any other legitimate roles operating the TOE) act in the best interests of the security of the organization, which includes being appropriately trained, following a security policy, and adhering to user guidance. It is also assumed that the administrators follow specific guidance to run the system configuration and the update of firmware and software regularly, in response to the release of patches or product updates due to known vulnerabilities and technical improvements.

c) It is assumed that the pre-shared key is confidential and randomly generated before it is input into the QKD module.

7.3 Assets analysis

Some data and functionality inside a QKD module shall be protected from leakage or damage in order to ensure the security of the QKD module. For the general QKD module defined in this document, the assets are identified in following list. However, the concrete list of assets defined in a PP or an ST can only be supplemented according to the specific implementation of the QKD module.

a) Final key output from the implementation of QKD protocols. To ensure the security of the final key, all the relevant security-related information shall also be treated as individual assets and protected from leakage or damage throughout a defined life cycle. In greater detail:

   1) The keying material includes:

      — the raw data, sifted data, error corrected data produced during the execution of the QKD system;

      — the QKD authentication key for message authentication over the classical channel;

      — the keys used for the confidentiality and integrity protection of communications between the KM and the QKD module for final key uploading (and optionally pre-shared key downloading).

   QKD protocols assume that parts of the raw data, sifted data, and error corrected data can be known by a threat agent following quantum state transmission and that parts can be disclosed during post-processing stage. However, such anticipated leakages and disclosures are estimated during parameter estimation to enable appropriate privacy amplification to be performed to generate the final key. Assets shall be protected according to the appropriate attack potential from any other leakage or damage.

   A sifting step (thus sifted data) is not necessary in some CV-QKD protocols using heterodyne measurements.

   2) The user authentication data includes passwords, PINs, credentials and relevant data for user authentication of the operator.

   3) Other security-related information includes audited events, audit data, control and management information communicated via the control and management interface, and other information that support the security of the TOE.

   The final key, keying material, authentication data and the relevant security-related information are recognized as a part of the TSF data of the TOE.

b) The functionalities of QKD modules that must be protected from misuse by illegitimate users.

7.4 Threats to conventional network components

7.4.1 Overview

As a particular type of network device, QKD modules are potentially vulnerable to attacks similar to conventional network devices. Any significant vulnerability hidden in QKD modules can potentially attract practical attacks from the perspective of cryptographic engineering practice. A closer look at the structure of a typical QKD module can potentially reveal ways that threat agents can conduct adverse actions via the network interfaces of the module, changing the operational environment or even probing the circuit of internal chips of the device (considering network-based attacks, side channel attacks and physical tampering attacks, for example). Specifically, threat agents can use various strategies to compromise the assets by circumventing the access control mechanism, breaking the message authentication scheme or abusing the maintenance functions of the QKD module. The diversity of attack paths makes it difficult to list all possible threats to QKD modules, but from a practical point of view, the following threats cited in 7.4.2 shall be addressed by QKD modules and their operational environment through either IT-related controls, or non-IT controls (such as environmental protections or organizational procedures/policies).

7.4.2 Threats from the perspective of network-based classical attacks

The description of threats for network devices, given in the collaborative Protection Profile for Network Devices[14], can be referred to as part of a threat analysis for QKD modules. Conventional network-based attacks are mainly conducted via the classical external interfaces of QKD modules (see 6.2), including the control and management interface, the key management interface and the classical channel interface. These attacks can be performed at a remote distance, where the threat agents are not required to approximate the TOE or physically get hold of the TOE. For convenience, the threats considered in this document are roughly grouped according to the relationship of attack paths and presented in alphabetical order.

NOTE The threats listed below are not intended to be a complete list of all possible threats to QKD modules, but reflect the current academic and industrial understandings on the security of network devices and QKD modules. In addition, the identified threats can have dependencies on each other. As threats are usually implemented by threat agent constructed attack paths, they can interact and interface with each other. However, compromising the assets of a QKD module is the common objective of all the identified threats.

a) Audit circumvention. As a particular type of network device, a QKD module is required to provide a system audit function to the administrators. This function should provide either the option to monitor the system execution status or the option to exploit recorded audit data. However, the audit implementation can potentially include faults that enable the threat agents to access, bypass, or modify the audit data or audit functionality without having administrator privileges and without alerting an administrator. The circumvention of the audit function further enables the threat agents to compromise the assets of a QKD module without an administrator noticing that the module has been compromised.

b) Cryptographic vulnerability exploitation. A QKD module employs cryptographic mechanisms to realize its core functionality, especially the functions related to post-processing procedure (including at least the message authentication and privacy amplification functions), key uploading to the relevant KM after a successful QKD session, and user authentication before login into the QKD module, etc. Threat agents can attempt to compromise a QKD module and its assets by exploiting any hidden vulnerabilities in cryptographic algorithms, or the design and implementation of the cryptographic protocols and procedures.

c) Failure exploitation. During the operation phase of a QKD module, various failures can occur for several possible reasons, including errors in the TOE, instability of the operational environment (including abnormal variations of the environmental temperature or the power supply), interference with communications over the quantum channel and/or classical channel conducted by the threat agents, attacks by threat agents exploiting unknown and hidden vulnerabilities in the TOE. It is important for the QKD module to preserve a secure state if a failure occurs, otherwise threat agents can exploit an achieved failure state to compromise the assets of the targeted QKD module.

d) Function abuse. During the development, pre-operation, operation and maintenance phases of the life cycle of a QKD module, some functions related to testing, debugging or management may be required to facilitate the development or administration purpose. These functions shall be managed well (including removing or locking them after life cycle phases transition) during the whole life cycle of the TOE. Otherwise, threat agents can abuse those functions to compromise the assets of the targeted QKD module.

e) Physical security violation. A QKD module should be protected from invasive and non-invasive physical attacks. The following discusses an excerpt of restricted physical attacks and should be completed for a concrete QKD implementation:

- A physical invasive attack results in a physical alteration of the QKD module. This class of attack is excluded from the scope of this document as it is assumed that the QKD module is appropriately protected by its operational environment in this document [see 7.2 a)].
- Some physical non-invasive attacks require the attack threat agent close enough to the QKD module, for example to induce faults or conduct simple/differential power or electromagnetic attacks. These attacks are also excluded from the discussion as it is assumed that the QKD module is appropriately protected by its operational environment [see 7.2 a)].
- This document only considers remotely exploitable physical non-invasive attacks, which can be conducted outside of the boundary of physical protection or even over a long distance from the QKD module (namely remotely exploitable physical attacks), such as timing attacks (see ISO/IEC TS 30104:2015, 9.2), cache-timing attacks or any other attacks not requiring direct contact with the QKD module to retrieve exploitable side-channel information.

f) Randomness defect exploitation. Random bit strings are used in a QKD module for the following purposes:

- random encoding of the quantum state;
- random selection of the measurement basis;
- random selection of bits for error estimation;
- random selection of the universal-hashing function for privacy amplification;
- random assignment to handle the double-click events;
- acting as the nonce for user authentication (e.g. the challenge-response based protocols);
- other purposes for post-processing procedure.

The NRBG in a QKD module is important to maintain the secure state of operation. Entropy deficiencies in the output of the NRBG can be exploited by threat agents to predict or directly retrieve information, in order to harm the above listed functions and compromise the assets of the TOE.

g) Residual data misuse. A QKD module is expected to handle security-related information as an essential part of producing final keys and maintaining its secure state. For security reasons, the validity period of parameters and information should be limited to a reasonable duration. In other words, after a specified timescale, they shall be deleted in a timely and irreversible manner from the QKD module. Otherwise, if threat agents penetrate a QKD module they can potentially extract or recover the parameters and information to compromise historical assets of the targeted QKD module.

h) Unauthorized access. Access to the management and maintenance functions of a QKD module requires appropriate secure access control mechanisms to be in place. Threat agents can attempt to exploit possible design and implementation vulnerabilities of the access control mechanisms by:

- penetrating the access control mechanism from the control and management interface;
- discovering erroneous configurations of the TOE to achieve access as an administrator or any other privileged operators;
- applying stolen or in other ways procured credentials to circumvent the access control mechanism as an administrator or any other privileged operators;

— (for some possible implementations) masquerading as a valid QKD module to trick other QKD modules into forming a QKD system and executing QKD sessions with it.

All of the above enable the threat agent to retrieve unauthorized information and compromise the assets of the QKD module.

EXAMPLE A QKD module can require user authentication before logging into the system, and can potentially operate access control mechanisms at the system-level to control any access to an asset. Especially, the plaintext of final keys is by design made inaccessible to any operator, even to the administrators.

7.5 Threats to quantum optical components

7.5.1 Overview

To better analyse the threats related to exploiting the security vulnerabilities of quantum optical components of QKD modules, active and passive vulnerabilities are considered which generally correspond to two different adversarial strategies of the threat agents. Active vulnerabilities are defined as leakage of information caused by an active type of attacks, such as a Trojan horse attack, a source tampering attack, or a blinding attack. Passive vulnerabilities comprise the side-channel vulnerabilities coming from the imperfections of the optical components, such as imperfect state modulation, pulse intensity fluctuations, and detection efficiency mismatch of single-photon detectors. The following is devoted to analysing these vulnerabilities in detail.

NOTE A more comprehensive survey of attacks on QKD systems can be found in the ETSI White Paper on the Implementation Security of Quantum Cryptography[13].

7.5.2 Threats exploiting optical source flaws

Threat agents can attempt to exploit the vulnerabilities of quantum optical components (including signal source and encoder) of the QKD transmitter module to compromise the final key. This class of threats may relate to the QKD transmitter module of both the PM-QKD protocol and MDI-QKD protocol.

EXAMPLE In a DV-QKD module, the phase of each signal pulse is typically supposed to be uniformly randomized, but in practice, this cannot be achieved in all cases. Where not achieved, the threat agents can try to partially distinguish the quantum states prepared by the QKD transmitter module by measuring these states in phase space. Other attacks to achieve the threat have also been discovered based on the flaws of source, such as source tampering attack, Trojan-horse attack, imperfect state preparation and un-randomization phase of signal source.

7.5.3 Threats exploiting optical detection vulnerabilities

Threat agents can attempt to exploit the vulnerabilities of one or more quantum optical components (including the decoder and detector) of the QKD receiver module. If successful, this can potentially enable them to compromise the final key. This type of threat can be to a QKD receiver module operating either a PM-QKD protocol or some EB-QKD protocols.

EXAMPLE It is known that two single-photon detectors are used in most QKD receiver modules, but it is difficult to perfectly match the two single-photon detectors in any degree of freedom, e.g. time, frequency, and polarization. Then, based on the mismatch of the single-photon detectors, it is possible for the threat agents to totally or partially control the click of the single-photon detector by controlling the parameters of the input quantum state. Other attacks have also been discovered based on the flaws of detection, such as a blinding attack, faked state attack, dead-time attack and wavelength attack.

7.5.4 Threats exploiting parameter adjustment vulnerabilities

Threat agents can attempt to exploit any vulnerabilities hidden in the implementation of the parameter adjustment procedure. This type of situation involves the threat agent managing to deceive the QKD modules to operate as if the QKD system were in a safe state, when this is not the case. If successful, this can lead to a compromise of the final key generated by the QKD modules. This type of threat can be to either a QKD transmitter or a receiver module operating a PM-QKD protocol, or to a transmitter module operating an MDI-QKD protocol, or to a receiver module operating an EB-QKD protocol.

EXAMPLE Before or during a QKD session, it is expected that the QKD transmitter module and the receiver module can adjust the parameters of their system, such that the timing of single-photon detectors match the arrival time of the quantum state. Threat agents can try to actively change the timing of the different signals used to adjust the time of the different single-photon detectors. If successful, an active time-mismatch vulnerability could have been introduced.

8 Extended security functional components for QKD implementation

8.1 General

Generally, the standardized security functional components defined in ISO/IEC 15408-2 can be used to describe the security requirements of QKD modules. However, since the standardized security functional components cannot be refined or tailored in a straightforward manner to appropriately address all of the special characteristics of QKD modules, extended security functional components shall be defined.

The standardized security functional class FTP (Trusted path/channels) in ISO/IEC 15408-2 is defined to specify requirements on the establishment of a trusted channel between network-connected parties (or more specifically, the TSF and another trusted IT product). Since QKD protocols can be used to achieve a similar goal (by noting that the final key generated by QKD protocols can be used to establish trust channels between the users of the keys), it is appropriate to extend the security functional components in the class of FTP to cover QKD security functions. Specifically, the extended security functional components FTP_QKD.1 and FTP_QKD.2 for specifying the implementation of QKD protocols are described in 8.2.

8.2 Extended security functional components to Class FTP: Trusted path/channels

8.2.1 Quantum key distribution (FTP_QKD)

8.2.1.1 Family behaviour

This family defines requirements for the key establishment between the QKD modules in a homogenous QKD system. This means that the QKD modules involved implement the same QKD protocol. The family includes requirements for the implementation of raw data generation and post-processing stages, corresponding to the general working flow of QKD modules described in 6.5.

This family should be included whenever there are requirements for cryptographic keys to be established securely by a QKD protocol.

8.2.1.2 Component levelling and description

Figure 6 shows the component levelling for this family.

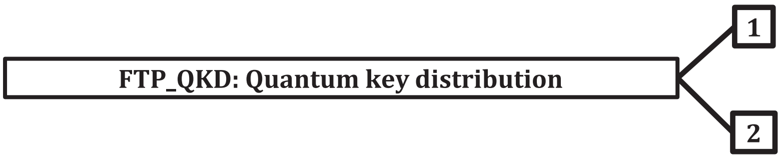

Figure 6 — FTP_QKD Quantum key distribution

FTP_QKD.1 QKD protocol and raw data generation require symmetric keys to be established in accordance with a defined protocol involving the transmission and detection of quantum signals. This includes configurations negotiation and parameter adjustment where needed.

FTP_QKD.2 QKD post-processing requires symmetric keys to be securely established by the QKD modules from the raw data according to the QKD protocol.

8.2.1.3 Management of FTP_QKD.1

The following actions can be considered for the management functions in FMT, including the management of:

a) the supported protocols of the QKD module;

b) the functional role that the QKD module supports;

c) the rules for carrying out message authentication;

d) the static parameters required by the QKD module;

e) the available configurations for the QKD module.

8.2.1.4 Management of FTP_QKD.2

The following action can be considered for the management functions in FMT:

a) Management of the supported schemes for each sub-procedure of the post-processing procedure.

8.2.1.5 Audit of FTP_QKD.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Failure of raw data generation procedure.

b) Minimal: Failure of a parameter adjustment procedure.

c) Minimal: Identifications of the implemented QKD protocol.

d) Minimal: Identifications and role of the communication parties.

e) Basic: Attempted execution of raw data generation procedure.

f) Basic: Triggering of a parameter adjustment procedure.

g) Detailed: The static parameters used in the implementation of the QKD protocol.

h) Detailed: The configurations negotiated by the QKD system during the execution.

i) Detailed: The message authentication mechanism chosen for the execution.

j) Detailed: The raw data generated in case of a failed execution of raw data generation procedure.

NOTE The levels of audit, such as “minimal”, “basic” and “detailed”, are defined by the components of the security audit data generation (FAU_GEN) family, as described in ISO/IEC 15408-2:2022, 7.1.3.6.

8.2.1.6 Audit of FTP_QKD.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Failure of a post-processing procedure, including the specific steps during which the procedure failed.

b) Basic: Attempted execution of a post-processing procedure.

c) Basic: The identification of the schemes used in the post-processing procedure for sifting, parameter estimation, error correction and privacy amplification.

d) Detailed: The intermediate values related to sifted data, corrected key or final key in case of a failed execution of post-processing stage.

8.2.1.7 FTP_QKD.1 QKD protocol and raw data generation

Component relationships:

Hierarchical to: No other components.

Dependencies: FTP_QKD.2 QKD post-processing

a) FTP_QKD.1.1

The TSF shall implement [assignment: QKD protocol] acting as [assignment: defined protocol role(s)].

b) FTP_QKD.1.2

The TSF shall implement one or more of the following mechanisms: [assignment: list of secure message authentication schemes] to authenticate relevant data transmitted over the classical channel, according to the following rules: [assignment: list of rules for carrying out the authentication].

c) FTP_QKD.1.3

The TSF shall permit [assignment: list of QKD modules of the TOE] to initiate execution of the QKD protocol.

d) FTP_QKD.1.4

The TSF shall enforce the following static protocol options: [assignment: list of options].

e) FTP_QKD.1.5

The TSF shall negotiate one of the following protocol configurations between the QKD modules of the TOE: [assignment: list of configurations] over the classical channel.

f) FTP_QKD.1.6

The TSF shall initiate [assignment: list of parameter adjustment procedures] to adjust parameters of it, with each of the assigned parameter adjustment procedures specified as follows:

1) Trigger methods: [selection: on demand by an authorized user, triggered by [assignment: list of detected failure events], triggered by [assignment: list of other trigger events]];

2) Restrictions on execution: [selection, choose one of: allowed to run simultaneously with QKD session(s), not allowed to run simultaneously with QKD session(s), [assignment: list of other restrictions]];

3) Parameters to be adjusted: [assignment: list of parameters to be adjusted].

g) FTP_QKD.1.7

During the execution of a parameter adjustment procedure, the TSF shall preserve a secure state. The TSF shall not execute any parameter adjustment procedure simultaneously with a QKD session, unless the parameter adjustment procedure is allowed to run simultaneously with QKD session(s).

h) FTP_QKD.1.8

The TSF shall indicate the status when the TOE is running the following operations: [selection: key generation, parameter adjustment procedures not allowed to run simultaneously with, or [assignment: list of other operations]].

i) FTP_QKD.1.9

The TSF shall generate raw data and pass it to the post-processing procedure.

8.2.1.8 FTP_QKD.2 QKD post-processing

Component relationships:

Hierarchical to:	No other components.
Dependencies:	FTP_QKD.1 QKD protocol and raw data generation

a) FTP_QKD.2.1

The TSF shall implement the post-processing procedure aligned with the QKD protocol specified in FTP_QKD.1.1.

b) FTP_QKD.2.2

During the post-processing stage, the TSF shall use one of the following mechanisms [assignment: sifting schemes] for sifting.

c) FTP_QKD.2.3

During the post-processing stage, the TSF shall use one of the following mechanisms [assignment: parameter estimation schemes] for parameter estimation.

d) FTP_QKD.2.4

During the post-processing stage, the TSF shall use one of the following mechanisms [assignment: error correction schemes] for error correction.

e) FTP_QKD.2.5

During the post-processing stage, the TSF shall use one of the following mechanisms [assignment: privacy amplification schemes] for privacy amplification.

f) FTP_QKD.2.6

During the post-processing stage, if the chosen error correction scheme does not include a consistency check the TSF shall check the consistency of the relevant keying material between the QKD modules of the TOE after error correction. This integrity check shall use one or more of the following consistency check schemes: [selection: error correction schemes, [assignment: list of other schemes]]. If an inconsistency is detected the TSF shall [selection: abort the QKD session without producing a final key, [assignment: list of actions]].

NOTE 1 An additional post-processing procedure can be performed after the consistency check, such as privacy amplification. If the mechanism used to perform the consistency checks involves any potential leak of information about the key, the potentially disclosed information is expected to be accounted for in the QKD protocol.

NOTE 2 The consistency check can be a part of the error correction scheme for some implementations.

8.2.2 User notes

8.2.2.1 FTP_QKD.1 QKD protocol and raw data generation

8.2.2.1.1 User application notes

The security functional component should be used in situations where two parties want to establish a symmetric key with QKD modules. The security functional component gives the flexibility to the author of a PP or an ST to specify the expected QKD protocol, and the roles that the QKD modules of the TOE can function as in the protocol. Message authentication is indispensable for a complete QKD protocol but the component leaves the author of a PP or an ST author to specify the schemes corresponding to the security objective of the protocols. For the QKD modules involved in the QKD protocol, their roles should be commensurate to each other.

The TOE may implement more than one QKD protocol, and some of the assignment and selection operations in the elements of FTP_QKD.1 may be specific to particular QKD protocols. In this case, it is recommended that the author of a PP or an ST iterates FTP_QKD.1 to specify the SFRs for each QKD protocol implementation separately. The iteration operation shall meet the requirements in ISO/IEC 15408-2:2022, 8.2.2.

EXAMPLE If a TOE implements two different QKD protocols, the author of a PP or an ST can iterate FTP_QKD.1 to form two SFRs as follows: FTP_QKD.1/1 QKD protocol and raw data generation (Protocol 1), and FTP_QKD.1/2 QKD protocol and raw data generation (Protocol 2).

8.2.2.1.2 Assignment operation

In FTP_QKD.1.1, the first assignment is intended to state the QKD protocol that has been implemented in the QKD module. The assigned QKD protocol shall be accompanied with an associated security proof. The security proof shall be approved by the responsible evaluation authority. An evaluation authority may take the opinion of a reputable group, such as a standards developing organization, into account in deciding whether to approve a security proof. The second assignment is intended to state the defined protocol role(s) of each QKD module in the TOE, e.g. “QKD transmitter party” and/or “QKD receiver party”.

In FTP_QKD.1.2, the first assignment is intended to state the message authentication scheme(s) that the QKD protocol uses for the classical channel. The assigned scheme(s) can be secure without relying on limiting the computational power of an adversary (e.g. based upon families of hash functions that are 2-Universal) or computationally secure. It should be consistent with the security objective of the TOE as well as the rules specified in the second assignment. The assigned authentication rule shall be consistent with the implemented QKD protocol. A rule can be “all data traffic over the classical channel shall be authenticated except for [assignment: list of data traffic that is not required to be authenticated]”.

In FTP_QKD.1.3, the assignment is intended to specify the permitted initiator(s) of the QKD protocol, which can be one of the QKD modules of the TOE, or the two modules of it, depending on the QKD protocol and the implementation strategy of the TOE.

In FTP_QKD.1.4, if the QKD protocol has static configuration options, the assignment is intended to specify the static protocol options for the QKD implementation, such as signal coding methods and clock frequency for synchronization. The assignment can be “None”, which means the QKD protocol has no static configuration options. In this case, the element of the SFR is void, and no evaluation activities are specified.

In FTP_QKD.1.5, if the execution of QKD protocol is allowed to be customized with some parameters, the assignment gives the QKD modules the flexibility to negotiate the appropriate configurations for the proper operation of the QKD modules. The configurations depend on the specific protocol chosen to be implemented in the QKD modules and the implementations themselves, such as the time synchronization data, heartbeat detection interval, or specific options in terms of the message authentication schemes or post-processing schemes specified in FTP_QKD.1.2 and FTP_QKD.2 respectively. The assignment can be “None”, which means no configurations should be negotiated as per the implementation of the QKD protocol. In this case, the element of the SFR is void, and no evaluation activities are specified.

In FTP_QKD.1.6, the first assignment is intended to specify all parameter adjustment procedures implemented by the TOE. The second assignment specifies the failure events that trigger each specific parameter adjustment procedure. The third assignment specifies additional events (if any) that trigger each specific parameter adjustment procedure. The fourth assignment specifies additional restrictions (if any) on the execution of the parameter adjustment procedure, and the fifth assignment specifies the security-related parameters that are adjusted by the specific parameter adjustment procedure.

In FTP_QKD.1.8, the assignment is intended to specify additional operations (if any) that shall be indicated by the QKD modules, see the explanation of the selection operation of this element in 8.2.2.1.3. The assignment can be “None”, which means no additional operations are required to be indicated.

8.2.2.1.3 Selection operation

In FTP_QKD.1.6, the first selection is intended to define the signals or methods that trigger the parameter adjustment procedure, e.g. requested by an authorized user, or in response to a failure event. The second selection is intended to specify the restrictions on the execution of the parameter adjustment procedure, such as whether it is allowed to run simultaneously with QKD session(s). FTP_QKD.1.6 gives the author of a PP or an ST the flexibility to specify such restrictions, and a security-related justification should be made in an ST and optionally in a PP.

In FTP_QKD.1.8, the selection is intended to specify the operations that shall be indicated by the QKD modules so the operator can understand the status of the QKD system over time, in order to take timely actions to deal with alarms or emergencies. The indication may be recorded in the audit data, or in the form of sound, light, etc.

8.2.2.2 FTP_QKD.2 QKD post-processing

8.2.2.2.1 User application notes

This component should be used to specify the requirements on the post-processing procedure of the TOE, which generally includes four sub-procedures: sifting, parameter estimation, error correction and privacy amplification. For each such sub-procedure, if more than one scheme is implemented by the TOE, the QKD modules should negotiate the schemes as a part of the protocol configurations as specified in FTP_QKD.1.5.

If more than one QKD protocol is implemented in the TOE and different protocols require different post-processing procedures, it is recommended that the author of a PP or an ST iterate FTP_QKD.2 to specify an SFR for the post-processing procedure of each QKD protocol. The iteration operation shall meet the requirements in ISO/IEC 15408-2:2022, 8.2.2.

EXAMPLE If a TOE implements two different QKD protocols and the protocols require different post-processing procedures, the author of a PP or an ST can iterate FTP_QKD.2 to form two SFRs as follows:

- FTP_QKD.2/1 QKD post-processing (protocol 1), with mutual dependencies with FTP_QKD.1/1 QKD protocol and raw data generation (protocol 1);
- FTP_QKD.2/2 QKD post-processing (protocol 2), with mutual dependencies with FTP_QKD.1/2 QKD protocol and raw data generation (protocol 2).

A QKD protocol may combine sub-procedures of the post-processing procedure in order to perform post-processing in a more optimal manner. In such cases the elements in FTP_QKD.2 can be refined or combined according to Clause 10 and ISO/IEC 15408-2:2022, 8.2.5.

8.2.2.2.2 Assignment operation

In FTP_QKD.2.2, the assignment is intended to specify the name(s) of the sifting scheme(s), and requires a detailed description of it in an ST, and optionally in a PP. This assignment shall be aligned with the QKD protocol assignment in FTP_QKD.1.1.

In FTP_QKD.2.3, the assignment is intended to specify the name(s) of the parameter estimation scheme(s), and requires a detailed description of it in an ST and optionally in a PP. This assignment shall be aligned with the QKD protocol assignment in FTP_QKD.1.1.

In FTP_QKD.2.4, the assignment is intended to specify the name(s) of the error correction scheme(s), and requires a detailed description of it in an ST and optionally in a PP. This assignment shall be aligned with the QKD protocol assignment in FTP_QKD.1.1.

In FTP_QKD.2.5, the assignment is intended to specify the name(s) of the privacy amplification scheme(s), and requires a detailed description of it in an ST and optionally in a PP. This assignment shall be aligned with the QKD protocol assignment in FTP_QKD.1.1.

In FTP_QKD.2.6, the first assignment is intended to specify the name(s) of the consistency check scheme(s) of the post-processing procedure, and requires a detailed description of it in an ST and optionally in a PP. The consistency check procedure may be implemented as a sub-function of the error correction scheme. The second assignment is intended to specify the possible actions that the TOE performs in case that an inconsistency is detected in the keying material. Depending on the implementation, the key pair comparison step can be executed explicitly or implied in other steps of the whole post-processing procedure.

8.2.2.2.3 Selection operation

In FTP_QKD.2.6, the first selection is intended to specify the consistency check scheme(s) used in the implementation of the post-processing procedure. The second selection is intended to specify the actions the TOE performs if an inconsistency in the keying material is detected when they are expected to be identical.

9 Security functional requirements for QKD modules

9.1 General

This clause describes a baseline set of security functional requirements (SFRs) that a QKD module shall satisfy (see Table 3 for a list of the SFRs). The fulfilment of these SFRs is crucial for the TOE to maintain the protection against the potential threats analysed in 7.4 and 7.5. Therefore, these SFRs are mandatory and are the basis for writing PPs and STs. Considering the various implementations of QKD modules and their operational environment however, there are specified conditions in Clause 10 for the author of a PP or an ST to omit or customize the SFRs. This provides enough flexibility for implementations. If this applies in a concrete case, the author of a PP or an ST shall provide a justification for any SFR modification or its omission. See Clause 10 for a more detailed explanation on the principle of SFR modification from the perspective of conformance.

The SFRs are described in three groups: the requirements on conventional network components (see 9.2), the requirements on the implementation of QKD protocols (see 9.3), and the requirements on quantum optical components (see 9.4). From the perspective of security functionality, each of the SFRs can be assigned to one or more specific functions of the TSF, and each function can be realized by either the conventional network components or the quantum optical components, or a combination of both. The correspondence between them is described in the third and fourth columns of Table 3, respectively.

To provide sufficient flexibility for the implementation of QKD modules, operations in most of the SFRs are not completed in this document. When writing a PP or an ST, the completion of each operation of the SFRs shall meet the requirements in ISO/IEC 15408-1:2022, 8.2 and the relevant requirements on the usage of the security functional components in ISO/IEC 15408-2. Specifically, for the completion of assignments and selections in SFRs coming from the standardized security functional components in ISO/IEC 15408-2, the relevant principles in ISO/IEC 15408-2 for each of those security functional components shall be consulted in order to determine if "None" is a valid completion or not. In addition, the application notes below each SFR provide guidance on the selection of it, and provide more specific requirements or recommendations for completing it.

Evaluation methods and activities related to the SFRs are specified in ISO/IEC 23837-2. The ISO/IEC 23837 series provides a general framework for security evaluation of QKD modules under the framework of ISO/IEC 15408 series, and can be used to facilitate the development of PPs for QKD modules. Guidance for developing protection profiles for QKD modules is given in Annex A.

Table 3 — Overview of the baseline set of SFRs for QKD modules

Subclause	Security functional requirements	Security functions	Implementation components
9.2.1	FAU_GEN.1	FUN_SCM	Conventional network components
9.2.2	FCS_CKM.6	FUN_KM	
9.2.3	FCS_COP.1	FUN_QKD, FUN_SCM, FUN_KM	
9.2.4	FCS_RNG.1	FUN_QKD	
9.2.5	FDP_ACC.1	FUN_SCM	
9.2.6	FDP_ACF.1	FUN_SCM	
9.2.7	FDP_IRC.1	FUN_SP	
9.2.8	FDP_ITC.1	FUN_SCM	
9.2.9	FIA_UAU.2	FUN_SCM	
9.2.10	FIA_UID.1	FUN_SCM	
9.2.11	FMT_LIM.1	FUN_SCM	
9.2.12	FMT_LIM.2	FUN_SCM	
9.2.13	FMT_MSA.1	FUN_SCM	
9.2.14	FMT_MTD.1	FUN_SCM	
9.2.15	FMT_SMF.1	FUN_SCM	
9.2.16	FMT_SMR.1	FUN_SCM	
9.2.17	FMT_EMS.1/Convention	FUN_SP	
9.2.18	FPT_FLS.1	FUN_SP	
9.2.19	FPT_ITC.1	FUN_KM	
9.2.20	FPT_ITI.1	FUN_KM	
9.2.21	FPT_RCV.2	FUN_SP	
9.2.22	FPT_TST.1	FUN_SP	
9.3.2	FTP_QKD.1	FUN_QKD	Conventional network components and quantum optical components
9.3.3	FTP_QKD.2	FUN_QKD	Conventional network components
9.4.2	FPT_EMS.1/Quantum	FUN_SP	Quantum optical components
9.4.3	FPT_PHP.3	FUN_SP	Conventional network components and quantum optical components

9.2 General requirements for conventional network components in QKD modules

9.2.1 FAU_GEN.1 Audit data generation

9.2.1.1 Requirement

a) FAU_GEN.1.1. The TSF shall be able to generate audit data of the following auditable events:

   1) Start-up and shutdown of the audit functions;

   2) All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and

   3) [assignment: *other specifically defined auditable events*].

b) FAU_GEN.1.2. The TSF shall record within the audit data at least the following information:

   1) Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

   2) For each auditable event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

9.2.1.2 Application note

The SFR specified in 9.2.1.1 is intended to protect QKD modules from the threat of audit circumvention.

In FAU_GEN.1.1, the first selection is intended to specify the level of audit for different auditable events. The selection operation shall be completed by the author of a PP or an ST by taking into account the auditable requirements defined in the chosen SFRs of the PP or ST. The first assignment in 9.2.1.1 a), 3) is for the author of a PP or an ST to assign other auditable events considering the implementation details, which may comprise none, or events of an SFR that are of a higher level than that determined by the first selection. In this regard, it is recommended that the author of a PP or an ST consider events related to the following actions or states:

- Account login: including account name, login time, logout time, as well as account name and time when the number of consecutive login failures for an account exceeds a threshold value specified by the author of a PP or an ST.
- User operation: including all the operation records and operation time of the account.
- System self-test: including tests performed, time of test and test outcome.
- System failure: including error status and failure time when an operational fault occurs.

In FAU_GEN.1.2, the assignment shall be completed by the author of a PP or an ST if more audit-relevant information is required for audit, otherwise “None” is assigned.

9.2.2 FCS_CKM.6 Timing and event of cryptographic key destruction

9.2.2.1 Requirement

a) FCS_CKM.6.1. The TSF shall destroy [assignment: *list of cryptographic keys (including keying material)*] when [selection: *no longer needed, (assignment: other circumstances for key or keying material destruction)*].

b) FCS_CKM.6.2. The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with some specified cryptographic key destruction methods [assignment: *cryptographic key destruction methods*] that meet the following: [assignment: *list of standards*].

9.2.2.2 Application note

The SFR specified in 9.2.2.1 is intended to protect QKD modules from the threat of residual data misuse.

In FCS_CKM.6.1, the first assignment includes cryptographic keys and keying material used or generated during the execution of the TOE. Depending on different situations, it is recommended that the two assignments are made according to the first column of Table 4.

Table 4 — Assignment of FCS_CKM.6.1

Cryptographic keys (including keying material)	**Circumstances**
Raw data, sifted data, error corrected data	Device decommissioning, or a specific system failure event occurs at the time when the keying material is being used during the execution of the QKD protocol.
Uploaded part of the final key	After the part has been successfully uploaded to the relevant KM, or a specific system failure event occurs during a key upload.
QKD authentication key	Device decommissioning, or the key has been consumed for a recent communication, or a specific system failure event occurs at the time when the key is being used.

In FCS_CKM.6.2, the author of a PP or an ST shall assign at least one value to the first assignment on the methods of cryptographic key destruction, which may include, for example, a direct overwriting with an unrelated constant value or a random pattern to the key variable, or invalidating the original reference to the key. The second assignment specifies the corresponding standard(s) which describes the cryptographic key destruction method assigned in the first assignment. If there are no standards corresponding to the key destruction method(s), a value of "None" may be assigned. Since different keys may be destroyed using different methods, the two assignments can be given in the form of a table. For example, the first column of the table lists the keys (or keying material) that shall be destroyed, the second column lists the key destruction method(s) corresponding to the keys (or keying material) in the same row, and the third column lists the standards corresponding to the destruction method(s) in the same row.

9.2.3 FCS_COP.1 Cryptographic operation

9.2.3.1 Requirement

FCS_COP.1.1. The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

9.2.3.2 Application note

The SFR specified in 9.2.3.1 is intended to protect the QKD module from the threats of cryptographic analysis and unauthorized access.

The first assignment specifies the cryptographic algorithms, which may provide:

- confidentiality and integrity protection of the communications between a QKD module and an external KM;
- confidentiality and integrity protection of the communications between a QKD module and an operator via the control and management interface;
- support to the user authentication function.

The second and third assignments specify the cryptographic algorithm which shall be used and its key size. The assignment shall be commensurate to the computational security requirements on the key management interface and the control and management interface of the TOE. For future assignment, it is recommended to consider fully understood, computationally secure and standardized quantum safe cryptographic algorithms so as to improve resistance against future attacks. The third assignment can describe how the key length is determined if it is not a constant length.

The fourth assignment defines the standards for the assigned cryptographic algorithm. If there are no standards available, a value "None" may be assigned.

If more than one cryptographic algorithm has been used in the implementation, the component can be iterated to specify all the applied algorithms.

9.2.4 FCS_RNG.1 Random number generation

9.2.4.1 Requirement

a) FCS_RNG.1.1. The TSF shall provide a [selection: *physical, hybrid physical*] random number generator that implements: [assignment: *list of security capabilities*].

b) FCS_RNG.1.2. The TSF shall provide [selection: *bits, octets of bits, numbers [assignment: format of the numbers]*] that meet [assignment: *a defined quality metric*].

9.2.4.2 Application note

The SFR specified in 9.2.4.1 is intended to specify security requirements on NRBG components of QKD modules, which is intended to protect the QKD modules from the threat of randomness defect exploitation.

In FCS_RNG.1.1, the assignment of security capabilities depends on the type of the implemented NRBG, including for example the self-testing capability of the NRBG (see the application note in ISO/IEC 15408-2:2022, E.5 for further detail).

In FCS_RNG.1.2, the assignment of a quality metric shall be consistent with the security definition of cryptographic operations, and the security definition of QKD. Similarly, the author of a PP or an ST is recommended to refer to the application note in ISO/IEC 15408-2:2022, E.5 for appropriate completion of the SFR.

EXAMPLE To clarify the completion of FCS_RNG.1, some examples here are drawn from the application note in ISO/IEC 15408-2:2022, E.5.

Security capability:

— A total failure test (of the implemented RBG) detects a total failure of the entropy source immediately when the RNG has started. When a total failure is detected, no random numbers are output.

— The online test detects non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.

Quality metrics:

— The average Shannon entropy per internal random bit exceeds 0,998.

— Each output bit is independent of all other output bits.

9.2.5 FDP_ACC.1 Subset access control

9.2.5.1 Requirement

FDP_ACC.1.1. The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].

9.2.5.2 Application note

The SFR specified in 9.2.5.1 is intended to protect the QKD modules from the threat of unauthorized access to the TOE. Access control is required to protect the TOE from malicious actions that compromise the assets.

In the first assignment, the author of a PP or an ST shall specify a uniquely named access control SFP to be enforced by the TSF, and the detail of the rules shall be described in FDP_ACF.1 (Security attribute-based access control).

The second assignment should be given in the form of a table with at least three columns to define the subjects, the objects and the operations allowed to perform on the corresponding objects. A subject is defined here as an active system process or entity of the QKD module, usually acting on behalf of authorized external entity/entities or a part of the TOE itself (see ISO/IEC 15408-2). An object is defined here as a passive entity in the TOE, usually being a container of data including keying material, or user authentication data. Operations defined here are the permitted actions a subject may perform on an object. Such operations are usually read, write, delete or use. The second assignment shall at least prohibit the output of keying material and user authentication data to any external entity, other than where this is part of a QKD protocol. The assignment shall ensure that security critical data input to or generated in the TOE is not released inappropriately to an external entity.

9.2.6 FDP_ACF.1 Security attribute-based access control

9.2.6.1 Requirement

a) FDP_ACF.1.1. The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].

b) FDP_ACF.1.2. The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

c) FDP_ACF.1.3. The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*].

d) FDP_ACF.1.4. The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

9.2.6.2 Application note

The SFR specified in 9.2.6.1 is intended to protect QKD modules from the threat of unauthorized access to the TOE, which shall be used as a companion SFR with FDP_ACC.1. The detail of the access control rules implemented in QKD modules shall be described by customizing each element in the SFR considering a specific implementation strategy. The assignments shall at least deny the output of keying material and user authentication data to any external entity as required in the FDP_ACC.1.

9.2.7 FDP_IRC.1 Information retention control

9.2.7.1 Requirement

a) FDP_IRC.1.1. The TSF shall enforce the [assignment: *information erasure policy*] on a [assignment: *list of objects*] required for [assignment: *list of operations*] so that the selected objects are deleted irreversibly and untraceably from the TOE promptly upon termination of the selected operations.

b) FDP_IRC.1.2. The TSF shall ensure that [assignment: *list of objects*] cannot be accessed after their release and prior to their irreversible and untraceable deletion.

9.2.7.2 Application note

The SFR specified in 9.2.7.1 is intended to protect QKD modules from the threat of residual data misuse, such that security-related information which is no longer needed cannot be exploited by the threat agents to compromise the security of QKD modules. In order to better alleviate the residual data misuse threat, FDP_IRC.1 shall be used in conjunction with the key destruction requirement FCS_CKM.6 (in which only key and keying material destruction are considered).

In FDP_IRC.1.1, it is recommended that the assignments are made according to Table 5.

Table 5 — Assignment of FDP_IRC.1.1

Objects	Operations	Information erasure policy
user authentication data (see 7.3)	identity authentication of the operator	a) Circumstance: No longer needed for the authentication process, or a system reset event occurs b) Erasure method: overwrite with an unrelated constant value or random pattern
other security related information (see 7.3)	security audit, and relevant system management or maintenance operations	a) Circumstance: No longer needed for the system audit and management process, or a system reset event occurs b) Erasure method: overwrite with an unrelated constant value or random pattern

In FDP_IRC.1.2, the author of a PP or an ST shall assign a list of objects that constitutes a subset of the list assigned in FDP_IRC.1.1.

9.2.8 FDP_ITC.1 Import of user data without security attributes

9.2.8.1 Requirement

a) FDP_ITC.1.1. The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] when importing user data, controlled under the SFP, from outside of the TOE.

b) FDP_ITC.1.2. The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

c) FDP_ITC.1.3. The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *additional importation control rules*].

9.2.8.2 Application note

The SFR specified in 9.2.8.1 is intended to protect QKD modules from the threat of unauthorized access to the TOE. The access control SFP shall be enforced when importing data from outside of a QKD module. The data which is expected to be imported externally includes the pre-shared key (used for the QKD authentication key) and system (initialization) configuration for the QKD module to work, which can be imported from the system control and management interface. In some extreme cases, when there are no more keys available within the QKD module to be used as the QKD authentication key, fresh keys may be downloaded from the relevant KM (or entered into the QKD module directly) to make the QKD system effective.

In FDP_ITC.1.1, the specified SFP in the first assignment shall have clear rules to control the security of data imports, and the confidentiality of the data shall be ensured during the importing process. The applied cryptographic algorithms for confidentiality protection shall be described in FCS_COP.1.

In FDP_ITC.1.3, if no additional importation control rules are needed, the assignment can be "None".

9.2.9 FIA_UAU.2 User authentication before any action

9.2.9.1 Requirement

FIA_UAU.2.1. The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

9.2.9.2 Application note

The SFR specified in 9.2.9.1 is intended to protect QKD modules from the threat of unauthorized access to the TOE. Before operating the QKD modules, a user shall be successfully authenticated through the control and management interface of QKD modules. This document does not limit the approaches for user authentication, but only requires the approach adopted by an implementation to be secure and commensurate with the whole security expectations on the QKD modules.

FIA_UAU.2 is intended for user authentication. For some implementations of a QKD system, mutual authentication between the QKD modules shall be performed before the system proceeds to the raw data generation stage, as described in the description of the initialization stage in 6.5. In this case, the author of a PP or an ST can use the SFRs FTP_ITC.1 or FTP_TRP.1 from ISO/IEC 15408-2, or define new components to specify the mutual authentication function, if any.

9.2.10 FIA_UID.1 Timing of identification

9.2.10.1 Requirement

a) FIA_UID.1.1. The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.

b) FIA_UID.1.2. The TSF shall require each user to be successfully identified before allowing any TSF-mediated actions on behalf of that user.

9.2.10.2 Application note

The SFR specified in 9.2.10.1 is intended to protect the QKD modules from the threat of unauthorized access to the TOE. The author of a PP or an ST may assign values to the TSF-mediated actions depending on specific conditions. If no actions can be performed before identification, "None" may be assigned.

9.2.11 FMT_LIM.1 Limited capabilities

9.2.11.1 Requirement

FMT_LIM.1.1. The TSF shall limit its capabilities so that in conjunction with FMT_LIM.2 (limited availability) the following policy is enforced [assignment: *Limited capability and availability policy*].

9.2.11.2 Application note

The SFR specified in 9.2.11.1 is intended to protect QKD modules from the threat of functions abuse. QKD modules may incorporate some functions designed for functional testing and maintenance, for use by the TOE designer or an administrator during certain phases of the TOE's life cycle. If some such functions are used by threat agents, it can potentially result in the most serious of compromises to some or all of the TOE, or even for the system to be destroyed, in some cases. Consequently, any QKD module shall thoroughly close/lock those functions or limit their availability or capability. The author of a PP or an ST shall explicitly list the functions (if any) that are categorized as testing functions and demonstrate that they have been limited in capability, or removed so they are no longer available. On the other hand, this document does not exclude there being no such testing functions in the TOE. In this case, “None” may be assigned or the SFR can be omitted when writing a PP or an ST.

9.2.12 FMT_LIM.2 Limited availability

9.2.12.1 Requirement

FMT_LIM.2.1. The TSF shall be designed in a manner that limits its availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment*: Limited capability and availability policy*].

9.2.12.2 Application note

The SFR specified in 9.2.12.1 is intended to protect QKD modules from the threat of functions abuse, which shall be used as a companion SFR of FMT_LIM.1. If the implementation strategy does not include testing functions in the TOE, “None” may be assigned or the SFR can be omitted when writing a PP or an ST. See the related explanation in the application note for FMT_LIM.1 in 9.2.11.2.

9.2.13 FMT_MSA.1 Management of security attributes

9.2.13.1 Requirement

FMT_MSA.1.1. The TSF shall enforce the [assignment: *access control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorized identified roles*].

9.2.13.2 Application note

The SFR specified in 9.2.13.1 is intended to protect QKD modules from the threat of unauthorized access to the TOE. The assignment of security attributes and the allowed operations on them depend on the authorized identified roles, which should be done in accordance with Table 6. See FMT_SMR.1 specified in 9.2.16 for the definition of security roles for the TOE.

Table 6 — Assignment of FMT_MSA.1.1

Security attributes	Role and operations
Adoption of a cryptographic algorithm. (If multiple alternative algorithms are implemented for the same purpose.)	Administrator: change_default, query, modify
Threshold value for failure event decision in FPT_RCV.2, such as: a) The maximal tolerable number of continuous failures of raw data generation stage during a defined period of time; b) The maximal tolerable number of continuous failures of post-processing stage during a defined period of time.	Administrator: change_default, query, modify
Static parameters or configurations of QKD protocols.	Administrator: change_default, query, modify

9.2.14 FMT_MTD.1 Management of TSF data

9.2.14.1 Requirement

FMT_MTD.1.1. The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].

9.2.14.2 Application note

The SFR specified in 9.2.14.1 is intended to protect QKD modules from the threat of unauthorized access to the TOE. Depending on the authorized identified roles, the allowed operations to the TSF data should be in accordance with Table 7. See FMT_SMR.1 specified in 9.2.16 for the definition of security roles for the TOE.

Table 7 — Assignment of FMT_MTD.1.1

TSF data	Role and operations
QKD authentication key	Administrator: modify, delete
PIN code (only if PIN-based user authentication is required by the TSF)	Administrator: change_default, modify, delete (PIN codes of all users)

9.2.15 FMT_SMF.1 Specification of management functions

9.2.15.1 Requirement

FMT_SMF.1.1. The TSF shall be capable of performing the following management functions: [assignment: *list of management functions to be provided by the TSF*].

9.2.15.2 Application note

The SFR specified in 9.2.15.1 is intended to protect QKD modules from threats including unauthorized access to the TOE. The management functions to be provided by the TSF may include:

- key management and system parameter configuration of a QKD module;
- audit log query and analysis;
- other system maintenance functions depending on the implementation strategy.

The author of a PP or an ST shall specify the management functions according to their implementation strategy, and "None" may be assigned if no management function is presented in the design. Furthermore, this security functional component works in conjunction with other components in the class of FMT. If the practice requires restricting the ability to use the management functions, other security functional components in the class of FMT (FMT_MOF.1 for example) should be chosen to express the specific requirements. See ISO/IEC 15408-2:2022, 13.8 for detail.

9.2.16 FMT_SMR.1 Security roles

9.2.16.1 Requirement

a) FMT_SMR.1.1. The TSF shall maintain the roles [assignment: *the authorized identified roles*].

b) FMT_SMR.1.2 The TSF shall be able to associate users with roles.

9.2.16.2 Application note

The SFR specified in 9.2.16.1 is intended to protect QKD modules from the threat of unauthorized access to the TOE. The authorized roles shall at least comprise "administrator". To leave more flexibility for the implementation, this document does not specify other possible roles for the TOE. The author of a PP or an ST can define further roles depending on the implementation strategy, such as "auditor" for defining the audit strategy for the TOE and managing audit records, "maintainer" for the maintenance of the QKD modules, and "identified user" for all identified users of the QKD modules.

9.2.17 FPT_EMS.1/Convention Emanation of TSF and User data

9.2.17.1 Requirement

FPT_EMS.1.1. The TSF shall ensure that the TOE does not emit emissions over its attack surface in such amount that these emissions enable access to TSF data and user data as specified in Table 8.

Table 8 — Assignment of FPT_EMS.1.1

ID	Emissions	Attack surface	TSF data	User data
1	Remotely exploitable side channel information leaked from the conventional network components, such as timing variations of operations with different inputs, cache missing information.	Classical channel	[assignment: *list of relevant security-related information*].	-
2	[assignment: *list of types of emissions*]	[assignment: *list of types of attack surface*]	[assignment: *list of types of TSF data*]	[assignment: *list of types of user data*]

9.2.17.2 Application note

The SFR specified in 9.2.17.1 is intended to protect QKD modules from remotely exploitable physical security attacks induced mainly by the vulnerabilities of the conventional network components (see physical security violation threat described in 7.4.2). Faulty implementation or insecure design of cryptographic devices can lead to leakage of relevant security-related information (such as authentication data or keying material etc.), other than as intended as part of a QKD protocol, during their operation. This leakage can potentially be exploited if the threat agent is able to discover and analyse the side channel. This is known as side channel attack (SCA). QKD protocols typically involve sending information over the classical channel without a requirement for confidentiality measures. Such information can include parts of the keying material. Information intentionally communicated under the QKD protocol in operation is not considered under FPT_EMS.1/Convention.

Most SCA methods cannot be operated remotely, as their setup requires physical presence of threat agent's equipment at the TOE electrical contacts or near the surfaces of the device surface. For example, simple and differential power analysis, as well as electromagnetic analysis cannot be executed remotely. Under assumption a) in 7.2, these attacks are countered by the physical protection of the operational environment of the TOE, and are therefore outside the scope of this document.

In other words, this document considers security functional requirements protecting against remotely exploitable physical attacks, such as timing attacks (including cache-timing) or other possible SCA methods. Such side channel information can be gathered by the threat agents through the classical channel, in active or passive ways.

The author of a PP or an ST shall fill in and detail the contents of Table 8 according to the specific implementations of the conventional network components of the TOE. The contents shall consider state-of-the-art analysis methods for SCAs and the relevant application note in ISO/IEC 15408-2, 2022, J.2.

9.2.18 FPT_FLS.1 Failure with preservation of secure state

9.2.18.1 Requirement

FPT_FLS.1.1. The TSF shall preserve a secure state when the following types of failures occur: [assignment: *list of types of failures in the TSF*].

9.2.18.2 Application note

The SFR specified in 9.2.18.1 is intended to protect QKD modules from the threat of failure exploitation. See the FPT_RCV.2.2 in 9.2.21 for the types of failure events that shall be considered. The term “secure state” refers to a state where the TOE operates with consistent TSF data and the TSF continues correct enforcement of the SFRs. It also comprises a state where a failure has been detected, but the TOE protects itself from exploitation of this failure state. For example, this protection can be the blocking of all interfaces except those that are only accessible to administrators. In case of those assigned failures, the TSF with a specific QKD implementation strategy may select to notify an administrator of the events.

9.2.19 FPT_ITC.1 Inter-TSF confidentiality during transmission

9.2.19.1 Requirement

FPT_ITC.1.1. The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorized disclosure during transmission.

9.2.19.2 Application note

The SFR specified in 9.2.19.1 is intended to ensure that QKD modules are cryptographically secure from the threat of cryptographic analysis. The TSF data considered here include (parts of) the final keys uploaded from a QKD module to a KM, and optionally the pre-shared key transmitted from the relevant KM to the QKD module, both transmitted via the key management interface. The TSF shall protect the confidentiality of the TSF data, which can be achieved by the use of cryptographic algorithms. These algorithms shall be specified in the SFR FCS_COP.1.

9.2.20 FPT_ITI.1 Inter-TSF detection of modification

9.2.20.1 Requirement

a) FPT_ITI.1.1. The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product within the following metric: [assignment: *a defined modification metric*].

b) FPT_ITI.1.2. The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform [assignment: *action to be taken*] if modifications are detected.

9.2.20.2 Application note

The SFR specified in 9.2.20.1 is intended to protect QKD modules from the threat of cryptographic analysis. The TSF data considered here includes the (part of the) final key uploaded from a QKD module to the KM, and optionally the pre-shared key transmitted from the relevant KM to the QKD module; both are transmitted via the key management interface. Integrity protection can be achieved by the use of cryptographic algorithms. These algorithms shall be specified in the SFR FCS_COP.1.

The first assignment shall be specified in accordance with the security property of the assigned algorithm to achieve integrity protection. Once a modification has been detected, the TSF shall discard the received data and take more actions based on the implementation. The second assignment shall respect this requirement.

9.2.21 FPT_RCV.2 Automated recovery

9.2.21.1 Requirement

a) FPT_RCV.2.1. When automated recovery from [assignment: *list of failures/service discontinuities*] is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

b) FPT_RCV.2.2. For [assignment: *list of failures/service discontinuities*], the TSF shall ensure the return of the TOE to a secure state using automated procedures.

9.2.21.2 Application note

The SFR specified in 9.2.21.1 is intended to protect QKD modules from the threat of failure exploitation. Before discussing the completion of this requirement, the meaning of it and its relation with other SFRs are explained first. In a maintenance mode, normal operation is usually impossible or severely restricted, as otherwise insecure situations can arise. Typically, only authorized users should be allowed to access this mode. Consequently, the SFR FPT_RCV.2 should work in conjunction with the SFR FMT_SMF.1 and/or other requirements in the class of FMT. For example, the maintenance mode may block all interfaces except those that are only accessible to administrators. The “secure state” refers to some state in which the TOE has consistent TSF data and the TSF continues correct enforcement of the SFRs. The mechanism is designed to detect exceptional conditions during operation falls under the requirements of FPT_FLS.1 and FPT_TST.1 (see 9.2.17 and 9.2.22 for detail).

In FPT_RCV.2.1, it is required to assign the failure or service discontinuity scenarios in which the TSF shall enter a maintenance mode and be manually recovered to a secure state, since automated recovery from these failures can be difficult to realize in practice. A PP or an ST shall include assignments that cover all of the following failure events [a), b) and c)] and the events should be detailed according to the implementation strategy of the TOE:

a) Excessive errors or failures in the raw data generation stage during a given time period. This may be caused by the following or other reasons:

- continuous problems during quantum state generation, transmission or detection;
- continuous problems executing a parameter adjustment procedure.

b) Excessive errors or failures in the post-processing stage during a given time period. This may be caused by the following or other reasons:

- continuous problems completing parameter estimation;
- continuous message authentication failures;
- continuous consistency check failures.

c) Excessive failures that are not automatically recoverable from one or more self-tests during the initialization stage. For example, a QKD module can have tried several times to complete the initialization stage but always experience the same failure. Consequently, it shall enter a maintenance mode, which should be defined as a secure state by the author of a PP or an ST, and provide the ability for manual recovery. The failure can be caused by the following or other reasons:

- bootstrap errors due to the malfunction of one or more major functional components inside a QKD module;
- failures of a start-up test or periodical self-testing (see FPT_TST.1).

To complete the above assignments, the author of a PP or an ST shall specify the relevant thresholds for failure decisions, and a corresponding function for security attribute management may be provided (see FMT_MSA.1 for detail). Moreover, when entering a maintenance mode, the TSF with a specific QKD implementation strategy may select to notify an administrator of the failure events and indicate the special operating mode entered.

In FPT_RCV.2.2, the assignment should consider at least the following failure events:

a) Failure events assigned in FTP_QKD.1.6. In this case, the TSF may attempt recovery by running a further parameter adjustment procedure.

b) Failure of a relevant consistency check of the keying material during the post-processing stage. In this case, the on-going QKD session shall terminate and all intermediate keying material related to this session shall be destroyed immediately. In the next step, the QKD modules launch a new QKD session automatically as normal.

c) Failure in mutual authentication between the QKD modules of the TOE (where a mutual authentication procedure is implemented between the QKD modules), or between a QKD module and an external IT-product (e.g. a relevant external KM). In such cases, the entities involved can try again to mutually authenticate each other.

The relationship between FPT_RCV.2.1 and FPT_RCV.2.2 is that when accumulated failures over a defined time period exceed the thresholds defined in FMT_MSA.1, FPT_RCV.2.1 comes into effect and the TOE enters a maintenance mode.

The destruction of keying material shall meet the requirement of FCS_CKM.6.

9.2.22 FPT_TST.1 TSF self-testing

9.2.22.1 Requirement

a) FPT_TST.1.1. The TSF shall run a suite of the following self-tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self-test should occur]*] to demonstrate the correct operation of [selection: *[assignment: parts of TSF], the TSF*]: [assignment: *list of self-tests run by the TSF*].

b) FPT_TST.1.2. The TSF shall provide authorized users with the capability to verify the integrity of [selection: *[assignment: parts of TSF data], TSF data*].

c) FPT_TST.1.3. The TSF shall provide authorized users with the capability to verify the integrity of [selection: *[assignment: parts of TSF], TSF*].

9.2.22.2 Application note

The SFR specified in 9.2.22.1 is intended to protect QKD modules from the threat of failure exploitation.

In FPT_TST.1.1, the first and second assignments shall at least cover the items listed in Table 9 and should be detailed as per the implementation strategy of the TOE.

Table 9 — Assignment of FPT_TST.1.1

Self-test	Time/condition	Method
NRBG	During initial start-up, or at the request of the authorized user	Statistical test or other approaches for health tests of NRBG
Implementation of classical cryptographic algorithm	When the algorithm is first used after system power on	Known-answer test of cryptographic algorithm
Software and firmware integrity	During initial start-up	Integrity verification using reference values stored internally within the QKD module