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.

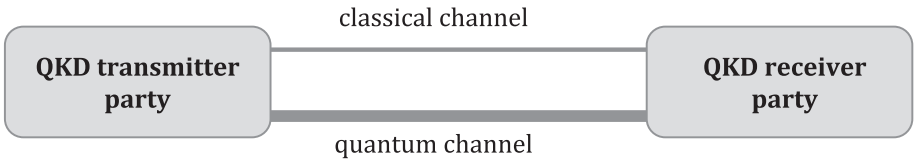

Figure 1 — Prepare-and-measure QKD protocol

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.

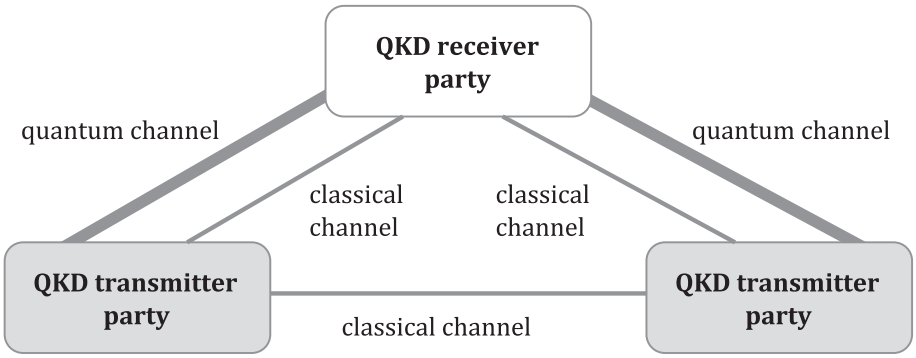

Figure 2 — MDI-QKD protocol

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.

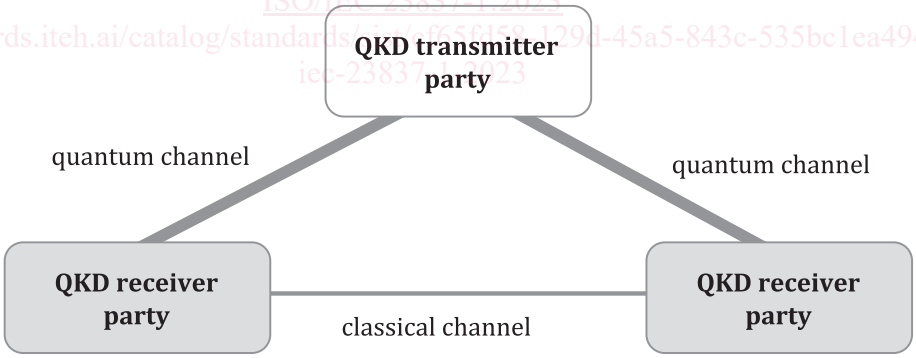

Figure 3 — EB-QKD protocol

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