ETSI GS QKD 016 V1.1.1 (2023-04)

Quantum Key Distribution (QKD); Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules

Disclaimer

The present document has been produced and approved by the Quantum Key Distribution (QKD) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGS/QKD-016-PP

Keywords
quantum cryptography, quantum key distribution

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Quantum Key Distribution (QKD).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The Protection Profile in the present document has not been certified. ISG QKD plans to submit this Protection Profile for certification and hopes to publish a revision containing a certified Protection Profile in future.

1 Scope

The present document specifies a Protection Profile (PP) for the security evaluation of pairs of Quantum Key Distribution (QKD) modules under the Common Criteria for Information Technology Security Evaluation (CC v3.1 rev5). The present document is applicable to a pair of QKD modules operating a prepare and measure QKD protocol that can form a complete QKD system when connected by an appropriate point-to-point QKD link. The PP specifies high-level requirements for the physical implementation through to the output of final secret keys.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] Common Criteria for Information Technology Security Evaluation: "Part 1: Introduction and General Model", Version 3.1, Revision 5, CCMB-2017-04-001, April 2017.

[2] Common Criteria for Information Technology Security Evaluation: "Part 2: Security Functional Components", Version 3.1, Revision 5, CCMB-2017-04-002, April 2017.

[3] Common Criteria for Information Technology Security Evaluation: "Part 3: Security assurance components", Version 3.1, Revision 5, CCMB-2017-04-003, April 2017.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GS QKD 005 (V1.1.1): "Quantum Key Distribution (QKD); Security Proofs".

[i.2] Joint Interpretation Library: "Minimum Site Security Requirements", Version 2.2, April 2019.

[i.3] Bundesamt für Sicherheit in der Informationstechnik AIS31 -- Wolfgang Killmann, Werner Schindler: "A proposal for: Functionality classes for random number generators", Version 2.0, September 2011.

[i.4] Bundesamt für Sicherheit in der Informationstechnik: "Evaluation of random number generators", Version 0.8.

[i.5] NIST Special Publication 800-90B: "Recommendation for the Entropy Sources Used for Random Bit Generation", January 2018.

[i.6] Jörn Müller-Quade and Renato Renner: "Composability in quantum cryptography", New J. of Phys. 11, 085006 (2009).

[i.7] ETSI TS 101 909-11 (V1.2.1): "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 11: Security".

[i.8] ISO 7498-2: "Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture", 1989.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms defined in CCMB-2017-04-001 [1] and the following apply:

active probing: physical probing with additional active physical interaction with the probed device

NOTE: Active physical interactions can force the TOE to produce leakage that would otherwise not be emitted.

ADR Signing Key (ASK): private key to sign ADR for export

Audit Data Records (ADR): organized data generated for auditable events

Authentication Reference Data (ARD): data used by the TOE to verify the AVD sent by a user and in turn authenticate the user

Authentication Verification Data (AVD): data used by the user to authenticate themselves to the TOE

authenticity: ability to ensure that the given information is without modification or forgery and was in fact produced by the entity that claims to have given the information

NOTE: See ETSI AT ETSI TS 101 909-11 [i.7].

calibration: operation performed on calibration data by a user, including the comparison of measurement values delivered by the TOE with those of a calibration standard of known accuracy

calibration data: physical parameters of the underlying platform, that are adjustable and verifiable by a user, and that are required to be properly adjusted for the TOE to perform the QKD protocol securely

NOTE: Calibration data is considered TSF data. Calibration data can also refer to physical properties requiring physical tools for modification.

certification body: body issuing Common Criteria certificates that is accredited by a nationally recognized accrediting body

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

coherent attack: most general type of eavesdropping attack on the quantum channel, where an adversary interacts multiple ancillas coherently with QKD signals and then performs a joint measurement on all the ancillas and/or QKD signals to extract information

cryptographic key: variable parameter that is used in and determines the functional output of a cryptographic algorithm or protocol

data integrity: property that data has not been altered or destroyed in an unauthorized manner

NOTE: See clause 3.3.21 in ISO/IEC 7498-2:1989 [i.8].

maintainer: user authorized to perform calibrations

operational state: states of the operational life-cycle

private key: confidential key used for asymmetric cryptographic mechanisms like decryption of cipher text, signature-creation for authentication proof, where it is infeasible for the adversary to derive the confidential private key from the known public key

public key: public known key used for asymmetric cryptographic mechanisms like encryption of cipher text, signature-verification for authentication verification, where it is infeasible for an adversary to derive the confidential private key from the known public key

prepare and measure QKD protocol: protocol for a QKD system to establish QKD keys in which one QKD module prepares quantum states and the other measures quantum states

QKD Authentication Key (QAK): shared secret used for authentication mechanisms between both QKD modules

NOTE: The authentication is required to ensure the proper functionality of the prepare and measure QKD protocol. The QKD authentication keys have to be available to the QKD modules before any communication using the QKD link can be established.

QKD key: pair of secret random bit strings established by a QKD system jointly in both QKD modules after successfully running a QKD protocol and considered to be identical

NOTE: QKD keys are exportable to authorized users for further use.

QKD link: set of active and/or passive components that connect a pair of QKD modules to enable them to perform QKD

QKD module: set of hardware, software, and/or firmware components that implements a part of a QKD protocol as well as cryptographic functions to be capable of securely establishing shared, confidential, random bit strings with at least one other QKD module

QKD protocol: set of operations that either aborts or agrees a shared, random, confidential bit string in the QKD modules

QKD system: pair of QKD modules, interconnected by a QKD link

QKD transaction: set of information defined by the ST author that is exchanged over the authenticated classical channel in a QKD link using QAK(s) that are not used by any other QKD transaction and that is limited by time, data exchanged and other limitations

Quantum Key Distribution (QKD): procedure involving the transport of quantum states to agree shared secret bit strings between remote parties using a protocol with security based on quantum entanglement or the impossibility of perfectly cloning or measuring the unknown transported quantum states

remote entities: human users or IT devices that eventually operate on behalf of human users, and communicate through a trusted path with the TOE

NOTE: The term is used solely in clause 11.1 to point out that communication between human users and the TOE is potentially indirect.

transaction: set of information defined by the ST author that is exchanged over a trusted path and limited by time, amount of data exchanged and additional limitations

trusted path: communication channel between a QKD module and a remote entity that is logically distinct from other communication paths and that provides assured identification of its end points and protection of the communicated data from modification and disclosure

NOTE: See the definition of the term "remote entity".

user: entity using the TOE

NOTE: A user can either be a machine (on behalf of a human or other machines) or a human interacting with the TOE.

User Definition Records (UDR): information about known users and their associated roles

User Transaction Key (UTK): set of distinct cryptographic keys, where each key is used exclusively to protect data on the trusted path either against modification or disclosure

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

A.xxx	Assumption
ADR	Audit Data Records
ARD	Authentication Reference Data
ASK	ADR Signing Key
AVD	Authentication Verification Data
CB	Certification Body
CC	Common Criteria
IT	Information Technology
O.xxx	Security Objective for the TOE
OE.xxx	Security Objective for the TOE Environment
OSP.xxx	Organisational Security Policy
P&M protocol	Prepare and Measure QKD protocol
PP	Protection Profile
QAK	QKD Authentication Key
QKD	Quantum Key Distribution
SAR	Security Assurance Requirements
SFP	Security Functional Policy
SFR	Security Functional Requirement
ST	Security Target
T.xxx	Threat
TOE	Target Of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
UDR	User Definition Records
UTK	User Transaction Key

4 Application Notes in the PP

Specific requirements apply to the use of Application Notes in different locations within a PP and its packages but it is important to note that in general Application Notes to SFRs can have normative impact on the evaluation of a product, including introducing new requirements.

5 PP introduction

5.1 PP reference

Title:	Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules
CC Version:	3.1 Revision 5
Author:	ETSI (ISG QKD)
Assurance Level:	EAL4 augmented with AVA_VAN.5 and ALC_DVS.2
Publication Date:	April 2023
Version Number:	V1.1.1

Keywords: Cryptographic Module, Cryptography, Quantum Key Distribution

5.2 PP Overview

This Protection Profile describes the security requirements for Quantum Key Distribution modules (QKD modules) that use a Prepare and Measure QKD protocol (P&M protocol). This PP considers the case, where both modules are located in environments with identical security requirements.

This PP deliberately offers degrees of freedom to ST authors in order to allow them to adapt to upcoming QKD standards and to foster innovative solutions in an upcoming technology. The developers and ST authors are advised to contact their Certification Body (CB) before and during development to establish a common interpretation. In particular, the CB can discourage certain cryptographic algorithms or protocols for this field of use that would formally be valid choices in this PP. The PP is written with several incompatible use cases, environments, and business models in mind. It offers options, choices, and places for text to be provided by an ST author to accommodate most of these. Some combinations can appear formally correct, but would be unacceptable to the CB. Developers are advised to agree on the ST with the CB before finalizing the architecture of the product.

5.3 TOE overview

5.3.1 TOE type

The Target of Evaluation (TOE) is a pair of QKD modules that can be connected together via a QKD link to form a QKD system. The TOE Security Functionality (TSF) provides a consistent subset of the functionality that is expected to be necessary in such QKD systems.

5.3.2 TOE definition

The TOE comprises a QKD system consisting of two QKD modules, but without the QKD link in between (see Figure 1). It furthermore includes the associated guidance documentation. The QKD link can pass through uncontrolled environment without physical protection, and does not provide any security services. The QKD link includes at least two communication channels, an authenticated classical channel and a quantum channel (see Figure 2). Unauthenticated classical channels can also be used, e.g. to synchronise the QKD modules in time. Analogue as well as digital communications can occur on unauthenticated classical communication channel(s). The communication using the QKD link is considered Inter-TSF communication.

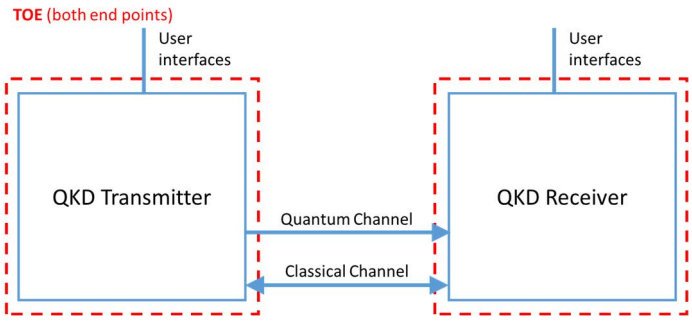

Figure 1: The TOE-boundary, i.e. the two QKD modules

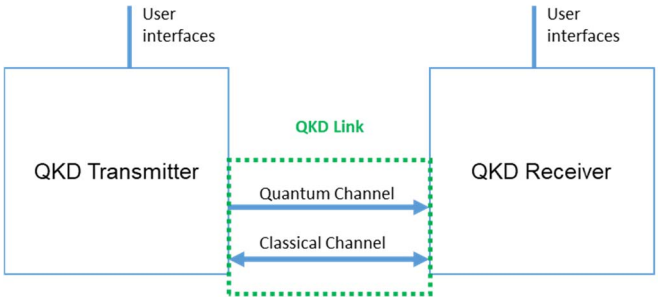

Figure 2: The QKD link

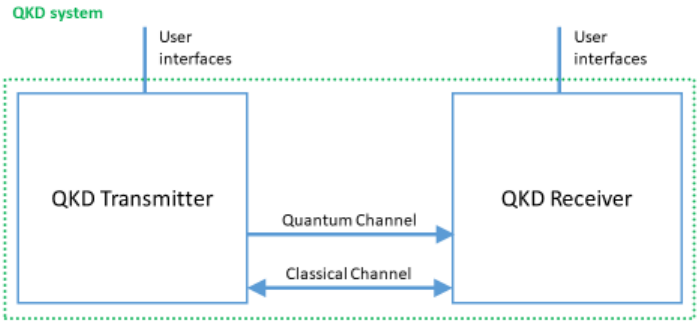

Figure 3: The QKD system

The purpose of the QKD system is to establish QKD keys where a pair of QKD modules, one being a QKD transmitter and one a QKD receiver, are connected together and mutually share authentication credentials (see Figure 3). QKD keys are shared, confidential, random bit strings in both QKD modules, which can be consumed by authorized users in well-defined chunks. The property "random" is used in the sense that the strings are unpredictable, uniformly distributed, and independent from each other, i.e. the QKD system implements a source with forward and backward secrecy. Each of these properties can be subject to imperfections.

The TOE implements a QKD protocol that has a security parameter composed from its sub-protocols. The security parameter denotes the maximum probability that any of the properties of the bit strings is not assured during a single execution of the QKD protocol that does not abort. The TOE ensures that this does not exceed some upper limit, according to an associated composed security proof. The ST introduction would be expected to detail this upper limit (security parameter threshold, see Application note 3) and summarise the important points from the related description in the TOE summary specification using plain words that non-QKD experts can also understand.

If these bit strings are successfully established for export, they are called QKD keys regardless of their appropriateness for or actual use as cryptographic keys.

NOTE 1: The TOE exports these QKD keys from each QKD module to authorized users. The TOE can use established shared bit strings for internal purposes. Bit strings used internally are not exported as QKD keys.

QKD systems can be modelled in a notion of information-theoretical security and this PP requires a security proof for the QKD protocol. SAR AVA_VAN.5 requires the actual establishment of these QKD keys to be resistant to attackers possessing high attack potential.

In order to establish QKD keys, the QKD system uses a P&M protocol as defined in [i.1]. Although these protocols can vary greatly, there is always a distinct sequence of stages:

1) The initialization stage is used to prepare both QKD modules for the establishment of a QKD key. It is not part of the core P&M protocol, but is required to initiate the QKD protocol. It can include self-tests, synchronizing the QKD modules, preparation of storage, etc. This stage is initiated upon a user's request for QKD key establishment.

2) During the quantum stage the QKD modules prepare and measure quantum states depending on the chosen P&M protocol and their respective role in it.