

ETSI GS QKD 016 V2.1.1 (2024-01)



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

Document Preview

ETSI GS QKD 016 V2.1.1 (2024-01)

<https://standards.iteh.ai/catalog/standards/etsi/3f69dc2b-f9da-48cb-acbb-01fd42046369/etsi-gs-qkd-016-v2-1-1-2024-01>

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.

ReferenceRGS/QKD-016ed2_PP

Keywordsquantum 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

Important notice

The present document can be downloaded from:

<https://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our

Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2024.
All rights reserved.

Contents

Intellectual Property Rights	9
Foreword.....	9
Modal verbs terminology.....	9
1 Scope	10
2 References	10
2.1 Normative references	10
2.2 Informative references.....	10
3 Definition of terms, symbols and abbreviations.....	11
3.1 Terms.....	11
3.2 Symbols.....	13
3.3 Abbreviations	13
4 Application Notes in the Protection Profile (PP)	14
5 PP introduction	14
5.1 PP reference.....	14
5.2 PP Overview.....	14
5.3 TOE overview	14
5.3.1 TOE type.....	14
5.3.2 TOE definition	15
5.3.3 TOE users	17
5.3.4 Method of use	18
5.3.5 Life-cycle	18
5.3.5.1 Overview	18
5.3.5.2 Calibration state	20
5.3.5.3 QKD state.....	21
5.3.5.4 Failure state	21
5.3.5.5 End of Life state	21
5.3.5.6 Non-TOE hardware/software/firmware available to the TOE.....	21
6 Conformance claims.....	21
6.1 CC conformance claims	21
6.2 Package claim.....	22
6.3 PP claim	22
6.4 Conformance rationale	22
6.5 Conformance statement.....	22
6.6 PP Application Notes	22
7 Security problem definition.....	22
7.1 Assets, TSF data, users, subjects, objects and security attributes.....	22
7.1.1 Assets and TSF data.....	22
7.1.2 Users and subjects.....	23
7.1.3 Objects	23
7.1.4 Security attributes	24
7.2 Threats.....	24
7.2.1 T.ServAcc Unauthorized access to data and functions in TOE	24
7.2.2 T.Session Session hijacking or piggybacking.....	24
7.2.3 T.QKDEave Eavesdropping on QKD link data	24
7.2.4 T.QKDMani Manipulation of QKD link data.....	24
7.2.5 T.ExplMal Exploitation of TOE malfunction	25
7.2.6 T.Observ Observation of TSF characteristics	25
7.3 Organizational security policies	25
7.3.1 OSP.QKDService Key distribution services of the TOE.....	25
7.3.2 OSP.Audit Audit for security operations	25
7.3.3 OSP.SecEoL Secure End of Life state	25
7.4 Assumptions	25

7.4.1	A.Maint Diligent maintenance.....	25
7.4.2	A.SecureOp Operation in a secure area	25
8	Security objectives	26
8.1	Security objectives for the TOE	26
8.1.1	Interpretation of security objectives.....	26
8.1.2	O.Identify Identification of users.....	26
8.1.3	O.AccCtrl Access control	26
8.1.4	O.QKD Quantum Key Distribution	26
8.1.5	O.QKDAuth Authenticated classical channel.....	26
8.1.6	O.Audit Audit for cryptographic TSF.....	27
8.1.7	O.TST Self-test	27
8.1.8	O.EMSec Emanation Security	27
8.1.9	O.Sanitize Secure End of Life state	27
8.1.10	O.SessionLimit Limitation of user sessions.....	27
8.2	Security objectives for the operational environment	28
8.2.1	OE.Trust Trustworthy users.....	28
8.2.2	OE.Audit Review and availability of audit records	28
8.2.3	OE.SecureOp Secure Operational environment.....	28
8.2.4	OE.Personnel Trustworthy personnel	28
8.3	Security objective rationale	28
8.3.1	Table of rationale	28
8.3.2	T.ServAcc	29
8.3.3	T.Session.....	29
8.3.4	T.QKDEave	29
8.3.5	T.QKDMani.....	29
8.3.6	T.ExplMal	29
8.3.7	T.Observe.....	30
8.3.8	OSP.QKDSERVICE	30
8.3.9	OSP.Audit.....	30
8.3.10	OSP.SecEoL	30
8.3.11	A.SecureOp.....	30
8.3.12	A.Maint	30
9	Extended component definition.....	31
9.1	Quantum Key Distribution (FCS_QKD).....	31
9.2	Sanitizing on State Change (FDP_RIP.3).....	34
9.3	Inter-TSF trusted channel - authenticated classical channel (FTP_ITC.2).....	35
10	Security requirements.....	36
10.1	Operations within this PP	36
10.2	Security functional requirements.....	37
10.2.1	User Identification and Management.....	37
10.2.2	Access Control.....	39
10.2.3	Audit Data.....	42
10.2.4	Reaching and preserving secure states.....	44
10.2.5	Authenticated classical channel of QKD link	46
10.2.6	QKD Key Establishment	47
10.2.7	Management	48
10.3	Security assurance requirements	50
10.3.1	Evaluation Assurance Level	50
10.3.2	Security assurance requirements rationale	51
10.4	Security requirements rationale	51
10.4.1	Dependency rationale	51
10.4.2	Rationale for security objectives.....	53
10.4.2.1	Table of rationale	53
10.4.2.2	O.Identify	53
10.4.2.3	O.AccCtrl	54
10.4.2.4	O.QKD	54
10.4.2.5	O.QKDAuth	54
10.4.2.6	O.Audit.....	55
10.4.2.7	O.TST.....	55
10.4.2.8	O.EMSec	55

10.4.2.9	O.Sanitize	55
10.4.2.10	O.SessionLimit	56
11	Packages	56
11.1	Trusted User Interfaces with Authentication	56
11.1.1	Identification	56
11.1.2	Introduction	56
11.1.2.1	Overview	56
11.1.2.2	TOE definition	56
11.1.2.3	Life-cycle	57
11.1.2.4	Non-TOE hardware/software/firmware available to the TOE	57
11.1.3	Security Problem Definition	57
11.1.3.1	Assets, TSF data, users, subjects, objects and security attributes	57
11.1.3.1.1	Assets and TSF data	57
11.1.3.1.2	Users and subjects	57
11.1.3.1.3	Objects	57
11.1.3.1.4	Security attributes	58
11.1.3.2	Threats	58
11.1.3.2.1	Rationale for defining additional threats	58
11.1.3.2.2	T.DataCompr Eavesdropping on data on user interfaces	58
11.1.3.2.3	T.DataMani Generation or manipulation of communication data	58
11.1.3.2.4	T.Combine Analysing and combining information at different interfaces	58
11.1.3.2.5	T.Masqu Generation or manipulation of data on user interfaces	58
11.1.3.2.6	T.Impersonate Impersonation of other users	58
11.1.3.3	Assumptions	58
11.1.3.3.1	A.SecComm Secure communication	58
11.1.4	Security Objectives	59
11.1.4.1	New objectives for the TOE	59
11.1.4.1.1	O.TPath Trusted path with user authentication	59
11.1.4.1.2	O.AuthFail Reaction to failed user authentication	59
11.1.4.2	Refined objectives for the TOE	59
11.1.4.2.1	O.EMSec Emanation Security	59
11.1.4.3	New objectives for the environment	59
11.1.4.3.1	OE.SecComm Protection of communication channel	59
11.1.4.3.2	OE.AuthData Secrecy and generation of authentication data	59
11.1.4.4	Refined objectives for the environment	59
11.1.4.4.1	Notes	59
11.1.4.4.2	OE.SecureOp Secure Operational environment	60
11.1.4.4.3	OE.Personnel Trustworthy personnel	60
11.1.4.5	Rationale for the refinements	60
11.1.4.5.1	O.EMSec	60
11.1.4.5.2	OE.SecureOp	60
11.1.4.5.3	OE.Personnel	61
11.1.4.6	Rationale for security objectives	61
11.1.4.6.1	T.Observe	61
11.1.4.6.2	T.DataCompr	61
11.1.4.6.3	T.DataMani	61
11.1.4.6.4	T.Masqu	61
11.1.4.6.5	T.Impersonate	61
11.1.4.6.6	A.SecComm	62
11.1.5	Security requirements	62
11.1.5.1	New requirements for the TOE	62
11.1.5.1.1	Trusted Path to remote users	62
11.1.5.1.2	User Authentication	64
11.1.5.2	Refined requirements for the TOE	64
11.1.5.3	SFR Dependency rationale	65
11.1.5.4	Rationale for the security requirements	65
11.1.5.4.1	Table of rationale	65
11.1.5.4.2	O.EMSec	65
11.1.5.4.3	O.TPath	66
11.1.5.4.4	O.AuthFail	66
11.2	TOE self-protection	66

11.2.1	Identification.....	66
11.2.2	Introduction.....	66
11.2.3	Security Problem Definition	67
11.2.3.1	Assets, TSF data, users, subjects, objects and security attributes.....	67
11.2.3.1.1	Assets and TSF data	67
11.2.3.1.2	Users and subjects	67
11.2.3.1.3	Objects.....	67
11.2.3.1.4	Security attributes.....	67
11.2.3.2	Threats.....	67
11.2.3.2.1	T.PhysAttack Physical attacks.....	67
11.2.3.3	Assumptions.....	67
11.2.3.3.1	A.SecureOp	67
11.2.4	Security Objectives	68
11.2.4.1	New objectives for the TOE.....	68
11.2.4.1.1	O.PhysProt Physical protection	68
11.2.4.2	Refined objectives for the TOE.....	68
11.2.4.2.1	O.EMSec Emanation Security	68
11.2.4.3	Refined objectives for the environment	68
11.2.4.3.1	OE.SecureOp Secure Operational environment	68
11.2.4.4	Rationale for the refinements	68
11.2.4.4.1	O.EMSec	68
11.2.4.4.2	OE.SecureOp	68
11.2.4.5	Rationale for the security objectives	69
11.2.4.5.1	T.PhysAttack	69
11.2.4.5.2	T.Combine	69
11.2.4.5.3	A.SecureOp	69
11.2.5	Security requirements	69
11.2.5.1	Introduction.....	69
11.2.5.2	New requirements for the TOE	69
11.2.5.3	Refined requirements for the TOE.....	70
11.2.5.4	SFR Dependency Rationale	70
11.2.5.5	Rationale for the Security Requirements.....	70
11.2.5.5.1	Table of rationale.....	70
11.2.5.5.2	O.PhysProt.....	70
11.2.5.5.3	O.EMSec	70
11.3	Provisioning and re-personalization after delivery.....	71
11.3.1	Identification.....	71
11.3.2	Introduction.....	71
11.3.2.1	Overview.....	71
11.3.2.2	Life-cycle	71
11.3.3	Security Problem Definition	72
11.3.3.1	Assets, TSF data, users, subjects, objects and security attributes.....	72
11.3.3.1.1	Assets and TSF data	72
11.3.3.1.2	Users and subjects	72
11.3.3.1.3	Objects.....	72
11.3.3.1.4	Security attributes.....	72
11.3.3.2	Threats.....	72
11.3.3.2.1	T.Initialize Compromised initialization of TSF data	72
11.3.3.3	Assumptions.....	73
11.3.3.3.1	A.SecureOp	73
11.3.4	Security Objectives	73
11.3.4.1	New objectives for the TOE.....	73
11.3.4.1.1	O.Personalization Access control to personalization.....	73
11.3.4.1.2	O.Pristine Proof of intactness after initial delivery.....	73
11.3.4.2	New objectives for the environment	73
11.3.4.2.1	Note	73
11.3.4.2.2	OE.Initialize Secure environment for initialization.....	73
11.3.4.3	Rationale for the refinements	74
11.3.4.3.1	A.SecureOp	74
11.3.4.4	Rationale for security objectives	74
11.3.4.4.1	T.Initialize	74
11.3.4.4.2	A.SecureOp	74

11.3.5	Security requirements	74
11.3.5.1	New requirements for the TOE	74
11.3.5.2	Refined requirements for the TOE	75
11.3.5.3	SFR Dependency Rationale	78
11.3.5.4	Rationale for the Security Requirements.....	79
11.3.5.4.1	Table of rationale.....	79
11.3.5.4.2	O.Personalization.....	79
11.3.5.4.3	O.Pristine.....	79
11.4	Local Authentication of Users.....	80
11.4.1	Identification.....	80
11.4.2	Introduction.....	80
11.4.2.1	Overview.....	80
11.4.2.2	TOE definition	80
11.4.2.3	Life-cycle	80
11.4.3	Security Problem Definition	80
11.4.3.1	Assets, TSF data, users, subjects, objects and security attributes.....	80
11.4.3.1.1	Assets and TSF data	80
11.4.3.1.2	Users and subjects	81
11.4.3.1.3	Objects.....	81
11.4.3.1.4	Security attributes	81
11.4.3.2	Threats.....	81
11.4.3.2.1	T.Masqu Generation or manipulation of data on user interfaces	81
11.4.3.2.2	T.Impersonate Impersonation of other users	81
11.4.3.3	Assumptions.....	81
11.4.3.3.1	A.AuthData Secure authentication credentials	81
11.4.4	Security Objectives.....	81
11.4.4.1	New security objectives for the TOE	81
11.4.4.1.1	O.I&A Identification and authentication of users.....	81
11.4.4.2	New objectives for the environment	81
11.4.4.2.1	OE.AuthDataUI Secrecy and generation of authentication data.....	81
11.4.4.3	Rationale for security objectives	82
11.4.4.3.1	T.Masqu.....	82
11.4.4.3.2	T.Impersonate.....	82
11.4.4.3.3	A.AuthData.....	82
11.4.5	Security requirements	82
11.4.5.1	New requirements for the TOE	82
11.4.5.1.1	User Authentication.....	82
11.4.5.2	SFR Dependency Rationale	83
11.4.5.3	Rationale for the Security Requirements.....	83
11.4.5.3.1	Table of rationale.....	83
11.4.5.3.2	O.I&A.....	83
12	Guidance for SFR for RNG.....	83
12.1	Introduction	83
12.2	RNG according to AIS 31	83
12.3	RNG according to NIST SP 800-90	84
Annex A (informative):	Roles, TOE users and TSFs	86
A.1	Rationale.....	86
A.2	Phases and important roles	86
A.3	Role-based authorization of TOE user access to TSFs	87
A.3.1	Assigning roles to TOE users	87
A.3.2	Associating user security attributes with user-subjects	87
A.3.3	Authorization of subjects according to role.....	87
A.4	Example sequences for requesting and exporting QKD keys	88
A.4.1	Basic key request and export sequence examples	88
A.4.2	Continuous key establishment and export sequence example	89
A.4.3	Key request and export sequence example needing additional functionality to be added to a PP/ST	90
A.5	Example layout of QKD modules, TOE users and physically protected areas	91

Annex B (informative):	Bibliography.....	92
History		93

iTeh Sa na ds (https://sta na ds. teh. a) i Do ument Pev ew

ETSI GS QKD 0 2 6 2 V 02.14 0-
http :/stand rd . teh. i/catalo /stand rd /etsi/3 6 f 92 d b c -d4 a b a e b 0 d 4 2 0 etsi-gs-q 3 k 0 6 d b 2 6 1 -4 -2- 0 0 2

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.

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:2022 Revision 1). 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](#)", CC:2022, Revision 1, CCMB-2022-11-001, November 2022.
- [2] Common Criteria for Information Technology Security Evaluation: "[Part 2: Security functional components](#)", CC:2022, Revision 1, CCMB-2022-11-002, November 2022.
- [3] Common Criteria for Information Technology Security Evaluation: "[Part 3: Security assurance components](#)", CC:2022, Revision 1, CCMB-2022-11-003, November 2022.
- [4] Common Criteria for Information Technology Security Evaluation: "[Part 4: Framework for the specification of evaluation methods and activities](#)", CC:2022, Revision 1, CCMB-2022-11-004, November 2022.
- [5] Common Criteria for Information Technology Security Evaluation: "[Part 5: Pre-defined packages of security requirements](#)", CC:2022, Revision 1, CCMB-2022-11-005, November 2022.
- [6] Common Methodology for Information Technology Security Evaluation: "[Evaluation methodology](#)", CEM:2022, Revision 1, CCMB-2022-11-006, November 2022.

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 -- Wolfgang Killmann, Werner Schindler: "A proposal for: Functionality classes for random number generators", Version 2.0, September 2011.
- NOTE: The Application notes and Interpretations for Schema (AIS) of the German Common Criteria certification scheme published by Bundesamt für Sicherheit in der Informationstechnik (BSI), the German Federal Office for Information Security, integrates [i.3] by reference within AIS 31 [i.4].
- [i.4] Bundesamt für Sicherheit in der Informationstechnik AIS 31: "Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren", Version 3, May 2013.
- [i.5] NIST SP 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 7498-2:1989: "Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given 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 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

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

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

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
AIS	Application notes and Interpretations for Schema
ARD	Authentication Reference Data
ASK	ADR Signing Key
AVD	Authentication Verification Data
BSI	Bundesamt für Sicherheit in der Informationstechnik (The German Federal Office for Information Security)
CB	Certification Body
CBC	Cipher Block Chaining
CC	Common Criteria
CD	Calibration Data
CMAC	Cipher-based Message Authentication Code
EAL	Evaluation Assurance Level
HMAC	Keyed-Hash Message Authentication Code
ID	Identity
IT	Information Technology
MAC	Message Authentication Code
O.xxx	Security Objective for the TOE
OE.xxx	Security Objective for the TOE Environment
OSP	Organisational Security Policy
OSP.xxx	Organisational Security Policy
P&M protocol	Prepare and Measure QKD protocol
PP	Protection Profile
PTRNG	Physical True Random Number Generator
QAK	QKD Authentication Key
QKD	Quantum Key Distribution
RNG	Random Number Generator
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 Protection Profile (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:	CC:2022 Revision 1
Author:	ETSI (ISG QKD)
Assurance Level:	EAL4 augmented with AVA_VAN.5 and ALC_DVS.2
Compilation Date:	2023-11-27
Version Number:	V2.1.1
Registration:	BSI-CC-PP-0120-2024 (please refer to the Certification Report from www.bsi.bund.de)
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.