Federal Office
for Information Security

Certification Report

BSI-CC-PP-0120-2024

for

Common Criteria Protection Profile — Pair of Prepare and Measure Quantum Key Distribution Modules, Version 2.1.1

developed by

European Telecommunications Standards Institute

Federal Office for Information Security (BSI), Postfach 20 03 63, 53133 Bonn, Germany
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat
erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-CC-PP-0120-2024

Common Criteria Protection Profile

Common Criteria Protection Profile — Pair of Prepare and Measure Quantum Key Distribution Modules, Version 2.1.1

developed by European Telecommunications Standards Institute

Assurance Package claimed in the Protection Profile:
Common Criteria Part 3 conformant
EAL 4 augmented by
AVA_VAN.5, ALC_DVS.2

valid until 17 January 2034

SOGIS Recognition Agreement

Common Criteria

The Protection Profile identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version CC:2022 for conformance to the Common Criteria for IT Security Evaluation (CC), Version CC:2022. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

This certificate applies only to the specific version and release of the Protection Profile and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the Protection Profile by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the Protection Profile by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria Recognition Arrangement

Bonn, 18 January 2024

For the Federal Office for Information Security

Sandro Amendola
Director-General

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

This page is intentionally left blank.

Contents

A Certification

1 Preliminary Remarks

Under the Act on the Federal Office for Information Security (BSIG), the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products as well as for Protection Profiles (PP).

A PP defines an implementation-independent set of IT security requirements for a category of products which are intended to meet common consumer needs for IT security. A PP claimed by a user, consumer or stakeholder for IT gives them the possibility to express their IT security needs without referring to a specific product. Product certifications can be based on Protection Profiles. For products which have been certified based on a Protection Profile an individual certificate will be issued but the results from a PP certification can be re-used for the Security Target evaluation within a product evaluation when conformance to the PP has been claimed.

Certification of the Protection Profile is carried out on the instigation of the BSI or a sponsor. A part of the procedure is the technical examination (evaluation) of the Protection Profile according to Common Criteria [1]. The evaluation is usually carried out by an evaluation facility recognised by the BSI or by BSI itself. The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

2 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security (BSIG)[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs[3]
- Special decrees issued by the Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3], including PP Certification
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821
Current version see website: http://www.gesetze-im-internet.de/bsig_2009/index.html

[2] Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231
Current version see website: http://www.gesetze-im-internet.de/bsizertv_2014/index.html

[3] BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365
Current version see website: https://www.bsi.bund.de/Gebuehrenverordnung

- Common Criteria for IT Security Evaluation (CC)[4] [1], version CC:2022, also published as ISO/IEC 15408
- Common Methodology for IT Security Evaluation [2], version CC:2022 also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Internal procedure for the issuance of a PP certificate

3 Recognition Agreements

In order to avoid multiple certification of the same Protection Profile in different countries a mutual recognition of IT security certificates - as far as such certificates are based on CC - under certain conditions was agreed. Therefore, the results of this evaluation and certification procedure can be re-used by the product certificate issuing scheme in the evaluation of a Security Target within a subsequent product evaluation and certification procedure.

3.1 European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level up to and including Common Criteria (CC) Evaluation Assurance Levels EAL 4, and in addition at higher recognition levels for IT-Products related to certain technical domains only. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

Details on recognition, the signatory nations, technical domains and the agreement itself can be found at https://www.sogis.eu.

3.2 International Recognition of CC – Certificates (CCRA)

The international Common Criteria Recognition Arrangement (CCRA) became effective in September 2014 in its current version. It defines the recognition of certificates for IT-products based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

Details on recognition, the signatory nations and the agreement itself can be found at https://www.commoncriteriaportal.org.

[4] Proclamation of the Federal Office for Information Security of 14 April 2023 on https://www.bsi.bund.de

4 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The PP Common Criteria Protection Profile — Pair of Prepare and Measure Quantum Key Distribution Modules, Version 2.1.1 has undergone the certification procedure at BSI.

The evaluation of the PP Common Criteria Protection Profile — Pair of Prepare and Measure Quantum Key Distribution Modules, Version 2.1.1 was conducted by the ITSEF SGS Digital Trust Services GmbH. The evaluation was completed on 12 December 2023. The ITSEF SGS Digital Trust Services GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the applicant is: European Telecommunications Standards Institute (ETSI).

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5 Validity of the certification result

This Certification Report only applies to the version of the Protection Profile as indicated.

In case of changes to the certified version of the Protection Profile, the validity can be extended to new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified Protection Profile, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the CC concepts and terms please refer to CC [1] Part 1 through 5.

The validity of this certificate ends as outlined on the certificate. The applicant and the sponsor of this certificate are recommended to review the technical content of the Protection Profile certified according to the evolvement of the technology and of the intended operational environment of the type of product concerned as well as according to the evolvement of the evaluation criteria. Such review should result in an update and a re-certification of the Protection Profile accordingly. Typically, technical standards are reviewed on a five years basis.

The limitation of validity of this PP certificate does not necessarily impact the validity period of a product certificate referring to this Protection Profile, but the certification body issuing a product certificate based on this Protection Profile should take it into its consideration on validity.

6 Publication

The PP Common Criteria Protection Profile — Pair of Prepare and Measure Quantum Key Distribution Modules, Version 2.1.1 has been included in the BSI list of the certified Protection Profiles, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). The PP itself will be published by the applicant ETSI (see also Internet: https://www.etsi.org/standards). Further information can be obtained from BSI-Infoline +49 228 9582-111.

[5] Information Technology Security Evaluation Facility

The Certification Report may be obtained in electronic form at the internet address stated above.

B Certification Results

The following results represent a summary of

- the certified Protection Profile,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Protection Profile Overview

The Protection Profile Common Criteria Protection Profile — Pair of Prepare and Measure Quantum Key Distribution Modules, Version 2.1.1 [6] is established by the European Telecommunications Standards Institute as a basis for the development of Security Targets in order to perform a certification of an IT-product (Quantum Key Distribution Modules – Prepare and Measure).

The Target of Evaluation (TOE) addressed by the PP 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.

The TOE comprises a QKD system consisting of two QKD modules, but without the QKD link in between. 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. Unauthenticated classical channels can also be used, e.g. to synchronize the QKD modules in time. Analogue as well as digital communications can occur on unauthenticated classical communication channel(s).

The TOE is intended for operation in an access-controlled environment and features only local user access. User identification can be as simple as connecting to the appropriate interface, while the access control policy of the environment ensures user authorization.

However, the PP does define packages for other common use cases. Users can connect to the TOE via a trusted path, which requires some external IT device. In this scenario users can be located remotely. In this case, the ST author can select the package defined in clause 11.1 [6], irrespective of whether the users are actually remote. In case the TOE itself features the interface for human users, the package in clause 11.4 [6] can be selected.

Another package deals with self protection of the security services of the TOE, if it can be deployed in an environment that cannot impede attackers possessing high attack potential (e.g. organized crime or foreign intelligence services). The ST author can consider selecting the package defined in clause 11.2 [6], if the TOE is intended for operation in a commercial grade environment.

The assets to be protected by a TOE claiming conformance to this PP are defined in the Protection Profile [6], chapter 7.1. Based on these assets the security problem definition is defined in terms of assumptions, threats and organisational security policies. This is outlined in the Protection Profile [6], chapters 7.2 to 7.4 for the base PP, and in chapter 11 for the packages.

These assumptions, threats and organisational security policies are split into security objectives to be fulfilled by a TOE claiming conformance to this PP and security objectives to be fulfilled by the operational environment of a TOE claiming conformance to this PP. These objectives are outlined in the PP [6], chapters 8.1 and 8.2 for the base PP, and in chapter 11 for the packages.

The Protection Profile [6] requires a Security Target based on this PP or another PP claiming this PP to fulfil the CC requirements for strict conformance.

2 Security Functional Requirements

Based on the security objectives to be fulfilled by a TOE claiming conformance to the PP, the security policy is expressed by the set of security functional requirements (SFR) to be implemented by a TOE. It covers the following issues (chapter 10 of [6]):

- Identification of users
- Access control
- Quantum Key Distribution
- Authenticated classical channel
- Audit for cryptographic TSF
- Self-test
- Emanation Security
- Secure End of Life state
- Limitation of user sessions
- Trusted path with user authentication
- Reaction to failed user authentication
- Emanation Security

Moreover, the following issues are addressed in the packages (chapter 11 of [6]):

- Physical protection
- Emanation Security
- Access control to personalization
- Proof of intactness after initial delivery
- Identification and authentication of users

These TOE security functional requirements are outlined in the PP [6], chapter 10 (base PP), and chapter 11 (packages). They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the SFR claim is called:

Common Criteria Part 2 extended

3 Assurance Requirements

The TOE security assurance package claimed in the Protection Profile is based entirely on the assurance components defined in part 3 of the Common Criteria. Thus, this assurance package is called:

Common Criteria Part 3 conformant
EAL 4 augmented by
AVA_VAN.5, ALC_DVS.2

(for the definition and scope of assurance packages according to CC see [1], part 3 for details).

4 Results of the PP-Evaluation

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all Application Notes and Interpretations of the Scheme (AIS) [4] as relevant for the TOE.

As a result of the evaluation the verdict PASS is confirmed for the assurance components of the class APE (Protection Profile evaluation).

The following assurance components were used:

APE_INT.1 PP introduction
APE_CCL.1 Conformance claims
APE_SPD.1 Security problem definition
APE_OBJ.2 Security objectives
APE_ECD.1 Extended components definition
APE_REQ.2 Derived security requirements

The results of the evaluation are only applicable to the Protection Profile as defined in chapter 1 of this report.

5 Obligations and notes for the usage

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.

In clause 11 the PP [6] defines several packages to support extended functionality of the TOE. ST authors may choose any of these considering that clauses 11.1 and 11.4 of [6] are mutually exclusive. If these packages do not reflect the actual extended security functionality, ST authors may extend the PP by their own modelling. In this case, the packages in clause 11 of [6] may serve as examples for orientation.

The ST/PP author shall adopt all formal items from a package, if conformance to this PP with that package is claimed. The PP [6] contains other application notes distributed through the document. The application notes are separated paragraphs that are marked with "Application Note" followed by a number.

6 Protection Profile Document

The Protection Profile Common Criteria Protection Profile — Pair of Prepare and Measure Quantum Key Distribution Modules, Version 2.1.1 [6] is being provided by the applicant ETSI. (See also Internet: https://www.etsi.org/standards.)

7 Definitions

7.1 Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security

CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ETSI	European Telecommunications Standards Institute
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
QKD	Quantum Key Distribution
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

7.2 Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

8 Bibliography

[1] ISO-Version:
ISO 15408:2022, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirements
https://www.iso.org/standard/72891.html
https://www.iso.org/standard/72892.html
https://www.iso.org/standard/72906.html
https://www.iso.org/standard/72913.html
https://www.iso.org/standard/72917.html

CCRA-Version:
CC:2022 R1, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirements
https://www.commoncriteriaportal.org

[2] ISO-Version:
ISO 18045:2022: Information technology Security techniques Methodology for IT security evaluation
https://www.iso.org/standard/72889.html

CCRA-Version:
CEM:2022 R1, Common Methodology for Information Technology Security Evaluation
https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[6].

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website

[6] Common Criteria Protection Profile — Pair of Prepare and Measure Quantum Key Distribution Modules, Version 2.1.1, ETSI (ISG QKD), Nov. 2023 (Compilation date).

[7] BSI-DSZ-CC-PP-0120 Evaluation Technical Report Summary, Version 1.0, 2023-11-28, SGS Digital Trust Services GmbH (confidential document)

[6] specially

- AIS 14, Version 7
- AIS 19, Version 9
- AIS 32, Version 7

C Annexes

List of annexes of this certification report

Annex A: Protection Profile Common Criteria Protection Profile — Pair of Prepare and Measure Quantum Key Distribution Modules, Version 2.1.1 [6] to be published by the applicant ETSI as “ETSI GS QKD 016 V2.1.1”.
(See also Internet: https://www.etsi.org/standards.)

Note: End of report