Federal Office
for Information Security

Certification Report

BSI-CC-PP-0107-2019

for

Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au), Version 0.9.5

developed by

Bundesamt für Sicherheit in der Informationstechnik

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-0107-2019

Common Criteria Protection Profile Configuration

Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au), Version 0.9.5

developed by Bundesamt für Sicherheit in der Informationstechnik
("Fachreferat TK11 - Sichere Halbleiter-Technologie")

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

Valid until 13 May 2029

SOGIS Recognition Agreement

Common Criteria

The Protection Profile Configuration identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. 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 Configuration 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 Configuration 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 Configuration 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, 14 May 2019
For the Federal Office for Information Security

Bernd Kowalski
Head of Division

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Contents

A Certification....6

1 Preliminary Remarks....6
2 Specifications of the Certification Procedure....6
3 Recognition Agreements....7
3.1 European Recognition of CC – Certificates (SOGIS-MRA)....7
3.2 International Recognition of CC – Certificates (CCRA)....7
4 Performance of Evaluation and Certification....8
5 Validity of the certification result....8
6 Publication....9

B Certification Results....10

1 Protection Profile Configuration Overview....11
2 Security Functional Requirements....11
3 Assurance Requirements....12
4 Results of the PP-Configuration-Evaluation....12
5 Obligations and notes for the usage....12
6 Protection Profile Document....12
7 Definitions....12
7.1 Acronyms....12
7.2 Glossary....13
8 Bibliography....14

C Annexes....15

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) and accompanying PP Configurations (PPC).

A PP Configuration (and its inherent PP Modules) defines an implementation-independent set of IT security requirements in conjunction with and on top of existing PPs (so called “base PPs”, or bPP) for a category of products which are intended to meet common consumer needs for IT security. A PP Configuration utilized by a user, consumer or stakeholder for IT gives them the possibility to individually customize their bPP in a certified manner, thus individually expressing their IT security needs without referring to a special product. Product certifications consequently can be based on the combination of base Protection Profile plus Protection Profile Configuration (bPP + PPC). For products which have been certified based on such a combination, an individual certificate will be issued but the results from a bPP + PPC certification can be re-used for the Security Target evaluation within a product evaluation when conformance to bPP + PPC has been claimed.

Certification of the Protection Profile Configuration 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 Configuration according to Common Criteria [1]. The evaluation is normally 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]
- BSI Schedule of Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3], including PP Certification

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

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

3 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408
- Common Methodology for IT Security Evaluation, Version 3.1 [2] 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 (PP Configuration).

3 Recognition Agreements

In order to avoid multiple certification of the same Protection Profile (or Protection Profile Configuration) 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 (and Protection Profile Configurations) 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 http://www.sogisportal.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 Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007

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-Configuration “Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au)“, Version 0.9.5 has undergone the certification procedure at BSI.

The evaluation of the PPC “Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au)“, Version 0.9.5 was conducted by the ITSEF TÜV Informationstechnik GmbH. The evaluation was completed on 10 May 2019. The ITSEF TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Bundesamt für Sicherheit in der Informationstechnik (Fachreferat TK11 - Sichere Halbleiter-Technologien).

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 Configuration as indicated.

In case of changes to the certified version of the Protection Profile Configuration, 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 Configuration, 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 for the concept of PPs, to CC [1] Part 2 for the definition of Security Functional Requirements components (SFR) and to CC [1] Part 3 for the definition of the Security Assurance Components, for the class AVA Vulnerability assessment and for the cross reference of Evaluation Assurance Levels (EALs) and assurance components.

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 Configuration 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 Configuration accordingly. Typically, technical standards are reviewed on a five years basis.

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

[5] Information Technology Security Evaluation Facility

6 Publication

The PP Configuration “Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au)“, Version 0.9.5 has been included in the BSI list of the certified Protection Profiles Configurations, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

1 Protection Profile Configuration Overview

The Protection Profile Configuration Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au), Version 0.9.5 [6] is established by the Bundesamt für Sicherheit in der Informationstechnik (Fachreferat TK11 - Sichere Halbleiter-Technologien) as a basis for the development of Security Targets in order to perform a certification of an IT-product, the so called Target of Evaluation (TOE).

The PPC under consideration provides additional TOE security functionality (TSF) with respect to the TSF of the Base-PP BSI-CC-PP-0104-2019 [8] in order to enable time service, time stamp service and security audit:

- The time service allows the user to query the internal time of the TSF.
- The time stamp service provides evidence that user data were presented to the TSF and exported audit data were generated at certain point in time and in a verifiable sequence. The validity of these user data and audit records can be verified.
- The audit functionality generates audit records on selected user activities controlled by the TSF and security events of the TOE defined by the Base-PP and the PP-Module. The Administrator role (cf. the Base-PP for definition of the roles) may be split in an additional role Auditor and Timekeeper.

Consequently, the Protection Profile Configuration is intended to be used within the Modular PP concept, as defined in [1].

The assets to be (additionally) protected by a TOE, claiming conformance to this PP Configuration, are defined in the PPC [6], chapter 6.1. 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 Configuration [6], chapters 6.2, 6.3 and 6.4, respectively.

The Protection Profile Configuration [6] requires the Protection Profile BSI-CC-PP-0104-2019 [8] to fulfil the CC requirements for strict conformance (see [6], section 5.3).

2 Security Functional Requirements

Based on the security objectives to be fulfilled by a TOE claiming conformance to this PP Configuration (and the underlying PP), the security policy is expressed by the set of security functional requirements (SFR) to be implemented by a TOE.

Specific details concerning these security policies can be found in the underlying PP [6] (section 6) and in section 9 of the PP Configuration [6].

The PP Configuration specific TOE security functional requirements are outlined in the PPC [6], chapter 9. 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 Configuration (as well as the base PP) 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 and 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-Configuration-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 ACE (Protection profile Configuration evaluation).

ACE_INT.1 PP-Module introduction,
ACE_CCL.1 PP-Module conformance claims,
ACE_SPD.1 PP-Module security problem definition,
ACE_OBJ.1 PP-Module security objectives,
ACE_ECD.1 PP-Module extended components definition,
ACE_REQ.1 PP-Module security requirements,
ACE_MCO.1 PP-Module consistency,
ACE_CCO.1 PP-Configuration consistency.

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

5 Obligations and notes for the usage

The following aspects need to be fulfilled when using the Protection Profile:

none.

6 Protection Profile Document

The Protection Profile Configuration “Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au)“, Version 0.9.5 [6] is being provided within a separate document as Annex A of this report.

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
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
bPP	base Protection Profile
PP	Protection Profile
PPC	Protection Profile Configuration
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] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017

Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 5, April 2017 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] PP Configuration: "Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au), Version 0.9.5", 2019-04-08, Bundesamt für Sicherheit in der Informationstechnik (Fachreferat TK11 - Sichere Halbleiter-Technologie)

[7] ETR-Summary: Evaluation Technical Report, "EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY)" Version 1, 2019-05-08, TÜV Informationstechnik GmbH (confidential document)

[8] Base PP: "Cryptographic Service Provider (PP CSP)", BSI-CC-PP-0104-2019, Version 0.9.8, Bundesamt für Sicherheit in der Informationstechnik (Fachreferat TK11 - Sichere Halbleiter-Technologie)

[6] specially

- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 41, Version 2, Guidelines for PPs and STs
- AIS 45, Version 2, Erstellung und Pflege von Meilensteinplänen

C Annexes

List of annexes of this certification report

Annex A: PPC “Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au)“, Version 0.9.5 [6] provided within a separate document.

Note: End of report