Federal Office
for Information Security

Certification Report

BSI-CC-PP-0082-V4-2019

for

Card Operating System Generation 2 (PP COS G2) Version 2.1

developed by

Bundesamt für Sicherheit in der Informationstechnik

sponsored by

gematik GmbH

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-0082-V4-2019

Common Criteria Protection Profile

Card Operating System Generation 2 (PP COS G2), Version 2.1

developed by Bundesamt für Sicherheit in der Informationstechnik
sponsored by gematik GmbH

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

Valid until 29 July 2029

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 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 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, 30 July 2019
For the Federal Office for Information Security

Joachim Weber
Head of Branch

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

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 special 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 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
- 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

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

4 Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007

- 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

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 http://www.sogisportal.eu.

3.2 International Recognition of CC – Certificates (CCRA)

The international Common Criteria Recognition Arrangement (CCRA) became effictive 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 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 Card Operating System Generation 2 (PP COS G2), Version 2.1 has undergone the certification procedure at BSI. This is a re-certification based on BSI-CC-PP-0082-V3-

2018. Specific results from the evaluation process based on BSI-CC-PP-0082-V3-2018 were re-used.

The evaluation of the PP Card Operating System Generation 2 (PP COS G2), Version 2.1 was conducted by the ITSEF SRC Security Research & Consulting GmbH. The evaluation was completed on 25 July 2019. The ITSEF SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the applicant is: Bundesamt für Sicherheit in der Informationstechnik.

The sponsor is: gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH.

The PP was developed by: Bundesamt für Sicherheit in der Informationstechnik.

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 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 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 Card Operating System Generation 2 (PP COS G2), Version 2.1 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]). 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 Card Operating System Generation 2 (PP COS G2), Version 2.1 [7] is established by the Bundesamt für Sicherheit in der Informationstechnik as a basis for the development of Security Targets in order to perform a certification of an IT-product, the Target of Evaluation (TOE).

The Target of Evaluation (TOE) defined in the PP is a smart card platform implementing the Card Operating System (COS) according to the specification [8] for the German health care system without any object system. The TOE is intended to be used within the German health care system as a platform for smart card products of the Card Generation 2, as for example an electronic Health Card (eHC), a Health Professional Card (HPC) or a Security Module Card of Type B (SMC-B), K (gSMC-K) or KT (gSMC-KT).

The TOE is required to comprise at least

- the Security IC Platform, i.e. the circuitry of the chip with the configuration and initialisation data applied to its security functionality and IC Dedicated Software (if applicable) with the configuration and initialisation data in relation to the IC Dedicated Software
- the IC Embedded Software (Card Operating System – including related configuration data) which, together with IC, fully implements feasible functions
- the wrapper for interpretation of exported TSF data
- the related user guidance
- and, if applicable, the translation table.

The TOE takes into account different optional functionalities as contained and modelled in the package 'Crypto Box', the package 'Contactless', the package 'PACE for Proximity Coupling Device', the package 'Logical Channel', the package 'RSA CVC' and the package 'RSA Key Generation', refer to the Protection Profile [7], chapters 7, 8, 9, 10, 11 and 12.

The TSF of the TOE defined in a Security Target (ST) claiming conformance to this PP comprises all security functionality available after delivery of the TOE including vendor specific commands for initialisation, personalisation and operational usage allowed but not described in the specification of the COS [8].

The TOE does not include any object system, i.e. the application specific structures like the Master File (MF), the Applications, the Application Dedicated Files (ADF), the Dedicated Files (DF), the Elementary Files (EF) and internal security objects (containing passwords, private keys etc.) including TSF data. The TOE and the intended application specific object system together build an initialised smart card product as for example an electronic Health Card (eHC), a Health Professional Card (HPC) or a Security Module Card of Type B (SMC-B), K (gSMC-K) or KT (gSMC-KT).

The typical life cycle phases for the present TOE type are IC and Smart Card Embedded software development, manufacturing, smart card product finishing, smart card personalisation and, finally, smart card end-usage.

The assets to be protected by a TOE claiming conformance to this PP are defined in the Protection Profile [7], chapter 3.1 and in addition for the TOE’s optional packages in the chapters 7.2.1, 8.2.1, 9.2.1, 10.2.1, 11.2.1 and 12.2.1 of [7]. 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 [7], chapters 3.2, 3.3 and 3.4 and in addition for the TOE's optional packages in the chapters 7.2.2, 7.2.3, 7.2.4, 8.2.2, 8.2.3, 8.2.4, 9.2.2, 9.2.3, 9.2.4, 10.2.2, 10.2.3, 10.2.4, 11.2.2, 11.2.3, 11.2.4, 12.2.2, 12.2.3 and 12.2.4 of [7].

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 [7], chapters 4.1 and 4.2 and in addition for the TOE's optional packages in the chapters 7.3, 8.3, 9.3, 10.3, 11.3 and 12.3 of [7].

The Protection Profile [7] 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 this 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:

- authentication of human users and external devices,
- storage of and access control on User Data,
- key management and cryptographic functions,
- management of TSF Data including life cycle support, and
- export of non-confidential TSF Data of the object systems if implemented on the platform.

These TOE security functional requirements are outlined in the PP [7], chapter 6.1 and for the TOE's optional packages in the chapters 7.4, 8.4, 9.4, 10.4, 11.4 and 12.4. 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

The PP claims strict conformance to Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, [9].

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
ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5

(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) [6] 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

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-CC-PP-0082-V3-2018, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on fosterage and evolution of the Protection Profile. It is now based on the updated COS-Specification [8] in version 3.12.0 from gematik. The command GET RANDOM was moved from the optional package “Logical Channel” to the mandatory part of the Protection Profile. The RSA encipher-/decipher functionality according to PKCS#1 V1.5 was removed from the modelling of cryptography.

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:

- The Protection Profile contains application notes, which the author of a product specific security target needs to consider.

6 Protection Profile Document

The Protection Profile Card Operating System Generation 2 (PP COS G2), Version 2.1 [7] is being provided within a separate document as Annex A of this report.

7 Definitions

7.1 Acronyms

ADF Application Dedicated File

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
COS	Card Operating System
CVC	Card Validation Code
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
EF	Elementary File
eHC	electronic Health Card
ETR	Evaluation Technical Report
gSMC-K	gerätespezifische Security Module Card Typ K
gSMC-KT	gerätespezifische Security Module Card Typ KT
HPC	Health Professional Card
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MF	Master File
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
RSA	Rivest-Shamir-Adleman Algorithm
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SMC-B	Security Module Card Typ B
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] Evaluation Technical Report BSI-CC-PP-0082-V4-2019, Version 3.8, 26 July 2019, Common Criteria Protection Profile Card Operating System Generation 2 (PP COS G2), SRC Security Research & Consulting GmbH (confidential document)

[7] Common Criteria Protection Profile Card Operating System Generation 2 (PP COS G2), BSI-CC-PP-0082-V4-2019, Version 2.1, 10 July 2019, Bundesamt für Sicherheit in der Informationstechnik

[8] Spezifikation des Card Operating System (COS), Elektrische Schnittstelle, Version 3.12.0, Revision 1, 15 May 2019, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[9] Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014, Eurosmart

[6] specially

- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile für Evaluationen nach CC
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 38, Version 2.0, Reuse of evaluation results

C Annexes

List of annexes of this certification report

Annex A: Protection Profile Card Operating System Generation 2 (PP COS G2), Version 2.1 [7] provided within a separate document.

Note: End of report