Federal Office
for Information Security

Certification Report

BSI-CC-PP-0099-V3-2024

for

Java Card System – Open Configuration Protection Profile Version 3.2, July 2024

developed by

Oracle Corporation

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-0099-V3-2024

Common Criteria Protection Profile

Java Card System – Open Configuration Protection Profile
Version 3.2, July 2024

developed by Oracle Corporation

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

valid until 17 October 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 CEM:2022 R1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version CC:2022 R1. 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 October 2024
For the Federal Office for Information Security

Sandro Amendola
Director-General

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

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 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] also published as ISO/IEC 15408
- Common Methodology for IT Security Evaluation [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 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] CC:2022: 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 Java Card System – Open Configuration Protection Profile, Version 3.2, July 2024 has undergone the certification procedure at BSI. This is a re-certification based on BSI-CC-PP-0099-V2-2020. Specific results from the evaluation process based on BSI-CC-PP-0099-V2-2020 were re-used.

The evaluation of the PP Java Card System – Open Configuration Protection Profile, Version 3.2, July 2024 was conducted by the ITSEF TÜV Informationstechnik GmbH. The evaluation was completed on 11 October 2024. 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: Oracle Corporation UK Limited.

The PP was developed by: Oracle Corporation.

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 Java Card System – Open Configuration Protection Profile, Version 3.2, July 2024 has been included in the BSI list of the certified Protection Profiles, which is published regularly (see also Internet: https://www.bsi.bund.de). 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 Java Card System – Open Configuration Protection Profile, Version 3.2, July 2024 [6] is established by the Oracle Corporation UK Limited 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 Protection Profile covers the Java Card specifications from versions 2.2.x up to version 3.2 of the Classic Edition. The specifications cover the Java Card Platform Virtual Machine, the Java Card Platform Runtime Environment and the Java Card Application Programming Interface. This Protection Profile applies to evaluations of open Java Card Platforms, that is, smart cards or similar devices enabled with Java Card technology that support post-issuance downloading of applications, referred to as Java Card technology-based applets.

The Java Card technology combines a subset of the Java programming language with a runtime environment optimized for smart cards and similar small-memory embedded devices. The main security goal of the Java Card Platform is to counter the unauthorized disclosure or modification of the code and data (keys, PINs, biometric templates, etc.) of applications and platform. In order to achieve this goal, the Java Card System provides strong security features such as the secure installation mechanism, firewall mechanism and dedicated API for security services.

The assets to be protected by a TOE claiming conformance to this PP are defined in the Protection Profile [6], chapter 5.1. 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 5.2, 5.3 and 5.4.

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], chapter 6.

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

To support proper and consistent usage of the PP, it is supplemented by the Supporting Documents as referenced in chapter 1.3 of the Protection Profile [6].

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:

- Core (Java Card Runtime Environment, Firewall Policy, and optional Logical Channels),
- Installation (of post-issuance applications),
- Applet Deletion,
- Object Deletion, and
- Secure Carrier (secure downloading of applications).

Specific details concerning the above mentioned security policies can be found in chapter 7 of the Protection Profile [6].

In addition, augmentation packages are defined in Appendix 1 of the PP that cover the following issues:

- Biometric Templates,
- Java Card Remote Method Invocation (JCRMI),
- Extended Memory,
- Sensitive Array,
- Sensitive Result,
- Monotonic Counters,
- Cryptographic Certificate Management,
- Key Derivation Functions (KDF) and
- System Time.

These TOE security functional requirements are outlined in the PP [6], chapter 7.1. They are all selected from Common Criteria Part 2. Thus the SFR claim is called:

Common Criteria Part 2 conformant

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, ALC_FLR.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) [5] 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-0099-V2-2020, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on updating specifications such as the migration from Common Criteria Version 3.1 Revision 5 to Common Criteria 2022 Revision 1. In consequence, the SFR claim is now Part 2 conformant as version 3.2 of the PP is modelled with components included in the CC catalogue. As part of the update the PP was augmented by ALC_FLR.2 – “Flaw reporting procedures”. The new version 3.2 of the Java Card specification is now addressed in the PP allowing new cryptographic constants in the Java Card API and configuration options for logical channels.

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:

A user of the PP shall carefully consider and apply all Application Notes included in the PP.

Further, the Appendix 1 in [6] introduces the augmentation packages specific to the optional features in Java Card specifications. This concerns the augmentation packages Biometric Templates, JCRMI, Extended Memory, Sensitive Array, Sensitive Result, Monotonic Counters, Cryptographic Certificate Management, Key Derivation Functions and System Time. It is the responsibility of the Security Target editor to include these security elements if the feature is supported. For instance, the ST writer shall indicate whether JCRMI is implemented in the TOE and whether it is activated or not. If the TOE provides JCRMI functionality, the full range of SFRs applies. Otherwise, the ST writer shall ignore JCRMI dedicated threats, objectives and requirements. This applies also to all Augmentation Packages and optional features.

Appendix 3 of the PP [6] provides a list of supported cryptographic algorithms introduced per Java Card version. A cryptographic assessment was not part of the PP evaluation. Neither the strength nor the suitability for use in a distinct TOE has been evaluated. When writing a Security Target claiming conformance to this PP, the author shall choose cryptographically strong algorithms and operation modes. Some further hints and guidelines can be derived from the ‘Technische Richtlinie BSI TR-02102’ (https://www.bsi.bund.de) and the ‘SOGIS Agreed Cryptographic Mechanisms’ (https://www.sogis.eu).

6 Protection Profile Document

The Protection Profile Java Card System – Open Configuration Protection Profile, Version 3.2, July 2024 [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

API Application Programming Interface

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
JCRMI	Java Card System Remote Method Invocation
PIN	Personal Identification Number
PP	Protection Profile
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

For further acronym explanations, see also Appendix 4 of the Protection Profile [6].

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, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security
- 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, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security
- 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/index.cfm

[2] ISO Version:
ISO 18045:2022: Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — 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/index.cfm

[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] Evaluation Technical Report BSI-CC-PP-0099-V3, Version 3, 14 October 2024, TÜV Informationstechnik GmbH (confidential document)

[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

[6] Java Card System – Open Configuration Protection Profile, Version 3.2, July 2024, BSI-CC-PP-0099-V3-2024, Oracle Corporation, SHA256: 8310c744504b3b003a80f0b1349a9971639c4b0a7a3af2749439446f3b942c9f

C Annexes

List of annexes of this certification report

Annex A: Protection Profile Java Card System – Open Configuration Protection Profile, Version 3.2, July 2024 [6] provided within a separate document.

Note: End of report