Certification Report

BSI-CC-PP-0105-V3-2025

for

Security Module Application for Electronic Record-keeping Systems (SMAERS), Version 3.0.2

developed by

Federal Office for Information Security

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

Certification Report V1.0 CC-PP-414 V3.67





BSI-CC-PP-0105-V3-2025

Common Criteria Protection Profile

Security Module Application for Electronic Record-keeping Systems (SMAERS) Version 3.0.2

developed by Federal Office for Information Security

Assurance Package claimed in the Protection Profile:

Common Criteria Part 3 conformant

EAL 2 augmented by

ALC_LCD.1, ALC_FLR.1 and ALC_CMS.3

valid until 26 March 2035



SOGIS Recognition Agreement



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, 27 March 2025
For the Federal Office for Information Security

Sandro Amendola Director-General



This page is intentionally left blank.

Contents

A Certification	€
 Preliminary Remarks	
6 Publication	
B Certification Results	10
 1 Protection Profile Overview. 2 Security Functional Requirements. 3 Assurance Requirements. 4 Results of the PP-Evaluation. 5 Obligations and notes for the usage. 6 Protection Profile Document. 7 Definitions. 7.1 Acronyms. 7.2 Glossary. 	
8 Bibliography	
C Annexes	16

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 Ordinance²
- BMI Regulations on Ex-parte Costs³
- 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]
- 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
- 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
- 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.

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 Security Module Application for Electronic Record-keeping Systems (SMAERS), Version 3.0.2 has undergone the certification procedure at BSI. This is a re-certification based on BSI-CC-PP-0105-V2-2020. Specific results from the evaluation process based on BSI-CC-PP-0105-V2-2020 were re-used.

The evaluation of the PP Security Module Application for Electronic Record-keeping Systems (SMAERS), Version 3.0.2 was conducted by the ITSEF TÜV Informationstechnik GmbH. The evaluation was completed on 11 March 2025. 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: Federal Office for Information Security, department T, which is an independent section within the BSI.

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 recertification 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 Security Module Application for Electronic Record-keeping Systems (SMAERS), Version 3.0.2 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 Security Module Application for Electronic Record-keeping Systems (SMAERS), Version 3.0.2 [5] is established by the Federal Office for Information Security 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 TOE type is a security module application implemented as software. The security module is part of a certified technical security system (CTSS) for electronic record-keeping systems (ERS).

The TOE application is either running on the platform of a CSP (referred to as platform-architecture), or running on a separate device communicating with the CSP via a trusted channel (referred to as client-server architecture). Depending on the overall architecture, different security requirements exist for a CSP.

The assets to be protected by a TOE claiming conformance to this PP are defined in the Protection Profile [5], chapter 3.1. 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 [5], chapter 3.4, 3.2 and 3.3.

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 [5], chapter 4.

The Protection Profile [5] requires a Security Target based on this PP [5] or another PP claiming this PP [5] to fulfil the CC requirements for strict conformance.

To support proper and consistent usage of the PP, it is supplemented by the Supporting Documents [7] to [10]. For the proper usage of the CSP in support of the PP [5] refer to the Supporting Documents [11] to [15].

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:

- · Cryptographic Support,
- User Data Protection,
- User Identification and Authentication.
- Security Management,
- Protection of the TSF,
- Trusted Path/Channels (applied by Package Trusted Channel between TOE and CSP only)
- Security Audit,
- Update Code Package Upgrade Functionality

These TOE security functional requirements are outlined in the PP [5], chapter 5.1. They are 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 2 augmented by ALC_LCD.1, ALC_FLR.1 and ALC_CMS.3

(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-0105-V2-2020, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was to adapt the PP to match new versions of the relevant Technical Guidelines in the context of the fiscalization of cash registers, i.e. BSI-TR-03151-1 [8] and BSI-TR-03153-1 [7], to address inconsistencies and ambiguities in the document that surfaced while performing product evaluations based on the prior version of the PP and to migrate the PP to the current version of the Common Criteria, i.e. CC:2022.

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 PP [5] defines several Application Notes that shall be considered when creating a security target and implementing a TOE that claims conformance to the PP [5].

Also, as the PP [5] was created to offer great flexibility with respect to different architectural designs, individual solutions of a SMAERS and CSP shall consider Chapter 1.2 (Non-TOE Hardware/Software/Firmware available to the TOE). A TOE that is based on this PP [5] can only be run together with a CC certified CSP component.

Additionally, individual Evaluation Activities (EA) associated with the augmentations ALC_LCD.1 and ALC_CMS.3 shall be performed as specified in the Assurance Refinements in Chapter 5.2.1 of the PP [5]. Further, additional Evaluation Activities associated with the life cycle of the security module of the TSS shall be performed according to the Supporting Document for Protection Profile SMAERS [10]. Please note that the Supporting Document for Protection Profile SMAERS [10] is not in the scope of this certification.

Also to support proper and consistent usage of the PP, it is supplemented by the Supporting Documents [7] to [10]. For the proper usage of the CSP in support of the PP [5] refer to the Supporting Documents [11] to [15].

6 Protection Profile Document

The Protection Profile Security Module Application for Electronic Record-keeping Systems (SMAERS), Version 3.0.2 [5] 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 ArrangementCC 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

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

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] 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] 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 TOE⁶.
- ⁶ Specially
 - AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile für Evaluationen nach CC
 - AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR für Evaluationen nach CC
 - AIS 23, Version 4, Zusammentragen von Nachweisen der Entwickler
 - AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

[5] Protection Profile "Security Module Application for Electronic Record-keeping Systems (SMAERS)", Version 3.0.2, 2025-01-21, Bundesamt für Sicherheit in der Informationstechnologie

- [6] Evaluation Technical Report, Version 1, 2025-01-21, "EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY)", TÜV Informationstechnik GmbH (confidential document)
- [7] Technische Richtlinie BSI TR-03153-1 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, Version 1.1.1, 2023-12-19, Bundesamt für Sicherheit in der Informationstechnologie
- [8] Technical Guideline BSI TR-03151-1 Secure Element API (SE API), Version 1.1.1, 2024-01-08, Bundesamt für Sicherheit in der Informationstechnologie
- [9] Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 5: Anwendungen der Secure Element API, Stand 2023, 2023-04-24, Bundesamt für Sicherheit in der Informationstechnologie
- [10] Supporting Document for Common Criteria Protection Profile SMAERS, Version 1.0, 2023-05-16, Bundesamt für Sicherheit in der Informationstechnologie
- [11] Protection Profile "Cryptographic Service Provider (CSP)", BSI-CC-PP-0104-2019, Version 0.9.8, 2019-02-19, Bundesamt für Sicherheit in der Informationstechnologie
- [12] Protection Profile "Configuration Cryptographic Service Provider Time Stamp Service and Audit", BSI-CC-PP-0107-2019, Version 0.9.5, 2019-04-08, Bundesamt für Sicherheit in der Informationstechnologie
- [13] Protection Profile "Configuration Cryptographic Service Provider Time Stamp Service and Audit Clustering", BSI-CC-PP-0108-2019, Version 0.9.4, 2019-04-08, Bundesamt für Sicherheit in der Informationstechnologie
- [14] Protection Profile "Cryptographic Service Provider Light", BSI-CC-PP-0111-2019, Version 1.0, 2019-11-12, Bundesamt für Sicherheit in der Informationstechnologie
- [15] Protection Profile "Configuration Cryptographic Service Provider Light Time Stamp Service and Audit", BSI-CC-PP-0113-2019, Version 1.0, 2020-07-15, Bundesamt für Sicherheit in der Informationstechnologie

- AIS 38, Version 2.0, Reuse of evaluation results
- AIS 41, Version 2, Guidelines for PPs and ST

C **Annexes**

List of annexes of this certification report

Protection Profile Security Module Application for Electronic Record-keeping Systems (SMAERS), Version 3.0.2[5] provided within a separate document. Annex A:

Note: End of report