Federal Office
for Information Security

Certification Report

BSI-CC-PP-0084-V2-2026

for

Security IC Platform Protection Profile including Functional Packages, Version 2.0

developed by

Infineon Technologies AG
NXP Semiconductors
STMicroelectronics
Thales

sponsored by

Eurosmart AISBL

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-0084-V2-2026

Common Criteria Protection Profile

Security IC Platform Protection Profile including Functional Packages, Version 2.0

developed by Infineon Technologies AG
NXP Semiconductors
STMicroelectronics
Thales
sponsored by Eurosmart AISBL

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 24 February 2036

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 15408:2022 and ISO/IEC 18045:2022.

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

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

Bonn, 25 February 2026

For the Federal Office for Information Security

Fabian Hodouschek L.S. Sandro Amendola
Head of Certification Director-General Directorate General S

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 (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]

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 2 December 2025, BGBl. 2025, no. 301, p. 2
Current version see website: http://www.gesetze-im-internet.de/bsig_2025/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 02 December 2025, Bundesgesetzblatt 2025, no. 301
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 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.

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

The PP Security IC Platform Protection Profile including Functional Packages, Version 2.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-CC-PP-0084-2014. Due to a change of the ITSEF, results from the evaluation process was not possible.

The evaluation of the PP Security IC Platform Protection Profile including Functional Packages, Version 2.0 was conducted by the ITSEF SGS Digital Trust Services GmbH. The evaluation was completed on 19 February 2026. The ITSEF SGS Digital Trust Services GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Eurosmart AISBL.

The PP was developed by: Infineon Technologies AG, NXP Semiconductors, STMicroelectronics and Thales.

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 Security IC Platform Protection Profile including Functional Packages, Version 2.0 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.

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

[5] Information Technology Security Evaluation Facility

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 IC Platform Protection Profile including Functional Packages’, Version 2.0, [5] is established by Eurosmart AISBL as a basis for the development of Security Targets in order to perform a certification of Security Integrated Circuits. It is an update, technically and according to CC:2022 Revision 1, of the Smartcard Protection Profile BSI-CC-PP-0084-2014 [6].

The TOE of the Protection Profile is a Security IC which is composed of a processing unit, security components, I/O ports (contact or contactless interface) and volatile and non-volatile memories. The Security IC may include IC Dedicated Software and optional address-based access control block, if they are delivered by the IC manufacturer.

A specific life-cycle is defined for the product considered as the TOE in chapters 1.3.5 and 11.1 of the Protection Profile [5]. The assets to be protected by a TOE claiming conformance to BSI-CC-PP-0084-V2-2026 are defined in the Protection Profile [5], chapters 3.1 and 11.1.3. 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], chapters 3.2, 3.3 and 3.4.

These assumptions, threats and organisational security policies are covered by 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 4.1 for the TOE itself, chapter 4.2 for the Security IC Embedded Software and chapter 4.3 for the Operational Environment. The Protection Profile [5] requires a Security Target based on this PP or another PP claiming this PP to fulfil the CC requirements for strict conformance.

The main changes of PP [5] compared to its previous version [6] is the update to CC:2022 Revision 1, a new functional package for address-based Access Control and a new package for Cryptographic services, which replaces the three packages Triple DES, AES and Hash. A summary is given in chapter 11.4 of the PP [5].

The PP also includes an Appendix, which is referred to as informative inside of the PP and has not been formally evaluated by the ITSEF.

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:

Protection of user data and support of the other SFRs against: Malfunction, Leakage, Physical Manipulation and Probing. Moreover the TOE's life-cycle is supported as well as the user Identification whereas the Abuse of Functionality is prevented. Furthermore, Random Number Generation is provided as Specific Functionality.

These TOE security functional requirements are outlined in the PP [5], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the SFR claim is called:

Common Criteria Part 2 extended

3 Assurance Requirements

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

Common Criteria Part 3 conformant
EAL 4 augmented by
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) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all Application Notes and Interpretations of the Scheme (AIS) [4] as relevant for the TOE.

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

The following assurance components were used:

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

This certification procedure is based on an update of the Common Criteria Protection Profile previously certified under BSI-CC-PP-0084-2014. The evaluation was done by a different ITSEF. In turn, results from previous evaluation could not be re-used.

The PP [5] is aligned with CC:2022, Revision 1, allowing to integrate several SFRs as standard components. It satisfies Eurosmart’s demands for state of the art modelling of security features in modern security ICs for both consumer and governmental markets.

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 holds numbered Application Notes that need to be considered by the ST authors. Some of which include requirements, i.e. “shall” statements.

Application Note 35 of the PP refers to a list of Agreed Cryptographic Mechanisms as part of the EUCC scheme. 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).

Chapter 10 of the PP [5] states Supporting Documents for proper and consistent usage. For TOE evaluations, the accepted version shall be agreed with the certification body as these technical documents will evolve over time to reflect state of the art ratings. The Bibliography in chapter 8 states versions in scope at the time of the evaluation of the PP [5] for certain documents from ENISA [8] to [14].

6 Protection Profile Document

The Protection Profile 'Security IC Platform Protection Profile including Functional Packages', Version 2.0 [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 Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ENISA	European Union Agency for Cybersecurity
ETR	Evaluation Technical Report
EUCC	European Union Cybersecurity Certification Scheme
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.

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.

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, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirements

https://www.commoncriteriaportal.org

[2] ISO-Version:
ISO 18045:2022: Information 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

[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] Common Criteria Protection Profile BSI-CC-PP-0084-V2 – Security IC Platform Protection Profile including Functional Packages, Version 2.0, 16 December 2025, Eurosmart, SHA256: 2e94f4e63974decaa750ee276116dd32217095b40eb5fd78f30f7ae0bf82a67e

[6] Common Criteria Protection Profile BSI-CC-PP-0084 – Security IC Protection Profile with Augmentation Packages, Version 1.0, 13 February 2014, Eurosmart

[7] Evaluation Technical Report Summary, BSI-CC-PP-0084-V2, Version 2.0, 10 February 2026, SGS Digital Trust Services GmbH (confidential document)

[8] EUCC scheme State-of-the-art document, Application of Common Criteria to Integrated Circuits, Version 2, December 2024, ENISA

[9] EUCC scheme State-of-the-art document, Security Architecture requirements (ADV_ARC) for smart cards and similar devices extended to Secure Sub Systems in SoCs, Version 1.1, October 2023, ENISA

[10] EUCC scheme State-of-the-art document, Application of attack potential to smartcards and similar devices, Version 2, February 2025, ENISA

[11] EUCC scheme State-of-the-art document, Composite product evaluation for Smart Cards and similar devices for CC 3.1, Version 2, December 2024, ENISA

[12] EUCC scheme State-of-the-art document, Minimum Site Security Requirements, Version 2, February 2025, ENISA

[13] EUCC scheme State-of-the-art document, Guidelines on cryptography, Agreed Cryptographic Mechanisms, Version 2, May 2025, ENISA

[14] EUCC scheme Guidelines on cryptography, Sub-group on Cryptography, Agreed Cryptographic Mechanisms, Version 2.0, April 2025, ENISA

[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

C Annexes

List of annexes of this certification report

Annex A: Protection Profile Security IC Platform Protection Profile including Functional Packages, Version 2.0 [5] provided within a separate document.

Note: End of report