Federal Office
for Information Security

Certification Report

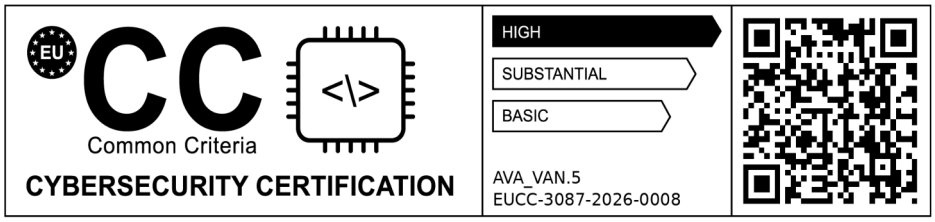
EUCC-3087-2026-0008

for

Security IC Platform Protection Profile including Functional Packages, Version 2.0

issued by

Eurosmart AISBL



Administration ID:

BSI-CC-PP-0084-V2-2026

BSI - Bundesamt für Sicherheit in der Informationstechnik, 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 9582-11

Contents

A. Certification....4

1. Preliminary Remarks....4
2. Specifications of the Certification Procedure....4
3. Mutual Recognition....5
4. Performance of Evaluation and Certification....6
5. Validity of the Certification Result....6
6. Publication....7

B. Certification Results....8

1. Protection Profile Overview....9
2. Security Functional Requirements....9
3. Assurance Requirements....10
4. Results of the PP-Evaluation....10
5. Obligations and notes for the usage....10
6. Identification of the PP....11
7. Protection Profile....11
8. Definitions....11
9. Bibliography....12

C. Annexes....15

A. Certification

1. Preliminary Remarks

The Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 [IR] establishes a Union-wide cybersecurity certification scheme for ICT products and Protection Profiles for conformity assessments using the requirements of Common Criteria.

By implementing the Cybersecurity Act [CSA], certification activities at assurance level ‘high’ and in duly justified cases at assurance level ‘substantial’ are reserved to the National Cybersecurity Certification Agency of a Member State.

In accordance to BSIG Act [BSIG], the Federal Office for Information Security (BSI) issues 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 product according to the security criteria referenced in the above mentioned Implementing Regulation (EU) 2024/482 as well as relevant application notes and interpretations published by the certification body of the BSI. Evaluation facilities notified by the German National Cybersecurity Certification Authority carry out the evaluation.

This Certification Report is the result of the certification activities carried out by the certification body of the BSI in conclusion of the technical evaluation. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The certification 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.

2. Specifications of the Certification Procedure

The certification body carries out its activities according to the criteria laid down in the following:

- Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) [IR]

- EUCC state-of-the-art documents of relevance to the TOE [SotA]
- Act on the Federal Office for Information Security [BSIG]
- BSI Certification and Approval Ordinance [ZertV]
- BMI Regulations on Ex-parte Costs [GebV]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior and Community)
- ISO/IEC 15408 as published on the day of issuance of this certificate and as mirrored by the Common Criteria for IT Security Evaluation [CC]
- ISO/IEC 18045 as published on the day of issuance of this certificate and as mirrored by the Common Methodology for IT Security Evaluation [CEM]
- DIN EN ISO/IEC 17065 standard
- EUCC programme: Scheme documentation describing the certification process (EUCC) [EUCC]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [AIS]

3. Mutual Recognition

3.1. EU Cybersecurity Certification Scheme on Common Criteria (EUCC)

Certificates issued under EUCC are recognised according to Implementing Regulation (EU) 2024/482 [IR]. Details of EUCC can be found at

https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en.

3.2. International Recognition of CC – Certificates (CCRA)

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.

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 Protection Profile Security IC Platform Protection Profile including Functional Packages, Version 2.0 [PP] has been certified under the EUCC scheme in accordance to the provisions of the Implementing Regulation (EU) 2024/482. The PP [PP] is an update of the Common Criteria Protection Profile previously certified under BSI-CC-PP-0084-2014 [PPv1]. Due to a change of the ITSEF, re-use of results from the previous evaluation process was not possible.
- The evaluation of the Protection Profile Security IC Platform Protection Profile including Functional Packages, Version 2.0 was conducted by SGS Digital Trust Services GmbH. The evaluation was completed on 30. July 2026. SGS Digital Trust Services GmbH is a notified evaluation facility (ITSEF).
- The Evaluation Technical Report [ETR] was provided by the ITSEF according to the Common Criteria [CC], the Methodology [CEM], and the requirements of the Scheme [IR].
- CC Version and Release: see [CC] and [CEM]
- Claimed Assurance level according to the CSA [CSA]: high
- 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 body monitors each individual evaluation to ensure a uniform application and interpretation of the criteria as well as uniform ratings.
- The certification activities are concluded with the comparability check and the production of this Certification Report. This work was completed by the certification body of the BSI.

5. Validity of the Certification Result

This Certification Report applies only to the version of the PP as identified in this document.

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 [CC] 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 notified to ENISA for publication on the website on European cybersecurity certification schemes https://certification.enisa.europa.eu/. Further information can be obtained from BSI-Infoline +49 228 9582-111.

This holder of the certificate[1] has to publish on its website this Certification Report and supplementary information. The Certification Report may also be obtained in electronic form at the internet address stated above.

[1] Eurosmart AISBL
Square de Meeûs 35
1000 Bruxelles
Belgium

B. Certification Results

The following chapters summarise the assessment results of the

- the certified Protection Profile,
- the relevant evaluation results from the evaluation facility, and
- complementary notes, statements and indications from the certification body.

1. Protection Profile Overview

The Protection Profile Security IC Platform Protection Profile including Functional Packages, Version 2.0 [PP] 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 [PPv1].

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 [PP].

The assets to be protected by a TOE claiming conformance to this PP are defined in [PP], 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 [PP], 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 [PP], 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 [PP] 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 [PP] compared to its previous version [PPv1] 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 [PP].

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 [PP], 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 2022 Part 2 extended

3. Assurance Requirements

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

Common Criteria Part 3 conformant
EAL 4 augmented by
ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5

(for the definition and scope of assurance packages according to CC see [CC], part 3 for details).

4. Results of the PP-Evaluation

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. Due to a change of the ITSEF, re-use of results from the previous evaluation process was not possible.

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 [PP] 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 [PP] for certain documents from ENISA [E1] to [E6].

The certification results apply only to the version of the PP indicated in the certificate and on the condition that all the statements and indications are kept as detailed in this Certification Report. Neither the BSI nor any other organisation that recognises or gives effect to this certificate implicitly or explicitly guarantee or endorse the certified PP.

6. Identification of the PP

The Target of Evaluation (TOE) is identified as follows:

Security IC Platform Protection Profile including Functional Packages, Version 2.0

Holder of the certificate: Eurosmart AISBL
Square de Meeûs 35
1000 Bruxelles
Belgium

7. Protection Profile

For the purpose of publishing, the Protection Profile [PP] is provided within a separate document as Annex A of this report.

SHA256 hash of the PP:
2e94f4e63974decaa750ee276116dd32217095b40eb5fd78f30f7ae0bf82a67e

8. Definitions

8.1. 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

8.2. 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 CC part 2 and/or assurance requirements not contained in CC part 3.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

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.

9. Bibliography

[CSA] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[IR] Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme and related amendments (EUCC)

[BSIG] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 02 December 2025, Bundesgesetzblatt 2025 I Nr. 301, S. 2

[ZertV] 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

[GebV] 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

[CC] ISO 15408:2022, 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.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

as mirrored by CCRA's edition:
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

[CEM] ISO 18045:2022: Information technology Security techniques Methodology for IT security evaluation
https://www.iso.org/standard/72889.html

as mirrored by CCRA's edition:
CEM:2022 R1, Common Methodology for Information Technology Security Evaluation
https://www.commoncriteriaportal.org

[EUCC] EUCC program of the BSI: Scheme documentation describing the certification process (EUCC), https://www.bsi.bund.de/zertifizierung

[SotA] EUCC state-of-the-art documents, https://certification.enisa.europa.eu/

[PUB] EUCC Certificates, periodically updated list published on ENISA's website on European cybersecurity certification schemes,
https://certification.enisa.europa.eu/

[AIS] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE, https://www.bsi.bund.de/AIS

[PP] 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

[ETR] Evaluation Technical Report Summary, BSI-CC-PP-0084-V2, Version 5.0, 30 July 2026, SGS Digital Trust Services GmbH (confidential document)

[PPv1] Common Criteria Protection Profile BSI-CC-PP-0084 – Security IC Protection Profile with Augmentation Packages, Version 1.0, 13 February 2014, Eurosmart

[E1] EUCC scheme State-of-the-art document, Application of Common Criteria to Integrated Circuits, Version 2, December 2024, ENISA

[E2] 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

[E3] EUCC scheme State-of-the-art document, Application of attack potential to smartcards and similar devices, Version 2, February 2025, ENISA

[E4] 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

[E5] EUCC scheme State-of-the-art document, Minimum Site Security Requirements, Version 2, February 2025, ENISA

[E6] EUCC scheme State-of-the-art document, Guidelines on cryptography, Agreed Cryptographic Mechanisms, Version 2, May 2025, ENISA

C. Annexes

List of annexes of this certification report

Annex A: Protection Profile provided within a separate document.