Federal Office
for Information Security

Certification Report

BSI-CC-PP-0125-2026

for

Security IC Platform Multi-assurance PP-Configurations, Version 1.0

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-0125-2026

Common Criteria Protection Profile Configuration

Security IC Platform Multi-assurance PP-Configurations, Version 1.0

developed by Infineon Technologies AG
NXP Semiconductors
STMicroelectronics
Thales

sponsored by Eurosmart AISBL

Assurance Package claimed in the Protection Profile Configuration:
Common Criteria Part 3 conformant
EAL 4 augmented by
ADV_SPM.1, ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5

valid until 24 February 2036

SOGIS Recognition Agreement

Common Criteria

The Protection Profile Configurations identified in this certificate have 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 PP-Configurations 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 Configurations 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 Profiles Configurations 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
Head of Certification

L.S.

Sandro Amendola
Director-General Directorate General S

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87 - 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....6
1 Preliminary Remarks....6
2 Specifications of the Certification Procedure....6
3 Recognition Agreements....7
3.1 European Recognition of CC – Certificates (SOGIS-MRA)....7
3.2 International Recognition of CC – Certificates (CCRA)....7
4 Performance of Evaluation and Certification....8
5 Validity of the certification result....8
6 Publication....8
B Certification Results....10
1 PP-Configuration overview....11
2 Security Functional Requirements....11
3 Assurance Requirements....12
4 Results of the PP-Configuration evaluation....12
5 Obligations and notes for the usage....12
6 PP-Configurations Document....12
7 Definitions....13
7.1 Acronyms....13
7.2 Glossary....13
8 Bibliography....14
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) and accompanying PP-Configurations (PPC).

A PP-Configuration (and its inherent PP Modules) defines an implementation-independent set of IT security requirements in conjunction with and on top of existing PPs (so called “base Protection Profiles”) for a category of products which are intended to meet common consumer needs for IT security. A PP Configuration utilized 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 consequently can be based on the combination of base Protection Profile plus Protection Profile Configuration (bPP + PPC). For products which have been certified based on such a combination, an individual certificate will be issued but the results from a bPP + PPC certification can be re-used for the Security Target evaluation within a product evaluation when conformance to bPP + PPC has been claimed.

Certification of the Protection Profile Configuration 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 Configuration 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

[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

- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3], including PP Certification
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC)[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 (PP Configuration)

3 Recognition Agreements

In order to avoid multiple certification of the same PP or PP-Configuration 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 PP or PP-Configuration 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] 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 Security IC Platform Multi-assurance PP-Configurations, Version 1.0 has undergone the certification procedure at BSI.

The evaluation of the PP Security IC Platform Multi-assurance PP-Configurations, Version 1.0 was conducted by the ITSEF SGS Digital Trust Services GmbH. The evaluation was completed on 23 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 PP-Configurations document as indicated.

In case of changes to the certified version of the PP-Configurations, 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 PP-Configurations, 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 certified PP-Configurations 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 PP-Configurations 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 Multi-assurance PP-Configurations, Version 1.0 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 PP-Configurations,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 PP-Configuration overview

The Security IC Platform Multi-assurance PP-Configurations, Version 1.0 [5] is established by the Eurosmart AISBL 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 PP-Configurations defined in [5] are composed of the base PP-0084-V2 [7] and a subset of functional packages and PP-Modules. All the PP-Modules have the PP-0084-V2 as base PP. The PP-Modules address functionality that is already in the scope of the base PP, but at a strictly higher assurance level including ADV_SPM.1. The TOE type is the same as in the base PP, a Security IC platform comprising hardware and IC Dedicated Software.

The selectable PP-Modules are defined in chapters 3.1 to 3.5 of the PP-Configurations [5]:

- PP-Module ‘Authentication of the Security IC’
- PP-Module ‘Loader 1’ (for usage in secured environment only)
- PP-Module ‘Loader 2’ (for usage by authorised users only)
- PP-Module ‘Address-based Access Control’
- PP-Module ‘Limited Test Features’, does not claim any functional package conformance

Each PP-Module claims conformance to the assurance package EAL4 augmented with ADV_SPM.1, ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5, including the refinements defined in the base PP [7].

The TOE implements physical protection of its assets and the assets of the Embedded Software against probing, forced and inherent information leakage, manipulation, and malfunctions induced by environmental stress as defined in the base PP [7]. Based on these assets the security problem definition is defined in terms of assumptions, threats and organisational security policies. This is outlined in the base PP [7], chapter 3. The PP-Modules do not add assets, OSPs nor assumptions.

The PP-Configurations require strict conformance of a Security Target claiming conformance to it.

2 Security Functional Requirements

Based on the security objectives to be fulfilled by a TOE claiming conformance to this PP-Configuration the security policy is expressed by the set of security functional requirements (SFR) to be implemented by a TOE.

Specific details concerning these security policies can be found in the base PP [7] chapter 6 and in chapters 3.x.5.1 of the PP-Configurations document [5] for each PP-Module.

The SFRs 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 PP-Configurations is based entirely on the assurance components defined in part 3 of the Common Criteria. Thus, this assurance package is called:

- Assurance — Common Criteria Part 3 conformant Multi-Assurance
- Global Assurance — EAL 4 augmented by ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5
- Assurance of the PP-Module-based sub-TSFs — EAL 4 augmented by ADV_SPM.1, 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-Configuration 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 ACE (PP-Configuration evaluation).

The following assurance components were used:

ACE_INT.1	PP-Module introduction
ACE_CCL.1	PP-Module conformance claims
ACE_SPD.1	PP-Module security problem definition
ACE_OBJ.2	PP-Module security objectives
ACE_ECD.1	PP-Module extended components definition
ACE_REQ.2	PP-Module derived security requirements
ACE_MCO.1	PP-Module consistency
ACE_CCO.1	PP-Configuration consistency

The results of the evaluation are only applicable to the PP-Configurations as defined in chapter 1.

5 Obligations and notes for the usage

The following aspects need to be fulfilled when using the PP-Configurations:

none

6 PP-Configurations Document

The Security IC Platform Multi-assurance PP-Configurations, Version 1.0 [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

bPP base Protection Profile

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

PP Protection Profile

PPC Protection Profile Configuration

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] PP-Configuration: Security IC Platform Multi-assurance PP-Configurations, Version 1.0, 16 December 2025, Eurosmart AISBL, SHA256: 6973adfb8dc9d9d4aff7796e2baf001ec3a12c506cb453482b22b3d7e6082607

[6] Evaluation Technical Report for BSI-CC-PP-0125 - Security IC Platform Multi-assurance PP-Configurations, Version 2.0, 10 February 2026, SGS Digital Trust Services 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

[7] Base PP: Security IC Platform Protection Profile including optional Functional Packages, BSI-CC-PP-0084-V2, Version 2.0, 16 December 2025, Eurosmart AISBL

C Annexes

List of annexes of this certification report

Annex A: Protection Profile Security IC Platform Multi-assurance PP-Configurations, Version 1.0 [5] provided within a separate document.

Note: End of report