Federal Office
for Information Security

Certification Report

BSI-CC-PP-0117-V2-2023

for

Secure Sub-System in System-on-Chip (3S in SoC), Version 1.8

developed by

EUROSMART

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-0117-V2-2023

Common Criteria Protection Profile

Secure Sub-System in System-on-Chip (3S in SoC), Version 1.8

developed by EUROSMART

Assurance Package claimed in the Protection Profile:
Strict conformant to BSI-CC-PP-0084-2014
Common Criteria Part 3 conformant
EAL 4 augmented by
ATE_DPT.2, AVA_VAN.5, ALC_DVS.2, ALC_FLR.2

valid until 19 December 2033

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 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.

Common Criteria Recognition Arrangement

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.

Bonn, 20 December 2023
For the Federal Office for Information Security

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

Matthias Intemann
Head of Section

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), Version CC:2022[4] [1] also published as ISO/IEC 15408
- Common Methodology for IT Security Evaluation, Version CC:2022 [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 effictive 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 PP Secure Sub-System in System-on-Chip (3S in SoC), Version 1.8 has undergone the certification procedure at BSI. This is a re-certification based on BSI-CC-PP-0117-2022. Specific results from the evaluation process based on BSI-CC-PP-0117-2022 were re-used.

The evaluation of the PP Secure Sub-System in System-on-Chip (3S in SoC), Version 1.8 was conducted by the ITSEF SGS Digital Trust Services GmbH. The evaluation was completed on 7 November 2023. 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 applicant is: Eurosmart AISBL.

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 Secure Sub-System in System-on-Chip (3S in SoC), Version 1.8 has been included in the BSI list of the certified Protection Profiles, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). 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 Secure Sub-System in System-on-Chip (3S in SoC), Version 1.8 [6] 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 (3S in SoC).

The TOE is a Protection Profile from Eurosmart. The TOE is strict conformant to BSI-CC-PP-0084-2014 [8].

The TOE type addressed by the PP is a "Secure Sub-System in System-on-Chip (3S in SoC)" implemented as a functional block of a System on Chip (SoC). The IT-product provides its security features and security services isolated from the remaining SoC components (logical and physical isolation).

The 3S in SoC comprises hardware (HW), firmware (FW) and software (SW). The aim is to provide functionalities such as root of trust (RoT), including the unique identification of each instance and the generation of random numbers, as well as optional security services such as cryptographic functions. The data stored and processed inside the 3S is protected by means of security features. The 3S in SoC may have dedicated interfaces that interact with other components of the SoC or with the external world.

The application areas the PP might be used for may include:

- User authentication and password storage
- Content protection
- Payment
- Subscriber identity module (SIM)
- Secure storage and management of digital identities
- Secure key storage
- Root of trust
- Storage of sensitive user data (e.g. healthcare records)

The assets to be protected by a TOE claiming conformance to this PP are defined in the Protection Profile [6], 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 [6], chapter 3.4, 3.2, 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 [6], chapter 4.

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

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 against malfunction

- Protection against abuse of functionality
- Protection against physical manipulation and probing
- Protection against leakage
- TOE identification and root of trust
- Generation of random numbers

and the following optional functional packages:

- Passive External Memory Package
- Secure External Memory Package
- Loader Package
- Crypto Package
- Composite Software Isolation Package
- Secure Update Package
- Package for Composite Software identity binding with asymmetric cryptography key

These TOE security functional requirements and optional packages are outlined in the PP [6], chapter 6 and 7. 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
ATE_DPT.2, AVA_VAN.5, ALC_DVS.2, ALC_FLR.2

(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

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-CC-PP-0117-2022, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on two new packages and a change to 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:

In case this PP is used to certify a product TOE based on programmable logic (PL) (e.g. for a Field Programmable Gate Array (FPGA)), additional SFRs and specific assurance activities related to the technology and life cycle aspects of FPGA might have to be specified in the Security Target.

The PP outlines several formal Application Notes and requirements/guidance specifying items to be addressed when compiling a Security Target. The ST author shall consider these Application notes and requirements/guidance if applicable to the product TOE to be evaluated.

6 Protection Profile Document

The Protection Profile Secure Sub-System in System-on-Chip (3S in SoC), Version 1.8 [6] is being provided within a separate document as Annex A of this report.

7 Definitions

7.1 Acronyms

3S Secure Sub-System

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

ETR Evaluation Technical Report

FPGA Field Programmable Gate Array

FW Firmware

HW Hardware

IT Information Technology

ITSEF	Information Technology Security Evaluation Facility
PL	Programmable Logic
PP	Protection Profile
RoT	Root of Trust
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SoC	System-on-Chip
ST	Security Target
SW	Software
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] ISO-Version:
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

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 technology Security techniques 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] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website

[6] Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile, BSI-CC-PP-0117-V2-2023, Version 1.8, 2023-10-26, Eurosmart

[7] BSI-CC-PP-0117-V2-2023 Evaluation Technical Report Summary, Version 1.1, 2023-11-03, SGS Digital Trust Services GmbH (confidential document)

[8] Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014

[6] specially

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 38, Version 2.0, Reuse of evaluation results

C Annexes

List of annexes of this certification report

Annex A: Protection Profile Secure Sub-System in System-on-Chip (3S in SoC), Version 1.8 [6] provided within a separate document.

Note: End of report