Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0882-V2-2019

for

S3CS9AB 32-Bit RISC Microcontroller for Smart Cards, Revision 0 with specific IC Dedicated Software

from

Samsung Electronics

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 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0882-V2-2019 (*)

Smartcard Controller

S3CS9AB 32-Bit RISC Microcontroller for Smart Cards, Revision 0 with specific IC Dedicated Software

from	Samsung Electronics
PP Conformance:	Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 5 augmented by AVA_VAN.5 and ALC_DVS.2

SOGIS
Recognition Agreement

Common Criteria

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. 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 product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

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 IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product 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, 11 December 2019

For the Federal Office for Information Security

Bernd Kowalski
Head of Division

L.S.

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

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 BSIG1 Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally 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.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

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[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of 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]
- 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), Version 3.1[4] [1] also published as ISO/IEC 15408.

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

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

3 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

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 and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

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.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates 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 current list of signatory nations and approved certification schemes can be seen on the website: https://www.commoncriteriaportal.org.

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.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2+ ALC_FLR components.

[4] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

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 product S3CS9AB 32-Bit RISC Microcontroller for Smart Cards, Revision 0 with specific IC Dedicated Software has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0882-2013. Specific results from the evaluation process BSI-DSZ-CC-0882-2013 were re-used.

The evaluation of the product S3CS9AB 32-Bit RISC Microcontroller for Smart Cards, Revision 0 with specific IC Dedicated Software was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 10 December 2019. 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: Samsung Electronics.

The product was developed by: Samsung Electronics.

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 applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 11 December 2019 is valid until 10 December 2024. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security

[5] Information Technology Security Evaluation Facility

Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product S3CS9AB 32-Bit RISC Microcontroller for Smart Cards, Revision 0 with specific IC Dedicated Software has been included in the BSI list of certified products, 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.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Samsung Electronics
17th Floor, B Tower DSR building
Samsungjeonja-ro 1-1 Hwaseong-si, Gyeonggi-do
South Korea 445-330

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE), the S3CS9AB 32-Bit RISC Microcontroller for Smart Cards, Revision 0 with specific IC Dedicated Software, is a smartcard integrated circuit which is composed of a processing unit, security components, the ESE interface, hardware circuit for testing purpose during the manufacturing process and volatile and non-volatile memories (hardware). The TOE also includes any IC Designer/Manufacturer proprietary IC Dedicated Software as long as it physically exists in the smartcard integrated circuit after being delivered by the IC Manufacturer. Such software (also known as IC firmware) is used for testing purpose during the manufacturing process but also provides additional services to facilitate the usage of the hardware and/or to provide additional services, including an AIS31 compliant random number generator.

The TOE is intended to be used in smart cards for particularly security relevant applications and for its previous use as developing platform for smart card operating systems. The TOE is the platform for the Smartcard Embedded Software, at which the term Smartcard Embedded Software is used for all operating systems and applications stored and executed on the TOE.

The TOE is dedicated to applications such as:

- Banking and finance applications for credit or debit cards, electronic purse (stored value cards) and electronic commerce.
- Network based transaction processing such a mobile phones (GSM SIM cards), pay TV (subscriber and pay-per-view cards), communication highways (Internet access and transaction processing).
- Transport and ticketing applications (access control cards).
- Governmental cards (ID cards, health cards, driving licenses).
- Multimedia applications and Digital Right Management protection.

As security features it provides:

- Security sensors or detectors including High and Low Temperature detectors, High Frequency filter, High and Low Supply Voltage detectors, Supply Voltage Glitch detectors, Light detector and the Passivation Removing Detector.
- Active Shields against physical intrusive attacks.
- Dedicated tamper-resistant design based on synthesizable glue logic and secure topology.
- Dedicated hardware mechanisms against side-channel attacks such as Internal Variable Clock, Random Wait Generator, Random Current Generator, RAM and EEPROM encryption mechanisms.
- Secure DES and AES Symmetric Cryptography support.
- The IC Dedicated Software includes:
  - A True Random Number Generator (DTRNG) for AIS31-compliant Random Number Generation.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007 [7].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 5 augmented by AVA_VAN.5 and ALC_DVS.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
SFR1	Failure with preservation of secure state
SFR2	Limited fault tolerance
SFR3	Resistance to physical attacks
SFR4	Subset access control
SFR5	Security attribute based access control
SFR6	Static attribute initialization
SFR7	Management of security attributes
SFR8	Specification of management functions
SFR9	Audit Storage
SFR10	Limited capabilities
SFR11	Limited availabilities
SFR12	Subset information flow control
SFR13	Basic internal transfer protection
SFR14	Basic internal TSF data transfer protection
SFR15	Random number generation
SFR16	Cryptographic operation

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [9], chapter 7.1.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [9], chapter 3.1 to 3.4.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification

Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

S3CS9AB 32-Bit RISC Microcontroller for Smart Cards, Revision 0 with specific IC Dedicated Software

The following table outlines the TOE deliverables:

No	Type	Identifier	Version	Form of delivery
1	HW	S3CS9AB 32-Bit RISC Microcontroller for Smart Card	0	Wafer or Module
2	SW	DTRNG	1.0	Object file in electronic form
3	SW	Test ROM Code	1.0	Included in S3CS9AB Test ROM
4	DOC	S3CS9AB Chip Delivery Specification [15]	1.3	Softcopy
5	DOC	S3CS9AB 32-Bit CMOS Microcontroller for Smart Card User's Manual [12]	1.0	Softcopy
6	DOC	Security Application Note S3CS9AB [13]	1.9	Softcopy
7	DOC	S3CS9AB HW DTRNG and DTRNG Library Application Note [14]	1.3	Softcopy
8	DOC	SC100 Reference Manual [11]	0.0	Softcopy

Table 2: Deliverables of the TOE

The TOE is identified by S3CS9AB Revision 0. Another characteristic of the TOE is the product code. This information is stored in the EEPROM and can be read out by the user of the card via the normal EEPROM read command. For the format of the product code see [15] chapter 4.

There are three different delivering procedures have to be taken into consideration:

- Delivery of the IC dedicated software components (IC dedicated SW, guidance) from the TOE manufacturer to the IC Embedded Software Developer.
- Delivery of the IC Embedded Software (SW object file, ROM data) from the IC Embedded Software Developer to the TOE Manufacturer.
- Delivery of the TOE (wafer or module) from the TOE Manufacturer to the Composite Product Manufacturer.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

The Security Policy of the TOE is to provide basic security functionalities to be used by the smart card operating system and the smart card application thus providing an overall smart card system security. Therefore, the TOE will implement a symmetric cryptographic block cipher algorithm to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols and it will provide a True Random Number Generator (DTRNG).

The TOE includes countermeasures against SPA, DPA and DFA attacks.

As the TOE is a hardware security platform, the security policy of the TOE is also to provide protection against leakage of information (e.g. to ensure the confidentiality of cryptographic keys during Triple-DES and AES cryptographic functions performed by the TOE), against physical probing, against malfunctions, against physical manipulations and against abuse of functionality. Hence the TOE shall

- maintain the integrity and the confidentiality of data stored in the memory of the TOE and
- maintain the integrity, the correct operation and the confidentiality of security functionalities (security mechanisms and associated functions) provided by the TOE.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance: OE.Plat-Appl, OE.Resp-Appl and OE.Process-Sec-IC. Details can be found in the Security Target [6] and [9], chapter 4.2.

5. Architectural Information

The S3CS9AB 32-Bit RISC Microcontroller for Smart Cards, Revision 0 with specific IC Dedicated Software provides a platform to a smart card operating system and smart card application software. A top level block diagram and a list of subsystems can be found within the TOE description of the Security Target Lite [9], chapter 1.2.2. The complete hardware description and the complete instruction set of the TOE is to be found in guidance documents delivered to the customer, see table 2.

The TOE consists of the 19 subsystems (17 hardware / 2 software). For the implementation of the TOE security functionalities basically the components processing unit (CPU) with ROM, RAM, I/O, EEPROM, BUS, Power Control, Timers, ESE_IF, Detectors and Security Control, True Random Number Generator (DTRNG), DES, AES, CRC, ACC, Reset, Clock, Testrom_code and the DTRNG Library are used. Security measures for physical protection are realised within the layout of the whole circuitry. The Special Function Registers, the CPU instructions and the various on-chip memories provide the interface to the software using the security functionalities of the TOE. For more details refer to [9], chapter 1.2.3.

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

The developer tests cover all security functionalities and all security mechanisms as identified in the functional specification.

The evaluators were able to repeat the tests of the developer by using the library of programs, tools and prepared chip samples delivered to the evaluator or at the developer's site. They performed independent tests to supplement, augment and to verify the tests performed by the developer. For the developer tests, repeated by the evaluator, other test parameters were used and the test equipment was varied. Security features of the TOE realised by specific design and layout measures were checked by the evaluators during layout inspections both in design data and on the final product.

The evaluation has shown that the actual version of the TOE provides the security functionalities as specified by the developer. The test results confirm the correct implementation of the TOE security functionalities.

For penetration testing the evaluators took all security functionalities into consideration. Intensive penetration testing was planned based on the analysis results and performed for the underlying mechanisms of security functionalities. The penetration tests considered both the physical tampering of the TOE and attacks which do not modify the TOE physically. The penetration tests results confirm that the TOE is resistant to attackers with high attack potential in the intended environment for the TOE.

8. Evaluated Configuration

In the broadest sense, the production of the mask sets for the chip production may be looked upon as the procedure for the system generation. The TOE is delivered in the following configuration:

- Smartcard IC S3CS9AB Revision 0.

No further generation takes place after delivery to the customer. After delivery the TOE only features one fixed configuration (NORMAL mode), which cannot be altered by the user. The TOE was tested in this configuration. All the evaluation and certification results therefore are only effective for this mode of operation of the TOE.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [8] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

(i) The Application of CC to Integrated Circuits

(ii) Application of Attack Potential to Smartcards

(iii) Guidance, Smartcard Evaluation

(see [4], AIS 25, AIS 37).

For RNG assessment the scheme interpretations AIS 31 was used (see [4]).

To support composite evaluations according to AIS 36 the document ETR for composite evaluation [10] was provided and approved. This document provides details of this platform evaluation that have to be considered in the course of a composite evaluation on top.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 5 package including the class ASE as defined in the CC (see also part C of this report)
- The components AVA_VAN.5 and ALC_DVS.2 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0882-2013, re-use of specific evaluation tasks was possible. The TOE hardware and software is identical to the once in BSI-DSZ-CC-0882-2013. The user guidance documents and the TOE life cycle were updated.

The evaluation has confirmed:

- PP Conformance: Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007 [7]
- for the Functionality: PP conformant plus product specific extensions
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 extended
  EAL 5 augmented by AVA_VAN.5 and ALC_DVS.2

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But Cryptographic Functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context).

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1.	Confidentiality	Encryption and decryption with 2-key Triple DES in ECB Mode	[SP800-67], [SP800-38A]	112	No	-
2.		Encryption and decryption with 3-key Triple DES in ECB Mode	[SP800-67], [SP800-38A]	168	No	-
3.		Encryption and decryption with AES in ECB Mode	[FIPS-197], [SP800-38A]	128	No	-
4.		Encryption and decryption with AES in CBC and OFB Mode	[FIPS-197], [SP800-38A]	128	Yes	-
5.	Cryptographic Primitives	Physical RNG PTG.2	Conformant to [AIS31]	N/A	Yes	Supports cryptographic implementations

Table 3: TOE cryptographic functionality

Reference of Legislatives and Standards quoted above:

[SP800-67] NIST Special Publication 800-67 – Revision 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, November 2017, National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce.

[SP800-38A] NIST SP800-38A, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, 2001, National Institute of Standards and Technology (NIST).

[FIPS-197] Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), November 2001, U.S. department of Commerce / National Institute of Standards and Technology (NIST).

[AIS31] Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 2013-05-15, Bundesamt für Sicherheit in der Informationstechnik.

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

Some security measures are partly implemented in this certified TOE, but require additional configuration or control or measures to be implemented by a product layer on top, e.g. the IC Dedicated Support Software and/or Embedded Software] using the TOE. For this reason the TOE includes guidance documentation (see table 2) which contains obligations and guidelines for the developer of the product layer on top on how to securely use this certified TOE and which measures have to be implemented in order to fulfil the security requirements of the Security Target of the TOE. In the course of the evaluation of the composite product or system it must be examined if the required measures have been correctly and effectively implemented by the product layer on top. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the document "ETR for composite evaluation" [10].

At the point in time when evaluation and certification results are reused there might be an update of the document "ETR for composite evaluation" available. Therefore, the certified products list on the BSI website has to be checked for latest information on reassessments, recertifications or maintenance result available for the product.

11. Security Target

For the purpose of publishing, the Security Target [9] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. 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
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level

ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

13.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

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.

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.

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.

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 - 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.

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017

Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, 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[7] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target of S3CS9AB 32-Bit RISC Microcontroller for Smart Cards with specific IC Dedicated Software, BSI-DSZ-CC-0882-V2-2019, Version 2.2, 14-10-2019, Samsung Electronics (confidential document)

[7] Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007

[8] Evaluation Technical Report Summary (ETR Summary), BSI-DSZ-CC-0882-V2, S3CS9AB Revision 0, Version 3, 02-12-2019, TÜViT (confidential document)

[9] Security Target Lite of S3CS9AB 32-Bit RISC Microcontroller for Smart Cards with specific IC Dedicated Software, BSI-DSZ-CC-0882-V2-2019, Version 2.1, 15-10-2019, Samsung Electronics (sanitised public document)

[10] ETR for composite evaluation according to AIS 36 for the Product S3CS9AB Revision 0, Version 3, 02-12-2019, TÜViT (confidential document)

[11] SC100 Reference Manual, Version 0.0, 15-07-2013, Samsung Electronics

[12] S3CS9AB 32-Bit CMOS Microcontroller for Smart Card User's Manual, Version 1.0, April 2013, Samsung Electronics

[13] Security Application Note S3CS9AB, Version 1.9, 14-10-2019, Samsung Electronics

[7] specifically

- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2, Reuse of evaluation results
- AIS 47, Version 1.1, Regelungen zu Site Certification

[14] S3CS9AB HW DTRNG and DTRNG Library Application Note, Version 1.3, 30-05-2019, Samsung Electronics

[15] S3CS9AB Chip Delivery Specification, Version 1.2, July 2013, Samsung Electronics

[16] SITE TECHNICAL AUDIT REPORT (STAR), PKL Co., Ltd., Cheonan, Version 4, 02-12-2019, TÜViT (confidential document)

[17] SITE TECHNICAL AUDIT REPORT (STAR), Toppan Photomasks Korea Ltd., Korea Icheon, Version 1, 19-10-2019, TÜViT (confidential document)

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailled definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3, Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment

Annex B of Certification Report BSI-DSZ-CC-0882-V2-2019

Evaluation results regarding development and production environment

The IT product S3CS9AB 32-Bit RISC Microcontroller for Smart Cards, Revision 0 with specific IC Dedicated Software (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 11 December 2019, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1 and ALC_TAT.2)

are fulfilled for the development and production sites of the TOE listed below:

Site	Address	Function
Samsung Giheung / Hwaseong (DSR Building)	Samsung Electronics. Co., Ltd. (Giheung) 1, Samsung-ro, Giheung-gu, Yongin-si, Gyeonggi-do, 17113 Korea, Samsung Electronics. Co., Ltd.(Hwaseong) 1, Samsung-jeonja-ro, Hwaseong-si, Gyeonggi-do, 18448 Korea	Development (IC and Test Programs).
Samsung Electronics Giheung & Hwaseong Factory (FAB 1, FAB 2, FAB 6, FAB S1)	Samsung Electronics. Co., Ltd. (Giheung) 1, Samsung-ro, Giheung-gu, Yongin-si, Gyeonggi-do, 17113 Korea, Samsung Electronics. Co., Ltd.(Hwaseong) 1, Samsung-jeonja-ro, Hwaseong-si, Gyeonggi-do, 18448 Korea	Giheung: Wafer Fabrication, Inking, DC test, Inspection, Grinding, Scrap, Stock. Hwaseong: Receipt of GDS file provided by clients (i.e. IC manufacturers), GDS file checking and optimisation for mask data generation, Mask Data Preparation, Data Center / IT (Server room).
Samsung Onyang	Samsung Electronics. Co., Ltd. 158, Baebang-ro, Baebang-eup, Asan-si, Chungcheongnam-do, 31489 Korea	Warehouse / Delivery, Grinding, Sawing, Assembly, Module testing.
PKL Cheonan	PKL Co., Ltd. 493-3 Sungsung-Dong, Cheonan-City, Choongcheongnam-Do, 330-300, Korea	Mask house.
Toppan Icheon	Toppan Photomasks Korea Ltd. 91, Wonjeok-ro 290 beon-gil, Sindun-myeon Icheon-Si, Gyeonggi-do 467-842 Korea	Mask house.

Site	Address	Function
HANA Micron Asan	HANA Micron Inc. 77 Yeonamyulgeum-ro, Umbong-Myeon, Asan-Si, Chung-Nam, 336-864 Korea	Grinding, Sawing, Assembly, Module testing.
Inesa Shanghai	Inesa Co., Ltd. No. 818 Jin Yu Road, Jin Qiao Export Processing Zone Pudong, Shanghai, China	Grinding, Sawing, Assembly, Warehouse / Delivery.
Tesna Pyeungtaek	TESNA Co., Ltd. No. 450-2 Mogok-Dong, Pyeungtaek-City, Gyeonggi, Korea	Wafer testing, Initialization, Pre-personalization.
ASE Korea	ASE Korea Inc. Sanupdanjigil 76, Paju, Korea	Grinding, Sawing, Packaging.
SFA Semicon	SFA Semicon Co. Ltd. Bumping Factory, 30, 2gongdan 7-gil, Seobuk-gu, Cheonan-si, Chungcheongnam-do, Korea 31075	Wafer Bumping.

Table 4: Relevant development/production sites for the TOE

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and [9]) are fulfilled by the procedures of these sites.

Note: End of report