Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0910-2016

for

S3FV5RP, S3FV5RK, S3FV5RJ, S3FV5RH 32-Bit RISC Microcontroller for Smart Cards, Revision 0 with optional Secure ECC Library (Version 1.01) including specific IC Dedicated Software

from

Samsung Electronics

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0910-2016 (*)

Smart Card Controller

S3FV5RP, S3FV5RK, S3FV5RJ, S3FV5RH 32-Bit RISC Microcontroller for Smart Cards, Revision 0 with optional Secure ECC Library (Version 1.01) including 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 ALC_DVS.2 and AVA_VAN.5

SOGIS
Recognition Agreement

Common Criteria

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 EAL5 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 4

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.

Common Criteria
Recognition Arrangement
for components up to
EAL 4

Bonn, 30 November 2016

For the Federal Office for Information Security

Thomas Gast   L.S.
Head of Division

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

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] 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.

---

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

Contents

A.   Certification

1.   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[2]

● BSI Certification and Approval Ordinance[3]

● BSI Schedule of Costs[4]

● 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[5] [1] also published as ISO/IEC 15408.

● 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]

2.   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.

2.1.   European Recognition of ITSEC/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 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). 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 new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. 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.sogisportal.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

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

2.2.   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 CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://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 nations listed above.

As the product certified has been accepted into the certification process before 08 September 2014, this certificate is recognized according to the rules of CCRA-2000, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained the components ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, ATE_DPT.3, AVA_VAN.5 that are not mutually recognised in accordance with the provisions of the CCRA-2000, for mutual recognition the EAL 4 components of these assurance families are relevant.

## 3.	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 S3FV5RP, S3FV5RK, S3FV5RJ, S3FV5RH 32-Bit RISC Microcontroller for Smart Cards, Revision 0 with optional Secure ECC Library (Version 1.01) including specific IC Dedicated Software has undergone the certification procedure at BSI.

The evaluation of the product S3FV5RP, S3FV5RK, S3FV5RJ, S3FV5RH 32-Bit RISC Microcontroller for Smart Cards, Revision 0 with optional Secure ECC Library (Version 1.01) including specific IC Dedicated Software was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 21 November 2016. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] 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.

## 4.	Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only 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 levels please refer to the excerpts from the criteria at the end of the Certification Report or in the CC itself.

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-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 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 30 November 2016 is valid until 29 November 2021. 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

---

6	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.

5.   Publication

The product S3FV5RP, S3FV5RK, S3FV5RJ, S3FV5RH 32-Bit RISC Microcontroller for Smart Cards, Revision 0 with optional Secure ECC Library (Version 1.01) including 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[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

---

[7]   Samsung Electronics
       B zone,17 Floor, B Tower, 1-1, Samsungjeonja-ro
       Hwaseong-si, Gyeonggi-do, 45-330
       South Korea

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 S3FV5RP, S3FV5RK, S3FV5RJ and S3FV5RH 32-Bit RISC Microcontroller for Smart Cards, Revision 0 with optional Secure ECC Library (Version 1.01) including specific IC Dedicated Software, is a smartcard integrated circuit which is composed of a processing unit, security components, contact based I/O ports, 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 optional ECC public key cryptographic library, and an PTG.2-compliant random number generator. The ECC library further includes the functionality of hash computation. The use for keyed hash operations like HMAC or similar security critical operations involving keys and other secrets, is not subject of this TOE and requires specific security improvements and DPA analysis including the operating system, which is not part of this TOE. However, this functionality is intended to be used for signature generation and verification only.

All other software is called Smartcard Embedded Software and is not part of the TOE.

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 [8].

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 ALC_DVS.2 and AVA_VAN.5.

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
TSF1	Environmental Security violation recording and reaction
TSF2	Access Control
TSF3	Non-reversibility of TEST and NORMAL modes
TSF4	Hardware countermeasures for unobservability
TSF5	Cryptography
TSF6	Loader

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 3.2 – 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:

S3FV5RP, S3FV5RK, S3FV5RJ, S3FV5RH 32-Bit RISC Microcontroller for Smart Cards, Revision 0 with optional Secure ECC Library (Version 1.01) including specific IC Dedicated Software

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	S3FV5RP, S3FV5RK, S3FV5RJ and S3FV5RH 32-Bit RISC Microcontroller for Smart Card	Rev. 0	Wafer or Module (send by trusted forwarder)
2	SW	Secure Boot loader code (V5RP_Bootloader_V0.2_20131213_release.zip)	0.2	Stored in User ROM on the IC
3	SW	Secure ECC Library (object code) (optional)	1.01	Encrypted email
4	SW	DTRNG Software Library	1.0	Encrypted email
5	DOC	Tornado-E ECC Library API Manual (PKA_Lib_AE0_APIManual_v0.21.pdf) [11]	0.21	Encrypted email
6	DOC	HW DTRNG and DTRNG library application note (S3FV5RP_DTRNG_AN_v1.3.pdf) [12]	1.3	Encrypted email
7	DOC	Hardware User's manual (S3FV5RP_UM_REV1.00.pdf) [15]	1.0	Encrypted email
8	DOC	Security Application Note (SAN_S3FV5RP_v0.6.pdf) [13]	0.6	Encrypted email
9	DOC	Chip Delivery Specification (DeliverySpec_S3FV5RP_Rev_11.pdf) [14]	1.1	Encrypted email

No	Type	Identifier	Release	Form of Delivery
10	DOC	Boot Loader Specification (TN091_S3FV5RP_for_Bootloader_Specification_v0.91.pdf) [16]	0.91	Encrypted email
11	DOC	SC300_Reference_Manual (SC300_Reference_Manual v0.0.pdf) [17]	0.0	Encrypted email

Table 2: Deliverables of the TOE

The S3FV5RP / S3FV5RK / S3FV5RJ / S3FV5RH Revision 0 devices contain a 256 byte special area (FLASH Security Area) mapped at address 0x400000h of the device that contains specific information on the device. It includes the Device Type, the product line indicator, the Test ROM Code version and the Secure boot loader Code version. DTRNG Software library and ECC library version are identified by the value in the library.

In [15] it is described how the customer can retrieve this information. Each individual TOE can therefore be traced unambiguously and thus assigned to the entire development and production process.

The TOE is delivered in form of wafers or sawn wafers (after phase 3) or in form of module (after phase 4). Details can be found in [15].

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:

● maintain the integrity of User Data and of the Security IC Embedded Software (when being executed/processed and when being stored in the TOE's memories) as well as

● maintain the confidentiality of User Data and of the Security IC Embedded Software (when being processed and when being stored in the TOE's memories).

> The Security IC may not distinguish between User Data which are public known or kept confidential. Therefore the security IC shall protect the confidentiality and integrity of the User Data, unless the Security IC Embedded Software chooses to disclose or modify it.

> In particular integrity of the Security IC Embedded Software means that it is correctly being executed which includes the correct operation of the TOE's functionality. Though the Security IC Embedded Software (normally stored in the ROM) will in many cases not contain secret data or algorithms, it must be protected from being disclosed, since for instance knowledge of specific implementation details may assist an attacker.

● maintain the correct operation of the security services provided by the TOE for the Security IC Embedded Software.

● provide random numbers.

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, OE.Process-Sec-IC and OE.Lim_Block_Loader. Details can be found in the Security Target [6] and [9], chapter 4.2.

5.   Architectural Information

The TOE consists of the hardware of the smart card security controller S3FV5RP / S3FV5RK / S3FV5RJ / S3FV5RH and the software consisting of a modular arithmetic library for support of ECC (optional) and a True Random Number Generator (DTRNG) library for AIS31-compliant Random Number Generation. The ECC library also includes the functionality of hash computation.

The hardware of the TOE consists of the following parts:

- S3FV5RP(1536Kbytes), S3FV5RK(1024Kbytes), S3FV5RJ(768Kbytes), and S3FV5RH(512Kbytes) FLASH/ 48K bytes RAM/ 5K bytes Crypto. RAM / 32K bytes ROM,
- 32-bit Central Processing Unit (CPU),
- Internal Voltage Regulator (IVR),
- Detectors & Security Logic,
- Digital True random number generator (DTRNG),
- Memory Protection Unit (MPU),
- Triple DES cryptographic coprocessor with 112 or 168 bits key size,
- AES cryptographic coprocessor with 128 bits, 192bits and 256bits key size,
- TORNADO-E supporting modular multiplications for the operand size up to 4128-bit and modular additions/subtractions for the operand size up to 544-bit,
- SHA-1 cryptography coprocessor.
- SHA-2 cryptography coprocessor,
- HMAC Hash message authentication code with SHA-1,SHA-2,
- Hardware UART ,GPIO,I2C,SPI,SWP,
- Internal Clock,
- Timers,
- Power on Reset,
- PARITY/ CRC-32 calculators,

as shown in [6] and [9] figure 1.

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

Developer's Test according to ATE_FUN

● All TSF and related sub-functions, subsystems and modules are tested in order to assure complete coverage of all SFR.

● Different classes of tests are performed to test the TOE in a sufficient manner:

• Simulation tests: Objective of the testing is the proof of the correctness of the logic with the help of simulation before starting the production.

• Production tests: These tests are performed for every single TOE. The aim of these tests is to check whether each chip is functioning correctly.

• Characterization tests: With these tests the influence of temperature, frequency, and voltage on the security functions are tested in detail.

• Application tests: With the application test the TOE is tested in NORMAL mode from customer's point of view.

• Qualification tests: With these tests the product reliability is assured.

• Penetration tests: Penetration tests are performed to find security flaws in the product.

Independent Testing according to ATE_IND

The evaluator's objective regarding this aspect was to test the functionality of the TOE and to verify the developer's test results by repeating developer's tests and additionally add independent tests.

In the course of the evaluation of the TOE the following classes of tests were carried out:

● Module / Wafer tests,

● Functional tests,

● Simulation tests,

● Hardware tests.

The tests are performed with the chip S3FV5RP / S3FV5RK / S3FV5RJ / S3FV5RH Revision 0. For the tests different chip types are prepared. One of these types is the configuration which is finally delivered to the user. The others contain special download functionality for test programs or have some security mechanisms deactivated. The entire functionality is the same for all chips.

Penetration Testing according to AVA_VAN

● The penetration testing was partially performed using the developer's testing environment, partially using the test environment of the evaluation body.

- All configurations of the TOE being intended to be covered by the current evaluation were tested.

- The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential high was actually successful.

- Systematic search for potential vulnerabilities and known attacks in public domain sources, use of a list of vulnerabilities ([AIS26_JIL-ATT-SC]), and from a methodical analysis of the evaluation documents.

- Analysis why these vulnerabilities are unexploitable in the intended environment of the TOE.

- If the rationale is suspect in the opinion of the evaluator penetration tests are devised.

- Even if the rational is convincing in the opinion of the evaluator penetration tests are devised for some vulnerabilities, especially to support the argument of non practicability of exploiting time in case of SPA, DPA and FI attacks.

8.   Evaluated Configuration

This certification covers the following configurations of the TOE: S3FV5RP / S3FV5RK / S3FV5RJ / S3FV5RH in Revision 0 as described in [6], [9] and [15].

The only difference between S3FV5RP, S3FV5RK, S3FV5RJ and S3FV5RH is at the FLASH memory size in a relation with customer meaning, say, S3FV5RP(1536Kbytes), S3FV5RK(1024Kbytes), S3FV5RJ(768Kbytes) and S3FV5RH(512Kbytes), which means that all 4 microcontrollers have the same layout.

9.   Results of the Evaluation

9.1. CC specific results

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 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 EAL 5 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:

- The Application of CC to Integrated Circuits,

- The Application of Attack Potential to Smartcards,

- Functionality classes and evaluation methodology of physical random number generators,

- Terminology and preparation of Smartcard evaluations,

(see [4] AIS 25, AIS 26, AIS 31, as well as 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.

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

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 ALC_DVS.2 and AVA_VAN.5 augmented for this TOE evaluation.

The evaluation has confirmed:

● PP Conformance: Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007 [8]

● for the Functionality: PP conformant plus product specific extensions
Common Criteria Part 2 extended

● for the Assurance: Common Criteria Part 3 conformant
EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5

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).

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
Key Generation	EC key generation	[ANS X9.62]	Key sizes corresponding to the used elliptic curves P-192 [FIPS186-4], brainpoolP{192}r1, brainpoolP{192}t1 [Brainpool], and secp {192}k1, secp{192}r1 [SEC_2]	No

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
	EC key generation	[ANS X9.62]	Key sizes corresponding to the used elliptic curves P-224, P-256, P-384 and P521 [FIPS186-4], brainpoolP{224, 256, 320, 384, and 512}r1, brainpoolP{224, 256, 320, 384, 512}t1 [Brainpool], and secp{224, 256}k1, secp{224, 256, 384, 521}r1 [SEC_2]	Yes
Cryptographic Primitive	TDES in ECB mode	[NIST SP800-67], [NIST SP800-38A]	|k| = 112, 168	No
	AES in ECB mode	[FIPS197], [NIST SP800-38A]	|k| = 128, 192, 256	No
	AES in CRT mode	[FIPS197], [NIST SP800-38A]	|k| = 128, 192, 256	Yes
	SHA224	[FIPS180-3]	None	--
	SHA256	[FIPS180-3]	None	--
	SHA384	[FIPS180-3]	None	--
	SHA512	[FIPS 180-3]	None	--
	SHA1	[FIPS 180-3]	None	--
Signature generation / verification	ECDSA signature generation / verification	[ANS X9.62]	Key sizes corresponding to the used elliptic curves P-192 [FIPS186-4], brainpoolP{192}r1, brainpoolP{192}t1 [Brainpool], and secp { 192}k1, secp{192}r1 [SEC_2]	No
	ECDSA signature generation / verification	[ANS X9.62]	Key sizes corresponding to the used elliptic curves P-224, P-256, P-384 and P521 [FIPS186-4], brainpoolP{224, 256, 320, 384, 512}r1, brainpoolP{224, 256, 320, 384, 512}t1 [Brainpool], and secp { 224, 256}k1, secp{224, 256, 384, 521}r1 [SEC_2]	Yes
Key Agreement	ECDH	[ANS X9.63]	Key sizes corresponding to the used elliptic curves P-192 [FIPS186-4], brainpoolP{192}r1, brainpoolP{192}t1 [RFC5639], and secp { 192}k1, secp{192}r1 [SEC_2]	No

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
	ECDH	[ANS X9.63]	Key sizes corresponding to the used elliptic curves P-224, P-256, P-384 and P521 [FIPS186-4], brainpoolP{224, 256, 320, 384, 512}r1, brainpoolP{224, 256, 320, 384, 512}t1 [Brainpool], and secp{ 224, 256}k1, secp{224, 256, 384, 521}r1 [SEC_2]	Yes
Random Number Generation	Physical True Random Number Generator	AIS31 Class PTG.2 [AIS31]	None	--

Table 3: TOE cryptographic functionality

[ANS X9.62]   American National Standard for Financial Services ANS X9.62-2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), November 16, 2005, American National Standards Institute.

[ANS X9.63]   American National Standard for Financial Services X9.63-2001, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, November 20, 2001, American National Standards Institute.

[NIST SP800-67] NIST Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Revised January 2012, Revision 1, National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce.

[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.

[FIPS197]   Federal Information Processing Standards Publication 197, November 26, 2001, Announcing the ADVANCED ENCRYPTION STANDARD (AES), National Institute of Standards and Technology.

[NIST SP800-38A] *NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation*, 2001-12, National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce.

[FIPS180-3]   *Federal Information Processing Standards Publication FIPS PUB 180-3, Secure Hash Standard (SHS), October* 2008, Information Technology Laboratory National Institute of Standards and Technology (NIST).

[Brainpool]   ECC Brainpool Standard Curves and Curve Generation, M. Lochter, Version 1.0, 2005 (available online at http://www.ecc-brainpool.org/ecc-standard.htm).

[FIPS 186-4]   Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013, U.S. department of Commerce / National Institute of Standards and Technology (NIST).

[SEC_2]   Standards For Efficient Cryptography – SEC 2: Recommended Elliptic Curve Domain Parameters, Standards for Efficient Cryptography Group (SECG), September 2000.

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.

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 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].

The TOE is delivered to the Composite Product Manufacturer and to the Security IC Embedded Software Developer. The actual end-consumer obtains the TOE from the Composite Product Issuer together with the application which runs on the TOE.

The Security IC Embedded Software Developer receives all necessary recommendations and hints to develop his software in form of the delivered documentation.

● All security hints described in [15] and the delivered documents [11], [12], [13], [16] and [17] have to be considered.

The Composite Product Manufacturer receives all necessary recommendations and hints to develop his software in form of the delivered documentation.

● All security hints described in [14] have to be considered.

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. Definitions

12.1. 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

12.2. 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.

13. Bibliography

[1]   Common Criteria for Information Technology Security Evaluation, Version 3.1,
        Part 1: Introduction and general model, Revision 4, September 2012
        Part 2: Security functional components, Revision 4, September 2012
        Part 3: Security assurance components, Revision 4, September 2012
        http://www.commoncriteriaportal.org

[2]   Common Methodology for Information Technology Security Evaluation (CEM),
        Evaluation Methodology, Version 3.1, Rev. 4, September 2012,
        http://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[8]
        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 BSI-DSZ-CC-0910-2016, Project Kiowa Security Target of Samsung
        S3FV5RP / S3FV5RK / S3FV5RJ / S3FV5RH 32-bit RISC Microcontroller for Smart
        Card with optional Secure ECC Library including specific IC Dedicated Software,
        Version 3.2, 2016-10-07, Samsung Electronics (confidential document)

[7]   Evaluation Technical Report, Version 6, 2016-11-21, Evaluation Ttechnical Report
        Summary (ETR SUMMARY), TÜV Informationstechnik GmbH, (confidential
        document)

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

[9]   Security Target BSI-DSZ-CC-0910-2016 Lite, Project Kiowa Security Target of
        Samsung S3FV5RP / S3FV5RK / S3FV5RJ / S3FV5RH 32-bit RISC Microcontroller
        for Smart Card with optional Secure ECC Library including specific IC Dedicated
        Software, Version 1.8, 2016-10-07, Samsung Electronics (sanitised public
        document)

---

[8]specifically

- AIS 25, Version 8, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document

- AIS 26, Version 9, 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 4, Kompositionsevaluierung including JIL Document and CC Supporting Document

[10]   Evaluation Technical for Composite Evaluation (ETR COMP) for the S3FV5RP / S3FV5RK / S3FV5RJ / S3FV5RH Revision 0, version 6, 2016-11-21, TÜV Informationstechnik GmbH. (confidential document)

[11]   *Tornado-E ECC Library API Manual*, Version 0.21, 2015-10-13, Samsung Electronics

[12]   *HW DTRNG and DTRNG Library Application Note*, Version 1.3, 2014-08-21, Samsung Electronics

[13]   *Security Application Note*, Version 0.6, 2016-10-06, Samsung Electronics

[14]   *Chip Delivery Specification*, Version 1.1, 2015-12, Samsung Electronics

[15]   *Hardware User's manual*, Version 1.0, 2014-06, Samsung Electronics

[16]   *Boot Loader Specification*, Version 0.91, 2014-07, Samsung Electronics

[17]   *SC300 Reference Manual*, Version 0.0, 2014-05-12, Samsung Electronics

This page is intentionally left blank.

C.   Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

"The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
    – **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
    – **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
    – **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
    – **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
    – the SFRs of that PP or ST are identical to the SFRs in the package, or
    – the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
    – the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
    – the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D."

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

"Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition"

Class ASE: Security Target evaluation (chapter 11)

"Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation."

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

"The following Sections describe the constructs used in representing the assurance classes, families, and components."
"Each assurance class contains at least one assurance family."
"Each assurance family contains one or more assurance components."

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model

Assurance Class	Assurance Components
	ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

"The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility."

Evaluation assurance level (EAL) overview (chapter 8.1)

"Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one

component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of "augmentation" allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an "EAL minus a constituent assurance component" is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Evaluation assurance level 1 (EAL 1) - functionally tested (chapter 8.3)

"Objectives

EAL 1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL 1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL 1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL 1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation."

Evaluation assurance level 2 (EAL 2) - structurally tested (chapter 8.4)

"Objectives

EAL 2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL 2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited."

Evaluation assurance level 3 (EAL 3) - methodically tested and checked (chapter 8.5)

"Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering."

Evaluation assurance level 4 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL 4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs."

Evaluation assurance level 5 (EAL 5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL 5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques."

Evaluation assurance level 6 (EAL 6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL 6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL 6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs."

Evaluation assurance level 7 (EAL 7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL 7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary"

Class AVA: Vulnerability assessment (chapter 16)

"The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE."

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users."

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

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0910-2016

Evaluation results regarding development and production environment

The IT product S3FV5RP, S3FV5RK, S3FV5RJ, S3FV5RH 32-Bit RISC Microcontroller for Smart Cards, Revision 0 with optional Secure ECC Library (Version 1.01) including 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 30 November 2016, 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:

Name of site / Company name	Address	Type of site
Giheung Plant	Samsung Electronics. Co., Ltd. San24, Nongseo-dong, Giheung-gu, Yongin-City, Gyeonggido, 449- 711, Korea	Production (Mask House, Wafer Fab, Initialisation and Pre-personalisation)
Hwasung Plant	Samsung Electronics. Co., Ltd. San #16, Banwol-Ri, Hwasung-Eup, Gyeonggi-Do, 445-701, Korea	Development (Development, Server room, Mask data preparation)
Onyang Plant I	Samsung Electronics. Co., Ltd., San #74, Buksoo-Ri, Baebang-Myun, Asan-City, Chungcheongnam-Do, 449-711, Korea	Production (Warehouse/Delivery)
Onyang Plant II	Samsung Electronics. Co., Ltd., San #74, Buksoo-Ri, Baebang-Myun, Asan-City, Chungcheongnam-Do, 449-711, Korea	Production (Grinding, Sawing, COB assembly, Module Testing)

Name of site / Company name	Address	Type of site
Cheonan Plant (PKL)	PKL Co., Ltd. Plant, 493-3 Sungsung-Dong, Cheonan-City, Choongcheongnam-Do, 330-300, Korea	Production (Mask House)
Asan Plant (Hanamicron)	HANAMICRON Co., Ltd., #95-1, Wonnam-Li, Umbong-Myeon, Asan-City, Choongcheongnam-Do, 449-711, Korea	Production (Grinding, Sawing, Module testing)
Shanghai Plant I (Inesa)	Inesa Co., Ltd., No. 818 Jin Yu Road, Jin Qiao Export Processing Zone Pudong, Shanghai, China	Production (Grinding, Sawing, COB Assembly, Warehouse/Delivery)
Shanghai Plant II (Eternal)	ETERNAL Co., Ltd., No.1755, Hong Mei South Road, Shanghai, China (Shanghai Plant II / ETERNAL)	Production (Sawing, COB Assembly, Warehouse/Delivery)
Pyeungtaek Plant (Tesna)	TESNA Co., Ltd., No. 450-2 Mogok-Dong, Pyeungtaek-City, Gyeonggi, Korea	Production (Wafer Testing)
Paju Plant (ASE)	ASE Korea Co., Ltd., Sanupdanjigil 76, Paju, Korea	Production (Grinding, Sawing, SIP Assembly)

Table 4: Relevant development/production sites

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.