Certification Report

BSI-DSZ-CC-0782-V3-2017

for

Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013, and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware)

from

Infineon Technologies AG

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0782-V3-2017 (*)

Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013, and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware)

from	Infineon Technologies AG
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 conformant extended
Assurance:	Common Criteria Part 3 conformant EAL 6 augmented by ALC_FLR.1

SOGIS
Recognition Agreement

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 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.

Bonn, 5 September 2017

For the Federal Office for Information Security

Common Criteria
Recognition Arrangement
for components up to
EAL 4

Bernd Kowalski   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.

---

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

3   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

4   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

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

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 this certificate is a re-certification of a certificate issued according to CCRA-2000 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_IMP.2, ADV_INT.3, ADV_SPM.1, ADV_TDS.5, ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_TAT.3, ATE_COV.3, ATE_DPT.3, ATE_FUN.2 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 Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013, and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware) has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0782-V2-2015. Specific results from the evaluation process BSI-DSZ-CC-0782-V2-2015 were re-used.

The evaluation of the product Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013, and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware) was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 30 August 2017. 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: Infineon Technologies AG.

The product was developed by: Infineon Technologies AG.

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 5 September 2017 is valid until 4 September 2022. Validity can be re-newed by re-certification.

---

[6]   Information Technology Security Evaluation Facility

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 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 Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013, and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware) 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]   Infineon Technologies AG
       Am Campeon 1-12
       85579 Neubiberg

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) is the Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013, and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware). The TOE provides a real 16-bit CPU-architecture and is compatible to the Intel 80251 architecture. The major components of the core system are the dual CPU (Central Processing Units), the MMU (Memory Management Unit) and MED (Memory Encryption/Decryption Unit). The dual interface controller is able to communicate using either the contact based or the contactless interface.

The TOE consists of a hardware, a firmware and a software part. The software part can be separated into the cryptographic libraries SCL, RSA, EC and SHA-2, as well as the supporting libraries Toolbox and Base. The SCL, RSA, EC, SHA-2 and Toolbox libraries provide the smartcard embedded software with specific functionalities.

This 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 term Smartcard Embedded Software is used in the following for all operating systems and applications stored and executed on the TOE. The TOE is the platform for the Smartcard Embedded Software.

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 6 augmented by ALC_FLR.1.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 7. 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
SF_DPM	Device Phase Management
SF_PS	Protection against Snooping
SF_PMA	Protection against Modification Attacks
SF_PLA	Protection against Logical Attacks
SF_CS	Cryptographic Support

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [9], chapter 8 (TOE Summary Specification).

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 4.1.2. 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 4.3, 4.1 and 4.2, respectively.

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:

Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013, and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware).

The following table outlines the TOE deliverables:

Type	Identifier	Release	Form of Delivery / Note
HW	M7892 Smart Card IC	B11 (produced in Dresden)	Complete module, package, with or without inlay mounting, in form of plain wafers, in an IC case or in bare dies.
FW	Flash Loader	FW Identifier 78.015.14.0 or 78.015.14.1 or 78.015.14.2	Stored in reserved area of ROM on the IC (patch in NVM)
FW	STS Self Test Software (the IC Dedicated Test Software)	FW Identifier 78.015.14.0 or 78.015.14.1 or 78.015.14.2	Stored in Test ROM on the IC (patch in NVM)
FW	RMS Resource Management System (the IC Dedicated Support Software)	FW Identifier 78.015.14.0 or 78.015.14.1 or 78.015.14.2	Stored in reserved area of ROM on the IC (patch in NVM)
FW	SAM library	FW Identifier 78.015.14.0 or 78.015.14.1 or 78.015.14.2	Stored in reserved area of ROM on the IC (patch in NVM)
SW	NVM image (including Embedded Software and crypto libraries)	–	Stored in Flash memory on the IC

Type	Identifier	Release	Form of Delivery / Note
SW	RSA library (optional)	RSA2048 v1.02.013 RSA4096 v1.02.013	Object code in electronic form
SW	EC library (optional)	EC v1.02.013	Object code in electronic form
SW	SHA-2 library (optional)	SHA-2v1.01	Object code in electronic form
SW	Toolbox (optional)	Toolbox v1.02.013	Object code in electronic form
SW	Base library (optional)	v1.02.013	Object code in electronic form
SW	SCL (optional)	v2.02.012	Object code in electronic form
DOC	*AMM Advanced Mode for Mifare-Compatible Technology Addendum to M7892 Hardware Reference Manual*	2013-09-24	Hardcopy or pdf-file
DOC	*M7892 Controller Family for Security Applications Hardware Reference Manual*	2015-09-21	Hardcopy or pdf-file
DOC	*M7892 Errata Sheet*	2017-06-21	Hardcopy or pdf-file
DOC	*M7892 Security Guidelines*	2017-06-28	Hardcopy or pdf-file
DOC	*16-bit Controller Family SLE 70 Programmer's Reference Manual*	2017-07-04	Hardcopy and pdf-file
DOC	*SLE70 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox (1.02.013)*	2017-06-20	Hardcopy and pdf-file
DOC	*SCL78 Symmetric Crypto Library for SCPv3 DES / AES 16-bit Security Controller User Interface*	2017-05-02	Hardcopy and pdf-file
DOC	*Crypto@2304T User Manual*	2010-03-23	Hardcopy and pdf-file
DOC	*SLx70 Family Secure Hash Algorithm SHA-2 (SHA 256/224, SHA 512/384) Library Version V1.01*	2009-11	Hardcopy and pdf-file
DOC	*SLx 70 Family Production and Personalization User' Manual*	2015-04-01	Hardcopy and pdf-file

Table 2: Deliverables of the TOE

The individual TOE hardware is uniquely identified by its identification data. The identification data contains the lot number, the wafer number and the coordinates of the chip on the wafer. Each individual TOE can therefore be traced unambiguously and thus assigned to the entire development and production process.

The hardware part of the TOE is identified by M7892 B11. Another characteristic of the TOE are the chip identification data. These chip identification data is accessible via the Generic Chip Identification Mode (GCIM).

This GCIM outputs a variety of unique information in order to uniquely determine the underlying hardware configuration. Additionally, a dedicated RMS function (see [15] section 9.16) allows a customer to extract the present hardware configuration and the original Chip Identifier Byte, which was valid before blocking.

The firmware part of the TOE is also identified also via the GCIM for all of the firmware parts STS, RMS, SAM, FL, and Mifare.

The SCL (optional), RSA (optional), EC (optional), SHA-2 (optional), Toolbox (optional), and Base library (optional), as separate software parts of the TOE, are also identified by their unique version numbers. The user can identify these versions by calculating the hash signatures of the provided library files. The mapping of these hash signatures to the version numbers is provided in the Security Target [6] and [9] section 10.

Please also note, that as the TOE is under control of the user software, the TOE Manufacturer can only guarantee the integrity up to the delivery procedure. It is in the responsibility of the Composite Product Manufacturer to include mechanisms in the implemented software (developed by the IC Embedded Software Developer) which allows detection of modifications after the delivery.

3.   Security Policy

The security policy is expressed by the given 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 implements a symmetric cryptographic block cipher algorithm (Triple-DES and AES) 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 (TRNG).

The SCL uses the symmetric cryptographic co-processor (SCP) of the hardware to provide the user with a software interface to the TDES and AES calculations and adds countermeasures against leakage and fault attacks.

The RSA library is used to provide a high level interface to RSA (Rivest, Shamir, Adleman) cryptography implemented on the hardware component Crypto@2304T and includes countermeasures against SPA, DPA and DFA attacks. The EC library is used to provide a high level interface to Elliptic Curve cryptography implemented on the hardware component Crypto@2304T and includes countermeasures against SPA, DPA and DFA attacks. The SHA-2 library provides the calculation of a hash value of freely chosen data input in the CPU.

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 AES, Triple-DES, RSA and EC 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.

Specific details concerning the above mentioned security policies can be found in the Security Target [6] and [9], chapter 7.

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 and measures to be taken by the IT environment and the user or the risk manager. The following topics are of relevance:

The ST only includes two security objective for the IC Embedded Software Developer, the objectives OE.Plat-Appl and OE.Resp-Appl.

The objective OE.Plat-Appl states that the IC Embedded Software Developer shall design his software so that the requirements from the data sheet, the TOE application notes, other guidance documents and findings of the TOE evaluation report are implemented. As all these documents ([12] - [20]) are identified as parts of the TOE and delivered to the IC Embedded Software Developer, the objective OE.Plat-Appl is fulfilled.The objective OE.Resp-Appl states that the IC Embedded Software Developer shall treat user data (especially keys) appropriately. The IC Embedded Software Developer gets sufficient information on how to protect user data adequate in the security guidelines [M7892_Sec].

Details can be found in the Security Target [6] and [9], chapters 5.2.1 and 5.2.2.

5.   Architectural Information

The TOE is an integrated circuit (IC) providing a platform for an operating sytem and application software used in smartcards but also in any other device or form factor requiring a high level of resistance against attackers. A top level block diagram and a list of subsystems can be found within the TOE description of the Security Target [6], chapter 2.1.

The TOE provides a real 16-bit CPU-architecture and is compatible to the Intel 80251 architecture. The major components of the core system are the two CPUs (Central Processing Units), the MMU (Memory Management Unit) and MED (Memory Encryption/Decryption Unit). The two CPUs control each other in order to detect faults and serve by this for data integrity. The TOE implements a full 16 MByte linear addressable memory space for each privilege level, a simple scalable Memory Management concept and a scalable stack size. The flexible memory concept consists of ROM- and Flash-memory as part of the non volatile memory (NVM), respectively Infineon SOLID FLASH™. For the Infineon SOLID FLASH™ memory the Unified Channel Programming (UCP) memory technology is used. Note that there is no user available on-chip ROM module anymore. The user software and data are now located in a dedicated and protected part of the Infineon SOLID FLASH™.

The two cryptographic co-processors serve the need of modern cryptography: The symmetric co-processor (SCP) combines both AES and Triple-DES with dual-key or triple-key hardware acceleration. The Asymmetric Crypto Co-processor, called Crypto2304T in the following, is an optimized version of the Crypto@1408 used in the SLE88-family with performance improvements for RSA-2048 bit (4096-bit with CRT) and Elliptic Curve (EC) cryptography.

The software part of the TOE consists of the cryptographic RSA-, EC-, SCL- and the SHA-2 libraries and the supporting Toolbox and Base libraries. If RSA or EC or Toolbox or combinations hereof are part of the shipment, automatically the Base Library is included.

The Flash Loader is a firmware located in the ROM (Read-Only Memory; patch in NVM) and enables the download of the user software or parts of it to the Infineon SOLID FLASH™ memory. After completion of the download the Flash Loader shall be locked by the by the user.

For more details please refer to the Security Target [6] and [9], chapters 1.2 and 2.2.2.

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 tests performed by the developer were divided into five categories:

● Simulation tests (design verification),

● Qualification tests,

● Verification Tests,

● Security Evaluation Tests,

● Production Tests.

The developer tests cover all security functionalities and all security mechanisms as identified in the security architecture description.

The evaluators were able to repeat the tests of the developer either 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 evaluators 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

This certification covers the following configurations of the TOE:

● Security Controller M7892 B11 (produced in Dresden).

Depending on the blocking configuration a M7892 product can have a different user available configuration as described in Security Target [6] and [9], chapter 1.1 and 1.2.

The available options are summed up in the Security Target [6] and [9], section 1.2:

● The available memory sizes of the SOLID FLASH™ NVM and RAM. Note that there is no user available ROM on the TOE,

● The availability of the cryptographic coprocessors,

● The availability and free combinations of the cryptographic libraries,

● The availability of the Flash Loader for available interfaces like ISO-7816, contactless ISO-14443,

● The availability of various interface options,

● The possibility to tailor the product by blocking on his own premises,

● The degree of freedom of the chip configuration is predefined by Infineon Technologies AG and made available via the order tool.

All possible TOE configurations are covered by the certificate. Note that there is no user available on-chip ROM module any more. The user software and data are now located in a dedicated and protected part of the SOLID FLASH™. According to the BPU option, a non limited number of configurations of the TOE may occur in the field. The number of various configurations depends on the order and purchase contract only.

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

For RNG assessment the scheme interpretations AIS 31 was used (see [4], AIS 25, AIS 26, AIS 31).

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 6 package including the class ASE as defined in the CC (see also part C of this report)

- The components ALC_FLR.1 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-0782-V2-2015, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on a newly included symmetric crypto library (SCL) and adjustments regarding crypto security functionality.

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 conformant extended

- for the Assurance: Common Criteria Part 3 conformant
  EAL 6 augmented by ALC_FLR.1

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).

The Security Target [6] and [9] (table 17 therein) provides a table detailing the available cryptographic functionality.

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).

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 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].

In addition, the following aspects need to be fulfilled when using the TOE:

- All security hints described in the delivered documents [12] to [20] 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 [21] have to be considered.

In addition the following hint resulting from the evaluation of the ALC evaluation aspect has to be considered:

- The IC Embedded Software Developer can deliver his software either to Infineon to let them implement it in the TOE (in Flash memory) or to the Composite Product Manufacturer to let him download the software in the Flash memory.

- The delivery procedure from the IC Embedded Software Developer to the Composite Product Manufacturer is not part of this evaluation and a secure delivery is required.

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

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
APB™	Advanced Peripheral Bus
APDU	Application Protocol Data Unit
API	Application Programming Interface
AXI™	Advanced eXtensible Interface Bus Protocol
BPU	Bill Per Use
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BOS	Boot Software
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CPU	Central Processing Unit
CCRA	Common Criteria Recognition Arrangement
Crypto2304T	Asymmetric Cryptographic Processor
CRC	Cyclic Redundancy Check
CRT	Chinese Reminder Theorem
DES	Data Encryption Standard; symmetric block cipher algorithm
DPA	Differential Power Analysis
DFA	Differential Failure Analysis
EAL	Evaluation Assurance Level
EC	Elliptic Curve Cryptography
ECC	Error Correction Code
ECDH	Elliptic Curve Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EDC	Error Detection Code
EDU	Error Detection Unit
EEPROM	Electrically Erasable and Programmable Read Only Memory
EMA	Electro Magnetic Analysis
ETR	Evaluation Technical Report
Flash EEPROM	Flash Memory
FL	Flash Loader software

FTL	Flash Translation Layer
FW	Firmware
GCIM	Generic Chip Identification Mode
GPIO	General Purpose IO
HW	Hardware
IC	Integrated Circuit
ID	Identification
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
I/O	Input/Output
IRAM	Internal Random Access Memory
MED	Memory Encryption and Decryption
MMU	Memory Management Unit
NVM	Non-Volatile Memory
OS	Operating system
PP	Protection Profile
PRNG	Pseudo Random Number Generator
PROM	Programmable Read Only Memory
RAM	Random Access Memory
RMS	Resource Management System
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rives-Shamir-Adleman Algorithm
SAM	Service Algorithm Minimal
SAR	Security Assurance Requirement
SCP	Symmetric Cryptographic Processor
SF	Security Feature
SFP	Security Functional Policy
SFR	Special Function Register, as well as Security Functional Requirement, the specific meaning is given in the context
SOLID FLASH™	An Infineon Trade Mark and Stands for Flash EEPROM Technology
SPA	Simple Power Analysis
SPI	Serial Peripheral Interface
SSC	Synchronous Serial Communication
ST	Security Target
STS	Self Test Software

SW	Software
SO	Security Objective
SWP	Single Wire Protocol
TOE	Target of Evaluation
TM	Test Mode (STS)
TSF	TOE Security Functions
TRNG	True Random Number Generator
TSC	TOE Security Functions Control
TSF	TOE Security Functionality
UART	Universal Asynchronous Receiver/Transmitter
UM	User Mode (STS)
UmSLC	User Mode Security Life Control
WLP	Wafer Level Package
3DES	Triple DES Encryption Standards

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-0782-V3-2017, Version 2.6, 2017-08-02, "Confidential
      Security Target M7892 B11 Recertification Common Criteria CCv3.1 EAL6
      augmented (EAL6+)", Infineon Technologies AG (confidential document)

[7]   Evaluation Technical Report for BSI-DSZ-CC-0782-V3-2017, Version 4, 2017-08-28,
      "Evaluation Technical Report – ETR (Summary)", Tüv Informationstechnik GmbH,
      (confidential document)

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

[8]specifically

- AIS1, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers, Version 13, 14.08.2008,

- AIS14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 03.08.2010,

- AIS19, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC, Version 9, 03.11.2014,

- AIS20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3.0, 15.05.2013,

- AIS25, Anwendung der CC auf Integrierte Schaltungen, Version 9, 15.03.2017,

- AIS26, Evaluationsmethodologie für in Hardware integrierte Schaltungen, Version 9, 21.03.2013,

- AIS31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3.0, 15.05.2013,

- AIS32, CC-Interpretationen im deutschen Zertifizierungsschema, Version 6, 08.07.2011,

- AIS34, Evaluation Methodology for CC Assurance Classes for EAL5+, Version 3, 03.09.2009,

- AIS35, Öffentliche Fassung eines Security Target (ST-lite), Version 2, 12.11.2007,

- AIS36, Kompositionsevaluierung, Version 5, 15.03.2017,

- AIS38, Wiederverwendung von Evaluationsergebnissen, Version 2, 28.09.2007,

- AIS46, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, Version 3, 04.12.2013.

[9]   Security Target BSI-DSZ-CC-0782-V3-2017, Version 2.6, 2017-08-02, "Security Target Lite M7892 B11 Recertification Common Criteria CCv3.1 EAL6 augmented (EAL6+)" (sanitised public document)

[10]   ETR for composite evaluation according to AIS 36 for the Product BSI-DSZ-CC-0782-V3-2017, Version 4, 2017-08-28, "Evaluation Technical Report for composite Evaluation (ETR Comp)", TÜV Informationstechnik GmbH (confidential document)

[11]   Configuration list for the TOE, Version 2.0, 2017-07-05, "Configuration Management Scope ALC for Common Criteria with Evaluation Assurance Level EAL6 augmented (EAL6+) M7892 B11" (confidential document)

[12]   SCL78 Symmetric Crypto Library for SCPv3 DES / AES 16-bit Security Controller User Interface, 2017-05-02, Infineon Technologies AG (confidential document)

[13]   SLE70 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox (1.02.013), 2017-06-20, Infineon Technologies AG (confidential document)

[14]   Crypto@2304T User Manual, 2010-03-23, Infineon Technologies AG

[15]   16-bit Controller Family SLE 70 Programmer's Reference Manual, 2017-07-04, Infineon Technologies AG (confidential document)

[16]   M7892 Errata Sheet, 2017-06-21, Infineon Technologies AG

[17]   M7892 SOLID FLASH Controller for Security Applications 16-bit Security Controller Family Hardware Reference Manual, Version 1.7.1, 2015-09-21, Infineon Technologies AG (confidential document)

[18]   AMM Advanced Mode for Mifare-Compatible Technology Addendum to M7892 Hardware Reference Manual. Version 1.1, 2013-09-24, Infineon Technologies AG (confidential document)

[19]   SLx 70 Family Secure Hash Algorithm SHA-2 (SHA 256/224, SHA 512/384) Library, Version 1.01, 2009-11, Infineon Technologies AG (confidential document)

[20]   M7892 Security Guidelines, 2017-06-28, Infineon Technologies AG (confidential document)

[21]   SLx 70 Family Production and Personalization User's Manual, 2015-04-01, Infineon Technologies AG (confidential document)

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

Table 3: 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

Table 4: 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

Table 5: 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
	ASE_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 6: 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-0782-V3-2017

Evaluation results regarding development and production environment

The IT product Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013, and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware) (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 5 September 2017, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.5, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_FLR.1, ALC_LCD.1, ALC_TAT.3)

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

Name of site / Company name	Address
Development:	
IFX Augsburg	Infineon Technologies AG Alter Postweg 101 86159 Augsburg Germany
IFX Bangalore	Infineon Technologies India Pvt. Ltd. Kalyani Platina, Sy. No. 6 & 24 Kundanahalli Village Krishnaraja Puram Hobli Bangalore India – 560066 India
IFX Bucharest	Infineon Technologies Romania Blvd. Dimitrie Pompeiu Nr. 6 Sector 2 020335 Bucharest Romania
IFX Milpitas	Infineon Technologies AG Chip Card and Security 640 North McCarthy Blvd Milpitas, CA 95035
IFX Munich	Infineon Technologies AG Am Campeon 1-12

Name of site / Company name	Address
	85579 Neubiberg Germany
IFX Graz	Infineon Technologies Austria AG Development Center Graz Babenbergerstr. 10 8020 Graz Austria
IFX Villach	Infineon Technologies Austria AG Siemensstr. 2 9500 Villach Austria
IFX Klagenfurt	Infineon Technologies Austria AG Lakeside B05 9020 Klagenfurt Austria
IFX Melaka	Infineon Technologies Sdn. Bhd. Batu Berendam FTZ 75350, Melaka Malaysia
Production:	
Amkor Manila	Amkor Technology Philippines Km. 22 East Service Rd. South Superhighway Muntinlupa City 1702 Philippines
	Amkor Technology Philippines 119 North Science Avenue Laguna Technopark, Binan Laguna 4024 Philippines
ARDT Hsin-Chu	Ardentec Corporation No. 3, Gungye 3rd Rd., Hsin-Chu Industrial Park, Hu-Kou, Hsin-Chu Hsien Taiwan 30351, R.O.C.
ARDT Singapore	Ardentec Singapore Pte. Ltd. 12 Woodlands Loop #02-00 Singapore 738283
ASK Burlington	ASK-intTag, LLC Building 966 1000 River St., Essex Junction, Vermont 05452 USA

Name of site / Company name	Address
DHL Singapore	DHL Exel Supply Chain Richland Business Centre 11 Bedok North Ave 4, Level 3, Singapore 489949
Disco Kirchheim	DISCO HI-TEC EUROPE GmbH Liebigstrasse 8 D-85551 Kirchheim Germany
DNP Agrate	DNP Photomask Europe S.p.A. Via C. Olivetti 2/A 20041 Agrate Brianza Italy
Exceet Paderborn	Exceet Paderbornexceet Card AG Senefelderstr. 10 D-33100 Paderborn Germany
G&D Nitra	Giesecke & Devrient Slovakia, s.r.o. Dolné Hony 11 94901 Nitra Slovakia
HID Galway	HID Global Ireland Teoranta Pairc Tionscail na Tullaigh Baile na hAbhann Co. Galway Ireland
IFX Dresden	Infineon Technologies Dresden GmbH & Co. OHG Königsbrücker Str. 180 01099 Dresden Germany
IFX Morgan Hill	Infineon Technologies North America Corp. 18275 Serene Drive Morgan Hill, CA 95037 USA
IFX Regensburg	Infineon Technologies AG Wernerwerkstraße 2 93049 Regensburg Germany
IFX Singapore	Infineon Technologies Asia Pacific PTE Ltd. 168 Kallang Way Singapore 349253
IFX Wuxi	Infineon Technologies (Wuxi) Co. Ltd.

Name of site / Company name	Address
	No. 118, Xing Chuang San Lu Wuxi-Singapore Industrial Park Wuxi 214028, Jiangsu P.R. China
K&N Großostheim	Infineon Technology AG Distribution Center Europe (DCE) Kühne & Nagel Stockstädter Strasse 10 – Building 8A 63762 Großostheim Germany
K&N Hayward	Kuehne & Nagel 30805 Santana Street Hayward, CA 94544 USA
Smartrac Bangkok	Smartrac Technology Ltd. 142/121/115 Moo Hi-Tech Industrial Estate Tambon Ban Laean Amphor Bang-Pa-In 13160 Ayutthaya Thailand
Toppan Dresden (via BSI-DSZ-CC-S-0087-2017)	Toppan Photomask, Inc Rähnitzer Allee 9 01109 Dresden Germany
Toppan Ranzan[9]	Toppan Printing Co., Ltd. Ranzan Plant 6-2, Hanami-Dai, Ranzan-Machi, Hiki-Gun, Saitama 355-0204 Japan

Table 7: Relevant development and 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.

[9]No remote IT support from other Toppan sites is performed.