Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0827-V5-2017

for

Infineon Technologies Smart Card IC (Security Controller) M9900 A22/G11, M9905 A11, M9906 A11 with optional RSA v1.03.006/v2.05.005, EC v1.03.006/v2.05.005, Toolbox v1.03.006/v2.05.005, Flash Translation Layer V1.01.0008, SCL v2.01.011/v2.02.010 and PSL v4.00.009 libraries with specific IC dedicated software

from

Infineon Technologies AG

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0827-V5-2017 (*)

Infineon Technologies Smart Card IC (Security Controller) M9900 A22/G11, M9905 A11, M9906 A11 with optional RSA v1.03.006/v2.05.005, EC v1.03.006/v2.05.005, Toolbox v1.03.006/v2.05.005, Flash Translation Layer V1.01.0008, SCL v2.01.011/v2.02.010 and PSL v4.00.009 libraries with specific IC dedicated software

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 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 and 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.

Common Criteria
Recognition Arrangement
for components up to
EAL 4

Bonn, 30 August 2017

For the Federal Office for Information Security

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

Bernd Kowalski
Head of Division

L.S.

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 ALC_DVS.2, AVA_VAN.5, ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_TAT.2 and ATE_DPT.3 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 Technologies Smart Card IC (Security Controller) M9900 A22/G11, M9905 A11, M9906 A11 with optional RSA v1.03.006/v2.05.005, EC v1.03.006/v2.05.005, Toolbox v1.03.006/v2.05.005, Flash Translation Layer V1.01.0008, SCL v2.01.011/v2.02.010 and PSL v4.00.009 libraries with specific IC dedicated software has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0827-V4-2016. Specific results from the evaluation process BSI-DSZ-CC-0827-V4-2016 were re-used.

The evaluation of the product Infineon Technologies Smart Card IC (Security Controller) M9900 A22/G11, M9905 A11, M9906 A11 with optional RSA v1.03.006/v2.05.005, EC v1.03.006/v2.05.005, Toolbox v1.03.006/v2.05.005, Flash Translation Layer V1.01.0008, SCL v2.01.011/v2.02.010 and PSL v4.00.009 libraries with specific IC dedicated software was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 28 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

[6] Information Technology Security Evaluation Facility

maximum validity of the certificate has been limited. The certificate issued on 30 August 2017 is valid until 29 August 2022. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

- 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,
- 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,
- 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 Technologies Smart Card IC (Security Controller) M9900 A22/G11, M9905 A11, M9906 A11 with optional RSA v1.03.006/v2.05.005, EC v1.03.006/v2.05.005, Toolbox v1.03.006/v2.05.005, Flash Translation Layer V1.01.0008, SCL v2.01.011/v2.02.010 and PSL v4.00.009 libraries with specific IC dedicated software has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[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 Technologies Smart Card IC (Security Controller) M9900 A22/G11, M9905 A11, M9906 A11 with optional RSA v1.03.006/v2.05.005, EC v1.03.006/v2.05.005, Toolbox v1.03.006/v2.05.005, Flash Translation Layer V1.01.0008, SCL v2.01.011/v2.02.010 and PSL v4.00.009 libraries with specific IC dedicated software.

Please note: For the M9900 design step A22, two further derivatives exist, which are called C22 and D22. These two derivatives do not resemble individual design steps, but are identical to the A22 design step with additional wafer level package (in case of C22) or wafer level ball grid array (in case of D22), see also [6] and [9], remark 1 on p.7.

In general and independent of any design steps, the TOE provides a real 32-bit CPU-architecture and is compatible to the ARMv7-M instruction set. The major components of the core system are the 32-bit CPU (Central Processing Unit), the Cache system, the MPU (Memory Protection Unit) and MED (Memory Encryption/Decryption Unit.

The TOE consists of the hardware part, the firmware parts and the software parts. The software parts comprise the asymmetric cryptographic libraries RSA and EC, the symmetric cryptographic library SCL for DES and AES and the additional optional libraries PSL, Toolbox, Base and FTL.

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 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 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 7.

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.

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 Technologies Smart Card IC (Security Controller) M9900 A22/G11, M9905 A11, M9906 A11 with optional RSA v1.03.006/v2.05.005, EC v1.03.006/v2.05.005, Toolbox v1.03.006/v2.05.005, Flash Translation Layer V1.01.0008, SCL v2.01.011/v2.02.010 and PSL v4.00.009 libraries with specific IC dedicated software.

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery / Note
1	HW	M9900 Smart Card IC	A22 (produced in Dresden)	Bare dies, plain wafers, complete modules or IC cases.
1a	HW	M9900 Smart Card IC	C22 (produced in Dresden)	Equal to the M9900 A22, with additional wafer level package (WLP).
1b	HW	M9900 Smart Card IC	D22 (produced in Dresden)	Equal to the M9900 A22, with additional wafer level ballgrid array (WLB).
1c	HW	M9900 Smart Card IC	G11 (produced in Tainan)	Bare dies, plain wafers, complete modules or IC cases.
1d	HW	M9905 Smart Card IC	A11 (produced in Dresden)	Bare dies, plain wafers, complete modules or IC cases.
1f	HW	M9906 Smart Card IC	A11 (produced in Dresden)s	Bare dies, plain wafers, complete modules or IC cases.

No	Type	Identifier	Release	Form of Delivery / Note
2	FW	Flash Loader	FW Identifiers M9900: 80 00 11 41 or 80 00 11 42 M9905: 80 00 11 51 M9906: 80 00 11 50	Stored in reserved area of the ROM on the IC (patch in NVM).
3	FW	BOS Boot System (the IC Dedicated Test Software)	FW Identifiers M9900: 80 00 11 41 or 80 00 11 42 M9905: 80 00 11 51 M9906: 80 00 11 50	Stored in Test ROM on the IC.
4	FW	RMS Resource Management System (the IC Dedicated Support Software)	FW Identifiers M9900: 80 00 11 41 or 80 00 11 42 M9905: 80 00 11 51 M9906: 80 00 11 50	Stored in reserved area of the ROM on the IC (patch in NVM).
5	FW	Mifare-compatible OS	FW Identifiers M9900: 80 00 11 41 or 80 00 11 42 M9905: 80 00 11 51 M9906: 80 00 11 50	Stored in reserved area of the ROM on the IC (patch in NVM). Optional.
6	SW	NVM image (including Embedded Software)	--	Stored in Flash memory on the IC.
7	SW	RSA library	RSA2048: 1.03.006 or 2.05.005 RSA4096: 1.03.006 or 2.05.005	Optional.
8	SW	EC library	1.03.006 or 2.05.005	Optional.
9	SW	Toolbox	1.03.006 or 2.05.005	Optional.

No	Type	Identifier	Release	Form of Delivery / Note
10	SW	Base library	1.03.006 or 2.05.005	Optional.
11	SW	Symmetric Crypto Library	2.01.011 or 2.02.010	Optional.
12	SW	Platform Support Layer	4.00.09	Optional.
13	SW	Management of Mifare-compatible Cards	01.03.0926 or 01.04.1275 (both optional)	Optional.
14	SW	Mifare-compatible Reader Mode Support	01.02.0800	Optional.
15	SW	Flash Translation Layer	1.01.0008	Optional.
16	DOC	SLE 97 32-bit Security Controller Family based on SC300 in 90 nm CMOS Technology M9900 Solid Flash Controller for HD-SIM Applications Hardware Reference Manual	Rev. 2.2 2013-10-25	Electronic document
17	DOC	M9900 Errata Sheet	2016-11-21	Electronic document
18	DOC	M9905 M9906 SLI/SLM 97 SOLID FLASH™ Families Errata Sheet	2017-01-30	Electronic document
19	DOC	M9900 Security Guidelines User's Manual	2017-06-30	Electronic document
20	DOC	32-bit ARM-based Security Controller SLE 97 Programmer's Reference Manual	2017-03-29	Electronic document
21	DOC	ARMv7-M Architecture Reference Manual	2010-02-12	Electronic document
22	DOC	SLE97 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox User Interface (v1.03.006)	2017-05-10	Electronic document (optional)
23	DOC	CL97 Asymmetric Crypto Library for Crypto@2304T RSA / EC / Toolbox User Interface (v2.05.005)	2017-05-10	Electronic document (optional)
24	DOC	SLE 97 Flash Translation Layer User's Manual	Rev. 1.0 2012-07-10	Electronic document

No	Type	Identifier	Release	Form of Delivery / Note
25	DOC	SLE 97 /SLC 14 Family Production and Personalization User's Manual	2014-08-10	Electronic document
26	DOC	SCL97 Symmetric Crypto Library for SCPv3 DES / AES 32-bit Security Controller User Interface	V2.01.011 2016-08-02	Electronic document (optional)
		SCL97 Symmetric Crypto Library for SCPv4 DES / AES 32-bit Security Controller User Interface	V2.02.010 2016-12-09	Electronic document (optional)
27	DOC	SLI97 Family PSL Reference Manual User's Manual	V4.00.09 2016-03-10	Electronic document (optional)
28	DOC	SLI97 Security Guidelines PSL V4.00.09	2017-08-18	Electronic document (optional)

Table 2: Deliverables of the TOE

A processing step during production testing incorporates the chip-individual features into the hardware of the TOE. The individual TOE hardware is uniquely identified by its serial number. The serial number comprises 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.

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.

The TOE can be delivered in various configurations, achieved by means of blocking and depending on the customer order. All product derivates of this TOE, including all configuration possibilities differentiated by the GCIM (Generic Chip Identification Mode) data and the configuration information output, are manufactured by Infineon Technologies AG. New configurations can occur at any time depending on the user blocking or by different configurations applied by the manufacturer. In any case the user is able to clearly identify the TOE hardware, its configuration and proof the validity of the certificate independently, meaning without involving the manufacturer. The various blocking options, as well as the means used for the blocking, are done during the manufacturing process or at user premises. Entirely all means of blocking (especially those firmware- and software parts responsible for the blocking, used at Infineon Technologies AG and/or the user premises) are subject of the evaluation. All resulting configurations of a TOE derivative are subject of the certificate. All resulting configurations are either at the predefined limits or within the predefined configuration ranges. For more information about blocking, see chapter 8.

Another characteristic of the TOE are the chip identification data. This chip identification data is accessible via the Generic Chip Identification Mode (GCIM). This GCIM outputs amongst other identifiers for the platform, chip mode, ROM code, chip type, design step, fabrication facility, wafer, die position, firmware identifier, temperature range, and frequency.

For further, detailed information regarding TOE identification see [6] and [9], p.7f (remark 1).

3. Security Policy

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

The Security Policy of the TOE is to provide basic security functionalities to be used by the smart card operating system and the smart card application, thus providing an overall smart card system security. Therefore, the TOE will implement a symmetric cryptographic block cipher algorithms (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 random number generation of appropriate quality.

The SCL uses the symmetric cryptographic co-processor (SCP) of the hardware to provide the user with a software interface to the DES 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 Crypto2304T 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 Crypto2304T and includes countermeasures against SPA, DPA and DFA attacks.

The PSL library provides the user with a standardised software interface to access different hardware and software parts of the TOE. The security relevant services, which can be accessed via the PSL are the RSA library, the EC library the SCL and the random number generation.

The SHA-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.

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: protection during composite manufacturing (OE.Process-Sec-IC), usage of hardware platform (OE.Plat-Appl) and treatment of user data (OE.Resp-Appl). Details can be found in the Security Target [6] and [9], chapter 5.2.

5. Architectural Information

The TOE is an integrated circuit (IC) providing a platform to a smart card operating system and smart card application software. A top level block diagram and a list of subsystems can be found within the TOE description of the Security Target Lite [9], chapter 2.1.

The TOE provides a real 32-bit CPU-architecture and is compatible to the ARMv7-M instruction set architecture. The major components of the core system are the 32-bit CPU as a variant of the ARM Secure Core SC300, the Cache system, the Memory Protection Unit and the Memory Encryption/Decryption Unit. For the more details about the real 32-bit CPU-architecture, please refer to Security Target [6] and [9], chapter 1.2 and 2.1.

Two co-processors for cryptographic operations are implemented on the TOE. The Crypto2304T for calculation of asymmetric algorithms like RSA and Elliptic Curve (EC) and the Symmetric Cryptographic Processor (SCP) for dual-key or triple-key triple-DES and AES calculations. These co-processors are especially designed for smart card applications with respect to the security and power consumption. The SCP module computes the complete DES algorithm within a few clock cycles and is especially designed to counter attacks like DPA, EMA and DFA. The Crypto2304T module provides basic functions for the implementation of RSA and EC cryptographic libraries.

The BOS (Boot Software) and the RMS (Resource Management System) compose the TOE firmware stored in the ROM and the patches hereof in the Infineon® SOLID FLASH™. All mandatory functions for start-up and internal testing (BOS) are protected by a dedicated hardware firewall. Additionally two levels are provided, the privileged level and the user level, both are protected by a hardwired Memory Protection Unit (MPU) setting. The RMS is accessible in privileged level only. The FL (Flash Loader) and the Mifare-compatible software compose the TOE software stored in the Infineon® SOLID FLASH™. The FL allows downloading of user software to the NVM during the manufacturing process and can be completely deactivated.

The RSA library is used to provide a high-level interface to RSA (Rivest, Shamir, Adleman) cryptography implemented on the hardware component Crypto2304T and includes countermeasures against SPA, DPA and DFA attacks. The routines are used for the generation of RSA key pairs, RSA signature verification, RSA signature generation and RSA modulus recalculation.

The EC library is used to provide a high-level interface to Elliptic Curve cryptography implemented on the hardware component Crypto2304T and includes countermeasures against SPA, DPA and DFA attacks. The routines are used for ECDSA signature generation, ECDSA signature verification, ECDSA key generation and Elliptic Curve Diffie-Hellman key agreement. The EC library is delivered as object code.

The Symmetric Crypto library (SCL) is used to provide a high level interface to DES/3TDES and AES symmetric cryptographic operations. It uses the SCP of the underlying hardware but implements also countermeasures against all known weaknesses of the SCP (e.g. dummy calculations and block repetitions). The symmetric crypto library consists of three C-library files Cipher.lib, AES.lib and DES.lib. Those library files will not be distributed individually. Therefore those three library files are called the Symmetric Crypto Library (SCL).

The Product Support Layer (PSL) library is used to provide a standardized interface to the hardware by making use of the RSA, ECC and SCL libraries. The provided interfaces are syntactically similar to Windows NT device driver calls. The drivers consist merely of wrapper code with no inherent security relevant parts.

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 test,
- Verification tests,
- Security Evaluation tests,
- Production tests.

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

The evaluators were able to repeat the tests of the developer either using the library of programs, tools and prepared chip samples delivered to the evaluator or at the developers site. They performed independent tests to supplement, augment and to verify the tests performed by the developer. The tests of the developer were repeated by sampling, by repetition of complete regression tests and by software routines developed by the evaluators and computed on samples with an evaluation operating system. 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 using bespoke equipment and expert know how. 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:

- Smartcard IC M9900 design step A22 (with derivatives C22, D22 - Dresden),
- Smartcard IC M9900 design step G11 (Tainan),
- Smartcard IC M9905 design step A11 (Dresden), and
- Smartcard IC M9906 design step A11 (Dresden).

This TOE is represented by various configurations called products, which are all derived from the equal hardware design M9900, M9905, M9906.

The M9900, M9905, M9906 products offer different configuration options, which a customer can choose. The mechanism to choose a configuration can be done by the following methods:

- by product selection or dialog-based in Tools,
- via Bill-per-Use (BPU) and Flash Loader (FL).

The degree of freedom for configuring the TOE is predefined by Infineon Technologies AG. The list of predefined TOE configurations is given in the SLE97 Hardware Reference Manual [13].

All these possible TOE configurations equal and/or within the specified ranges are covered by the certificate. Beside fix TOE configurations, which can be ordered as usual, this TOE implements optionally the so called Bill-Per-Use (BPU) ability. This solution enables the customer to tailor the product on his own to the required configuration by blocking parts of the chip on demand into the final configuration at his own premises, without further delivery or involving support by Infineon Technology AG. Customers, who are intended to use this feature receiving the TOE in a predefined configuration including the Flash Loader software, enhanced with the BPU blocking software. The blocking information is part of a chip configuration area and can be modified by customers using specific APDUs. Once a final blocking is done, further modifications are disabled. The BPU software part is only present on the products which have been ordered with the BPU option. In all other cases this software is not present on the product. For more details please refer to the Security Target Lite [9], chapter 2.1.8.

Depending on the blocking configuration a product can have different user available configurations, as detailed in [6] and [9] section 2.1.8.

As noted above the user has the possibility to tailor the crypto co-processor part of the TOE during the manufacturing process by deselecting the Asymmetric Cryptographic Processor (Crypto2304T) or the Symmetric Cryptographic Processor (SCP). Hence if the asymmetric cryptographic co-processor is blocked, the user will not be able to use the RSA, EC and Toolbox library, because they use this co-processor to perform their basic calculations. The hardware based DES and AES calculations, as well as the SCL operations are not available in case that the SCP is blocked. In order to use the PSL both co-processors, as well as the asymmetric and symmetric cryptographic libraries need to be available.

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
- Guidance, Smartcard Evaluation

  (see [4], AIS 25, AIS 26, AIS 31).

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.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0827-V4-2016, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on libraries and respective documentation.

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).

In the Security Target [6] and [9], section 7.3 provides a list of the TOE's cryptographic mechanisms. Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' in section 7.3 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.

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 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] - [22] 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 [23] 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 SOLID FLASH^{TM}) 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] Confidential Security Target BSI-DSZ-CC-0827-V5-2017, Version 2.7.5, 2017-08-18, "Confidential Security Target M9900, M9905, M9906 including optional Software Libraries RSA-EC-SCL-PSL", Infineon (confidential document)

[7] Evaluation Technical Report for BSI-DSZ-CC-0827-V5-2017, Version 3, 2017-08-21, Evaluation Technical Report Summary, TÜV Informationstechnik GmbH, (confidential document)

[8] specifically

- AIS 19, Version 9, Anwendungshinweise und Interpretationen zum Schema (AIS)
- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC
- AIS 23, Version 3, Zusammentragen von Nachweisen der Entwickler
- 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
- AIS 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluierungen
- AIS 38, Version 2, Reuse of evaluation results

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

[9] Security Target Lite BSI-DSZ-CC-0827-V5-2017, Version 2.7.5, 2017-08-18, “Security Target Lite M9900, M9905, M9906 including optional Software Libraries RSA-EC-SCL-PSL”, Infineon (sanitised public document)

[10] ETR for composite evaluation according to AIS 36 for the Product BSI-DSZ-CC-0827-V5-2017, Version 3, 2017-08-21, “Evaluation Technical Report for Composite Evaluation”, TÜV Informationstechnik (confidential document)

[11] Configuration list for the TOE, 1.1, 2017-05-24, “Configuration Management Scope M9900, M9905, M9906 including optional Software Libraries RSA-EC-SCL-PSL”, Infineon (confidential document)

[12] M9900 Security Guidelines User’s Manual, 2017-06-30, Infineon

[13] SLE97 M9900 Hardware Reference Manual, Version 2.2, 2013-10-25, Infineon

[14] 32-bit ARM-based Security Controller, SLE 97, Programmer’s Reference Manual, Rev. 3.7, 2017-03-29, Infineon

[15] SLE 97 32-bit Security Controller Family based on SC300 in 90 nm CMOS Technology M9900 Solid Flash Controller for HD-SIM Applications Hardware Reference Manual, 2013-10-25, Infineon

[16] M9905 M9906 SLI/SLM 97 SOLID FLASH™ Families Errata Sheet, 2017-01-30, Infineon

and

M9900 Errata Sheet, 2016-11-21, Infineon

[17] ARMv7-M Architecture Reference Manual, ID 021310, 2010-02-12, ARM Limited

[18] SLE97 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox User Interface, Version 1.03.006, 2017-05-10, Infineon

[19] CL97 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox User Interface, Version 2.05.005, 2017-05-10, Infineon

[20] SCL97 Symmetric Crypto Library for SCPv3 DES / AES 32-bit Security Controller User Interface (v2.01.011), 2016-08-02, Infineon

and

SCL97 Symmetric Crypto Library for SCPv4 DES / AES 32-bit Security Controller User Interface (v2.02.010), 2016-12-09, Infineon

[21] SLI97 Security Guidelines PSL V4.00.09, 2017-08-18, Infineon

[22] SLE 97 Flash Controller Family Flash Translation Layer User’s Manual, Version 1.0, 2012-07-10, Infineon

[23] SLE 97 / SLC 14 Family Production and Personalization User’s Manual, 2014-08-10, Infineon

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
	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 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

Annex B of Certification Report BSI-DSZ-CC-0827-V5-2017

Evaluation results regarding development and production environment

The IT product Infineon Technologies Smart Card IC (Security Controller) M9900 A22/G11, M9905 A11, M9906 A11 with optional RSA v1.03.006/v2.05.005, EC v1.03.006/v2.05.005, Toolbox v1.03.006/v2.05.005, Flash Translation Layer V1.01.0008, SCL v2.01.011/v2.02.010 and PSL v4.00.009 libraries with specific IC dedicated software (Targ et 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 and 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 August 2017, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. 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**
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
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 T site 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
DHL Singapore	DHL Exel Supply Chain Richland Business Centre 11 Bedok North Ave 4, Level 3, Singapore 489949

Name of site / Company name	Address
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
G&D Nitra	Giesecke & Devrient Slovakia, s.r.o. Dolné Hony 11 94901 Nitra Slovakia
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. 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

Name of site / Company name	Address
Toppan Dresden	Toppan Photomask, Inc Rähnitzer Allee 9 01109 Dresden Germany
TSMC Tainan	Taiwan Semiconductor Manufacturing Company Ltd. 1, Nan-Ke North Rd. Tainan Science Park Tainan 741-44 Taiwan

Table 7: List of 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.