Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0827-V7-2018

for

Infineon Technologies Smart Card IC (Security Controller) M9900 A22, M9900 C22, M9900 D22, M9900 G11, M9905 A11, M9906 A11 with optional Software Libraries RSA2048, RSA4096, EC, Toolbox, Base, FTL, SCL, HCL, and PSL, and with specific IC dedicated software

from

Infineon Technologies AG

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0827-V7-2018 (*)

Infineon Technologies Smart Card IC (Security Controller) M9900 A22, M9900 C22, M9900 D22, M9900 G11, M9905 A11, M9906 A11 with optional Software Libraries RSA2048, RSA4096, EC, Toolbox, Base, FTL, SCL, HCL, and PSL, and 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
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 14 September 2018

For the Federal Office for Information Security

Joachim Weber
Head of Branch

L.S.

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the 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.

2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.

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

2 Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

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

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

3. Recognition Agreements

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

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

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

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

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

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

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

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

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

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Infineon Technologies Smart Card IC (Security Controller) M9900 A22, M9900 C22, M9900 D22, M9900 G11, M9905 A11, M9906 A11 with optional Software Libraries RSA2048, RSA4096, EC, Toolbox, Base, FTL, SCL, HCL, and PSL, and with specific IC dedicated software has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0827-V6-2017. Specific results from the evaluation process BSI-DSZ-CC-0827-V6-2017 were re-used.

The evaluation of the product Infineon Technologies Smart Card IC (Security Controller) M9900 A22, M9900 C22, M9900 D22, M9900 G11, M9905 A11, M9906 A11 with optional Software Libraries RSA2048, RSA4096, EC, Toolbox, Base, FTL, SCL, HCL, and PSL, and with specific IC dedicated software was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 4 September 2018. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: 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.

5. Validity of the Certification Result

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

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

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

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

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 14

[5] Information Technology Security Evaluation Facility

September 2018 is valid until 13 September 2023. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

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

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

6. Publication

The product Infineon Technologies Smart Card IC (Security Controller) M9900 A22, M9900 C22, M9900 D22, M9900 G11, M9905 A11, M9906 A11 with optional Software Libraries RSA2048, RSA4096, EC, Toolbox, Base, FTL, SCL, HCL, and PSL, and with specific IC dedicated software has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[6] 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, M9900 C22, M9900 D22, M9900 G11, M9905 A11, M9906 A11 with optional Software Libraries RSA2048, RSA4096, EC, Toolbox, Base, FTL, SCL, HCL, and PSL, and with specific IC dedicated software.

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 are differentiated into: the asymmetric cryptographic libraries RSA and EC, the symmetric cryptographic library SCL for DES and AES and the additional optional libraries PSL, Toolbox, Base, FTL and HCL.

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] and [9] 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, M9900 C22, M9900 D22, M9900 G11, M9905 A11, M9906 A11 with optional Software Libraries RSA2048, RSA4096, EC, Toolbox, Base, FTL, SCL, HCL, and PSL, and 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, Firmware-ID: 80001141 (BOS-V1) and 80001142 (BOS-V2)	A22 (produced in Dresden)	Bare dies, plain wafers, complete modules or IC cases.
1a	HW	M9900 Smart Card IC Firmware-ID: 80001141 (BOS-V1) and 80001142 (BOS-V2)	C22 (produced in Dresden)	Equal to the M9900 A22, with additional wafer level package (WLP).
1b	HW	M9900 Smart Card IC Firmware-ID: 80001141 (BOS-V1) and 80001142 (BOS-V2)	D22 (produced in Dresden)	Equal to the M9900 A22, with additional wafer level ballgrid array (WLB).
1c	HW	M9900 Smart Card IC Firmware-ID: 80001141 (BOS-V1) and 80001142 (BOS-V2)	G11 (produced in Tainan)	Bare dies, plain wafers, complete modules or IC cases.
1d	HW	M9905 Smart Card IC Firmware-ID: 80001151 (BOS-V1)	A11 (produced in Dresden)	Bare dies, plain wafers, complete modules or IC cases.
1f	HW	M9906 Smart Card IC Firmware-ID: 80001150 (BOS-V1)	A11 (produced in Dresden)	Bare dies, plain wafers, complete modules or IC cases.
Firmware				

No	Type	Identifier	Release	Form of Delivery / Note
2	FW	Flash Loader	FW Identifier 80 00 11 41 or 80 00 11 42 or 80 00 11 50 or 80 00 11 51	Stored in reserved area of the ROM on the IC (patch in NVM).
3	FW	BOS Boot System (the IC Dedicated Test Software)	FW Identifier 80 00 11 41 or 80 00 11 42 or 80 00 11 50 or 80 00 11 51	Stored in Test ROM on the IC.
4	FW	RMS Resource Management System (the IC Dedicated Support Software)	FW Identifier 80 00 11 41 or 80 00 11 42 or 80 00 11 50 or 80 00 11 51	Stored in reserved area of the ROM on the IC (patch in NVM).
5	FW	Mifare-compatible Reader Mode Support Library (out of scope of evaluation)	01.02.0800	Stored in reserved area of the ROM on the IC (patch in NVM). Optional.
6	FW	Management of Mifare-compatible Cards Library (out of scope of evaluation)	01.03.0927, 01.04.1275	Stored in reserved area of the ROM on the IC (patch in NVM). Optional.
Software / Libraries (optional)				
7	SW	RSA library	RSA2048 2.05.005 (not for G11) or 2.07.003 RSA4096 2.05.005 (not for G11) or 2.07.003	Optional.
8	SW	EC library	2.05.005 (not for G11) or 2.07.003	Optional.
9	SW	Toolbox	2.05.005 (not for G11) or 2.07.003	Optional.
10	SW	Base library	2.05.005 (not for G11) or 2.07.003	Optional.

No	Type	Identifier	Release	Form of Delivery / Note
11	SW	Symmetric Crypto Library	2.01.011, 2.02.010 or 2.04.003. For G11: None.	Optional.
12	SW	Platform Support Layer	4.00.010, 5.00.06 For G11: None.	Optional.
13	SW	Management of Mifare-compatible Cards	01.03.0927 or 01.04.1275	Optional.
14	SW	Mifare-compatible Reader Mode Support	01.02.0800	Optional.
15	SW	Flash Translation Layer	1.01.0008	Optional.
16	SW	Hash Cryptographic Library	1.01.003 For G11: None.	Optional.
Guidance				
17	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*	2013-10-25, v2.2	Document in electronic form.
18	DOC	M9900 Errata Sheet	2016-11-21, v2.1	Document in electronic form.
19	DOC	M9905 M9906 Errata Sheet	2017-01-30, v2.2	Document in electronic form.
20	DOC	M9900 Security Guidelines User's Manual	2018-07-03	Document in electronic form.
21	DOC	32-bit ARM-based Security Controller SLE 97 Programmer's Reference Manual	2017-03-29, v3.7	Document in electronic form.
22	DOC	ARMv7-M Architecture Reference Manual (ID021310)	2010-02-12	Document in electronic form.

No	Type	Identifier	Release	Form of Delivery / Note
23	DOC	SLE 97 /SLC 14 Family Production and Personalization User's Manual	2014-08-10	Document in electronic form.
Optional Guidance				
24	DOC	CL97 Asymmetric Crypto Library for Crypto@2304T RSA / EC / Toolbox User Interface (v2.05.005)	2017-05-10	Optional (Document in electronic form.)
25	DOC	CL97 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox User Interface (v2.07.003)	2018-05-24	Optional (Document in electronic form.)
26	DOC	SLE 97 Flash Translation Layer User's Manual (for FTL v1.01.0008)	2012-07-10, v1.0	Optional (Document in electronic form.)
27	DOC	HCL97-CPU-L90 Hash Crypto Library for CPU SHA (for HCL v1.01.003)	2018-05-22, v1.01.003	Optional (Document in electronic form.)
28	DOC	SLI97 Family PSL Reference Manual User's Manual (PSL v4.00.09, but also applicable to PSL v4.00.10)	2016-08-04	Optional (Document in electronic form.)
29	DOC	SLI97 Release Notes (PSL V4.00.10)	2018-06-07, v1.1	Optional (Document in electronic form.)
30	DOC	SLx97 Platform Support Layer Library Programmer's Reference Manual (PSL v5.00.06)	2018-07-06, v5.4	Optional (Document in electronic form.)
31	DOC	PSL Security Guidelines (PSL v4.00.10)	2018-06-07, v1.6	Optional (Document in electronic form.)
32	DOC	PSL Security Guidelines (PSL v5.00.06)	2018-07-06, v2.5	Optional (Document in electronic form.)
33	DOC	SCL97 Symmetric Crypto Library for SCPv3 DES / AES 32-bit Security Controller User Interface (V2.01.011)	2016-08-02	Optional (Document in electronic form.)

No	Type	Identifier	Release	Form of Delivery / Note
34	DOC	SCL97 Symmetric Crypto Library for SCPv4 DES / AES 32-bit Security Controller User Interface (V2.02.010)	2016-12-09	Optional (Document in electronic form.)
35	DOC	SCL97 Symmetric Crypto Library for SCPv3 DES / AES 32-bit Security Controller User Interface (for SCL v2.04.003)	2018-05-22	Optional (Document in electronic form.)

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.

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.

In detail, regarding identification:

The TOE can be delivered in various configurations, achieved by means of blocking and depending on the customer order.

All product derivatives of this TOE, including all configuration possibilities differentiated by the Generic Chip Identification Mode (GCIM) data and the configuration information output, are manufactured by Infineon Technologies AG. However, the Smartcard Embedded Software respectively user software is *not* part of the TOE.

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 and the firmware respectively software parts involved in 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 below.

The hardware part of the TOE is identified by M9900 A22/G11/C22/D22, M9905 A11, M9906 A11. Another characteristic of the TOE is the chip identification data. The 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, temperature range, and system frequency.

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

In detail, regarding delivery:

“TOE Delivery” is uniquely used to indicate

- after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or
- after Phase 4 (or before Phase 5) if the TOE is delivered in form of packaged products.

Therefore three different delivering procedures have to be taken into consideration:

- Delivery of the IC dedicated software components (IC dedicated SW, guidance) from the TOE manufacturer to the IC embedded software developer.
- Delivery of the IC embedded software (ROM / Flash data, initialisation and pre-personalization data, Bundle Business package) from the IC embedded software developer to the TOE manufacturer.
- Delivery of the final TOE from the TOE manufacturer to the composite product manufacturer. After phase 3 the TOE is delivered in form of wafers or sawn wafers, after phase 4 in form of modules (with or without inlay antenna).

The TOE is delivered via the logistics sites:

- DHL Singapore (Distribution Center Asia),
- G&D Neustadt,
- K&N Großostheim (Distribution Center Europe),
- K&N Hayward (Distribution Center USA).

3. Security Policy

The security policy enforced is defined by the selected 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. Please note that the “*_Sec1” functions of the SCLs are not covered by this evaluation, in contrast to the evaluated “*_Sec2” counterparts.

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 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, the HCL (only for PSL v5.00.06) and the random number generation.

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 Chapter 7 and 8 of the Security Target (ST).

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) [Phase 5-6, optional Phase 4], usage of hardware platform (OE.Plat-Appl) and treatment of user data (OE.Resp-Appl) [both Phase 1]. Details can be found in the Security Target [6] and [9], chapter 5.2.

5. Architectural Information

The TOE is a SmartCard (Security IC). Detailed information on the TOE hardware architecture is to be found in [6] and [9] section 2.1.

Regarding the different libraries available and their dependencies:

The RSA2048 and RSA4096 libraries are variants of the same RSA library. They differ only in the maximum key size: the RSA2048 library supports keys of up to 2112 bits and the RSA4096 library supports keys of up to 4224 bits. All other functionalities are identical.

The RSA library, ECC library, and Toolbox library are parts of the Asymmetric Cryptographic Library (ACL). All selected parts of the ACL have to be of the same version number. If at least one of the ACL parts is selected a Base Library (not in scope of the evaluation) is automatically included.

The Platform Support Library (PSL) provides a standardised interface to the hardware, directly or via the ACL or SCL libraries. As such it functions as a wrapper and provides no security relevant parts. If the PSL library v4.00.10 is part of the shipment, the RSA, EC, Base libraries v2.05.005 and the SCL library v2.01.011 are automatically included. If the PSL library v5.00.06 is part of the shipment, the RSA, EC, Base libraries v2.07.003, the SCL library v2.04.003 and the HCL library v1.01.003 are automatically included.

If the Symmetric Cryptographic Processor is blocked no hardware-based DES and AES calculations can be performed by the TOE. Furthermore the SCL cannot be used.

Blocking the Crypto2304T co-processor means that the RSA, ECC and Toolbox library cannot be used, because they perform their basic calculations on this co-processor.

6. Documentation

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

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

7. IT Product Testing

The developer performed five categories of tests:

- Simulation Tests (Design Verification),
- Qualification Tests / Software Verification,
- Verification Tests,
- Security Evaluation Tests, and
- 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 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 forthe 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:

- Smartcard IC M9900 A22 (Dresden; or C22 / D22 for the additional derivatives WLP / WLB),

- Smartcard IC M9900 G11 (Tainan),
- Smartcard IC M9905 A11 (Dresden), and
- Smartcard IC M9906 A11 (Dresden).

This TOE is represented by various configurations called products, which are all derived from the equal hardware design M9900, M9905 and M9906. The same mask is used to produce different products of the TOE.

The M9900, M9905 and M9906 product offers 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.

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 configuration.

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 (Crypto@2304T) 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 (see also chapter 5 “architectural information”).

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:

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 1, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers, Version 14, 2017-10-11,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 2010-08-03,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 19, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 9, 2014-11-03,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 2013-05-15,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 23, Zusammentragen von Nachweisen der Entwickler, Version 4, 2017-03-15,
- Application Notes and Interpretation of the Scheme (AIS) – AIS 25, Anwendungen der CC auf integrierte Schaltungen, Version 9, 2017-03-15,,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 26, Evaluationsmethodologie für in Hardware integrierte Schaltungen, Version 9, 2013-03-21,
- Special Attack Methods for Smartcards and Similar Devices, Version 1.4, 2011-06-08,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 2013-05-15,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 32, CC-Interpretationen im deutschen Zertifizierungsschema, Version 7, 2011-06-08,
- Application Notes and Interpretation of the Scheme (AIS) – AIS 34, Evaluation Methodology for CC Assurance Classes for EAL5+ (CC v2.3 & v3.1) and EAL6 (CC v3.1), Version 3, 2009-09-03,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 35, Öffentliche Fassung eines Security Target (ST-lite), Version 2, 2007-11-12,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 36, Kompositionsevaluierung, Version 5, 2017-03-15,

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 37, Terminologie und Vorbereitung von Smartcard-Evaluierungen, Version 3, 2010-05-17,
- Application Notes and Interpretation of the Scheme (AIS) – AIS 38, Reuse of evaluation results, Version 2, 2007-09-28,
- Application Notes and Interpretation of the Scheme (AIS), AIS 41, Guidelines for PPs and STs, Version 2, 2011-01-31,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 46, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, Version 3, 2013-12-04

are considered.

Additionally the CC Supporting Mandatory Technical Documents

- Joint Interpretation Library – The Application of CC to Integrated Circuits, Version 3.0, February 2009,
- Joint Interpretation Library – Application of Attack Potential to Smartcards, Version 2.9, 2013-01,
- CC Supporting Document, Mandatory Technical Document, Composite product evaluation for Smart Cards and similar devices, Version 1.0, Revision 1, September 2007, CCDB-2007-09-001,
- CC Supporting Document Guidance, Smartcard Evaluation, Version 2.0, February 2010, CCDB-2010-03-001
- CC Supporting Document, Guidance, ETR template for composite evaluation of Smart Cards and similar devices, Version 1.0, Revision 1, September 2007, CCDB-2007-09-002

are considered.

For RNG assessment the scheme interpretations AIS 20/31 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 of it.

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-V6-2017, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on libraries and respective guidance 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).

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. 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) only:

Purpose	**Cryptographic Mechanism**	**Standard of Implementation**	**Key Size in Bits**	**Security Level above 100 Bits**
Key Agreement	ECDH	[X963] [FIPS186-4] [RFC5639]	Key sizes corresponding to the used elliptic curves P-{192, 224, 256, 384, 521}, K-{163, 233, 283, 409}, B-{163, 233, 283, 409} [DSS], brainpoolP{160, 192, 224,256,320,384,512}r1, brainpoolP{160, 192, 224,256,320,384,512}t1 [ECC]	Key sizes 160, 163, 192: no Key sizes >= 224 : yes
Cryptographic Primitive	3DES in CBC mode	[NIST SP800-67] [NIST SP800-38A]	|k| = 112, 168	168: Yes, 112: No
	3DES in ECB mode	[NIST SP800-67] [NIST SP800-38A]	|k| = 112, 168	No
	3DES in CTR mode	[NIST SP800-67]	|k| = 112, 168	168: Yes, 112: No

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
		[NIST SP800-38A]		
	3DES in CFB mode	[NIST SP800-67] [NIST SP800-38A]	|k| = 112, 168	168: Yes, 112: No
	3DES in CMAC mode	[NIST SP800-67] [NIST SP800-38A]	|k| = 112, 168	168: Yes, 112: No
	3DES CBC-MAC mode	[ISO_9797-1] [FIPS197]	|k| = 112, 168	No
	AES in CBC mode	[FIPS197] [NIST SP800-38A]	|k| = 128, 192, 256	Yes
	AES in ECB mode	[FIPS197] [NIST SP800-38A]	|k| = 128, 192, 256	No
	AES in CTR mode	[FIPS197] [NIST SP800-38A]	|k| = 128, 192, 256	Yes
	AES in CFB mode	[FIPS197] [NIST SP800-38A]	|k| = 128, 192, 256	Yes
	AES in CBC-MAC mode	[ISO_9797-1] [FIPS197]	|k| = 128, 192, 256	Yes
	AES in CMAC mode	[NIST SP800-38B] [FIPS197]	|k| = 128, 192, 256	Yes
	RSA encryption / decryption / signature generation / verification (only modular exponentiation part)	[PKCS #1] for key generation see below table	Modulus length = 1976 - 4096	Yes
	ECDSA signature generation / verification	[X962] [FIPS186-4] [RFC5639]	Key sizes corresponding to the used elliptic curves P-{192, 224, 256, 384, 521}, K-{163, 233, 409, 283}, B-163, {233, 283, 409} [DSS], brainpoolP{160, 192, 224,256,320,384,512}r1, brainpoolP{160, 192, 224,256,320,384,512}t1 [ECC]	Key sizes 160, 163, 192: no Key sizes >= 224 : yes
	Physical True RNG PTG.2	[AIS31]	N/A	N/A

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
	SHA-1 Hash	[FIPS180-4]	N/A	N/A
	SHA-2 Hash	[FIPS180-4]	N/A	N/A

Table 3: TOE cryptographic functionality

In addition to table 3 above, the following rating applies regarding RSA Key Gen:

Purpose	Cryptographic Mechanism	Standard of Implemen - tation	Key Size in Bits	Security Level above 100 Bits
Key Generation (ACL v2.07.003)	RSA Key Generation in ACL v2.07.003, utilizing the preparative function “CryptoGeneratePrime()” or the function “CryptoRSAKeyGen()”	n/a	1976 - 4096	Yes

Table 4: TOE cryptographic functionality – RSA Key Gen

For the Cryptographic Functionality

- CryptoGeneratePrimeMask() which might be used in conjunction with RSA Key Generation in ACL v2.05.005 and v2.07.003,

no statement on the respective cryptographic strength can be given.

The Flash Loader's cryptographic strength was also not assessed by BSI. However, the evaluation according to the TOE's Evaluation Assurance Level did not reveal any implementation weaknesses.

Please note, that this holds true also for those algorithms, where no cryptographic 100-Bit-Level assessment was given. Consequently, the targeted Evaluation Assurance Level has been achieved for those functionalities as well.

Detailed results on conformance have been compiled into the report [27].

Reference of Legislatives and Standards quoted above:

[X963] American National Standard for Financial Services, ANS X9.63–2011, Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2011-12, American National Standard Institute.

[FIPS186-4] Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013, U.S. department of Commerce / National Institute of Standards and Technology (NIST).

[RFC5639] RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, 2010-03.

[NIST SP800-67] NIST SP800-67 Revision 1, Recommendation for Triple Data Encryption Algorithm (TDEA) Block Cipher, 2012-01, National Institute of Standards and Technology (NIST).

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

[ISO_9797-1] Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, 1999-12, ISO/IEC.

[FIPS197] Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), November 2001, U.S. department of Commerce / National Institute of Standards and Technology (NIST).

[PKCS #1] PKCS #1 v2.2: RSA Cryptography Standard, 2012-10, RSA Laboratories.

[X962] American National Standard for Financial Services, ANS X9.62–2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005-11, American National Standard Institute.

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

[FIPS180-4] FIPS PUB 180-4 Federal Information Processing Standards Publication Secure Hash Standard (SHS), August 2015, Information Technology Laboratory National Institute of Standards and Technology.

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 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].

Please also note that the "*_Sec1" functions of the SCLs (Symmetric Cryptographic Libraries) are not covered by this evaluation, in contrast to the evaluated "*_Sec2" counterparts.

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

- All security hints described in the delivered documents [12]-[25] (also listed in Table 2) 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 [26] have to be considered.

In addition the following hints 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

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile

SAR Security Assurance Requirement

SFP Security Function Policy

SFR Security Functional Requirement

ST Security Target

TOE Target of Evaluation

TSF TOE Security Functionality

12.2. Glossary

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

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

Extension - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

13. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017,
https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7] https://www.bsi.bund.de/AIS

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

[6] Confidential Security Target BSI-DSZ-CC-0827-V7-2018, Version 3.7, 2018-08-17, "Confidential Security Target M9900, M9905, M9906 including optional Software Libraries RSA-EC-SCL-HCL-PSL", Infineon (*confidential document*)

[7] Evaluation Technical Report, BSI-DSZ-CC-0827-V7-2018 Version 2, 2018-08-21, "EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY)", TÜV Informationstechnik GmbH, *(confidential document)*

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

[9] Security Target Lite for BSI-DSZ-CC-0827-V7-2018, Version 3.7, Date 2018-08-17, "Security Target Lite M9900, M9905, M9906 including optional Software Libraries RSA-EC-SCL-HCL-PSL", Infineon (sanitised public document)

[10] ETR for composite evaluation according to AIS 36 for the Product BSI-DSZ-CC-0827-V7-2018, Version 2, Date 2018-08-21, "EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP)", TÜV Informationstechnik GmbH (confidential document)

[11] Configuration list for the TOE, v1.4, 2018-06-06, "Configuration Management Scope M9900, M9905, M9906 including optional Software Libraries RSA-EC-SCL-PSL", Infineon (confidential document)

[12] M9900 Security Guidelines User's Manual, 2018-07-03, Infineon

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

[14] SLE 97, Programmer's Reference Manual, Rev. 3.7, 2017-03-29, Infineon

[15] M9905 M9906 Families Errata Sheet, Rev. 2.2, 2017-01-30, Infineon

and

M9900 Errata Sheet, Rev. 2.1, 2016-11-21, Infineon

[16] ARMv7-M Architecture Reference Manual, ARM DDI 0403D ID021310, 2010-02-12, ARM Limited

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

[18] CL97 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox User Interface, Version 2.07.003, 2018-05-24, Infineon

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

and

[7] See section 9.1 for a detailed list of used AIS and supporting documents

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

and

SCL97 Symmetric Crypto Library for SCPv3 DES / AES 32-bit Security Controller User Interface (v2.04.003), 2018-05-22, Infineon

[20] PSL Security Guidelines (PSL version v4.00.09 and v4.00.10), revision 1.6, 2018-06-07, Infineon

[21] SLI 97 Family PSL Reference Manual User's Manual (PSL v4.00.09 but applicable to PSL v4.00.10), v4.00.09, 2016-08-04, Infineon

[22] SLI97 PSL Release Notes (PSL v4.00.10), v1.1, 2018-06-07, Infineon

[23] PSL Security Guidelines (PSL v5.00.06), v2.5, 2018-07-06, Infineon

[24] SLx97 Platform Support Layer Library Programmer’s Reference Manual (PSL v5.00.06), v5.4, 2018-07-06, Infineon

[25] SLE 97 Flash Translation Layer User’s Manual, v1.0, 2012-07-10, Infineon

[26] SLE97 / SLC14 Family Production and Personalization User’s Manual, Edition Aug. 10, 2014, 2014-08-10, Infineon

[27] SINGLE EVALUATION REPORT ADDENDUM to ETR-Part ASE, AVA, AGD, ADV, Cryptographic Standards Compliance Verification, v1, 2018-06-22, TÜV Informationstechnik GmbH (confidential document)

C. Excerpts from the Criteria

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

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

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

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment

Annex B of Certification Report BSI-DSZ-CC-0827-V7-2018

Evaluation results regarding development and production environment

The IT product Infineon Technologies Smart Card IC (Security Controller) M9900 A22, M9900 C22, M9900 D22, M9900 G11, M9905 A11, M9906 A11 with optional Software Libraries RSA2048, RSA4096, EC, Toolbox, Base, FTL, SCL, HCL, and PSL, and with specific IC dedicated software (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations 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 14 September 2018, 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, ALC_TAT.2)

are fulfilled for the development and production sites of the TOE.

The relevant delivery sites are as follows:

Site ID	Company name and address
DHL Singapore	DHL Exel Supply Chain Richland Business Centre 11 Bedok North Ave 4, Level 3, Singapore 489949
G&D Neustadt	Giesecke & Devrient Secure Data Management GmbH Austraße 101b 96465 Neustadt bei Coburg Germany
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

Table 5: TOE Delivery / Distribution 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.

Note: End of report