Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0964-V4-2019

for

Infineon Technologies Security Controller M7794 A12 / G12 with optional RSA2048/4096v1.02.013 or v2.00.002, EC v1.02.013 or v2.00.002 and Toolbox v1.02.013 or v2.00.002 libraries and 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-0964-V4-2019 (*)

Infineon Technologies Security Controller M7794 A12 / G12 with optional RSA2048/4096v1.02.013 or v2.00.002, EC v1.02.013 or v2.00.002 and Toolbox v1.02.013 or v2.00.002 libraries 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, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

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

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 28 May 2019

For the Federal Office for Information Security

Bernd Kowalski   L.S.
Head of Division

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

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 Security Controller M7794 A12 / G12 with optional RSA2048/4096v1.02.013 or v2.00.002, EC v1.02.013 or v2.00.002 and Toolbox v1.02.013 or v2.00.002 libraries and with specific IC-dedicated software as undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0964-V3-2017. Specific results from the evaluation process BSI-DSZ-CC-0964-V3-2017 were re-used.

The evaluation of the product Infineon Technologies Security Controller M7794 A12 / G12 with optional RSA2048/4096v1.02.013 or v2.00.002, EC v1.02.013 or v2.00.002 and Toolbox v1.02.013 or v2.00.002 libraries and with specific IC-dedicated software was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 21 May 2019. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: 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 28 May 2019 is valid until 27 May 2024. Validity can be re-newed by re-certification.

---

[5]   Information Technology Security Evaluation Facility

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,

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

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

6.   Publication

The product Infineon Technologies Security Controller M7794 A12 / G12 with optional RSA2048/4096v1.02.013 or v2.00.002, EC v1.02.013 or v2.00.002 and Toolbox v1.02.013 or v2.00.002 libraries 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 1-15
       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 smart card IC (Security Controller) M7794 A12 and G12 with optional Software Libraries RSA2048 v1.02.013 or v2.00.002 – RSA4096 v1.02.013 or v2.00.002 – EC v1.02.013 or v2.00.002 – Toolbox v1.02.013 or v2.00.002 and with specific IC dedicated software. The IC Embedded Software is not part of the evaluation. The IC is intended to be used in smart cards for particularly security-relevant applications. The TOE provides a real 16-bit CPU-architecture with proprietary enhancements in the instruction set. The major components of the core system are the CPU (Central Processing Unit), the MMU (Memory Management Unit) and MED (Memory Encryption/Decryption Unit). The dual interface controller is able to communicate using either the contact based or the contactless interface.

The TOE consists of a hardware part, a firmware part and a software part that is the cryptographic libraries RSA and EC and the supporting libraries Toolbox and Base. RSA, EC and Toolbox provide certain functionality to the Smartcard Embedded Software. The libraries come in two different versions which can be selected by the user during the ordering process. However the library versions cannot be mixed between each other.

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: The life cycle of the TOE is split up into several phases. Different operation modes help to protect the TOE during each phase of its lifecycle.
SF_PS	Protection against Snooping: The TOE uses various means to protect from snooping of memories and busses and prevents single stepping.
SF_PMA	Protection against Modifying Attacks: This TOE implements protection against modifying attacks of memories, alarm lines and sensors.
SF_PLA	Protection against Logical Attacks:

TOE Security Functionality	Addressed issue
	Memory access of the TOE is controlled by a Memory Management Unit (MMU), which implements different privileged levels. The MMU decides, whether access to a physical memory location is allowed based on the access rights of the privilege levels.
SF_CS	Cryptographic Support: The TOE is equipped with an asymmetric and a symmetric hardware accelerator and also software modules to support several asymmetric cryptographic operations. It further provides random numbers to meet class PTG.2 of AIS31.

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 4.1 and 4.2.

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 Security Controller M7794 A12 / G12 with optional RSA2048/4096v1.02.013 or v2.00.002, EC v1.02.013 or v2.00.002 and Toolbox v1.02.013 or v2.00.002 libraries and with specific IC-dedicated software.

The following table outlines the TOE deliverables:

Type	Identifier	Release	Form of Delivery
HW	M7794 Smart Card IC	A12 (produced in Dresden) or G12 (produced in Tainan - TSMC)	Postal transfer in cages as wafer, IC case or packages (see [6] and [9], section 2.2.5.

Type	Identifier	Release	Form of Delivery
SW	RSA library (optional)	RSA2048 v1.02.013 or v2.00.002 RSA4096 v1.02.013 or v2.00.002	Secured download (L251 Library File, object code) via ishare.
SW	EC library (optional)	EC v1.02.013 or v2.00.002	Secured download (L251 Library File, object code) via ishare.
SW	Toolbox (optional)	Toolbox v1.02.013 or v2.00.002	Secured download via ishare.
FW	Flash Loader	FW Identifier 77.017.12.0 or 77.017.12.2 or 77.017.13.2	On-chip software
FW	STS Self Test Software (the IC Dedicated Test Software)		
FW	RMS Resource Management System (the IC Dedicated Support Software)		
FW	Mifare compatible software interface		
DOC	M7794 Controller Product Group for Payment Applications Hardware Reference Manual	V1.1, 2011-11-02	Secured download (personalized PDF) via ishare.
DOC	AMM Advanced Mode for Mifare-Compatible Technology Addendum to M7794 Hardware Reference Manual	V1.1, 2011-11-03	Secured download (personalized PDF) via ishare.
DOC	16-bit Controller Family SLE 70 Programmer's Reference Manual	V9.5, 2017-05-10	Secured download (personalized PDF) via ishare.
DOC	SLE 77 Controller Family Errata Sheet	V6.1, 2017-06-21	Secured download (personalized PDF) via ishare.
DOC	SLE77 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox User Interface (1.02.013)	2017-05-10	Secured download (personalized PDF) via ishare.
DOC	SLE77 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox User Interface (2.00.002)	2017-05-10	Secured download (personalized PDF) via ishare.
DOC	Crypto@2304T User Manual	2010-03-23	Secured download (personalized PDF) via ishare.
DOC	M7794 Security Guidelines	2019-03-21	Secured download (personalized PDF) via ishare.
DOC	Option 2 for Fast Startup	2014-11-20	Secured download (personalized PDF) via ishare.

Type	Identifier	Release	Form of Delivery
DOC	SLx 70 Family Production and Personalization User's Manual	2015-04-01	Secured download (personalized PDF) via ishare.

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.

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 hardware part of the TOE is identified by M7794 A12 and G12. Another characteristic of the TOE are the chip identification data. These chip identification data is accessible via the Generic Chip Identification Mode (GCIM) and is chip specific as they contain amongst others identifiers for the platform, chip mode, ROM code, chip type, design step, and other information. All information can be gained by a dedicated the firmware function, for details see [17], section 4.26 and [13], section 7.10.3.

Depending on the configuration a M7794 A12 and G12 product can have e.g. different user available memory sizes and can come with or without individual accessible cryptographic co-processor. Furthermore different interface options are available (see [6] and [9], table 2) by order or by BPU.

Thus, in the field, the IC Embedded Software Developer can clearly identify a product in question by the Generic Chip Identification Mode and the user guidance.

In addition to the hardware part, the TOE consists of firmware parts and software parts:

The firmware part of the TOE is identified also via the GCIM.

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

3.   Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE.

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

The 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.

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 packaging, finishing and personalization, usage of hardware platform and treatment of user data. The augmented organizational security policy P.Add-Functions, derived from the additional security functionality of the cryptographic libraries, the augmented assumption A.Key-Function, related to the usage of key-depending functions, and the threat of memory access violation T.Mem-Access, due to specific TOE memory access control functionality, have been added. Details can be found in the Security Target [6] and Security Target Lite [9], chapter 4.3.

5.   Architectural Information

The TOE is an integrated circuits (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 major components of the core system are the CPU, the MMU (Memory Management Unit) and MED (Memory Encryption/Decryption Unit). The TOE implements a 16-MByte linear addressable memory space, a simple scaleable Memory Management concept and a scaleable stack size. The flexible memory concept consists of ROM and SOLID FLASH™.

The symmetric coprocessor (SCP) combines both AES and triple DES with dual-key or triple-key hardware acceleration. The asymmetric crypto coprocessor, called Crypto2304T in the following, supports RSA-2048 bit (4096-bit with CRT) and Elliptic Curve (EC) cryptography.

The software part of the TOE consists of the cryptographic libraries RSA and EC, the Toolbox and Base library. If RSA or EC or Toolbox is part of the shipment, the Base Library is automatically included. The Base Library provides the low level interface to the asymmetric cryptographic coprocessor and has no user available interface.

Part of the evaluation are the RSA straight operations with key lengths from 1024 bits to 2048 bits, and the RSA CRT operations with key lengths of 1024 bits to 4096 bits. Note that key lengths below 1024 bits are not included in the certificate.

The Flash Loader is a firmware located in the user-ROM and allowing downloading the user software or parts of it to the NVM memory. The download is only possible after successful authentication. After completion of the download the Flash Loader can be permanently deactivated by the user.

For more details please refer to the Security Target Lite [6] and [9], chapter 1.2 and 2.2.

6.   Documentation

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

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

7.   IT Product Testing

The tests performed by the developer (and partly by the evaluator) were divided into five categories:

- Simulation tests (design verification):

    In the course of the development of the TOE simulation tests are carried out. These simulation tests yield CRC sums, which are used in the further testing.

- Qualification tests:

    For each mask version a qualification test is performed. Via the results of these tests a qualification report is generated. The positive result of the qualification is one part of the necessary testing results documented with the qualification report. The qualification report is completed after the verification testing (see below) and the security evaluation (see below) are performed successfully. The tests performed and their results are listed in the qualification report. The results of the tests are the basis on which it is decided, whether the TOE is released to production.

- Verification Tests:

    With these tests in user mode the functionality of the end user environment is checked.

- Security Evaluation Tests:

    In the context of security evaluation testing the security mechanisms is tested again in the user mode only focusing on security. Here is not only verified that the security functionality is working as this was already tested on every single TOE during production, but also it is tested how well the security functionality is working and the effectiveness is calculated. This step is necessary as the mechanisms work together and that must be evaluated in the user mode.

- Production Tests:

    Before delivery on every chip production tests are performed. These tests use the CRC checksums attained by the simulation tests. The aim of these tests is to check whether each chip is functioning correctly.

The 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 showed 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 M7794 A12 (produced in Dresden),

● Smartcard IC M7794 G12 (produced in Tainan).

Depending on the blocking configuration a M7794 A12 and G12 product can have e.g. different user available memory sizes and can come with or without individual accessible cryptographic co-processor. More information are given in [6] and [9], section 2.2.7.

The entire configuration is done during the manufacturing process of the TOE according to the choice of the user or by Bill Per Use (BPU). BPU allows a customer to block chips on demand at the customer´s premises. Customers, who intend to use this feature receive the TOEs in a predefined configuration. The blocking information is part of a chip configuration area. Dedicated blocking information can be modified by customers using specific APDUs. Once final blocking is done, further modifications are disabled.

The dedicated RMS functions allow a customer to extract the present hardware configuration and the original Chip Identifier Byte, which was valid before blocking. The blocking mechanism is also part of the evaluation. For more details please refer to the Security Target [6] and [9], chapter 2.2.7 and 2.2.8.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

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

The following guidance specific for the technology was used:

● The Application of CC to Integrated Circuits,

● The Application of Attack Potential to Smartcards,

● Functionality classes and evaluation methodology of physical random number generators

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

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

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

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

● All components of the EAL 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-0964-V3-2017, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on documentation changes.

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).

An overview over the claimed cryptopgraphic functionalities is given in the Security Target [6] and [9], section 7.1.4. Any Cryptographic Functionality therein, that is marked in column '*Security Level above 100 Bits*' with '*no*', achieves a security level of lower than 100 Bits (in general context).

Please note:

- RSA key generation is not in scope of this certification, thus no assessment on the respective cryptographic strengths can be given (as no respective SFRs are claimed).

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].

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

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

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

- All security hints described in [21] have to be considered.

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

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

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

11. Security Target

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

12. Regulation specific aspects (eIDAS, QES)

None.

13. Definitions

13.1. 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

13.2. Glossary

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

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

14. Bibliography

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

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

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

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

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

[6]   Security Target BSI-DSZ-CC-0964-V4-2019, Version 2.5, 2019-04-02, "Security
        Target M7794 A12/G12 Including optional software libraries RSA – EC - Toolbox",
        Infineon Technologies AG (confidential document)

[7]   Evaluation Technical Report for BSI-DSZ-CC-0964-V4-2019, Version 2, 2019-04-08,
        Evaluation Technical Report 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 BSI-DSZ-CC-0964-V4-2019, Version 2.5, 2019-04-02, "Security
        Target Lite M7794 A12/G12 Including optional software libraries RSA – EC -
        Toolbox", Infineon Technologies AG (sanitised public document)

[10]   ETR for composite evaluation according to AIS 36 for the Product BSI-DSZ-CC-
        0964-V4-2019, Version 2, 2019-04-08, Evaluation Technical Report for Composite
        Evaluation (ETR-COMP), TÜV Informationstechnik GmbH (confidential document)

[7]specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers

- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)

- AIS 19, Version 9, Verbindlich Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren

- AIS 23, Version 4, Zusammentragen von Nachweisen der Entwickler

- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document

- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document

- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)

- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies

- AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document

- AIS 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluierungen

- AIS 38, Version 2, Reuse of evaluation results

- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[11]   Configuration list for the TOE, Version 1.1, 2014-12-09, Configuration Management Scope M7794 A12 and G12 including optional Software Libraries RSA – EC – Toolbox (confidential document)

[12]   M7794 Security Guidelines, 2019-03-21, Infineon Technologies AG, (confidential document)

[13]   M7794 Controller Product Group for Payment Applications Hardware Reference Manual, Version 1.1, 2011-11-02, Infineon Technologies AG, (confidential document)

[14]   AMM Advanced Mode for Mifare Compatible Technology Addendum to M7794 Hardware Reference Manual, Rev.1.1, 2011-11-03, Infineon Technologies AG, (confidential document)

[15]   Option 2 for Fast Startup, 2014-11-20, Infineon Technologies AG, (confidential document)

[16]   16-bit Controller Family SLE 70 Programmer's Reference Manual, 2017-05-10, Infineon Technologies AG, (confidential document)

[17]   SLE 77 Controller Family Errata Sheet, Version 6.1, 2017-06-21, Infineon Technologies AG, (confidential document)

[18]   Crypto@2304T User Manual, 2010-03-23, Infineon Technologies AG, (confidential document)

[19]   SLE77 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox User Interface (1.02.013), Version 1.02.013, 2017-05-10, Infineon Technologies AG, (confidential document)

[20]   SLE77 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox User Interface (2.00.002), Version 2.00.002, 2017-05-10, Infineon Technologies AG, (confidential document)

[21]   SLx 70 Family Production and Personalization User's Manual, 2015-04-01, Infineon Technologies AG, (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 detailed 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-0964-V4-2019

Evaluation results regarding development and production environment

The IT product Infineon Technologies Security Controller M7794 A12 / G12 with optional RSA2048/4096v1.02.013 or v2.00.002, EC v1.02.013 or v2.00.002 and Toolbox v1.02.013 or v2.00.002 libraries 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, 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 28 May 2019, 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 <u>of the TOE</u>.

The relevant distribution sites are listed below:

Site name	Company name and adress
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
IFX Morgan Hill	Infineon Technologies North America Corp. 18275 Serene Drive Morgan Hill, CA 95037 USA
K&N Großostheim	Kühne & Nagel Stockstädter Strasse 10 – Building 8A 63762 Großostheim Germany

Table 3: Relevant production and development sites

For all sites, 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