Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0879-V5-2022

for

Infineon Security Controller M7893 B11 with optional RSA2048 v2.03.008, SHA-2 V1.01, Toolbox v2.03.008 and with specific IC dedicated software (firmware)

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-0879-V5-2022 (*)

Infineon Security Controller M7893 B11 with optional RSA2048 v2.03.008, SHA-2 V1.01, Toolbox v2.03.008 and with specific IC dedicated software (firmware)

from	Infineon Technologies AG
PP Conformance:	Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007
Functionality:	PP strictly conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 6 augmented by ALC_FLR.1

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, 19 October 2022

For the Federal Office for Information Security

Sandro Amendola
Head of Division

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....6
1. Preliminary Remarks....6
2. Specifications of the Certification Procedure....6
3. Recognition Agreements....7
4. Performance of Evaluation and Certification....8
5. Validity of the Certification Result....8
6. Publication....9
B. Certification Results....10
1. Executive Summary....11
2. Identification of the TOE....13
3. Security Policy....15
4. Assumptions and Clarification of Scope....15
5. Architectural Information....15
6. Documentation....16
7. IT Product Testing....16
8. Evaluated Configuration....17
9. Results of the Evaluation....17
10. Obligations and Notes for the Usage of the TOE....19
11. Security Target....20
12. Regulation specific aspects (eIDAS, QES)....20
13. Definitions....20
14. Bibliography....23
C. Excerpts from the Criteria....26
D. Annexes....27

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]
- BMI Regulations on Ex-parte Costs [3]
- Special decrees issued by the Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community)
- 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 BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- 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.sogis.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 and ALC_FLR components.

[4] Proclamation of the Bundesministerium des Innern und für Heimat 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 Security Controller M7893 B11 with optional RSA2048 v2.03.008, SHA-2 V1.01, Toolbox v2.03.008 and with specific IC dedicated software (firmware), has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0879-V4-2020. Specific results from the evaluation process BSI-DSZ-CC-0879-V4-2020 were re-used.

The evaluation of the product Infineon Security Controller M7893 B11 with optional RSA2048 v2.03.008, SHA-2 V1.01, Toolbox v2.03.008 and with specific IC dedicated software (firmware), was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 2 September 2022. 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 19 October 2022 is valid until 18 October 2027. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

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 Security Controller M7893 B11 with optional RSA2048 v2.03.008, SHA-2 V1.01, Toolbox v2.03.008 and with specific IC dedicated software (firmware), has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[6] Infineon Technologies AG
Melli-Beese-Str. 9
86159 Augsburg

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 an Infineon Security Controller M7893 B11 with optional Software Library RSA2048 v2.03.008, SHA-2 v1.01, and Toolbox v2.03.008, as well as with specific IC dedicated software (firmware). The TOE provides a real 16-bit CPU-architecture and is compatible to the 80251 microcontroller architecture. The major components of the core system are the two CPUs (Central Processing Units), acting as one, 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 Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007 [8].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 6 augmented by ALC_FLR.1.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 7.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
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: The memory access control of the TOE uses a memory management unit (MMU) to control the access to the available physical memory by using virtual memory addresses and to segregate the code and data to a privilege level model. The MMU controls the address permissions of up seven privileged levels and gives the software the possibility to define different access rights. The address permissions of the privilege levels are controlled by the MMU. In case of an access violation the MMU will trigger a reset and then a trap service routine can react on the access violation.
SF_CS	Cryptographic Support: The TOE is equipped with hardware accelerators and software modules to support standard symmetric and asymmetric cryptographic operations. The components are a symmetric coprocessor supporting the DES and AES algorithms (note that AES

TOE Security Functionality	Addressed issue
	is not in scope of the evaluation) and a combination of a coprocessor and software modules to support RSA cryptography. Furthermore, the TOE is equipped with an optional SHA-2 library and HASH module as well as an AIS31 conformant TRNG that meets the functionality class PTG.2.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [9], chapter 8.

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 Security Controller M7893 B11 with optional RSA2048 v2.03.008, SHA-2 V1.01, Toolbox v2.03.008 and with specific IC dedicated software (firmware)

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	M7893 Smart Card IC	B11 (produced in Dresden)	Complete modules, with or without inlay mounting, with or without inlay antenna mounting, in form of plain wafers, in an IC case or in bare dies
2	SW	RSA library (optional)	RSA2048 v2.03.008	Object code in electronic form
3	SW	SHA-2 library (optional)	SHA-2 v1.01	Object code in electronic form
4	SW	Toolbox library (optional)	Toolbox v2.03.008	Object code in electronic form
5	FW	STS Self Test Software (the IC Dedicated Test Software)	FW-identifier 78.019.03.4	Stored in test ROM on the IC (patch in SOLID FLASH)
6	FW	RMS Resource Management System (the IC Dedicated Support Software)	FW-identifier 78.019.03.4	Stored in reserved area of user ROM on the IC (patch in SOLID FLASH)
7	FW	Service Algorithm (SA)	FW-identifier 78.019.03.4	Stored in reserved area of user ROM on the IC (patch in SOLID FLASH)
8	FW	Flash Loader	FW-identifier 78.019.03.4	Stored in reserved area of user ROM and parts of it in SOLID FLASH on the IC (patch in SOLID FLASH)
9	SW[7]	ROM code (including Embedded Software and crypto libraries)	–	Stored in User ROM on the IC
10	SW[8]	NVM image (including Embedded Software and crypto libraries)	–	Stored in Flash memory on the IC
11	DOC	SLx 70 Family Production and Personalization User' Manual	2015-04-01	Personalized pdf-file
12	DOC	M7893 Hardware Reference Manual	Version 3.0, 2019-06-24	Personalized pdf-file
13	DOC	M7893 Errata Sheet	Version 5.0, 2020-05-07	Personalized pdf-file
14	DOC	M7893 Security Guidelines	2022-08-18	Personalized pdf-file
15	DOC	16-bit Security Controller Family SLE 70 Programmer's Reference Manual	Version 9.14, 2019-12-03	Personalized pdf-file

[7]Only in case the IC Embedded Software Developer provides Infineon with code for ROM.

[8]Only in case the IC Embedded Software Developer provides Infineon with code for Flash memory.

No	Type	Identifier	Release	Form of Delivery
16	DOC	SLE70 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox User Interface (2.03.008)	2021-07-27	Personalized pdf-file (optional)
17	DOC	Crypto@2304T User Manual	2010-03-23	Personalized pdf-file
18	DOC	SLx70 Family Secure Hash Algorithm SHA-2 (SHA 256/224, SHA 512/384) Library Version V1.01	2020-08-19	Personalized pdf-file (optional)
19	DOC	AMM Advanced Mode NRG SAM Addendum	Version 2.0, 2019-10-22	Personalized pdf-file (optional)

Table 2: Deliverables of the TOE

The delivery documentation describes in a sufficient manner how the various procedures and technical measures provide for the detection of modifications and any discrepancies between the TOE respective parts of it send by the TOE Manufacturer and the version received by the Composite Product Manufacturer.

Furthermore,the delivery documentation describes in a sufficient manner how the various procedures and technical measures provide for the detection of modifications and any discrepancies between the TOE respective parts of it send by the TOE Manufacturer and the version received by the Composite Product Manufacturer.

Three different delivery 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).

Respective distribution centers are listed in Appendix B (see below).

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

The hardware part of the TOE is identified as M7893 B11. Another characteristic of the TOE are the chip identification data. These chip identification data is accessible via the Generic Chip Identification Mode (GCIM) see [16] chapter 7.10.3.

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

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

For further, detailed information regarding TOE identification see [6] and [9], section 1.2.

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

3. Security Policy

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

The TOE implements a symmetric cryptographic block cipher algorithm (TDES) 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 Crypto@2304T and includes countermeasures against SPA, DPA and DFA attacks. The SHA-2 library provides the calculation of a hash value of freely chosen data input in the CPU.

As the TOE is a hardware security platform, the security policy of the TOE is also to provide protection against leakage of information (e.g. to ensure the confidentiality of cryptographic keys during TDES and RSA 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: OE.Plat-Appl (Usage of Hardware Platform), OE.Resp-Appl (Treatment of User Data) and OE.Process-Sec-IC (Protection during Composite product manufacturing). Details can be found in the Security Target [6] and [9], chapter 5.2.

5. Architectural Information

The TOE is an integrated circuit (IC) providing a platform for an operating sytem and application software used in smartcards but also in any other device or form factor requiring a high level of resistance against attackers. A top level block diagram and a list of subsystems can be found within the TOE description of the Security Target [6] and [9], chapter 2.1.

The TOE consists of a core system, memories, computing peripherals, system peripherals, standard peripherals, an analogue module and the connecting busses. The major components of the core system are the double CPU (Central Processing Units) including

the internal encryption leaving no plain data, the MMU (Memory Management Unit) and MED (Memory Encryption/Decryption Unit). The Block diagram provides a simplified overview upon the hardware subsystems in the Security Target [6] and [9], figure 1.

The symmetric co-processor (SCP) combines both AES (note that AES is not in scope of evaluation) and Triple-DES with dual-key or triple-key hardware acceleration. The Asymmetric Crypto Co-processor is called Crypto2304T and provides hardware support for asymmetric algorithms like RSA and EC (EC is not part of evaluation).

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

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): 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 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 for the underlying mechanisms of security functionalities. The penetration tests considered both the physical tampering of the TOE and attacks, which do not modify the TOE physically. The penetration tests results confirm that the TOE is resistant to attackers with high attack potential in the intended environment for the TOE.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

- Smartcard IC M7893 B11.

Depending on the blocking configuration, a M7893 product can have a different user available configuration as described in Security Target [6] and [9], chapter 1.1. The M7893 B11 allows for a maximum of configuration possibilities defined by the customer order following the market needs. For example, a M7893 B11 product can come in one project with the fully available ROM and SOLID FLASH™ Non Volatile Memory (NVM) or in another project without any user available ROM and with any other SOLID FLASH™ NVM-size below the physical implementation size, or with a different RAM size. Even more, the user has the free choice, whether he needs the symmetric co-processor SCP, or the asymmetric co-processor Crypto2304T, or both, or none of them. In addition, the user decides, whether the TOE comes with a combination of software libraries or without any. And, to be even more flexible, various interface options can be chosen as well.

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:

(i) The Application of CC to Integrated Circuits

(ii) The Application of Attack Potential to Smartcards,

(iii) Functionality classes and evaluation methodology of physical random number generators,

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

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

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

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

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

- All components of the EAL 6 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.1 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0879-V4-2020, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the removal of the CRT-based RSA signature generation and decryption (RSA-v2.03.008), the RSA4096 library removal, the removal of Elliptic Curve Cryptography library and SCL library.

Beside the changes above, the scope of the evaluation is reduced as the following SFRs (and the associated functionality) are removed:

- FCS_COP.1/AES,
- FCS_CKM.4/AES,
- FCS_CKM.1/RSA-v2.03.008.

Further, the block cipher modes for FCS_COP.1/TDES were reduced to ECB, and the CRT-based RSA signature generation / decryption was removed from scope (FCS_COP.1/RSA-v2.03.008), the Cryptographic key generation (FCS_CKM.1/RSA-v2.03.008)is removed from the scope.

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 strictly conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 6 augmented by ALC_FLR.1

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 table in annex C of part D of this report 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.

Conformance evaluation and assessment to claimed cryptographic functionality standards is documented in the confidential report “Cryptographic Standards Compliance Verification” [21]. For a list of standards see annex C of part D.

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.

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

Some security measures are partly implemented in this certified TOE, but require additional configuration or control or measures to be implemented by a product layer on top, e.g. the IC Dedicated Support Software and/or Embedded Software using the TOE. For this reason the TOE includes guidance documentation (see table 2) which contains obligations and guidelines for the developer of the product layer on top on how to securely use this certified TOE and which measures have to be implemented in order to fulfil the security requirements of the Security Target of the TOE. In the course of the evaluation of the composite product or system it must be examined if the required measures have been correctly and effectively implemented by the product layer on top. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the document "ETR for composite evaluation" [10].

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

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

- All security hints described in the delivered documents [19], [16], [17], [15], [14], [18], [13], and [12], especially the recommendations for secure usage in [19] and [16, 2.11 / 9.1] have to be considered.
- The SHA-2 implementation is not intended to be used on confidential input data. For such use cases, specific security improvements and side channel analysis are recommended (see [18, 2.3.2] and [19, 10.4]).

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 [20] have to be considered.

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

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

BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CC	Common Criteria for IT Security Evaluation
CCRA	Common Criteria Recognition Arrangement
CEM	Common Methodology for Information Technology Security Evaluation
CI	Chip Identification Mode (STS-CI)
CIM	Chip Identification Mode (STS-CI), same as CI
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
Crypto2304T	Asymmetric Cryptographic Processor
CRT	Chinese Reminder Theorem
DCLB	Digital Contactless Bridge
DES	Data Encryption Standard; symmetric block cipher algorithm
DFA	Differential Failure Analysis
DPA	Differential Power 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
FW	Firmware
GCIM	Generic Chip Identification Mode
HW	Hardware
IC	Integrated Circuit
ICO	Internal Clock Oscillator
ID	Identification
IMM	Interface Management Module
IRAM	Internal Random Access Memory
IT	Information Technology

ITP	Interrupt and Peripheral Event Channel Controller
ITSEF	Information Technology Security Evaluation Facility
I/O	Input/Output
MED	Memory Encryption and Decryption
MMU	Memory Management Unit
NVM	Non-Volatile Memory
OS	Operating system
ST	Security Target
PEC	Peripheral Event Channel
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
SFR	Special Function Register, as well as Security Functional Requirement, the specific meaning is given in the context
SO	Security Objective
SOLID FLASH™	An Infineon Trade Mark and Stands for Flash EEPROM Technology
SPA	Simple Power Analysis
ST	Security Target
STS	Self Test Software
SW	Software
TOE	Target of Evaluation
TM	Test Mode (STS)
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
WDT	Watch Dog Timer
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[9] 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 Lite BSI-DSZ-CC-0879-V5-2022, Version 4.6, 2022-08-18, Public Security Target M7893 B11, Infineon Technologies AG (sanitised public document)

[7] Evaluation Technical Report, Version 2, 2022-10-13, EVALUATION TECHNICAL REPORT (ETR Summary) Common Criteria CC 3.1 (EAL6 augmented with ALC_FLR.1) , TÜV Informationstechnik GmbH (confidential document)

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

[9] Security Target BSI-DSZ-CC-0879-V5-2022, Version 4.6, 2022-08-18, Confidential Security Target M7893 B11, Infineon Technologies AG (confidential document)

[10] ETR for composite evaluation according to AIS 36 for the Product BSI-DSZ-CC-0879-V5-2022, Version 2, 2022-10-13, EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP), Common Criteria CC 3.1 (EAL6 augmented with ALC_FLR.1), TÜV Informationstechnik GmbH (confidential document)

[9] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 14, Version 7, Anforderungen an den Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 9, Anwendungshinweise und Interpretationen zum Schema (AIS)
- 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 38, Version 2, Reuse of evaluation results
- AIS 41, Version 2, Anleitungen zur Erstellung von Protection Profiles and Security Targets
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren
- AIS 47, Version 1.1, Regelungen zur Zertifizierung von Entwicklungs- und Produktionsstandorten nach Common Criteria (Site Certification)

[11] Configuration list for the TOE of BSI-DSZ-CC-0879-V5-2022, Version 3.1, 2022-06-14, Chipcard and Security, Configuration Management Scope ALC, M7893 B11, Infineon Technologies AG (confidential document)

[12] SLE70 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox User Interface (2.03.008),v2.03.008,2021-07-27, Infineon Technologies AG

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

[14] 16-bit Controller Family SLE 70 Programmer's Reference Manual, v9.14, 2019-12-03, Infineon Technologies AG

[15] M7893 Errata Sheet, v5, 2020-05-07, Infineon Technologies AG

[16] M7893 Hardware Reference Manual, v3.0, 2019-06-24, Infineon Technologies AG

[17] AMM Advanced Mode for NRG SAM Addendum to M7893 Hardware Reference Manual, v2.0, 2019-10-22, Infineon Technologies AG

[18] SLx70 Family Secure Hash Algorithm SHA-2 (SHA 256/224, SHA 512/384) Library Version V1.01, 2020-08-19, Infineon Technologies AG

[19] M7893 Security Guidelines, 2022-08-18, Infineon Technologies AG

[20] SLx 70 Family Production and Personalization User' Manual, 2015-04-01, Infineon Technologies AG

[21] Cryptographic Standards Compliance Verification Report, Version 2, 2022-05-30, SINGLE EVALUATION REPORT ADDENDUM to ETR-Part ASE Cryptographic Standards Compliance Verification , 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 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 C: Overview and rating of cryptographic functionalities implemented in the TOE

Annex B of Certification Report BSI-DSZ-CC-0879-V5-2022

Evaluation results regarding development and production environment

The IT product Infineon Security Controller M7893 B11 with optional RSA2048 v2.03.008, SHA-2 V1.01, Toolbox v2.03.008 and with specific IC dedicated software (firmware), (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations 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 19 October 2022, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.5, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_FLR.1, ALC_LCD.1, ALC_TAT.3)

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

Beside the production and development sites, the relevant TOE distribution centres are as follows:

Distribution Center name	Company name and address
DHL Singapore	DHL Supply Chain Singapore Pte Ltd., Advanced Regional Center Tampines LogisPark 1 Greenwich Drive Singapore 533865
IFX Morgan Hill	Infineon Technologies North America Corp. 18275 Serene Drive Morgan Hill, CA 95037 USA
K&N Großostheim	Kühne & Nagel Stockstädter Strasse 10 63762 Großostheim Germany
KWE Shanghai	KWE Kintetsu World Express (China) Co., Ltd. Shanghai Pudong Airport Pilot Free Trade Zone No. 530 Zheng Ding Road Shanghai, P.R. China

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.

Annex C of Certification Report BSI-DSZ-CC-0879-V5-2022

Overview and rating of cryptographic functionalities implemented in the TOE

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
1	Cryptographic Primitive	TDES	[NIST SP800-67]	|k| = 112, 168	No
2	Cryptographic Primitive	TDES in ECB mode	[NIST SP800-67], [NIST SP800-38A]	|k| = 112, 168	No
3	Cryptographic Primitive	RSA encryption/ decryption/ signature generation/ verification (only modular exponentiation part)	[PKCS #1], [IEEE_P1363]	Modulus length = 1976 - 2048	Yes
4		Physical True RNG PTG.2	[AIS31]	N/A	N/A
5		SHA-{256, 512} (SW)	[FIPS180-4]	None	N/A
6		SHA-256 (HW)	[FIPS180-4]	None	N/A

Table 3: TOE cryptographic functionality

Referenced documents in Table 3:

[NIST SP800-67] NIST Special Publication 800-67 – Revision 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher – Revised November 2017, National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce.

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

[FIPS180-4] *FIPS BUB 180-4 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Secure Hash Standard (SHS),* August 2015, U.S. department of Commerce / National Institute of Standards and Technology.

[IEEE_P1363] *IEEE Standard Specifications for Public-Key Cryptography,* January 2000, Microprocessor and Microcomputer Standards Committee of the IEEE Computer Society.

[PKCS #1] *RSA Cryptography Specifications Version 2.2*, November 2016, Internet Engineering Task Force (IETF).

Note: End of report