

Certification Report

BSI-DSZ-CC-0782-V5-2020

for

Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013 or v2.07.003, EC v1.02.013 or v2.07.003, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013 or v2.07.003, and Toolbox v1.02.013 or v2.07.003 libraries 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-0782-V5-2020 (*)

Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013 or v2.07.003, EC v1.02.013 or v2.07.003, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013 or v2.07.003, and Toolbox v1.02.013 or v2.07.003 libraries and with specific IC dedicated software (firmware)

from Infineon Technologies AG

PP Conformance: Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007

Functionality: PP conformant plus product specific extensions
Common Criteria Part 2 extended

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



SOGIS
Recognition Agreement



The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

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

Bonn, 26 November 2020

For the Federal Office for Information Security

Sandro Amendola
Head of Division

L.S.



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



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..... | 12 |
| 3. Security Policy..... | 16 |
| 4. Assumptions and Clarification of Scope..... | 16 |
| 5. Architectural Information..... | 17 |
| 6. Documentation..... | 18 |
| 7. IT Product Testing..... | 18 |
| 8. Evaluated Configuration..... | 18 |
| 9. Results of the Evaluation..... | 19 |
| 10. Obligations and Notes for the Usage of the TOE..... | 23 |
| 11. Security Target..... | 24 |
| 12. Regulation specific aspects (eIDAS, QES)..... | 24 |
| 13. Definitions..... | 24 |
| 14. Bibliography..... | 26 |
| C. Excerpts from the Criteria..... | 28 |
| D. Annexes..... | 29 |

A. Certification

1. Preliminary Remarks

Under the BSIG¹ 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 Security¹
- BSI Certification and Approval Ordinance²
- BSI Schedule of Costs³
- 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 3.1⁴ [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 3 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.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.

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 Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013 or v2.07.003, EC v1.02.013 or v2.07.003, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013 or v2.07.003, and Toolbox v1.02.013 or v2.07.003 libraries and with specific IC dedicated software (firmware), has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0782-V4-2018. Specific results from the evaluation process BSI-DSZ-CC-0782-V4-2018 were re-used.

The evaluation of the product Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013 or v2.07.003, EC v1.02.013 or v2.07.003, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013 or v2.07.003, and Toolbox v1.02.013 or v2.07.003 libraries and with specific IC dedicated software (firmware), was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 9 November 2020. 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

⁵ Information Technology Security Evaluation Facility

26 November 2020 is valid until 25 November 2025. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

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

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

6. Publication

The product Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013 or v2.07.003, EC v1.02.013 or v2.07.003, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013 or v2.07.003, and Toolbox v1.02.013 or v2.07.003 libraries and with specific IC dedicated software (firmware) has been included in the BSI list of certified products, which is published regularly (see also Internet: <https://www.bsi.bund.de> and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer⁶ 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 Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013 or v2.07.003, EC v1.02.013 or v2.07.003, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013 or v2.07.003, and Toolbox v1.02.013 or v2.07.003 libraries and with specific IC dedicated software (firmware). The TOE provides a real 16-bit CPU-architecture and is compatible to the Intel 80251 architecture. The major components of the core system are the dual CPU (Central Processing Units), the MMU (Memory Management Unit) and MED (Memory Encryption/Decryption Unit). The dual interface controller is able to communicate using either the contact based or the contactless interface.

The TOE consists of a hardware, a firmware and a software part. The software part can be separated into the cryptographic libraries SCL, RSA, EC and SHA-2, as well as the supporting libraries Toolbox and Base. The SCL, RSA, EC, SHA-2 and Toolbox libraries provide the smartcard embedded software with specific functionalities. The Toolbox- and Base libraries do not implement any security functionality.

This TOE is intended to be used in smart cards for particularly security relevant applications and for its previous use as developing platform for smart card operating systems. The term Smartcard Embedded Software is used in the following for all operating systems and applications stored and executed on the TOE. The TOE is the platform for the Smartcard Embedded Software.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007 [8].

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

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 7. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

| TOE Security Functionality | Addressed issue |
|----------------------------|---|
| SF_DPM | Device Phase Management |
| SF_PS | Protection against Snopping |
| SF_PMA | Protection against Modification Attacks |
| SF_PLA | Protection against Logical Attacks |
| SF_CS | Cryptographic Support |

Table 1: TOE Security Functionalities

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

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 4.1.2. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [9], chapter 4.3, 4.1 and 4.2, respectively.

This certification covers the configurations of the TOE as outlined in chapter 8.

Compared to the previous certification of M7892 B11 (BSI-DSZ-CC-0782-V4-2018) a variety of penetration tests have been renewed. Also, several new production and distribution sites have been added, some former sites have been removed. - Moreover:

- Guidance Documentation has been updated.
- RSA-4K *encryption* is no longer part of the TOE.
- For Crypto-Lib v.1.02.013, ECC key lengths 160 and 163 Bit have been *excluded*.

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). See also section 9.2 of this certification report.

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:

Infinion Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013 or v2.07.003, EC v1.02.013 or v2.07.003, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013 or v2.07.003, and Toolbox v1.02.013 or v2.07.003 libraries and with specific IC dedicated software (firmware)

The following table outlines the TOE deliverables:

| No. | Type | Item / Identifier | Release / Version | Form of Delivery / Evaluator's comments |
|-----|------|---|--|---|
| 1. | HW | M7892 Security Controller | B11 (produced in Dresden) | Complete module, package, with or without inlay mounting, in form of plain wafers, in an IC case or in bare dies. |
| 2. | FW | STS Self Test Software (the IC Dedicated Test Software) | FW Identifier 78.015.14.0 or 78.015.14.1 or 78.015.14.2 | Stored in the ROM on the IC (patch in NVM). |

| No. | Type | Item / Identifier | Release / Version | Form of Delivery / Evaluator's comments |
|-----|------|--|--|---|
| 3. | FW | RMS Resource Management System (the IC Dedicated Support Software) | FW Identifier 78.015.14.0 or 78.015.14.1 or 78.015.14.2 | Stored in a reserved area of the ROM on the IC (patch in NVM). |
| 4. | FW | SAM Service Algorithm Minimal | FW Identifier 78.015.14.0 or 78.015.14.1 or 78.015.14.2 | Stored in a reserved area of the ROM on the IC (patch in NVM). |
| 5. | FW | NRG software interface routines | FW Identifier 78.015.14.0 or 78.015.14.1 or 78.015.14.2 | Stored in a reserved area of the ROM on the IC (patch in NVM). |
| 6. | FW | Flash Loader | FW Identifier 78.015.14.0 or 78.015.14.1 or 78.015.14.2 | Stored in a reserved area of the ROM on the IC (patch in NVM). |
| 7. | SW | NVM image (including Embedded Software) | – | Stored in Flash memory on the IC. |
| 8. | SW | RSA library | RSA2048 v1.02.013 / v2.07.003 RSA4096 v1.02.013 / v2.07.003 | Library files via secure iShare. Optional; depending on order. |
| 9. | SW | EC library | v1.02.013 / v2.07.003 | Library files via secure iShare. Optional; depending on order. |
| 10. | SW | SHA-2 library | v1.01 | Library files via secure iShare. Optional; depending on order. |
| 11. | SW | Toolbox | v1.02.013 / v2.07.003 | Library files via secure iShare. Optional; depending on order. |

| No. | Type | Item / Identifier | Release / Version | Form of Delivery / Evaluator's comments |
|-----|------|---|---------------------------------|--|
| 12. | SW | Base library | v1.02.013 / v2.07.003 | Library files via secure iShare. Optional; depending on presence of RSA, EC, and Toolbox library. |
| 13. | SW | SCL | v2.02.012 | Library files via secure iShare. Optional; depending on order. |
| 14. | DOC | <i>M7892 SOLID FLASH™ Controller for Security Applications Hardware Reference Manual</i> | Revision 3.0 2019-06-24 | Electronic document via secure iShare. |
| 15. | DOC | <i>M7892 Errata Sheet</i> | Revision 7.1 2019-12-18 | Electronic document via secure iShare. |
| 16. | DOC | <i>AMM Advanced Mode for NRG SAM Addendum to M7892 Hardware Reference Manual</i> | Revision 2.0 2019-10-28 | Electronic document via secure iShare. |
| 17. | DOC | <i>M7892 Security Guidelines</i> | 2020-07-17 | Electronic document via secure iShare. |
| 18. | DOC | <i>16-bit Security Controller Family SLE 70 Programmer's Reference Manual</i> | Revision 9.14 2019-12-03 | Electronic document via secure iShare. |
| 19. | DOC | <i>SLx 70 Family Production and Personalization User' Manual</i> | 2015-04-01 | Electronic document via secure iShare. |
| 20. | DOC | <i>SLE70 Crypto@2304T User Manual</i> | 2010-03-23 | Electronic document via secure iShare. |
| 21. | DOC | <i>SLE70 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox, User Interface (1.02.013)</i> | 2020-10-05 | Electronic document via secure iShare. Optional; delivered if the RSA, EC, or Toolbox library v1.02.013 is ordered. |
| 22. | DOC | <i>CL70 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox, 16-bit Security Controller, User Interface (2.07.003)</i> | 2019-05-27 | Electronic document via secure iShare. Optional; delivered if the RSA, EC, or Toolbox library v2.07.003 is ordered. |
| 23. | DOC | <i>SLx70 Family – Secure Hash Algorithm SHA-2 (SHA 256/221, SHA 512/384) Library Version V1.0.1</i> | 2020-08-19 | Electronic document via secure iShare. Optional; delivered if the SHA-2 library is ordered. |

| No. | Type | Item / Identifier | Release / Version | Form of Delivery / Evaluator's comments |
|-----|------|---|-------------------|--|
| 24. | DOC | <i>SCL78 Symmetric Crypto Library for SCP v3, DES / AES, 16-bit Security Controller, User Interface</i> | 2017-05-02 | Electronic document via secure iShare. Optional; delivered if the SCL is ordered. |

Table 2: Deliverables of the TOE

The delivery documentation describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the user's site including the necessary intermediate delivery procedures.

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 sent 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-personalisation data) 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 by M7892 B11. Another characteristic of the TOE are the chip identification data. These chip identification data is accessible via the Generic Chip Identification Mode (GCIM).

This GCIM outputs a variety of unique information in order to uniquely determine the underlying hardware configuration. Additionally, a dedicated RMS function allows a customer to extract the present hardware configuration. The firmware part of the TOE is identified also via the GCIM.

The SCL (optional), RSA (optional), EC (optional), SHA-2 (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 either by using the function `CryptoGetVersion()` for the RSA, EC, Toolbox and Base Library, by using the function `Cipher_GetVersion()` for the SCL, by using the function `sha_lib_version()` for the SHA, or by calculating the hash signatures of the provided library files. The mapping of these hash signatures to the version numbers is provided in Security Target [6] and [9], section 10.

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 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 and integrity of data by encryption and MAC calculation and to support secure authentication protocols and it will provide a true random number generator (TRNG).

Furthermore, the TOE provides the user with the optional SCL library, which is used to provide a high level interface to the TDES and AES calculations of the symmetric coprocessor of the TOE.

The RSA library is used to provide a high level interface to RSA (Rivest, Shamir, Adleman) cryptography implemented on the hardware component Crypto@2304T and includes countermeasures against SPA, DPA and DFA attacks. The EC library is used to provide a high level interface to Elliptic Curve cryptography implemented on the hardware component Crypto@2304T and includes countermeasures against SPA, DPA and DFA attacks.

As the TOE is a hardware security platform, the security policy of the TOE is also to provide protection against leakage of information (e.g. to ensure the confidentiality of cryptographic keys during AES, Triple-DES, RSA and EC cryptographic functions performed by the TOE), against physical probing, against malfunctions, against physical manipulations and against abuse of functionality. Hence, the TOE shall

- maintain the integrity and the confidentiality of data stored in the memory of the TOE and
- maintain the integrity, the correct operation and the confidentiality of security functionalities (security mechanisms and associated functions) provided by the TOE.

Specific details concerning the above mentioned security policies can be found in chapter 7 and 8 of the Security Target [6] and [9].

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:

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

The objective OE.Plat-Appl states that the IC Embedded Software Developer shall design his software so that the requirements from the data sheet, the TOE application notes, other guidance documents and findings of the TOE evaluation report are implemented. As all these documents are identified as parts of the TOE and delivered to the IC Embedded Software Developer, the objective OE.Plat-Appl is fulfilled.

The objective OE.Resp-Appl states that the IC Embedded Software Developer shall treat user data (especially keys) appropriately. The IC Embedded Software Developer gets sufficient information on how to protect user data adequate in the security guidelines [21].

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

5. Architectural Information

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

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

The two cryptographic coprocessors serve the need of modern cryptography: The symmetric coprocessor (SCP) combines both AES and Triple-DES with dual-key or triple-key hardware acceleration. The Asymmetric Crypto Coprocessor, called Crypto@2304T in the following, is optimized for RSA-2048 bit (4096-bit with CRT) and Elliptic Curve (EC) cryptography.

The software part of the TOE consists of the cryptographic RSA-, EC-, SCL and the SHA-2 libraries and the supporting Toolbox and Base libraries. The Base library is used internally by the RSA, the EC and the Toolbox library, thus if one of the aforementioned libraries is ordered, the Base library will be automatically included in the delivery.

The Flash Loader is a piece of software located in the ROM, but some parts of it are also stored in the SOLID FLASH™ NVM. It enables the download of the user software or parts of it to the SOLID FLASH™ NVM. After completion of the download the Flash Loader shall be locked by the user.

For more details please refer to the Security Target [6] and [9], chapters 1.3 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 were divided into five categories:

- Simulation tests (design verification),
- Qualification tests,
- Verification Tests,
- Security Evaluation Tests,
- Production Tests.

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

The evaluator was able to repeat the tests of the developer by 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 evaluator, 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 M7892 B11 (produced in Dresden, Germany).

Depending on the blocking configuration, a M7892 B11 product can have e.g. different user available memory sizes and can come with or without individual accessible cryptographic coprocessors.

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

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

- The availability of the cryptographic coprocessors.
- The user has the free choice for combinations of optional cryptographic libraries. The TOE can be delivered with either v1.02.013 or v2.07.003 (or none) of these libraries.
- The availability of the Flash Loader for available interfaces like ISO-7816, contactless ISO-14443.
- The availability of various interface options.
- The possibility to tailor the product by blocking on his own premises.
- The degree of freedom of the chip configuration is predefined by Infineon Technologies AG and made available via the order tool.

All possible TOE configurations equal and/or within the below specified ranges are covered by the certificate. Note that there is no user available on-chip ROM module anymore. The user software and data are now located in a dedicated and protected part of the SOLID FLASH™ NVM. According to the BPU option, a not limited number of configurations of the TOE may occur in the field. The number of various configurations depends on the user and purchase contract only.

9. Results of the Evaluation

9.1. CC specific results

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

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

The following guidance specific for the technology was used:

- The Application of CC to Integrated Circuits
- The Application of Attack Potential to Smartcards
- Functionality classes and evaluation methodology of physical random number generators

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

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

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

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

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

- The components ALC_FLR.1 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0782-V4-2018, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on newly conducted penetration tests and adjustment of guidance documentation.

The evaluation has confirmed:

- PP Conformance: Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007 [8]
- for the Functionality: PP conformant plus product specific extensions
Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
EAL 6 augmented by ALC_FLR.1

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (<https://www.bsi.bund.de>).

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context) only.

Note in particular:

- RSA-4K *encryption* is no longer part of the TOE.
- For Crypto-Lib v.1.02.013, ECC key lengths 160 and 163 Bit have been *excluded*.

| No. | Purpose | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Security Level above 100 Bits |
|-----|-------------------------|--------------------------------------|-----------------------------------|--|-------------------------------|
| 1 | Key Agreement | ECDH | [ANS X9.63], [ISO_15946-3] | Key sizes corresponding to the used elliptic curves P-{192, 224}, K-233, B-233 [FIPS186-4] and brainpoolP{192, 224}r1, brainpoolP{192, 224}t1 [RFC5639] | no |
| 2 | | ECDH | [ANS X9.63], [ISO_15946-3] | Key sizes corresponding to the used elliptic curves P-{256, 384, 521}, K-409, B-{283, 409} [FIPS186-4], brainpoolP{256,320,384,512}r1, brainpoolP{256,320,384,512}t1 [RFC5639] | yes |
| 3 | Cryptographic Primitive | TDES | [NIST SP800-67] | k = 112 (legacy mode), 168 | 168 Bit: yes |
| 4 | | TDES in ECB mode | [NIST SP800-67], [NIST SP800-38A] | k = 112 (legacy mode), 168 | no |
| 5 | | TDES in Blinding Feedback Mode (BLD) | Proprietary | k = 112 (legacy mode), 168 | no |
| 6 | | TDES in CBC, CFB and CTR mode | [NIST SP800-67], [NIST SP800-38A] | k = 112 (legacy mode), 168 | 168 Bit: yes |
| 7 | | TDES in Recrypt | proprietary | k = 112 (legacy mode), 168 | 168 Bit: yes |
| 8 | | TDES in CBC-MAC and CBC-MAC-ELB | [NIST SP800-67], [ISO_15946-3] | k = 112 (legacy mode), 168 | no |
| 9 | | AES | [FIPS197] | k = 128, 192, 256 | yes |
| 10 | | AES in ECB mode | [FIPS197], [NIST SP800-38A] | k = 128, 192, 256 | no |
| 11 | | AES in CBC, CFB and CTR mode | [FIPS197], [NIST SP800-38A] | k = 128, 192, 256 | yes |
| 12 | AES in Recrypt Mode | proprietary | k = 128, 192, 256 | yes | |

| No. | Purpose | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Security Level above 100 Bits |
|-----|---------|--|---|--|-------------------------------|
| 13 | | AES in Blinding Feedback Mode (BLD) | proprietary | k = 128, 192, 256 | no |
| 14 | | AES in CBC-MAC and CBC-MAC-ELB | [FIPS197], [ISO_9797-1] | k = 128, 192, 256 | no |
| 15 | | RSA encryption / decryption / signature generation / verification (only modular exponentiation part) | [PKCS #1], [IEEE_P1363] | Modulus length = 1976 – 4096 (for <i>Encryption</i> : TOE only covers modulus length up to 2048) | yes |
| 16 | | RSA key Generation using CryptoGenerate Prime (only valid for ACL v2.07.003) | Proprietary The generated keys meet [PKCS #1], Sections 3.1 and 3.2 and [IEEE_P1363], Section 8.1.3.1. | k = 1976 - 4096 | yes |
| 17 | | RSA key Generation using CryptoGenerate PrimeMask (only valid for ACL v2.07.003) | Proprietary The generated keys meet [PKCS #1], Sections 3.1 and 3.2 and [IEEE_P1363], Section 8.1.3.1. | k = 1976 - 4096 | <i>Not rated by BSI</i> |
| 18 | | ECDSA signature generation / verification / key generation | [ANS X9.62], [IEEE_P1363], [ISO_14888-3], [ISO_15946-1], [ISO_15946-2] | Key sizes corresponding to the used elliptic curves P-{192, 224}, K-233, B-233 [FIPS186-4] and brainpoolP{192, 224}r1, brainpoolP{192, 224}t1 [RFC5639] | no |
| 19 | | ECDSA signature generation / verification / key generation | [ANS X9.62], [IEEE_P1363], [ISO_14888-3], [ISO_15946-1], [ISO_15946-2] | Key sizes corresponding to the used elliptic curves P-{256, 384, 521}, K-409, B-{283, 409} [FIPS186-4], brainpoolP{256,320,384,512}r1, brainpoolP{256,320,384,512}t1 [RFC5639] | yes |
| 20 | | Physical True | [AIS31] | N/A | n/a |

| No. | Purpose | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Security Level above 100 Bits |
|-----|---------|-------------------------|----------------------------|------------------|-------------------------------|
| | | RNG PTG.2 | | | |
| 21 | | SHA-{256, 512} | [FIPS180-4] | None | n/a (keyless operation) |

Table 3: TOE cryptographic functionality

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 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].

At the point in time when evaluation and certification results are reused there might be an update of the document "ETR for composite evaluation" available. Therefore, the certified products list on the BSI website has to be checked for latest information on reassessments, recertifications or maintenance result available for the product.

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

- All security hints described in the delivered documents [12] to [22] have to be considered.

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

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 |
| 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 |
| CCRA | Common Criteria Recognition Arrangement |
| CC | Common Criteria for IT Security Evaluation |
| CEM | Common Methodology for Information Technology Security Evaluation |
| cPP | Collaborative Protection Profile |
| Crypto2304T | Asymmetric Cryptographic Processor |
| CRC | Cyclic Redundancy Check |
| CRT | Chinese Remainder 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 |
| ETR | Evaluation Technical Report |
| GCIM | Generic Chip Identification Mode |
| IT | Information Technology |
| ITSEF | Information Technology Security Evaluation Facility |
| MMU | Memory Management Unit |
| PP | Protection Profile |
| PRNG | Pseudo Random Number Generator |
| RNG | Random Number Generator |
| SAR | Security Assurance Requirement |
| SFP | Security Function Policy |
| SFR | Security Functional Requirement |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Functionality |

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 TOE⁷
<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/zertifizierungsreporre>
- [6] Security Target BSI-DSZ-CC-0782-V5-2020, Version 4.1, 2020-10-21, "Confidential Security Target M7892 B11 Recertification Common Criteria CCv3.1 EAL6 augmented (EAL6+)", Infineon Technologies AG (confidential document)
- [7] Evaluation Technical Report for BSI-DSZ-CC-0782-V5-2020, Version 5, 2020-11-06, "Evaluation Technical Report – ETR (Summary)", TÜV Informationstechnik GmbH, (confidential document)
- [8] Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007

⁷specifically

- AIS1, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers, Version 14, 11.10.2017,
- AIS14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 03.08.2010,
- AIS19, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC, Version 9, 03.11.2014,
- AIS20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 15.05.2013,
- AIS25, Anwendung der CC auf Integrierte Schaltungen, Version 9, 15.03.2017,
- AIS26, Evaluationsmethodologie für in Hardware integrierte Schaltungen, Version 10, 03.07.2017,
- AIS31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 15.05.2013,
- AIS32, CC-Interpretationen im deutschen Zertifizierungsschema, Version 7, 08.06.2011,
- AIS34, Evaluation Methodology for CC Assurance Classes for EAL5+, Version 3, 03.09.2009,
- AIS35, Öffentliche Fassung eines Security Target (ST-lite), Version 2, 12.11.2007,
- AIS36, Kompositionsevaluierung, Version 5, 15.03.2017,
- AIS38, Wiederverwendung von Evaluationsergebnissen, Version 2, 28.09.2007,
- AIS46, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, Version 3, 04.12.2013.

- [9] Security Target BSI-DSZ-CC-0782-V5-2020, Version 4.1, 2020-10-21, "Security Target Lite M7892 B11 Recertification Common Criteria CCv3.1 EAL6 augmented (EAL6+)" (sanitised public document)
- [10] ETR for composite evaluation according to AIS 36 for the Product BSI-DSZ-CC-0782-V5-2020, Version 5, 2020-11-06, "Evaluation Technical Report for composite Evaluation (ETR Comp)", TÜV Informationstechnik GmbH (confidential document)
- [11] Configuration list for the TOE, Version 3.0, 2017-09-29, "Configuration Management Scope ALC for Common Criteria with Evaluation Assurance Level EAL6 augmented (EAL6+) M7892 B11" (confidential document)
- [12] SCL78 Symmetric Crypto Library for SCPv3 DES / AES 16-bit Security Controller User Interface, 2017-05-02, Infineon Technologies AG (confidential document)
- [13] SLE70 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox (1.02.013), 2020-10-05, Infineon Technologies AG (confidential document)
- [14] SLE70 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox (2.07.003), 2019-05-27, Infineon Technologies AG (confidential document)
- [15] Crypto@2304T User Manual, 2010-03-23, Infineon Technologies AG
- [16] 16-bit Controller Family SLE 70 Programmer's Reference Manual, 2019-12-03, Infineon Technologies AG (confidential document)
- [17] M7892 Errata Sheet, 2019-12-18, Infineon Technologies AG
- [18] M7892 SOLID FLASH Controller for Security Applications 16-bit Security Controller Family Hardware Reference Manual, Revision 3.0, 2019-06-24, Infineon Technologies AG (confidential document)
- [19] AMM Advanced Mode for NRG SAM Addendum to M7892 Hardware Reference Manual, Version 2.0, 2019-10-28, Infineon Technologies AG (confidential document)
- [20] SLx 70 Family Secure Hash Algorithm SHA-2 (SHA 256/224, SHA 512/384) Library, Version 1.01, 2020-08-19, Infineon Technologies AG (confidential document)
- [21] M7892 Security Guidelines, 2020-07-17, Infineon Technologies AG (confidential document)
- [22] 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/>

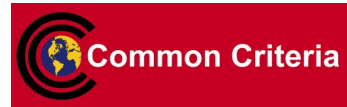
D. Annexes

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-0782-V5-2020

Evaluation results regarding development and production environment



The IT product Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013 or v2.07.003, EC v1.02.013 or v2.07.003, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013 or v2.07.003, and Toolbox v1.02.013 or v2.07.003 libraries and with specific IC dedicated software (firmware) (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations 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 26 November 2020, 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.

The relevant TOE distribution centers are as follows:

| Distribution Center name | Address |
|--------------------------|---|
| DHL Singapore | DHL Supply Chain Singapore Pte Ltd., Advanced Regional Center Tampines LogisPark 1 Greenwich Drive Singapore 533865 |
| 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 |
| 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 |

| Distribution Center name | Address |
|--------------------------|--|
| K&N Großostheim | Kühne & Nagel Stockstädter Strasse 10 63762 Großostheim Germany |

Table 4: TOE Distribution Centers

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and [9]) are fulfilled by the procedures of these sites.

Note: End of report