Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0891-V5-2021

for

Infineon Security Controller M7892 Design Steps D11 and G12, with specific IC dedicated firmware, including the Flash Loader enhanced by the Mutual Authentication Extension (MAE)

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-0891-V5-2021(*)

Smartcard Controller

Infineon Security Controller M7892 Design Steps D11 and G12, with specific IC dedicated firmware, including the Flash Loader enhanced by the Mutual Authentication Extension (MAE)

from	Infineon Technologies AG
PP Conformance:	Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014
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

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 EAL5 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, 11 October 2021

For the Federal Office for Information Security

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

Matthias Intemann
Head of Branch

L.S.

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....10
2. Identification of the TOE....11
3. Security Policy....14
4. Assumptions and Clarification of Scope....14
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....19
12. Regulation specific aspects (eIDAS, QES)....20
13. Definitions....20
14. Bibliography....22

C. Excerpts from the Criteria....24

D. Annexes....25

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 (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]

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 Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

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

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

4. 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 Design Steps D11 and G12, with specific IC dedicated firmware, including the Flash Loader enhanced by the Mutual Authentication Extension (MAE), has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0891-V4-2019. Specific results from the evaluation process BSI-DSZ-CC-0891-V4-2019 were re-used.

The evaluation of the product Infineon Security Controller M7892 Design Steps D11 and G12, with specific IC dedicated firmware, including the Flash Loader enhanced by the Mutual Authentication Extension (MAE), was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 11 October 2021. 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

[5] Information Technology Security Evaluation Facility

maximum validity of the certificate has been limited. The certificate issued on 11 October 2021 is valid until 10 October 2026. 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 Design Steps D11 and G12, with specific IC dedicated firmware, including the Flash Loader enhanced by the Mutual Authentication Extension (MAE), has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[6] Infineon Technologies AG
Am Campeon 1-12
85579 Neubiberg

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is the **Infineon Security Controller M7892 Design Steps D11 and G12, with specific IC dedicated firmware, including the Flash Loader enhanced by the Mutual Authentication Extension (MAE)**.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014 [8].

The Target of Evaluation (TOE) is the Infineon Technologies AG Security Controller (Integrated Circuit IC), M7892 Design Steps D11 and G12 with specific IC dedicated 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 two CPUs (Central Processing Units), the MMU (Memory Management Unit), and the 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 the hardware part and the firmware part.

This TOE is intended to be used in smart cards for particularly security relevant applications and as a 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 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 all selected from Common Criteria Part 2. Thus, the TOE is CC Part 2 conformant.

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:

TOE Security Functionality	Addressed issue
	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_CS	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 to seven privileged levels and gives the software the possibility to define different access rights.
SF_MAE	Mutual Authentication Extension (optional): In TOE provides a mutual authentication between production equipment and the TOE according to ISO 9798-2. Only if the production equipment was successfully authenticated by an external authenticate command, the Flash Loader is activated to download software to the TOE's Non Volatile Memory. Furthermore, it contains an internal authenticate command by which the authenticity of a copy of the TOE can be verified.

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 4.1.3. 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, 4.4.2.

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

The vulnerability assessment results, as stated within this certificate, do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

Infineon Security Controller M7892 Design Steps D11 and G12, with specific IC dedicated firmware, including the Flash Loader enhanced by the Mutual Authentication Extension (MAE),

The hardware part of the TOE is identified by M7892 G12 and D11. Another characteristic of the TOE are the chip identification data. These chip identification data is accessible via the Generic Chip Identification Mode (GCIM).

Apart from the GCIM data, the individual TOE hardware is uniquely identified by a 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 following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	M7892 Security Controller	D11 or G12	Complete modules, with or without inlay mounting, in form of plain wafers or in any IC case (for example TSSOP28, VQFN32, VQFN40, CCS-modules, etc.) or in bare dies or whatever type of package or even in no package.
2	FW	STS Self-Test Software (the IC Dedicated Test Software), RMS Resource Management System (the IC Dedicated Support Software), SAM (Service Algorithm Minimal), NRG[7] Software Interface Routines, and FL (Flash Loader)	FW Identifier 78.015.14.0 or 78.015.14.1 or 78.015.14.2 or 78.015.18.2	Stored in reserved area of the ROM on the IC (patch in NVM)
		Mutual Authentication Extension (MAE)	v8.00.006	Optional; depending on order.
3	SW	NVM image (including Embedded Software)	-	NVM image (including Embedded Software)
4	DOC	M7892 SOLID FLASH™ Controller for Security Applications Hardware Reference Manual [17]	2019-06-24	-
5		SLx 70 Family Production and Personalization User's Manual [13]	2015-04-01	-
6		16-bit Controller Family SLE 70 Programmer's Reference Manual [11]	2019-12-03	-
7		M7892 Security Guidelines [12]	2021-08-04	-
8		M7892 Errata Sheet [15]	2019-12-18	-
9		SLE70 Crypto@2304T User Manual [16]	2010-03-23	Optional; delivered if asymmetric crypto co-processor is ordered.
10		AMM Advanced Mode for NRG SAM Addendum to M7892 Hardware Reference Manual [18]	2019-10-28	Optional; delivered if AMM is ordered.
11		Production and Personalization Mutual Authentication Extension for the SLx70 family in 90 nm [14]	2017-07-26	Optional; delivered if the MAE is ordered.

[7]NRG does not provide any TOE security functionality (TSF) and is not part of the evaluation.

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.

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.

In general, the TOE - or parts thereof - are delivered between the following three parties (as defined in [8]):

- IC Embedded Software Developer,
- TOE Manufacturer (compromises all roles before TOE delivery),
- Composite Product Manufacturer (compromises all roles after TOE delivery except the end consumer).

Accordingly, three different delivery procedures have to be taken into consideration:

1. Delivery of the IC dedicated software components (IC dedicated SW, guidance) from the TOE Manufacturer to the IC Embedded Software Developer.
2. Delivery of the IC Embedded Software (ROM / Flash data, initialisation and pre-personalisation data) from the IC Embedded Software Developer to the TOE Manufacturer.
3. 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 M7892 G12 and D11. 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 (see [11] section 9.16) allows a customer to extract the present hardware configuration and the original Chip Identifier Byte, which was valid before blocking.

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

For further, detailed information regarding TOE identification see [9], section 1.1.

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. In principle, 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.

These functionalities cover the following issues:

Therefore, the TOE will implement a symmetric cryptographic block cipher algorithm (TDES and AES) to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols and it will provide a true random number generator (TRNG).

Furthermore, the TOE provides the user with an optional MAE firmware component, which safeguards the access to the Flash Loader and thus, the secure download of the user software or parts of it to the SOLID FLASH™ NVM.

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 or TDES cryptographic functions performed by the TOE), against physical probing, against malfunctions, against physical manipulations, and against abuse of functionality.

In more general and CC formal terms, besides providing certain secrutiy functionalities, the TOE shall

●maintain the integrity and the confidentiality of data stored in the memory of the TOE.

●maintain the integrity, the correct operation and the confidentiality of security functionalities (security mechanisms and associated functions) provided by the TOE.

Specific details concerning the above-mentioned security policies can be found in Chapter 7 and 8 of the Security Target (ST) [6],[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 includes one security objective for the IC Embedded Software Developer, the objective OE.Resp-Appl:

● 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 adequately in the security guidelines [12].

The ST includes four security objectives for the operational environment (for the Composite Product Manufacturer), the objectives OE.Process-Sec-IC, OE.Lim_Block_Loader, OE.Loader_Usage/Package1+ and OE.TOE_Auth:

● OE.Process-Sec-IC states that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible

copy, modification, retention, theft or unauthorised use). This means that the phases after TOE delivery are assumed to be protected appropriately.

The Composite Product Manufacturer therefore has to be informed only about the general requirement resulting from OE.Process-Sec-IC. The Composite Product Manufacturer is informed about these requirements resulting from OE.Process-Sec-IC in [13].

● OE.Lim_Block_Loader states that the Composite Product Manufacturer will protect the Loader functionality against misuse, limit the capability of the Loader and terminate irreversibly the Loader after intended usage of the Loader.

This objective is relevant for the Composite Product Manufacturer. He is responsible for permanently deactivating the flash loader (if the flash loader is available) before delivery to the end user.

● OE.Loader_Usage/Package1+ states that the authorized user must fulfil the access conditions required by the Loader, whereby the OE.TOE_Auth states that the operational environment shall support the authentication verification mechanism and know authentication reference data of the TOE.

● The Composite Product Manufacturer is informed about these requirements resulting from OE.Process-Sec-IC and OE.Lim_Block_Loader in [13] and [11, section 15.1].

The requirements resulting from OE.Loader_Usage/Package1+ and OE.TOE_Auth are given in [14].

Details can be found in the Security Target [6] and [9], chapter 4.

5. Architectural Information

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 two CPUs (Central Processing Units), the MMU (Memory Management Unit), and the MED (Memory Encryption/Decryption Unit). The dual interface controller is able to communicate using either the contact based or the contactless interface.

The flexible memory concept consists of ROM- and Flash-memory as part of the non volatile memory (NVM), respectively Infineon® SOLID FLASH™. For the Infineon® SOLID FLASH™ memory the Unified Channel Programming (UCP) memory technology is used. 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 Infineon® SOLID FLASH™.

The TOE consists of the hardware part and the firmware part.

This TOE is intended to be used in smart cards for particularly security relevant applications and as a 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.

Regarding the security functionality of the TOE, the Symmetric Crypto coprocessor (SCP) is of special importance. The SCP provides functionalities for symmetric cryptography. The TOE can be ordered with or without the SCP. If a TOE is ordered without SCP, it is deactivated during the manufacturing process and cannot be reactivated by the user. Deselecting the SCP has no impact on any other security policy of the TOE. It is exactly equivalent to the situation where the user decides just not to use the functionality.

Further, the TOE can be ordered with or without the Asymmetric Crypto Coprocessor (Crypto@2304T). If a TOE is ordered without Crypto@2304T, it is deactivated during the manufacturing process and cannot be reactivated by the user. Please note that the Crypto@2304T does not implement any SFR.

An overview of the hardware of the TOE is given in [6] chapter 1.1 / 2.2.1

The Flash Loader is a firmware located in the IFX-ROM (Read-Only Memory) and enables the download of the user software or parts of it to the Infineon® SOLID FLASH™ memory. After completion of the download, the Flash Loader shall be locked by the by the user.

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 following groups of tests were performed by the developer:

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

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

The 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.

In the course of the evaluation of the TOE the following classes of tests were carried out:

- Module tests,
- Simulation tests,
- Emulation tests,
- Tests in user mode,
- Tests in test mode,
- Hardware tests,
- MAE tests.

With these kinds of tests the entire security functionality of the TOE was tested.

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 that 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:

- Hardware tests,
- MAE tests.

Depending on the blocking configuration a M7892 product can have a different user available configuration as described in Security Target [6] and [9], chapter 1.1 and 1.2.

- 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 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 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 non limited number of configurations of the TOE may occur in the field. The number of various configurations depends on the order 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(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.

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-0891-V4-2019, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on penetration test updates, changes to the software, security claims and guidance. As a result, guidance documentation has been updated ([11],[12],[15]).

The evaluation has confirmed:

PP Conformance:	Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014 [8]
for the Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
for the Assurance:	Common Criteria Part 3 conformant 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 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.

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 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 [11], [12], [15] to [18] have to be considered.

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

- All security hints described in [13] and [14] have to be considered.

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

- The IC Embedded Software Developer can deliver his software either to Infineon to let them implement it in the TOE (in Flash memory) or to the Composite Product Manufacturer to let him download the software in the Flash memory.
- The delivery procedure from the IC Embedded Software Developer to the Composite Product Manufacturer is not part of this evaluation and a secure delivery is required.

11. Security Target

For the purpose of publishing, the Security Target [9] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of

the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
API	Application Programming Interface
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
CI	Chip Identification Mode (STS-CI)
CIM	Chip Identification Mode (STS-CI), same as CI
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard; symmetric block cipher algorithm
EAL	Evaluation Assurance Level
EC	Elliptic Curve Cryptography
ECC	Error Correction Code
Flash EEPROM	Flash Memory
FL	Flash Loader software
FW	Firmware
GCIM	Generic Chip Identification Mode
HW	Hardware
IC	Integrated Circuit
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
N/A	Not applicable

NVM	Non-Volatile Memory
PP	Protection Profile
RMS	Resource Management System
SAM	Service Algorithm Minimal
SAR	Security Assurance Requirement
SCP	Symmetric Cryptographic Processor
SF	Security Feature
SFP	Security Function Policy
SFR	Security Functional Requirement
SO	Security Objective
ST	Security Target
STS	Self-Test Software
SW	Software
TDES	triple DES
TOE	Target of Evaluation
TM	Test Mode (STS)
TSF	TOE Security Functionality
UM	Userr Mode (STS)

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[8]
https://www.bsi.bund.de/AIS

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

[8] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 9, Verbindlich Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluierungen
- AIS 38, Version 2, Reuse of evaluation results

[6] Security Target BSI-DSZ-CC-0891-V5-2021, Version 3.6, 2021-08-05, “Security Target Common Criteria EAL6 augmented / EAL6+ M7892 Design Steps D11 and G12”, Infineon Technologies AG (confidential document)

[7] Evaluation Technical Report for certification BSI-DSZ-CC-0891-V5-2021, Version 4, 2021-10-08, “Evaluation Technical Report Summary (ETR Summary)”, TÜV Informationstechnik GmbH (confidential document)

[8] Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014

[9] Security Target Lite for BSI-DSZ-CC-0891-V5-2021, Version 3.6, 2021-08-05 , “Security Target Lite Common Criteria EAL6 augmented / EAL6+ M7892 Design Steps D11 and G12”, Infineon Technologies AG (sanitised public document)

[10] ETR for composite evaluation (according to AIS 36) for BSI-DSZ-CC-0891-V5-2021, Version 4, 2021-10-08, “Evaluation Technical Report for Composite Evaluation (ETR Comp)”, TÜV Informationstechnik GmbH (confidential document)

[11] 16-bit Security Controller Family SLE 70 Programmer’s Reference Manual, v9.14, 2019-12-03, Infineon Technologies AG

[12] M7892 Security Guidelines , 2021-08-04, Infineon Technologies AG

[13] SLx 70 Family Production and Personalization User’s Manual, 2015-04-01, Infineon Technologies AG

[14] Production and Personalization Mutual Authentication Extension for SLx 70 family in 90 nm, Rev. 1.2, 2017-07-26, Infineon Technologies AG

[15] M7892 Errata Sheet, v7.1,2019-12-18, Infineon Technologies AG

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

[17] M7892 SOLID FLASH™ Controller for Security Applications Hardware Reference Manual, V3.0, 2019-06-24, Infineon Technologies AG

[18] AMM Advanced Mode for NRG SAM Addendum to M7892 Hardware Reference Manual, V2 , 2019-10-28, Infineon Technologies AG

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-0891-V5-2021

Evaluation results regarding development and production environment

The IT product Infineon Security Controller M7892 Design Steps D11 and G12, with specific IC dedicated firmware, including the Flash Loader enhanced by the Mutual Authentication Extension (MAE), (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 11 October 2021, 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_LCD.1, ALC_TAT.3)

are fulfilled for the development and production sites of the TOE listed below:

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
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,

Distribution Center Name	Address
	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-0891-V5-2021

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, yes
		AES	[FIPS197]	|k| = 128, 192, 256	yes
2	Confidentiality	TDES in ECB mode, CBC mode	[NIST SP800-38A]	|k| = 112, 168	no, yes (CBC) no (ECB)
3		TDES in Recrypt mode, BLD mode	Proprietary implementation	|k| = 112, 168	no (BLD)
4		AES in ECB mode, CBC mode	[FIPS197], [NIST SP800-38A]	|k| = 128, 192, 256	no (ECB) yes (CBC)
5	RNG	Physical True RNG PTG.2	[AIS31]	N/A	N/A

Table 3: TOE cryptographic functionality

Note: End of report