Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1110-V4-2021

for

Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions

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-1110-V4-2021 (*)

Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions

SOGIS
Recognition Agreement

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 Basic Flaw Remediation

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

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

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

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

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

Bonn, 4 August 2021

For the Federal Office for Information Security

Sandro Amendola
Head of Division

L.S.

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

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

This page is intentionally left blank.

Contents

A. Certification

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]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.

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

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

3 BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

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

3. Recognition Agreements

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

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

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

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

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

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

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

3.2. International Recognition of CC – Certificates (CCRA)

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

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

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

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

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

4. Performance of Evaluation and Certification

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

The product Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1110-V3-2020. Specific results from the evaluation process BSI-DSZ-CC-1110-V3-2020 were re-used.

The evaluation of the product Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 22 July 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 maximum validity of the certificate has been limited. The certificate issued on 4 August 2021 is valid until 3 August 2026. Validity can be re-newed by re-certification.

[5] Information Technology Security Evaluation Facility

The owner of the certificate is obliged:

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

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

6. Publication

The product Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions h as been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[6] Infineon Technologies AG
Am Campeon 1-15
85579 Neubiberg

B. Certification Results

The following results represent a summary of

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

1. Executive Summary

The Target of Evaluation (TOE) is the Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions.

It 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 MED (Memory Encryption/Decryption Unit). The dual interface controller is able to communicate using either the contact based or the contactless interface.

This TOE is intended to be used in smart cards for particular 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 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 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 Basic Flaw Remediation.

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

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

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

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [9], chapter 7.4 (Security Requirements Rationale).

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.

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 IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions.

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/ SW	IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h and IFX_CCI_000022h design step H13. with dedicated firmware as given in the ST [6] and [9] Firmware (TSF parts) includes: • BOS, • Flash Loader (optional), • RMS. Non-TSF parts are: • NRG, • RFAPI.	HW-Version: H13 FW-Version 80.100.17.0 or 80.100.17.1 or 80.100.17.2 or 80.100.17.3 Note: The two production lines can be identified via GCIM (see [6] and [9], section 2.2.6).	Postal transfer in cages or metal boxes (see [6] and [9], section 2.2.5).
2	SW	Libraries (to be chosen optionally):		Secure download (L251 Library File) via ishare.
		Base library (to be chosen depending on presence of RSA, EC, and Toolbox)	v2.08.007 or v2.07.003 or v2.06.003 or v3.33.003	

No	Type	Identifier	Release	Form of Delivery
		RSA2048,	V2.06.003 or V2.07.003 or V2.08.007 or V3.33.003	
		RSA4096,	V2.06.003 or V2.07.003 or V2.08.007 or V3.33.003	
		EC,	V2.06.003 or V2.07.003 or V2.08.007 or V3.33.003	
		Toolbox (not in scope of evaluation; not part of TSF),	V2.06.003 or V2.07.003 or V2.08.007 or V3.33.003	
		HSL,	V01.22.4346 or V02.01.6634 or V03.11.8339 or V03.12.8812	
		SCL,	V02.02.010 or V02.04.002 or V02.13.001	
		NRG, (not in scope of evaluation; not part of the TSF)	V02.04.3957	
		CIPURSE™ CL	V2.00.0004	
		Hash Crypto Lib (HCL)	V1.12.001	
3	Doc	16-bit Security Controller – V01 Errata sheet [13]	Rev.11.0, 2019-11-26	Secured download via ishare or on demand via encrypted email.
4	Doc	16-bit Security Controller – V01 Hardware Reference Manual [12]	Rev. 7.0, Infineon, 2019-06-11	Secured download via ishare or on demand via encrypted email.
5	Doc	16-Bit Security Controller - V01, Security Guidelines [11]	Rev. 1.01-2596, Infineon, 2020-08-20	Secured download via ishare or on demand via encrypted email.
6	Doc	CIPURSE™ Crypto Library, CCLX2xCIP v02.00.0004, CIPURSE™ V2, Compliant to OSPT™ Alliance CIPURSE™ V2 Cryptographic Protocol, User Interface [19]	Rev. 1.6, Infineon, 2018-02-02	Personalized PDF via secured download or on demand via encrypted mail.

No	Type	Identifier	Release	Form of Delivery
7	Doc	ACL52-Crypto2304T-C65 Asymmetric Crypto Library, RSA / ECC / Toolbox, 16-bit Security Controller, User Interface, [14]	Rev. 2.08.007, Infineon, 2021-05-17	Personalized PDF via secured download or on demand via encrypted mail.
8	Doc	CL52 Asymmetric Crypto Library for Crypto@2304T, RSA/ECC/Toolbox, 16-bit Security Controller, User Interface also [14]	Rev. 2.07.003, Infineon, 2021-05-17	Personalized PDF via secured download or on demand via encrypted mail.
9	Doc	CL52 Asymmetric Crypto Library for Crypto@2304T, RSA/ECC/Toolbox, 16-bit Security Controller, User Interface (with included Errata Sheet of 10th May 2017) also [14]	Rev. 2.06.003, Infineon, 2021-05-14	Personalized PDF via secured download or on demand via encrypted mail.
10	Doc	ACL52-Crypto2304T-C65 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox 16-bit Security Controller User interface manual also [14]	Rev. 3.33.003, Infineon, 2021-04-15	Personalized PDF via secured download or on demand via encrypted mail.
11	Doc	Crypto@2304T V3 User manual [15]	Rev. 1.4.1, Infineon, 2014-11-10	Secured download via ishare or on demand via encrypted email.
12	Doc	Hardware Support Library for SLCx2 (HSL) as active document [18]	1st version: Rev. 01.22.4346 (2016), Infineon, 2nd version: Rev. 02.01.6634 (2017-03-01), Infineon, 3rd version: Rev. 03.11.8339 (2018-07-12), Infineon, 4th version: Rev. 03.12.8812 (document v1.1, 2019-07-08), Infineon,	Personalized PDF via secured download or on demand via encrypted mail.

No	Type	Identifier	Release	Form of Delivery
13	Doc	Production and Personalization, 16-bit Security Controller in 65 nm [17]	Rev. 3.6, Infineon, 2019-06-24	Secured download via ishare or on demand via encrypted email.
14	Doc	16-bit Security Controller 65-nm Technology, Programmer's Reference Manual [16]	Rev. 9.14, Infineon, 2019-12-03	Secured download via ishare or on demand via encrypted email.
15	Doc	SCL52 Symmetric Cryptogaphic Library for DES / AES, 16-bit Security Controller, User Interface (2.02.010) [20]	Version 2.02.010, Infineon, 2016-12-09	Personalized PDF via secured download or on demand via encrypted mail.
		SCL52 Symmetric Cryptogaphic Library for DES / AES, 16-bit Security Controller, User Interface (2.04.002) also [20]	Version 2.04.002, Infineon, 2018-05-22	
		SCL52-SCP-v4-C65 Symmetric Cryptographic Library for SCP-v4 AES/DES/MAC, 16-bit Security Controller, User Interface also [20]	Version 2.13.001, Infneon, 2020-11-05	
		HCL52-CPU-C65 Hash Crypto Library for CPU SHA 16-bit Security Controller User interface manual [22]	Version 1.12.001, 2020-01-14	

Table 2: Deliverables of the TOE

Please note that NRG functionality, RFAPI and toolbox are out of scope of this evaluation, hence no evaluated TOE guidance documentation applies. However, respective developer provided documentation may be available. User discretion is advised.

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 send by the TOE Manufacturer and the version received by the Composite Product Manufacturer.

Three different delivery procedures have to be taken into consideration:

- Delivery of the IC dedicated software components (IC dedicated SW, guidance) from the TOE Manufacturer to the IC Embedded Software Developer.

- Delivery of the IC Embedded Software (ROM / Flash data, initialisation and pre-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) or any other packaging form as offered.

Respective distribution centers are listed in Appendix B (see end of document).

The individual TOE hardware is uniquely identified by its identification data. 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 IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h and IFX_CCI_000022h design step H13.

Another characteristic of the TOE are the chip identification data. These chip identification data is accessible via the Generic Chip Identification Mode (GCIM), especially the distinction between both wafer fab lines (see [6] and [9], section 2.2.6).

At TOE start-up the so called GCIM can be chosen by applying special signalling in contactless or contact based communication and the TOE outputs then the generic chip identification data (unless another configuration option is chosen). This data contain the firmware identifier accompanied with the certification identifier, the design step and even more tracking information. In combination with [12] (section 6.5) the user can identify the data, interpret it and retrieve the TOE versioning information. This information includes also the required mapping of firmware identifier and certification identifier.

The optional software libraries can be identified by their unique version numbers and by calculating a hash value (e.g. SHA-256) over the delivered lib-files (.lib) and comparing the calculated vales to the values stated in Security Target [6] and [9], section 11.

3. Security Policy

The security policy enforced is defined by the selected set of security functional requirements and implemented by the TOE. It covers the following issues:

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

The RSA library (all versions) 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 (all versions) 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.

Furthermore, the TOE also contains an (optional) version of the CIPURSE™ Cryptographic Library (CCL), which can be used to implement a CIPURSE™ V2 conformant protocol in the IC embedded software.

Besides that, the TOE can come with the optional Hardware Support Library (HSL in four alternative versions) providing a simplified interface for NVM management and provides the possibility to write tearing safe into the 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, 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 sections 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 and measures to be taken by the IT environment, the user or the risk manager.

The following topics are of relevance:

The ST includes the following security objective for the IC embedded software developer: OE.Resp-Appl.

The objective OE.Resp-Appl states that the IC embedded software developer shall treat user data (especially keys) of the composite product appropriately. The IC embedded software developer gets sufficient information on how to protect user data adequately in the security guidelines [11].

The ST includes the following security objectives for the operational environment, which are relevant for the Composite Product Manufacturer: OE.Process-Sec-IC, OE.Lim_Block_Loader, OE.Loader_Usage and OE.TOE_Auth.

The objective OE.Process-Sec-IC requires the protection of the TOE, as well as of its manufacturing and test data up to the delivery to the end-consumer. As defined in [6] and [9], section 2.2.5, the TOE can be delivered to the composite product manufacturer after phase 3 or after phase 4. However, the single chips are identical in all cases. This means that the test mode is deactivated and the TOE is locked in the user mode. Therefore it is not necessary to distinguish between these forms of delivery. Since the developer has no information about the security requirements of the implemented IC embedded software it is not possible to define any actual security requirements for the environment of the composite product manufacturer.

The objective OE.TOE_Auth requires that the environment has to support the authentication and verification mechanism and has to know the corresponding

authentication reference data. The composite product manufacturer receives sufficient information with regard to the authentication mechanism in [17], section 3.2.2.

The objective OE.Loader_Usage requires that the authorised user has to support the trusted communication with the TOE by protecting the confidentiality and integrity of the loaded data and he has to meet the access conditions defined by the flash loader. [17], section 3 provides sufficient information regarding this topic.

The objective OE.Lim_Block_Loader requires the composite product manufacturer to protect the loader against misuse, to limit the capability of the loader and to terminate the loader irreversibly after the intended usage. The permanent deactivation of the flash loader is described in [17], section 3.5.3. This objective for the environment originates from the “Package 1: Loader dedicated for usage in secured environment only”. However, this TOE also implements “Package 2: Loader dedicated for usage by authorized users only” and thus the flash loader can also be used in an unsecure environment and is able to protect itself against misuse if the authentication and download keys are handled appropriately.

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] and [9], chapter 2.1.

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 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 linear addressable memory space for each privilege level and a simple scalable Memory Management concept. The flexible memory concept consists of ROM- and Flash-memory as part of the non volatile memory (NVM). There is no user available on-chip ROM module. The user software and data are now located in a dedicated and protected part of the NVM.

The two cryptographic co-processors serve the need of modern cryptography: The symmetric co-processor (SCP) combines both AES and Triple-DES with dual-key or triple-key hardware acceleration. The Asymmetric Crypto Co-processor is used for RSA and Elliptic Curve (EC) cryptography.

The software part of the TOE consists of the cryptographic CIPURSE™, EC-, RSA- and symmetric cryptography libraries and the supporting Toolbox libraries (note: Toolbox library is out of scope of the certification).

The Flash Loader is a firmware located in the ROM and enables the download of the user software or parts of it to the NVM. After completion of the download and before delivery the final user the Flash Loader shall be locked 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

Regarding functional testing:

Different classes of functional tests were performed by the developer to test the TOE:

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

The developer's testing results demonstrate that the TSFs behave as specified. The developer's testing results also demonstrate that the TOE behaves as expected.

In the course of the evaluation of the TOE, the following classes of functional tests were carried out by the ITSEF:

- Module tests,
- Simulation tests,
- Emulation tests,
- Tests in user mode,
- Tests in test mode,
- Hardware tests,
- Optional library tests,
- repetition of developer tests (see above).

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

The results of the (functional) developer tests, which have been repeated by the evaluator, matched the results the developer stated.

Overall the TSF has been functionally tested against the functional specification, the TOE design and the security architecture description. The tests demonstrate that the TSF performs as specified.

Regarding AVA related tests:

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential high was actually successful in the TOE's operational environment as defined in [6] and [9], provided that all measures required by the developer are applied.

The embedded software has to implement the security advices given in [11] - [20].

8. Evaluated Configuration

The evaluated derivate of the TOE is IFX_CCI_000003h (with options/other identifiers, see below), H13 with firmware and optional software libraries (CIPURSE™ CL, RSA2048 2k and 4k, EC, Toolbox, HSL, NRG, SCL) with revisions stated in section 2. The flash loader (part of FW) was enabled on evaluated derivative.

An extensive overview over all possible configuration options is given in the Security Target [6] and [9] in table 4.

The evaluation results, also including results of tests performed by the developer, are valid for all hardware derivates of the configuration IFX_CCI_000003h H13 (including all further identifiers 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 00022h in design step H13). All identifiers represent the equal hardware platform but name differences in configurations or market segments. Configuration differences are achieved by blocking only. The firmware and optional software libraries (RSA2048 2k and 4k, EC, Toolbox, NRG, HSL, SCL libraries, CIPURSE™) were examined in those revisions, which are stated in table 2 (above).

The evaluation results are valid for all configurations and blocking options of the hardware stated in table 4 of the Security Target [6] and [9]. Depending on configuration, blocking option and on selection of optional software libraries, some of the services might be unavailable to the user. The unavailable services have no security impact on the TOE. The user must ensure a working configuration, e.g. the RAM size shall be selected to fulfill the minimum requirement of RSA library, if it was also selected as an option. The evaluation results apply to all configurations of Flash Loader, BPU and PIN-Letter as stated in table 3 of the Security Target [6] and [9].

The evaluation results cannot be extended to further versions/derivates of the TOE and/or other production sites without any extra investigations.

Developer and evaluator tested the TOE in these configurations in which the TOE is delivered and which is described above and in Section 2.

9. Results of the Evaluation

9.1. CC specific results

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

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

The following guidance specific for the technology was used:

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 1, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers, Version 14, 2017-10-11, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 2010-08-03, Bundesamt für Sicherheit in der Informationstechnik.

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 19, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 9, 2014-11-03, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 2013-05-15, Herausgeber: Zertifizierungsstelle des BSI im Rahmen des Zertifizierungsschemas, Bundesamt für Sicherheit in der Informationstechnik.
- A proposal for: Functionality classes for random number generators, W. Killmann, W. Schindler, Version 2.0, 2011-09-18, T-Systems GEI GmbH and Bundesamt für Sicherheit in der Informationstechnik. (same as [AIS31_KS2011])
- Developer evidence for the evaluation of a deterministic random number generator, Version 0.9, 2013-02-28, Bundesamt für Sicherheit in der Informationstechnik.
- Evaluation Report as part of the Evaluation Technical Report, Part B – ETR-Part Deterministic Random Number Generator, Template-Version 0.10, 2013-02-28, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 23, Zusammentragen von Nachweisen der Entwickler, Version 4, 2017-03-15, Bundesamt für Sicherheit in der Informationstechnik.
- CC Supporting Document Guidance – Collection of Developer Evidence, Version 1.5, April 2012, CCDB-2012-04-005.
- Joint Interpretation Library – Collection of Developer Evidence, Version 1.5, January 2012.
- Application Notes and Interpretation of the Scheme (AIS) – AIS 25, Anwendungen der CC auf integrierte Schaltungen, Version 9, 2017-03-15, Bundesamt für Sicherheit in der Informationstechnik.
- CC Supporting Document Mandatory Technical Document – Security Architecture requirements (ADV_ARC) for smart cards and similar devices, Version 2.1, April 2014, CCDB-2012-04-004.
- CC Supporting Document Guidance – Security Architecture requirements (ADV_ARC) for smart cards and similar devices – Appendix 1, Version 2.0, April 2012.
- CC Supporting Document Mandatory Technical Document – The Application of CC to Integrated Circuits, Version 3.0, Revision 1, March 2009, CCDB-2009-03-002.
- Joint Interpretation Library – Security Architecture requirements (ADV_ARC) for smart cards and similar devices – Appendix 1, Version 2.0, January 2012.
- Joint Interpretation Library – The Application of CC to Integrated Circuits, Version 3.0, February 2009.
- Joint Interpretation Library – Security requirements for post-delivery code loading, Version 1.0, February 2016.
- Validity of conducted tests on Security Smart Card ICs in dependence of test date, Version 1, 2017-03-15, Bundesamt für Sicherheit in der Informationstechnik.

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 26, Evaluationsmethodologie für in Hardware Integrierte Schaltungen, Version 10, 2017-07-03, Bundesamt für Sicherheit in der Informationstechnik.
- Auswahl geeigneter Chips für DPA-Messungen, Version 1.1, 2008-12-07, Bundesamt für Sicherheit in der Informationstechnik.
- Special Attack Methods for Smartcards and Similar Devices, Version 1.4, 2011-06-08, Bundesamt für Sicherheit in der Informationstechnik.
- CC Supporting Document Mandatory Technical Document – Requirements to perform Integrated Circuit Evaluations, Version 1.1, May 2013, CCDB-2013-05-001.
- Joint Interpretation Library – Application of Attack Potential to Smartcards, Version 3.1, 2020.
- Joint Interpretation Library – Attack Methods for Smartcards and Similar Devices, Version 2.4, 2020, confidential.
- Joint Interpretation Library – Requirements to perform Integrated Circuit Evaluations, Version 1.1, February 2013.
- Application Notes and Interpretation of the Scheme (AIS) – AIS 27, Transition from ITSEC to CC, Version 5, 2010-08-17, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 2013-05-15, Bundesamt für Sicherheit in der Informationstechnik.
- A proposal for: Functionality classes for random number generators, W. Killmann, W. Schindler, Version 2.0, 2011-09-18, T-Systems GEI GmbH and Bundesamt für Sicherheit in der Informationstechnik. (same as [AIS20_KS2011])
- Developer evidence for the evaluation of a physical true random generator, Version 0.8, 2013-02-28, Bundesamt für Sicherheit in der Informationstechnik.
- Evaluation Report as part of the Evaluation Technical Report, Part B – ETR-Part True Physical and Hybrid Random Number Generator, Template-Version 0.7, 2013-02-28, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 32, CC-Interpretationen im deutschen Zertifizierungsschema, Version 7, 2011-06-08, Bundesamt für Sicherheit in der Informationstechnik.
- Application Notes and Interpretation of the Scheme (AIS) – AIS 34, Evaluation Methodology for CC Assurance Classes for EAL5+ (CC v2.3 & v3.1) and EAL6 (CC v3.1), Version 3, 2009-09-03, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 35, Öffentliche Fassung eines Security Target (ST-lite), Version 2, 2007-11-12, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 36, Kompositionsevaluierung, Version 5, 2017-03-15, Bundesamt für Sicherheit in der Informationstechnik.

- CC Supporting Document Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, Version 1.4, December 2015, CCDB-2015-12-001.
- Joint Interpretation Library – Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018.
- CC Supporting Document Guidance – ETR template for composite evaluation of Smart Cards and similar devices, Version 1.1, December 2015, CCDB-2015-12-002.
- Joint Interpretation Library – ETR template for composite evaluation of Smart Cards and similar devices, Version 1.1, August 2015.
- Joint Interpretation Library – Certification of “open” smart card products, Version 1.1 (for trial use), 2013-02-04.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 37, Terminologie und Vorbereitung von Smartcard-Evaluierungen, Version 3, 2010-05-17, Bundesamt für Sicherheit in der Informationstechnik.
- CC Supporting Document Guidance – Smartcard Evaluation, Version 2.0, February 2010, CCDB-2010-03-001.
- Application Notes and Interpretation of the Scheme (AIS) – AIS 38, Reuse of evaluation results, Version 2, 2007-09-28, Bundesamt für Sicherheit in der Informationstechnik.
- Application Notes and Interpretation of the Scheme (AIS) – AIS 41, Guidelines for PPs and STs, Version 2, 2011-01-31, Bundesamt für Sicherheit in der Informationstechnik.
- Guidance Document – The PP/ST Guide, Version 2, Revision 0, 2010-08, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 46, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, Version 3, 2013-12-04, Bundesamt für Sicherheit in der Informationstechnik.
- Review-Protokoll zum (Krypto-)AVA-KickOff, Template-Version/Date: 2019-08-23, Bundesamt für Sicherheit in der Informationstechnik.
- Minimal Requirements for Evaluating Side-Channel Attack Resistance of Elliptic Curve Implementations, Version 1.0.4, 2011-07-01, BSI.
- Methodology for cryptographic rating of memory encryption schemes used in smartcards and similar devices, Version 1.0, 2013-10-31, BSI.
- Minimum Requirements for Evaluating Side-Channel Attack Resistance of RSA, DSA and Diffie-Hellman Key Exchange Implementations, Version 1.0, 2013-01-14, BSI.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 47, Regelungen zu Site Certification, Version 1.1, 2013-12-04, Bundesamt für Sicherheit in der Informationstechnik.
- Guidance for Site Certification, Version 1.1, 2013-12-04, Bundesamt für Sicherheit in der Informationstechnik.
- Joint Interpretation Library – Minimum Site Security Requirements, Version 3.0, 02/2020.

(see [4] for respective AIS references).

For RNG assessment the scheme interpretations AIS 20/31 was used (see [4]).

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE. Please note that those parts, which are to be read in the GBIC context (see [6] and [9] Annex, section 10), are solely relevant in the GBIC context and not in the CC context (hence for CC these are out of scope).

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 Basic Flaw Remediation augmented for this TOE evaluation.

This is a re-certification based on BSI-DSZ-CC-1110-V3-2020.

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 EAL 6 augmented by ALC_FLR.1 Basic Flaw Remediation.

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 (which originates from the ITSEF-evaluated table in [7] and in this certification report is enhanced by the 100 bit column) provides an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context) only.

Purpose / Service	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
Symmetric Cryptographic Co Processor (HW)				
Cryptographic Primitive	TDES in modes	[NIST SP800-67], [ISO_18033-3]		

Purpose / Service	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
	ECB (confidentiality)	[NIST SP800-38A]	|k| = 112, 168	No
	CBC (confidentiality)	[NIST SP800-38A]	|k| = 112, 168	168: Yes, 112: No
	CBC-MAC (integritiy)	[ISO_9797-1], [NIST SP800-38A]	|k| = 112, 168	No
	CBC-MAC-ELB (integrity)	[ISO_9797-1], [NIST SP800-38A]	|k| = {112, 168} + key length for ELB	No
Cryptographic Primitive	AES in modes	[FIPS197], [ISO_18033-3]		
	ECB (confidentiality)	[NIST SP800-38A]	|k| = 128, 192, 256	No
	CBC (confidentiality)	[NIST SP800-38A]	|k| = 128, 192, 256	Yes
	CBC-MAC (integrity)	[ISO_9797-1], [NIST SP800-38A]	|k| = 128, 192, 256	No
	CBC-MAC-ELB (integrity)	[ISO_9797-1], [NIST SP800-38A]	|k| = 128, 192, 256 + key length for ELB	No
Symmetric Cryptographic Libraries				
Cryptographic Primitive	AES in modes	[FIPS197]		
	ECB (confidentiality)	[NIST SP800-38A]	|k| = 128, 192, 256	No
	CBC, CTR, CFB (confidentiality)	[NIST SP800-38A]	|k| = 128, 192, 256	Yes
	PCBC (confidentiality)	[Schneier]	|k| = 128, 192, 256	Yes
Cryptographic Primitive	TDES in modes	[NIST SP800-67]		
	ECB (confidentiality)	[NIST SP800-38A]	|k| = 112 and 168 bits	No
	CBC, CTR and CFB (confidentiality)	[NIST SP800-38A]	|k| = 112 and 168 bits	168: Yes, 112: No
	PCBC (confidentiality)	[Schneier]	|k| = 112, 168	168: Yes, 112: No
Cryptographic Primitive	CMAC			
	TDES-CMAC (integrity) Available only with SCL v2.04.002 or SCL v2.13.001.	[NIST SP800-38B]	168	No

Purpose / Service	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
	Retail MAC (integrity) Available only with SCL v2.13.001.	[ISO_9797-1]	|k| = 168	No
	AES-CMAC (integrity) Available only with SCL v2.04.002 or SCL v2.13.001.	[NIST SP800-38B]	|k| = 128, 192, 256	No
Random Number Generation				
Cryptographic Primitive	Hybrid Physical True Random Number Generation (PTG.2, PTG.3, DRG.2, DRG.3)	Proprietary, correspond to [AIS20], or [AIS31]	N/A	N/A
RSA library v2.06.003				
	RSA encryption (confidentiality)	[PKCS #1, 5.1.1] [IEEE_P1363, 8.2.2]	512 – 2112	Yes
	RSA decryption with and without CRT (confidentiality)	[PKCS #1, 5.1.2] [IEEE_P1363, 8.2.1 (I) / 8.2.3] [PKCS #1, 5.1.2] [IEEE_P1363, 8.2.1 (II) / 8.2.3]	w/o CRT: 512 – 2112 w/ CRT: 512 – 4224	Yes
	RSA signature generation with and without CRT (authenticity)	[PKCS #1, 5.2.1] [IEEE_P1363, 8.2.1 (I) / 8.2.4] [PKCS #1, 5.2.1] [IEEE_P1363, 8.2.1 (II) / 8.2.4]	w/o CRT: 512 – 2112 w/ CRT: 512 – 4224	Yes
	RSA signature verification (only modular exponentiation part)	[PKCS #1, 5.2.2] [IEEE_P1363, 8.2.5]	512 – 4224	Yes
Key Generation	Key generation using CryptoGeneratePrimeMask	Proprietary The generated keys meet [PKCS #1], Sections 3.1 and 3.2 and [IEEE_P1363], Section 8.1.3.1.	512 – 4224	See text below table 4
RSA libraries v2.07.003 + v2.08.007 + v3.33.003				

Purpose / Service	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
	RSA encryption (confidentiality)	[PKCS #1, 5.1.1] [IEEE_P1363, 8.2.2]	512 – 2112	Yes
	RSA decryption with and without CRT (confidentiality)	[PKCS #1, 5.1.2] [IEEE_P1363, 8.2.1 (I) / 8.2.3] [PKCS #1, 5.1.2] [IEEE_P1363, 8.2.1 (II) / 8.2.3]	w/o CRT: 512 – 2112 w/ CRT: 512 – 4224	Yes
	RSA signature generation with and without CRT (authenticity)	[PKCS #1, 5.2.1] [IEEE_P1363, 8.2.1 (I) / 8.2.4] [PKCS #1, 5.2.1] [IEEE_P1363, 8.2.1 (II) / 8.2.4]	w/o CRT: 512 – 2112 w/ CRT: 512 – 4224	Yes
	RSA signature verification (only modular exponentiation part)	[PKCS #1, 5.2.2] [IEEE_P1363, 8.2.5]	512 – 4224	Yes
Key Generation	Key generation using CryptoGeneratePrime	Proprietary The generated keys meet [PKCS #1], Sections 3.1 and 3.2 and [IEEE_P1363], Section 8.1.3.1	512 – 4224	See table 4 below
	Key generation using CryptoGeneratePrimeMask (Available only with ACLv2.08.007 or ACL v2.07.003 [or ACL v2.06.003, see above])	Proprietary The generated keys meet [PKCS #1], Sections 3.1 and 3.2 and [IEEE_P1363], Section 8.1.3.1.	512 – 4224	See text below table 4

Purpose / Service	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
	Key generation using CryptoRSAKeyGenMask_PQ (Available only with ACL v3.33.003, Prime generation method follows [FIPS186-4, B.3.3] but due to key size considered proprietary.)	Proprietary The generated keys meet [PKCS #1], Sections 3.1 and 3.2, [IEEE_P1363], Section 8.1.3.1 and FIPS186-4, B.3.3] (for >= 2048 bit)	512 – 4224	512 – 2047: N/A 2048 – 4224: Yes (due to FIPS)
EC libraries v2.06.003 + v2.07.003 +v2.08.007 + v3.33.003				
	ECDSA signature generation (authenticity)	[ANS X9.62, 7.3], [ISO_14888-3, 6.4.3], [IEEE_P1363, 7.2.7]	Key sizes corresponding to the used elliptic curves NIST: P-{192, 224, 256, 384, 521}, K-{163, 233, 283, 409}, B-{233, 283, 409} [FIPS186-4]; brainpool: P{160, 192, 224, 256, 320, 384, 512}t1, P{160, 192, 224, 256, 320, 384, 512}r1 [RFC5639]	Key sizes 160, 163, 192: no Key sizes >= 224 : yes
	ECDSA signature verification (authenticity)	[ANS X9.62, 7.4.1], [ISO_14888-3, 6.4.4], [IEEE_P1363, 7.2.8]	Key sizes corresponding to the used elliptic curves NIST: P-{192, 224, 256, 384, 521}, K-{163, 233, 283, 409}, B-{233, 283, 409} [FIPS186-4]; brainpool: P{160, 192, 224, 256, 320, 384, 512}t1, P{160, 192, 224, 256, 320, 384, 512}r1 [RFC5639]	Key sizes 160, 163, 192: no Key sizes >= 224 : yes
	ECDH (key agreement)	[ANS X9.63, 5.4.1], [ISO_11770-3, D.6] [IEEE_P1363, 7.2.1]	Key sizes corresponding to the used elliptic curves NIST: P-{192, 224, 256, 384, 521}, K-{163, 233, 283, 409}, B-{163, 233, 283, 409} [FIPS186-4]; brainpool: P{160, 192, 224, 256, 320, 384, 512}t1, P{160, 192, 224, 256, 320, 384, 512}r1 [RFC5639]	Key sizes 160, 163, 192: no Key sizes >= 224 : yes
	Key generation	[ANS X9.62, A.4.3], [ISO_14888-3, 6.4.2], [IEEE_P1363, A.16.9]	Key sizes corresponding to the used elliptic curves NIST: P-{192, 224, 256, 384, 521}, K-{163, 233, 283, 409}, B-{163, 233, 283, 409} [FIPS186-4]; brainpool: P{160, 192, 224, 256, 320, 384, 512}t1, P{160, 192, 224, 256, 320, 384, 512}r1 [RFC5639]	Key sizes 160, 163, 192: no Key sizes >= 224 : yes
CIPURSE™				

Purpose / Service	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
	CIPURSE™ Session Key Agreement AES	[CIPURSE-1, 5.3], [NIST SP800-38A]	AES $\|K_0\|$ = 128 bits	Yes
	CIPURSE™ Authentication AES	[CIPURSE-1, 5.3 / 6.3], [NIST SP800-38A]	AES $\|K_0\|$ = 128 bits	Yes
	CIPURSE™ Secure Messaging for Integrity	[CIPURSE-1, 6.3], [CIPURSE-2, P.2], [NIST SP800-38A]	MAC based on AES $\|K_0\|$ = 128 bits	No
	CIPURSE™ Secure Messaging for Confidentiality	[CIPURSE-1, 6.4], [NIST SP800-38A]	AES $\|K_0\|$ = 128 bits	Yes
Hash Crypto Library (HCL)				
Hash calculations	SHA-1	[FIPS 180-4]	N/A	N/A
	SHA-224	[FIPS 180-4]	N/A	N/A
	SHA-256	[FIPS 180-4]	N/A	N/A
	SHA-384	[FIPS 180-4]	N/A	N/A
	SHA-512	[FIPS 180-4]	N/A	N/A
	SHA-512/224	[FIPS 180-4]	N/A	N/A
	SHA-512/256	[FIPS 180-4]	N/A	N/A

Table 3: TOE cryptographic functionality

In addition, the following rating applies regarding RSA key generation:

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
Key Generation (ACL v2.07.003, v2.08.007, v3.33.003)	RSA Key Generation, utilizing the preparative function “CryptoGeneratePrime()” or the function “CryptoRSAKeyGen()”	n/a	1976 - 4096	Yes

Table 4: TOE cryptographic functionality

It is explicitly remarked, that for the Cryptographic Functionalities

- CryptoGeneratePrimeMask() which might be used in conjunction with RSA Key Generation in ACL v2.07.003 and v2.08.007,
- CryptoRSAKeyGen(), CryptoGeneratePrime(), CryptoGeneratePrimeMask() and related of ACL v2.06.003

no statement on the respective cryptographic strength can be given.

Conformance evaluation and assessment to claimed cryptographic functionality standards is documented in the confidential report “Cryptographic Standards Compliance Verification” [21]

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

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

Reference of Legislatives and Standards quoted above:

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

[ANS X9.62] American National Standard for Financial Services ANS X9.62-2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), November 16, 2005, American National Standards Institute.

[ANS X9.63] American National Standard for Financial Services X9.63-2011, Public Key Cryptography for the Financial Services Industry - Key Agreement and Key Transport Using Elliptic Curve Cryptography, December 21, 2011, American National Standards Institute

[CIPURSE-1] CIPURSE(TM) V2 Cryptographic Protocol issued by OSPTTM Alliance, 2012-09-28

[CIPURSE-2] CIPURSE(TM) V2 Cryptographic Protocol issued by OSPTTM Alliance, 2014-09-18 (with errata and precision list)

[FIPS197] Federal Information Processing Standards Publication 197, Announcing the ADVANCED ENCRYPTION STANDARD (AES), 2001-11-26, National Institute of Standards and Technology (NIST)

[IEEE_P1363] IEEE P1363. Standard specifications for public key cryptography. IEEE, 2000

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

[ISO_11770-3] ISO 11770-3: Information technology - Security techniques – Key management Part 3: Mechanisms using asymmetric techniques, ISO/ IEC 11770-3:2008

[ISO_14888-3] ISO 14888-3: Information technology - Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms, ISO/IEC 14888-3:2006

[ISO_18033-3] ISO 18033-3: Information technology - Security techniques – Encryption algorithms – Part 3: Block ciphers, ISO/IEC 18033-3:2005

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

[NIST SP800-38B] NIST SP800-38A, Recommendation for Block Cipher Modes of Operation, The CMAC Mode for Authentication, 2005-05, National Institute of Standards and Technology (NIST)

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

[PKCS-1] PKCS #1: RSA Cryptography Standard, Version 2.2, October 27, 2012, RSA Laboratories

[RFC5639] RFC 5639 - Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, IETF Trust and the persons identified as the document authors, March 2010 (http://www.ietf.org/rfc/rfc5639.txt)

[Schneier] Bruce Schneier, Applied Cryptography, Second Edition, John Wiley & Sons, 1996

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.

Furthermore:

The TOE is delivered to the composite product manufacturer and to the security IC embedded software developer. The actual end-consumer obtains the TOE from the composite product issuer together with the application which runs on the TOE.

The security IC embedded software developer receives all necessary recommendations and hints to develop his software in form of the delivered documentation.

- All security hints described in the delivered documents in [11] – [20] and [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.

- All security hints described in [17] have to be considered.

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

- The security IC embedded software developer can deliver his software either to Infineon to let them implement it in the TOE (in the Flash memory) or to the composite product manufacturer to let him download the software in the Flash memory.
- The delivery procedure from the security IC embedded software developer to the composite product manufacturer is not part of this evaluation and a secure delivery is required.

11. Security Target

For the purpose of publishing, the Security Target [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

AIS	Application Notes and Interpretations of the Scheme
BOS	Boot Operating System
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

DRNG	Deterministic random number generator
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FW	Firmware
GBIC	German Banking Industry Committee
HRNG	Hybrid random number generator
HSL	Hardware Support Library
HW	Hardware
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
NVM	Non volatile memory
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
SCL	Symmetric cryptographic library
SCP	Symmetric cryptographic processor
TOE	Target of Evaluation
TRNG	True random number generator
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 TOE[7] https://www.bsi.bund.de/AIS

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

[6] Confidential Security Target for BSI-DSZ-CC-1110-V4-2021, Version 3.4, 2021-05-18, “Confidential Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h design step H13”, Infineon Technologies AG (confidential document)

[7] Evaluation Technical Report for the Product BSI-DSZ-CC-1110-V4-2021, Version 1, 2021-07-01, “Evaluation Technical Report - 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] Public Security Target BSI-DSZ-CC-1110-V4-2021, Version 1.9, 2021-05-18, “Public Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h design step H13”, Infineon Technologies AG (sanitised public document)

[7] See section 9.1 on usage of specific AIS.

[10] ETR for composite evaluation according to AIS 36 for the Product BSI-DSZ-CC-1110-V4-2021, Version 1, 2021-07-01, ETR for composite evaluation (EFC), TÜV Informationstechnik GmbH (confidential document)

[11] See table 2 in section B.2

[12] See table 2 in section B.2

[13] See table 2 in section B.2

[14] See table 2 in section B.2

[15] See table 2 in section B.2

[16] See table 2 in section B.2

[17] See table 2 in section B.2

[18] See table 2 in section B.2

[19] See table 2 in section B.2

[20] See table 2 in section B.2

[21] “Cryptographic Standards Compliance Verification”, Version 1, 2020-04-20, TÜV Informationstechnik GmbH (confidential document)

[22] See table 2 in section B.2

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-1110-V4-2021

Evaluation results regarding development and production environment

The IT product Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions (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 4 August 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_FLR.1, ALC_LCD.1, ALC_TAT.3) are fulfilled for the development and production sites of the TOE.

Besides the production and development sites, 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 b. Coburg
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
K&N Großostheim	Kühne & Nagel Stockstädter Strasse 10 63762 Großostheim Germany

Table 5: 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