

BSI-DSZ-CC-1107-V6-2025

for

**IFX_CCI_00002Dh, IFX_CCI_000039h,
IFX_CCI_00003Ah, IFX_CCI_000044h,
IFX_CCI_000045h, IFX_CCI_000046h,
IFX_CCI_000047h, IFX_CCI_000048h,
IFX_CCI_000049h, IFX_CCI_00004Ah,
IFX_CCI_00004Bh, IFX_CCI_00004Ch,
IFX_CCI_00004Dh, IFX_CCI_00004Eh T11 with
firmware 80.306.16.0 & 80.306.16.1 & 80.312.02.0,
optional NRG™ SW 05.03.4097, opt.HSL
v3.52.9708, UMSLC lib v01.30.0564, opt. SCL
v2.15.000 and v2.11.003, opt. ACL v3.02.000 and
v3.33.003 and v3.34.000 and 3.35.001, opt. RCL
v.1.10.007, opt. HCL v1.13.002 and guidance**

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



Deutsches

erteilt vom



IT-Sicherheitszertifikat

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1107-V6-2025 (*)

Smartcard Controller

**IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah,
IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h,
IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h,
IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch,
IFX_CCI_00004Dh, IFX_CCI_00004Eh T11 with firmware 80.306.16.0 &
80.306.16.1 & 80.312.02.0, optional NRG™ SW 05.03.4097, opt.HSL
v3.52.9708, UMSLC lib v01.30.0564, opt. SCL v2.15.000 and v2.11.003,
opt. ACL v3.02.000 and v3.33.003 and v3.34.000 and 3.35.001, opt. RCL
v.1.10.007, opt. HCL v1.13.002 and guidance**

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
Common Criteria Part 2 extended

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

valid until: 9 July 2030



SOGIS
Recognition Agreement



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

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), CEM:2022 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), CC:2022. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

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

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

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

Bonn, 10 July 2025

For the Federal Office for Information Security

Sandro Amendola
Director-General

L.S.



Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 87 - 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.....	11
1. Executive Summary.....	12
2. Identification of the TOE.....	13
3. Security Policy.....	16
4. Assumptions and Clarification of Scope.....	17
5. Architectural Information.....	18
6. Documentation.....	18
7. IT Product Testing.....	18
8. Evaluated Configuration.....	19
9. Results of the Evaluation.....	20
10. Obligations and Notes for the Usage of the TOE.....	33
11. Security Target.....	34
12. Regulation specific aspects (eIDAS, QES).....	34
13. Definitions.....	34
14. Bibliography.....	36
C. Excerpts from the Criteria.....	39
D. Annexes.....	40

A. Certification

1. Preliminary Remarks

Under the BSIG¹ Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security¹
- BSI Certification and Approval Ordinance²
- BMI Regulations on Ex-parte Costs³
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licensing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version CC:2022⁴ [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), CC:2022 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

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

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

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

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

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

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

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

3.2. International Recognition of CC – Certificates (CCRA)

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

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

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

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

⁴ Proclamation of the Bundesamtes für Sicherheit in der Informationstechnik vom 14. April 2023 auf <https://www.bsi.bund.de>

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 IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11 with firmware 80.306.16.0 & 80.306.16.1 & 80.312.02.0, optional NRG™ SW 05.03.4097, opt.HSL v3.52.9708, UMSLC lib v01.30.0564, opt. SCL v2.15.000 and v2.11.003, opt. ACL v3.02.000 and v3.33.003 and v3.34.000 and 3.35.001, opt. RCL v.1.10.007, opt. HCL v1.13.002 and guidance has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1107-V5-2024. Specific results from the evaluation process BSI-DSZ-CC-1107-V5-2024 were re-used.

The evaluation of the product IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11 with firmware 80.306.16.0 & 80.306.16.1 & 80.312.02.0, optional NRG™ SW 05.03.4097, opt.HSL v3.52.9708, UMSLC lib v01.30.0564, opt. SCL v2.15.000 and v2.11.003, opt. ACL v3.02.000 and v3.33.003 and v3.34.000 and 3.35.001, opt. RCL v.1.10.007, opt. HCL v1.13.002 and guidance was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 1 July 2025. 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 evaluated guidance documentation are observed,
- the product is operated in the environment as specified 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. 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

⁵ Information Technology Security Evaluation Facility

updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis. Therefore the BSI reserves the right to revoke the certificate, especially if a exploitable vulnerability of the certified product gets to known.

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 10 July 2025 is valid until 9 July 2030. 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.
4. to close the minor-nonconformities from STARs [28], [29] no later than February 2026

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 IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11 with firmware 80.306.16.0 & 80.306.16.1 & 80.312.02.0, optional NRG™ SW 05.03.4097, opt.HSL v3.52.9708, UMSLC lib v01.30.0564, opt. SCL v2.15.000 and v2.11.003, opt. ACL v3.02.000 and v3.33.003 and v3.34.000 and 3.35.001, opt. RCL v.1.10.007, opt. HCL v1.13.002 and guidance has been included in the BSI list of certified products, which is published regularly in the listing found at the BSI Website <https://www.bsi.bund.de/dok/Zertifizierung-Gesamtlisten>. Further information can be obtained from BSI-Infoline +49 (0)228 9582-111.

Further copies of this Certification Report can be requested from the developer⁶ of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

⁶ Infineon Technologies AG
Am Campeon 1-15
85579 Neubiberg

B. Certification Results

The following results represent a summary of

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

1. Executive Summary

The Target of Evaluation (TOE) is the Infineon Security Controller IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11 with firmware 80.306.16.0 & 80.306.16.1 & 80.312.02.0, optional NRG™ SW 05.03.4097, opt.HSL v3.52.9708, UMSLC lib v01.30.0564, opt. SCL v2.15.000 and v2.11.003, opt. ACL v3.02.000 and v3.33.003 and v3.34.000 and 3.35.001, opt. RCL v.1.10.007, opt. HCL v1.13.002 and guidance.

The Security Target [5] 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 [7].

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 [5] and Security Target lite [8], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
SF_DPM	Device Phase Management: The life cycle of the TOE is split up into several phases. Different operation modes help to protect the TOE during each phase of its lifecycle.
SF_PS	Protection against Snooping: The TOE uses various means to protect from snooping of memories and busses and prevents single stepping.
SF_PMA	Protection against Modifying Attacks: This TOE implements protection against modifying attacks of memories, alarm lines and sensors.
SF_PLA	Protection against Logical Attacks: The memory model of the TOE provides two distinct, independent levels and the possibility to define up to eight memory regions with different access rights enforced by the Memory Protection Unit (MPU).
SF_CS	Cryptographic Support: The TOE is equipped with several hardware accelerators and software modules to support the standard symmetric and asymmetric cryptographic operations like RSA, EC, TDES, and AES. Additionally, the TOE is equipped with a Hybrid Random Number Generator and a random crypto library providing four different modes of operation: hybrid random number generation, true random number generation, deterministic random number generation and key stream generation. Furthermore, a hash crypto library provides SHA-1 and SHA-2 generation.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [5] and Security Target lite [8], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [5] and [8], chapter 3.1.2. 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 [5] and [8], chapter 3.

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:

IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11 with firmware 80.306.16.0 & 80.306.16.1 & 80.312.02.0, optional NRG™ SW 05.03.4097, opt.HSL v3.52.9708, UMSLC lib v01.30.0564, opt. SCL v2.15.000 and v2.11.003, opt. ACL v3.02.000 and v3.33.003 and v3.34.000 and 3.35.001, opt. RCL v.1.10.007, opt. HCL v1.13.002 and guidance

The following table outlines the TOE deliverables:

No	Type	Identifier	Release Version	/	Form of Delivery
1	HW	IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh	T11 (design step)		By customer order
2	FW	BOS, RFAPI (ROM part) & POWS	80.306.16.0 80.306.16.1 80.312.02.0	or or	Stored on the delivered hardware.
3	FW	Flash Loader	09.12.0005 09.14.0002	or	Stored on the delivered hardware.
4	SW	NRG™ SW (optional)	05.03.4097		Secure download (L251 Library File) via ishare.
5	SW	HSL (optional)	v3.52.9708		Secure download (L251 Library File) via ishare.
6	SW	UMSLC	v01.30.0564		Secure download (ARM Library File) via ishare.

No	Type	Identifier	Release Version	/	Form of Delivery
7	SW	SCL (optional)	v2.15.000 v2.11.003	or	Secure download (L251 Library File) via ishare.
8	SW	ACL (optional)	v3.35.001 v3.34.000 v3.33.003 v3.02.000	or or or	Secure download (L251 Library File) via ishare.
9	SW	RCL (optional)	v1.10.007		Secure download (L251 Library File) via ishare.
10	SW	HCL (optional)	v1.13.002		Secure download (L251 Library File) via ishare.
11	DOC	32-bit Security Controller - V11, Hardware Reference Manual	v6.2 2020-12-21		Personalized PDF via secure iShare server
12	DOC	SLx1/SLx3 (40 nm) Security Controllers, Programmer's Reference Manual	v5.6 2023-07-06		Personalized PDF via secure iShare server
13	DOC	32-bit Security Controller - V11, Security Guidelines	v1.00-2976 2023-06-19		Personalized PDF via secure iShare server
14	DOC	Production and personalization, 32-bit security controller (Flash Loader 09.12.0005)	v9.12 2023-03-02		Personalized PDF via secure iShare server
15	DOC	SLx3 (40 nm) Security Controllers Production and Personalization Manual (Flash Loader 09.14.0002)	V9.14 2023-07-21		Personalized PDF via secure iShare server
16	DOC	32-bit Security Controller Crypto2304T V3, User Manual (optional)	V3.0 2024-06-21		Personalized PDF via secure iShare server
17	DOC	<i>HSL SLCx7 V11, Hardware Support Library (optional)</i>	v03.52.9708 2021-01-25		Personalized PDF via secure iShare server
18	DOC	<i>UMSLC library for SLCx7 in 40nm</i>	v01.30.0564 2019-06-19		Personalized PDF via secure iShare server
19	DOC	<i>SCL37-SCP-v440-C40 Symmetric Crypto Library for SCP-v440 AES/DES/MAC (optional)</i>	v2.11.003 2021-06-16		Personalized PDF via secure iShare server
20	DOC	<i>SCL37-SCP-v440-C40 Symmetric Crypto Library for SCP-v440 AES/DES/MAC (optional)</i>	v2.15.000 2023-07-20		Personalized PDF via secure iShare server
21	DOC	<i>ACL37-Crypto2304T-C40 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox (optional)</i>	v3.02.000 2024-08-16		Personalized PDF via secure iShare server
22	DOC	<i>ACL37-Crypto2304T-C40 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox (optional)</i>	V3.33.003 2024-08-16		Personalized PDF via secure iShare server
23	DOC	<i>ACL37-Crypto2304T-C40 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox (optional)</i>	V3.34.000 2024-08-16		Personalized PDF via secure iShare server

No	Type	Identifier	Release Version	Form of Delivery
24	DOC	<i>ACL37-Crypto2304T-C40 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox (optional)</i>	v3.35.001 2024-11-15	Personalized PDF via secure iShare server
25	DOC	<i>RCL37-X-C40 Random Crypto Library for SCP-v440 & RNG-v3 DRBG/HWRNG 32-bit Security Controller, User interface manual (optional)</i>	v1.10.007 2020-06-16	Personalized PDF via secure iShare server
26	DOC	<i>HCL37-CPU-C40 Hash Crypto Library for CPU SHA 32-bit Security Controller, User interface manual (optional)</i>	v1.13.002 2020-05-07	Personalized PDF via secure iShare server

Table 2: Deliverables of the TOE

Please note that NRG™ functionality and most toolbox functionality are out of scope of this evaluation (unless stated otherwise), 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 sent by the TOE Manufacturer and the version received by the Composite Product Manufacturer.

Three different delivery procedures have to be taken into consideration:

- Delivery of the IC dedicated software components (IC dedicated SW, guidance) from the TOE Manufacturer to the IC Embedded Software Developer.
- Delivery of the IC Embedded Software (ROM / Flash data, initialisation and pre-personalisation data) from the IC Embedded Software Developer to the TOE Manufacturer.
- Delivery of the final TOE from the TOE Manufacturer to the Composite Product Manufacturer. After phase 3 the TOE is delivered in form of wafers or sawn wafers, after phase 4 in form of modules (with or without inlay antenna) 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_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh design step T11.

Another characteristic of the TOE are the chip identification data. These chip identification data are accessible via the Generic Chip Identification Mode (GCIM) (see [11], chapter 4.5).

At TOE start-up the so called GCIM can be chosen by applying special signalling in contactless or contact based communication and the TOE then outputs the generic chip identification data (unless another configuration option is chosen). This data contains the firmware identifier accompanied with the certification identifier, the design step and even more tracking information. In combination with [11] (chapter 4.5) the user can identify the data, interpret it and retrieve the TOE versioning information. This information also includes 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 values to the values stated in Security Target [5] and Security Target Lite [8], chapters 9 - 15

3. Security Policy

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

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

The RSA library is used to provide a high-level interface to RSA (Rivest, Shamir, Adleman) cryptography implemented on the hardware component Crypto2304T and includes countermeasures against SPA, DPA and DFA attacks. The EC library is used to provide a high-level interface to Elliptic Curve cryptography implemented on the hardware component Crypto2304T and includes countermeasures against SPA, DPA and DFA attacks. The optional Hash Crypto Library provides a high-level interface for performing cryptographic hash functions and includes countermeasures against SPA, DPA and DFA attacks. The RCL provides a high-level interface for obtaining random data. This can be deterministic data from an AES CTR_DRBG or non-deterministic data that is provided by the underlying hardware. The RCL includes countermeasures against SPA, DPA and DFA attacks.

Besides that, the TOE can come with the optional Hardware Support Library (HSL) 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 security policies mentioned above can be found in chapters 6 and 7 of the Security Target [5] and Security Target lite [8].

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

The ST only includes one security objective for the IC embedded software developer:

- 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 [13].

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

- 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 the Security Target [5] and Security Target lite [8], Chapter 1.4.5 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 Infineon has no information about the security requirements of the implemented IC embedded software it is not possible to define any concrete 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 [14], chapter 1.2 an 2.1.5 / [27], chapter 1.2 an 2.1.8. Please note that this objective is only valid in case the Flash Loader is ordered with mutual authentication (i.e., option External Authentication is unavailable).
- 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. [15], chapter 4 / [26], chapter 4 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 [15], chapter 2.1.2.2 / [27], chapter 2.1.4.2. 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.

- The objective OE.Secure_Load_ACode is only applicable in life cycle phase 7 and in case of Flash Loader v09.14.0002. In this case the user software is required to support the secure image loading (during phase 7/in-field update) by providing the relevant key material for the image.
- The objective OE.Secure_Delivery complements the second item of the previous OE in case the TOE is ordered with a (temporarily) deactivated FL (Flash Loader). In this case, the customer is required to implement mechanisms to prevent attacks during TOE transport as required by the security needs of the loaded IC Embedded Software. This requirement is provided to the user as part of [14] chapter 4:

On delivery, if the application is active, then the application is responsible for transport protection.

- The objective OE.Prevent_Masquerade addresses two aspects:
 - the support of a trusted communication channel identical to OE.Loader_Usage, however, with reference to the one-way authentication (external authentication), and
 - the user is required to implement mechanisms to prevent masquerading attack in case the FL is ordered with external authentication.

The first item is addressed in [14], chapter 3 just as OE.Loader_Usage. The second item is addressed in [14], chapter 2.1.5 as follows:

- External authentication with ECB in an alternative authentication methods that is provided for backwards compatibility and smoother integration to CCM. This method is provided as an order option in SecureX, and can only be configured during Infineon production. If the external authentication method is used, then there is no protection against masquerading attacks.

5. Architectural Information

For further information on the TOE architecture, see Security Target [5] and Security Target lite [8], chapter 1 (especially chapters 1.3 and 1.4).

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 [5] and Security Target lite [8].

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 functional 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 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 penetration testing was partially performed using the developer's testing environment, partially using the test environment of the evaluation body.

All configurations of the TOE being intended to be covered by the current evaluation were tested.

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 successful in the TOE's operational environment as defined in the Security Target [5] and and Security Target lite [8], provided that all measures required by the developer are applied.

The embedded software must implement the security advice given in [11] – [25], [27] (if applicable).

8. Evaluated Configuration

An extensive overview over all possible configuration options is given in the Security Target [5] and and Security Target lite [8] in chapters 1.4.5 and 1.4.7.

This certification covers the following configurations of the TOE: The TOE is comprised of firmware and optional software libraries with revisions stated in section B.2. The flash loader (part of FW) was enabled on evaluated derivatives.

The evaluation results, also including results of tests performed by the developer, are valid for all hardware derivatives mentioned above. 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 were examined in those revisions, which are stated in table 2.

The evaluation results are valid for all configurations and blocking options of the hardware stated in chapter 1.4.7 of the Security Target [5] and Security Target lite [8]. 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. The evaluation results apply to all configurations of Flash Loader, BPU and PIN-Letter as stated in the Security Target [5] and Security Target lite [8].

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

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [6] 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.
- 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.
- 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.
- Security Architecture requirements (ADV_ARC) for smart cards, and similar devices extended to Secure Sub-Systems in SoC, Version 2.1, 2021-07, Joint Interpretation Working Group.
- CC Supporting Document Guidance – Security Architecture requirements (ADV_ARC) for smart cards and similar devices – Appendix 1, Version 2.0, April 2012.
- Joint Interpretation Library – Security Architecture requirements (ADV_ARC) for smart cards and similar devices – Appendix 1, Version 2.0, January 2012.
- The Application of CC to Integrated Circuits, Version 4.0, 2024-04, Joint Interpretation Working Group
- Security requirements for post-delivery code loading, Version 2.0, 2024-09, Joint Interpretation Working Group.
- 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.
- Special Attack Methods for Smartcards and Similar Devices, Version 1.4, 2011-06-08, Bundesamt für Sicherheit in der Informationstechnik.
- Application of Attack Potential to Smartcards and Similar Devices, Version 3.2.1, 2024-02, Joint Interpretation Working Group,
- Attack Methods for Smartcards and Similar Devices, Version 2.5 (confidential), 2022-05, Joint Interpretation Working Group.
- 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.
- 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.
- Composite product evaluation and certification, Version 1.6, 2024-04, Joint Interpretation Working Group.
- Joint Interpretation Library – Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018.
- Joint Interpretation Library – ETR template for composite evaluation of Smart Cards and similar devices, Version 1.1, August 2015.
- Certification of “open” smart card products, Version 2.0, 2024-05, Joint Interpretation Working Group,
- 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.
- 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 39, Formal Methods, Version 3, 2008-10-24, Bundesamt für Sicherheit in der Informationstechnik.
- Application Notes and Interpretation of the Scheme (AIS) – AIS 40, Use of Interpretation for Security Evaluation and Certification of Digital Tachographs, Version 1, 2005-06-28, 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.
- Application Notes and Interpretation of the Scheme (AIS) – AIS 42, Guidelines for the Developer Documentation, Version 1, 2008-05-21, 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.

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 47, Regelungen zu Site Certification, Version 1.1, 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.
- Methodology for cryptographic rating of memory encryption schemes used in smartcards and similar devices, Version 1.0, 2013-10-31, BSI.
- Guidelines for Evaluating Side-Channel-Attack Resistance of RSA, DSA and Diffie-Hellman Key Exchange Implementations, Version 2024-01, 2024-02-29, Bundesamt für Sicherheit in der Informationstechnik.
- 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 AIS20/31 was used (see [4]).

To support composite evaluations according to AIS 36 the document ETR for composite evaluation [9] was provided and approved. This document provides details of this platform evaluation that have to be considered in the course of a composite evaluation on top.

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

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

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

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-1107-V5-2024, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the change on the evaluation methodology, on changes on the guidance documents and on performing of penetration tests.

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 [7]
- for the Functionality: PP conformant
Common Criteria Part 2 extended

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

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

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

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 120 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (<https://www.bsi.bund.de>).

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 120 Bits*' of the following table with '*no*' achieves a security level of lower than 120 Bits (in general context) only.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments	Security Level above 120 Bits
Symmetric Coprocessor (SCP)						
1	Cryptographic primitive	TDES	[NIST SP800-67], [ISO_18033-3]	112, 168	-	-
2	Cryptographic primitive	AES	[FIPS197], [ISO_18033-3]	128, 192, 256	-	-
3	Confidentiality	No.1 in ECB mode for encryption and decryption	[NIST SP800-38A]	112, 168	-	No
4	Confidentiality	No.1 in CBC mode for encryption and decryption	[NIST SP800-38A]	112, 168	-	No
5	Confidentiality	No. 2 in ECB mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	-	No
6	Confidentiality	No.2 in CBC mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	-	Yes

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments	Security Level above 120 Bits
Symmetric Cryptographic Libraries (both SCLs)						
7	Cryptographic primitive	TDES	[NIST SP800-67]	112, 168	-	-
8	Cryptographic primitive	AES	[FIPS197]	128, 192, 256	-	-
9	Confidentiality	No.7 in ECB mode for encryption and decryption	[NIST SP800-38A]	112, 168	-	No
10	Confidentiality	No.7 in CBC mode for encryption and decryption	[NIST SP800-38A]	112, 168	-	No
11	Confidentiality	No.7 in CTR mode for encryption and decryption	[NIST SP800-38A]	112, 168	-	No
12	Confidentiality	No.7 in CFB mode for encryption and decryption	[NIST SP800-38A]	112, 168	-	No
13	Integrity protection	No.7 in CMAC mode for MAC generation	[NIST SP800-38B]	112, 168	-	No
14	Integrity protection	No.7 in Retail MAC (Algorithm 3) for MAC generation	[ISO9797-1]	112	-	No
15	Confidentiality	No.8 in ECB mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	-	No
16	Confidentiality	No.8 in CBC mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	-	Yes
17	Confidentiality	No.8 in CTR mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	-	Yes
18	Confidentiality	No.8 in CFB mode for encryption and	[NIST SP800-38A]	128, 192, 256	-	Yes

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments	Security Level above 120 Bits
		decryption				
19	Integrity protection	No.8 in CMAC mode for MAC generation	[NIST SP800-38B]	128, 192, 256	-	No
Asymmetric Cryptographic Library (ACL) v3.02.000						
20	Confidentiality	RSA encryption	[PKCS #1, 5.1.1], [IEEE_P1363, 8.2.2]	1024 – 2112	-	No
21	Confidentiality	RSA decryption	[PKCS #1, 5.1.2], [IEEE_P1363, 8.2.1 (I) / 8.2.3]	1024 – 2112	-	No
22	Confidentiality	decryption with CRT	[PKCS #1, 5.1.2], [IEEE_P1363, 8.2.1 (II) / 8.2.3]	1024 – 4224	-	Yes for key size >= 2800 bit
23	Authenticity	signature generation	[PKCS #1, 5.2.1], [IEEE_P1363, 8.2.1 (I) / 8.2.4]	1024 – 2112	-	No
24	Authenticity	signature generation with CRT	[PKCS #1, 5.2.1], [IEEE_P1363, 8.2.1 (II) / 8.2.4]	1024 – 4224	-	Yes for key size >= 2800 bit
25	Authenticity	signature verification	[PKCS #1, 5.2.2], [IEEE_P1363, 8.2.5]	1024 – 4224	-	Yes for key size >= 2800 bit
26	Key generation	RSA key generation returning CRT key components dp, dq and qinv (prime generation not included)	[PKCS #1, 3.1 / 3.2], [IEEE_P1363, 8.1.3.1]	1024 – 4224	Method CRT	Yes for key size >= 2800 bit
27	Key generation	RSA key generation returning key representation n and d (prime generation not included)	[PKCS #1, 3.1 / 3.2], [IEEE_P1363, 8.1.3.1]	1024 – 2112	Method n_d	No
28	Key generation	RSA key generation returning key representation p, q and d (prime	[IEEE_P1363, 8.1.3.1]	1024 – 2047	Method p_q_d; Prime generation method follows [FIPS186-4, B.3.3] but due to key size	No

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments	Security Level above 120 Bits
		generation included)			considered proprietary.	
29	Key generation	RSA key generation returning key representation p, q and d (prime generation included)	[IEEE_P1363, 8.1.3.1] [FIPS186-4, B.3.3]	2048 – 2112	Method p_q_d	No
30	N/A	Supported elliptic curves: - All curves in [FIPS186-4], - All curves in [RFC5639].	[FIPS186-4] [RFC5639]	N/A	–	-
31	Part of Cryptographic primitive	EC point addition on curves listed in No.30	N/A	160 – 521	-	Not applicable
32	Authenticity	ECDSA signature generation on curves listed in No.30	[ANS X9.62, 7.3], [IEEE_P1363, 7.2.7]	160 – 521	hash calculation of ECDSA is not implemented by the library and lies in the responsibility of the user.	No for key size 160,163,192, 224 Yes for key sizes >=250
33	Authenticity	ECDSA signature verification on curves listed in No.30	[ANS X9.62, 7.4.1] [IEEE_P1363, 7.2.8]	160 – 521	hash calculation of ECDSA is not implemented by the library and lies in the responsibility of the user.	No for key size 160,163,192, 224 Yes for key sizes >=250
34	Key agreement	Elliptic Curve Diffie-Hellman (ECDH) key agreement on curves listed in No.30	[ANS X9.63, 5.4.1] [ISO_11770-3, D.6] [IEEE_P1363, 7.2.1]	160 – 521	–	No for key size 160,163,192, 224 Yes for key sizes >=250

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments	Security Level above 120 Bits
						>=250
35	Key generation	Elliptic Curve key generation on curves listed in No.30	[ANS X9.62, A.4.3] [IEEE_P1363, A.16.9]	160 – 521	–	No for key size 160,163,192, 224 Yes for key sizes >=250
Asymmetric Cryptographic Libraries (ACLs) v3.33.003, v3.34.000 and 3.35.001						
36	Confidentiality	RSA encryption	[PKCS-1, 5.1.1] [IEEE_P1363, 8.2.2]	1024 – 4224	–	Yes for key size >= 2800 bit
37	Confidentiality	RSA decryption	[PKCS-1, 5.1.2] [IEEE_P1363, 8.2.1 (I) / 8.2.3]	1024 – 2112	–	No
38	Confidentiality	RSA decryption with CRT	[PKCS-1, 5.1.2] [IEEE_P1363, 8.2.1 (II) / 8.2.3]	1024 – 4224	–	Yes for key size >= 2800 bit
39	Authenticity	RSA signature generation	[PKCS-1, 5.2.1] [IEEE_P1363, 8.2.1 (I) / 8.2.4]	1024 – 2112	–	No
40	Authenticity	RSA signature generation with CRT	[PKCS-1, 5.2.1] [IEEE_P1363, 8.2.1 (II) / 8.2.4]	1024 – 4224	–	Yes for key size >= 2800 bit
41	Authenticity	RSA signature verification	[PKCS #1, 5.2.2] [IEEE_P1363, 8.2.5]	1024 – 4224	–	Yes for key size >= 2800 bit
42	Key generation	RSA key generation returning CRT key components dp, dq and qinv (prime generation not included)	[PKCS-1, 3.1 / 3.2] [IEEE_P1363, 8.1.3.1]	1024 – 4224	Method CRT	Yes for key size >= 2800 bit
43	Key generation	RSA key generation returning key representation n	[PKCS-1, 3.1 / 3.2] [IEEE_P1363, 8.1.3.1]	1024 – 2112	Method n_d	No

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments	Security Level above 120 Bits
		and d (prime generation not included)				
44	Key generation	RSA key generation returning key representation p, q and d (prime generation included)	[IEEE_P1363, 8.1.3.1]	1024 – 2047	Method p_q_d; Prime generation method follows [FIPS186-4, B.3.3] but due to key size considered proprietary.	No
45	Key generation	RSA key generation returning key representation p, q and d (prime generation included)	[IEEE_P1363, 8.1.3.1] [FIPS186-4, B.3.3]	2048 – 2112	Method p_q_d	No
46	Supporting Function for Cryptographic primitive (available only for ACL v3.35.001)	Prime number generation	-	length of prime: 512 – 2112 Bits	Method PRIME_GEN; Proprietary prime number generation method, which follows [PrimeGen]	Not applicable
47	Supporting Function for Cryptographic primitive	Generation of probable primes, Miller Rabin test	[FIPS186-4, B.3.3 / C.3.1]	length of prime: 512 – 2064 Bits	Method 2PRIME_GEN	Not applicable
48	Supporting Function for Cryptographic primitive	Primality test	–	length of prime: 512 – 2112 Bits	Method PRIME_CHECK; Proprietary primality test	Not applicable
49	Supporting Function for Cryptographic primitive	Primality test	[FIPS186-4, C.3.1 / C.3.2]	length of prime: 512 – 2064 Bits	Method PRIME_CHECK_M ASK	Not applicable
50	Key agreement	RSA Diffie-Hellman (DH) key agreement	[N186-4, B.5.5] [RSA-PKCSB, 5.2.1 / 5.1.2] [IEEE1336, 8.2.4 / 8.2.3]	1024 – 4224	Method RSA_DH	Yes for key size >= 2800 bit

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments	Security Level above 120 Bits
51	N/A	Supported elliptic curves: - All curves in [FIPS186-4], - All curves in [RFC5639].	[FIPS186-4], [RFC5639]	N/A	–	N/A
52	Supporting Function for Cryptographic primitive	EC point addition on curves listed in No.51	N/A	160 521	– –	Not applicable
53	Authenticity	ECDSA signature generation on curves listed in No.51	[ANS X9.62, 7.3] [IEEE_P1363, 7.2.7]	160 521	– hash calculation of ECDSA is not implemented by the library and lies in the responsibility of the user.	No for key size 160,163,192, 224 Yes for key sizes ≥250
54	Authenticity	ECDSA signature verification on curves listed in No.51	[ANS X9.62, 7.4.1] [IEEE_P1363, 7.2.8]	160 521	– hash calculation of ECDSA is not implemented by the library and lies in the responsibility of the user.	No for key size 160,163,192, 224 Yes for key sizes ≥250
55	Key agreement	Elliptic Curve Diffie-Hellman (ECDH) key agreement on curves listed in No.51	[ANS X9.63, 5.4.1] [ISO_11770-3, D.6] [IEEE_P1363, 7.2.1]	160 521	– –	No for key size 160,163,192, 224 Yes for key sizes ≥250
56	Key generation	Elliptic Curve key generation on curves listed in No.51	[ANS X9.62, A.4.3] [IEEE_P1363, A.16.9]	160 521	– –	No for key size 160,163,192, 224 Yes for key sizes ≥250

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments	Security Level above 120 Bits
57	PACE integrated mapping	Point encoding for the ECDH-integrated mapping on curves listed in No.51	[ICAO_11, B.2]	160 – 521	–	Not applicable
Flash Loader						
58	Confidentiality	No.2 in CCM mode for encryption and decryption	[NIST SP800-38C]	128	–	Not rated
59	Authenticity	No.2 in CCM mode for MAC verification	[NIST SP800-38C]	128	–	Not rated
60	Authentication	Mutual authentication protocol based on No.59	[AGD_PPUM, 2.1.5] / [AGD_PPUM_FU, 2.1.8]	128	–	Not rated
61	Authentication	External authentication protocol based on No.5	[AGD_PPUM, 2.1.5] / [AGD_PPUM_FU, 2.1.8]	128	–	Not rated
Random Number generation (Hardware)						
62	RNG	Physical RNG	PTG.2 in [AIS31]	N/A	–	Not applicable
63	RNG	Hybrid RNG	corresponds to PTG.3 in [AIS31]	N/A	–	Not applicable
64	RNG	Deterministic RNG	corresponds to DRG.3 in [AIS20]	N/A	–	Not applicable
65	RNG	Deterministic RNG	corresponds to DRG.4 in [AIS20]	N/A	–	Not applicable
Random Crypto Library (RCL) v1.10.007						
66	RNG	Physical RNG	PTG.2 in [AIS31]	N/A	The RCL acts as interface to the PTG.2 hardware RNG	Not applicable
67	RNG	Deterministic RNG	corresponds to DRG.3 in [AIS20] [NIST SP800-90A]	128, 256	CTR_DRBG	Not applicable

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments	Security Level above 120 Bits
68	RNG	Deterministic RNG	corresponds to DRG.4 in [AIS20] [NIST SP800-90A]	128, 256	CTR_DRBG	Not applicable
Hash Crypto Library (HCL) v1.13.002						
69	Hash calculation	SHA-1	[FIPS180-4]	N/A	–	Not applicable
70	Hash calculation	SHA-224	[FIPS180-4]	N/A	–	Not applicable
71	Hash calculation	SHA-256	[FIPS180-4]	N/A	–	Not applicable
72	Hash calculation	SHA-384	[FIPS180-4]	N/A	–	Not applicable
73	Hash calculation	SHA-512	[FIPS180-4]	N/A	–	Not applicable
74	Hash calculation	SHA-512/224	[FIPS180-4]	N/A	–	Not applicable
75	Hash calculation	SHA-512/256	[FIPS180-4]	N/A	–	Not applicable

Table 3: TOE cryptographic functionality

The TOE's memory encryption, named ICS ("ICS-C8") and not separately listed above, was successfully evaluated according to BSI's "Methodology for cryptographic rating of memory encryption schemes used in smartcards and similar devices" (Version 1.0, 2013-10-31).

Further conformance evaluation and assessment to claimed cryptographic functionality standards is documented in the confidential report "Cryptographic Standards Compliance Verification" [25].

Reference of Legislatives and Standards quoted above:

[AIS20] Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 2013-05-15, Bundesamt für Sicherheit in der Informationstechnik

[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
[AGD_PPUM]	see reference [14] in bibliography (chapter 14)
[FIPS186-4]	Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013, U.S. department of Commerce / National Institute of Standards and Technology (NIST)
[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_11770-3]	ISO 11770-3: Information technology - Security techniques – Key management Part 3: Mechanisms using asymmetric techniques, ISO/IEC 11770-3:2008
[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 SP800-38B, Recommendation for Block Cipher Modes of Operation, The CMAC Mode for Authentication, 2005-05, National Institute of Standards and Technology (NIST)
[NIST SP800-38C]	NIST SP800-38C, Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality, 2004-05 with updates as of 2007-07-20, 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)

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" [9].

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] – [14], [15] – [25], [27] have to be considered.
- The composite product manufacturer receives all necessary recommendations and hints to develop his software in form of the delivered documentation.

11. Security Target

For the purpose of publishing, the Security Target [8] 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 [5] 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
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
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

13.2. Glossary

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

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

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

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

Informal – Expressed in natural language.

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

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

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

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

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/CC
ISO-Version:
ISO 15408:2022, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirements_
<https://www.iso.org/standard/72891.html>
<https://www.iso.org/standard/72892.html>
<https://www.iso.org/standard/72906.html>
<https://www.iso.org/standard/72913.html>
<https://www.iso.org/standard/72917.html>
CCRA-Version:
CC:2022 R1, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirement
<https://www.commoncriteriaportal.org>
- [2] Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology
ISO-Version:
ISO 18045:2022: Information technology Security techniques Methodology for IT security evaluation
<https://www.iso.org/standard/72889.html>
CCRA-Version:
CEM:2022 R1, Common Methodology for Information Technology Security Evaluation
<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 licensing (CC-Stellen), <https://www.bsi.bund.de/zertifizierung>
- [4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE
<https://www.bsi.bund.de/AIS>
- [5] Security Target BSI-DSZ-CC-1107-V6-2025, Version 7.3, 2025-05-06, IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h,

- IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11 Security Target, Infineon Technologies AG (confidential document)
- [6] Evaluation Technical Report, Version 1, 2025-06-06, EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY), TÜV Informationstechnik GmbH, (confidential document)
- [7] Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014
- [8] Security Target Lite BSI-DSZ-CC-1107-V6-2025, Version 7.3, 2025-05-06, IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11 Security Target Lite, Infineon Technologies AG. (sanitised public document)
- [9] ETR for composite evaluation according to AIS 36 for BSI-DSZ-CC-1107-V6-2025, Version 1, 2025-06-06, EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP), TÜV Informationstechnik GmbH (confidential document)
- [10] Configuration list for the TOE, Version 2.0, 2021-03-02, "Infineon Technologies AG Chipcard and Security Evaluation Documentation Life Cycle Support", Infineon Technologies AG (confidential document)
- [11] 32-bit Security Controller – V11, Hardware Reference Manual, V6.2, 2020-12-21, Infineon Technologies AG
- [12] 32-bit Security Controller, SLx1/SLx3 Controller Family, Programmer's Reference Manual, V5.6, 2023-07-06 Infineon Technologies AG
- [13] 32-bit Security Controller – V11, Security Guidelines, V1.00-2976, 2023-06-19, Infineon Technologies AG
- [14] Production and personalization 32-bit security controller, V09.12, 2023-03-02, Infineon Technologies AG
- [15] 32-bit Security Controller, Crypto2304T V3, User Manual (optional) , V3.0, 2024-06-21, Infineon Technologies AG
- [16] HSL for SLCx7V11a Hardware Support Library (optional), V03.52.9708, 2021-01-25, Infineon Technologies AG
- [17] UMSLC library for SLCx7 in 40nm, User Mode Security Life Control, V01.30.0564, 2019-06-19, Infineon Technologies AG
- [18] SCL37-SCP-v440-C40, Symmetric Crypto Library for SCP-v440 AES/DES/MAC, 32-bit Security Controller, User interface manual (optional) V2.11.003, 2021-06-16, Infineon Technologies AG
- [19] SCL37-SCP-v440-C40, Symmetric Crypto Library for SCP-v440 AES/DES/MAC, 32-bit Security Controller, User interface manual (optional) V2.15.000, 2023-07-20, Infineon Technologies AG
- [20] ACL37-Crypto2304T-C40, Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox, 32-bit Security Controller, User interface manual (optional), V3.02.000, 2024-08-16, Infineon Technologies AG

- [21] ACL37-Crypto2304T-C40, Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox, 32-bit Security Controller, User interface manual (optional), V3.33.003, 2024-08-16, Infineon Technologies AG
- [22] ACL37-Crypto2304T-C40 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox 32-bit Security Controller User interface manual (optional), V3.34.000, 2024-08-16, Infineon Technologies AG
- [23] ACL37-Crypto2304T-C40 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox 32-bit Security Controller User interface manual (optional), V3.35.001, 2024-11-15, Infineon Technologies AG
- [24] RCL37-X-C40 Random Crypto Library for SCP-v440 & RNG-v3 DRBG/HWRNG 32-bit Security Controller, User interface manual (optional), V1.10.007, 2020-06-16, Infineon Technologies AG
- [25] HCL37-CPU-C40 Hash Crypto Library for CPU SHA 32-bit Security Controller, User interface manual (optional), V1.13.002, 2020-05-07, Infineon Technologies AG
- [26] "Cryptographic Standards Compliance Verification", Version 2, 2024-08-23, TÜV Informationstechnik GmbH (confidential document)
- [27] SLx3 (40 nm) Security Controllers Production and Personalization Manual Flash Loader V9 Field update, V09.14, 2023-07-21, Infineon Technologies AG
- [28] SITE TECHNICAL AUDIT REPORT (STAR) Infineon Technologies Dresden GmbH & Co. KG, Version 1, 2025-05-02, TÜV Informationstechnik GmbH
- [29] SITE TECHNICAL AUDIT REPORT (STAR) Infineon Technologies IT-Services GmbH, Klagenfurt, Version 1, 2025-05-02, TÜV Informationstechnik GmbH

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria in its CCRA Documents can be followed:

- On conformance claim definitions and descriptions refer to CC:2022 part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC:2022 Part 3 chapter 6.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CCRA CC:2022 Part 5.
- On the assurance class ASE for Security Target evaluation refer to CC:2022 Part 3 chapter 9
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC:2022 Part 3 chapters 7 to 15
- The table 1 in CC:2022 part 5, Chapter 4.2 summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published as the CCRA Version at
<https://www.commoncriteriaportal.org/cc/index.cfm>

The CC are published as the ISO/IEC Version at
<https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>

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-1107-V6-2025

Evaluation results regarding development and production environment



The IT product IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11 with firmware 80.306.16.0 & 80.306.16.1 & 80.312.02.0, optional NRG™ SW 05.03.4097, opt.HSL v3.52.9708, UMSLC lib v01.30.0564, opt. SCL v2.15.000 and v2.11.003, opt. ACL v3.02.000 and v3.33.003 and v3.34.000 and 3.35.001, opt. RCL v.1.10.007, opt. HCL v1.13.002 and guidance (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version CEM:2022 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 CC:2022.

As a result of the TOE certification, dated 10 July 2025, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (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 listed in Table 4:

Distribution Center name	Address
DHL Singapore	DHL Exel Supply Chain Singapore Pte Ltd., Advanced Regional Center Tampines LogisPark 1 Greenwich Drive Singapore 533865
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	Distribution Center Europe (DCE) Kühne & Nagel Stockstädter Strasse 10 63762 Großostheim Germany

Tabelle 4: TOE Distribution Centers

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [5] and Security Target lite[8]. 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 [5] and Security Target lite [8]) are fulfilled by the procedures of these sites.

Note: End of report