Federal Office
for Information Security

# Certification Report

# BSI-DSZ-CC-1102-V2-2025

for

**IFX_CCI_001Fh, IFX_CCI_002Fh, IFX_CCI_0030h, IFX_CCI_0033h, IFX_CCI_0035h, IFX_CCI_0036h, IFX_CCI_0038h in the design steps S11 and M11 with software libraries: HSL v2.62.7626 (optional) and UMSLC v01.00.0234, with specific IC-dedicated firmware (BOS and Flash Loader)**

from

**Infineon Technologies AG**

# Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

**BSI-DSZ-CC-1102-V2-2025** (*)

Smartcard Controller

**IFX_CCI_001Fh, IFX_CCI_002Fh, IFX_CCI_0030h, IFX_CCI_0033h, IFX_CCI_0035h, IFX_CCI_0036h, IFX_CCI_0038h in the design steps S11 and M11 with software libraries: HSL v2.62.7626 (optional) and UMSLC v01.00.0234, with specific IC-dedicated firmware (BOS and Flash Loader)**

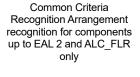| | |
|---|---|
| from | Infineon Technologies AG |
| PP Conformance: | Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014 |
| Functionality: | PP conformant plus product specific extensions Common Criteria Part 2 extended |
| Assurance: | Common Criteria Part 3 conformant EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5 |
| valid until: | 19 February 2030 |

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), 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.

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

Bonn, 20 February 2025
For the Federal Office for Information Security

Sandro Amendola                    L.S.
Director-General

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

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 und für Heimat (Federal Ministry of the Interior and Community)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), CC:2022 [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), CEM: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.     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_001Fh, IFX_CCI_002Fh, IFX_CCI_0030h, IFX_CCI_0033h, IFX_CCI_0035h, IFX_CCI_0036h, IFX_CCI_0038h in the design steps S11 and M11 with software libraries: HSL v2.62.7626 (optional) and UMSLC v01.00.0234, with specific IC-dedicated firmware (BOS and Flash Loader) has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1102-2019. Specific results from the evaluation process BSI-DSZ-CC-1102-2019 were re-used.

The evaluation of the product IFX_CCI_001Fh, IFX_CCI_002Fh, IFX_CCI_0030h, IFX_CCI_0033h, IFX_CCI_0035h, IFX_CCI_0036h, IFX_CCI_0038h in the design steps S11 and M11 with software libraries: HSL v2.62.7626 (optional) and UMSLC v01.00.0234, with specific IC-dedicated firmware (BOS and Flash Loader) was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 17 February 2025. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[4] 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

---

[4]    Information Technology Security Evaluation Facility

maximum validity of the certificate has been limited. The certificate issued on 20 February 2025 is valid until 19 February 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.

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_001Fh, IFX_CCI_002Fh, IFX_CCI_0030h, IFX_CCI_0033h, IFX_CCI_0035h, IFX_CCI_0036h, IFX_CCI_0038h in the design steps S11 and M11 with software libraries: HSL v2.62.7626 (optional) and UMSLC v01.00.0234, with specific IC-dedicated firmware (BOS and Flash Loader) has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[5] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

---

[5]     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 Smart Card IC (Security Controller) IFX_CCI_001Fh, IFX_CCI_002Fh, IFX_CCI_0030h, IFX_CCI_0033h, IFX_CCI_0035h, IFX_CCI_0036h, IFX_CCI_0038h in the design steps S11 and M11 with software libraries: HSL v2.62.7626 (optional) and UMSLC v01.00.0234, with specific IC-dedicated firmware (BOS and Flash Loader) as well as User Guidance.

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 5 augmented by ALC_DVS.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 6. 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 Modifying 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.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], 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 [6] and [9], 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_001Fh, IFX_CCI_002Fh, IFX_CCI_0030h, IFX_CCI_0033h, IFX_CCI_0035h, IFX_CCI_0036h, IFX_CCI_0038h in the design steps S11 and M11 with software libraries: HSL v2.62.7626 (optional) and UMSLC v01.00.0234, with specific IC-dedicated firmware (BOS and Flash Loader)**

The following table outlines the TOE deliverables:

| No | Type | Identifier | Release | Form of Delivery |
|---|---|---|---|---|
| 1 | HW/SW | IFX_CCI_001Fh, IFX_CCI_002Fh, IFX_CCI_0030h, IFX_CCI_0033h, IFX_CCI_0035h, IFX_CCI_0036h, IFX_CCI_0038h | S11 and M11 (produced in Singapore) | Plain wafers in an IC case or in bare dies. |
| 2 | FW | Flash Loader | v8.07.007 | Located at the end of User NVM for non-blocked derivatives. |
| 3 | DOC | BOS | FW identifier: 80.304.01.0 | Stored in IFX ROM region on IC (BOS Patch Area in IFX region on NVM). |
| 4 | SW | HSL library (optional) | v2.62.7626 | Secure download (object code) via ishare. (optional) |
| 5 | SW | UMSLC library | v01.00.0234 | Secured download (PDF) via ishare |
| 6 | DOC | 32-bit Security Controller – V15, Hardware Reference Manual | | Secured download (PDF) via ishare |
| 7 | DOC | SLx1/SLx3 (40 nm) security controllers, Programmer's Reference Manual, SLCx7_DFP | | Secured download (PDF) via ishare |
| 8 | DOC | 32-bit Security Controller – V15, Security Guidelines | | Secured download (PDF) via ishare |
| 9 | DOC | Production and personalization, 32-bit Arm-based security controller | | Secured download (PDF) via ishare |
| 10 | DOC | HSL library for SLCx7 in 40nm (optional) | | Secured download of compiled html help (chm) file via ishare. (optional) |
| 11 | DOC | UMSLC library for SLCx7 in 40nm, Version 01.00.0234 | | Secured download of compiled html help (chm) file via ishare. |

Table 2: Deliverables of the TOE

The individual TOE hardware is uniquely identified by its identification data.

As the TOE is under control of the user software, the TOE manufacturer can only guarantee the integrity up to the delivery procedure. It is in the responsibility of the composite product manufacturer to include mechanisms in the implemented software

(developed by the IC embedded software developer) which allows detection of modifications after the delivery.

<u>In detail, regarding identification:</u>

The hardware part of the TOE is identified by its Common Criteria Identifiers (CCI) IFX_CCI_001Fh, IFX_CCI_002Fh, IFX_CCI_0030h, IFX_CCI_0033h, IFX_CCI_0035h, IFX_CCI_0036h, IFX_CCI_0038h and the design steps S11 and M11. The complete chip identification data is accessible via the Generic Chip Identification Mode (GCIM). The Generic Chip Identification Mode (GCIM) can be activated after power-on with a dedicated signalling sequence and is also accessible by the user software. This GCIM outputs amongst other identifiers for the platform, chip mode, ROM code, chip type, design step, fabrication facility, wafer, die position, firmware, temperature range, system frequency and the CCI. The interpretation of the chip identification data is described in [HRM, 4.6.2].

Additionally, the customer can identify the present configuration by reading the relevant data in the IFX-Mailbox Area (see [13] section 8.10]).

Several bytes of the GCIM include the Common Criteria Certification Identifier, which can be used to uniquely identify the certified TOE. These identifiers reflect the name of the TOE as given in the ST. Note, that these identifiers are used by the developer only for this TOE and reflect the same underlying basic hardware.

In addition to the hardware part, the TOE consists of firmware parts and software parts:

The firmware part of the TOE is identified also via the GCIM. The versions for the individual firmware parts can be mapped as well as the hardware.

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

"TOE Delivery" is uniquely used to indicate

● after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or

● after Phase 4 (or before Phase 5) if the TOE is delivered in form of packaged products.

Therefore three different delivering procedures have to be taken into consideration:

● Delivery of the IC dedicated software components (IC dedicated SW, guidance) from the TOE manufacturer to the IC embedded software developer.

● Delivery of the IC embedded software (ROM / Flash data, initialisation and pre-personalization data, Bundle Business package) from the IC embedded software developer to the TOE manufacturer.

● Delivery of the final TOE from the TOE manufacturer to the composite product manufacturer. After phase 3 the TOE is delivered in form of wafers or sawn wafers, after phase 4 in form of modules (with or without inlay antenna).

The TOE is delivered via the logistics sites:

● DHL Singapore,

● KWE Shanghai,

● K&N Großostheim (Distribution Center Europe).

# 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 provide a True Random Number Generator (TRNG).

The optional HSL provides functionality via APIs to the Smartcard Embedded Software, which contains SOLID FLASH™ NVM service routines and functionality for tearing-safe programming of SOLID FLASH™ NVM.

The UMSLC library provides a wrapper around the UMSLC hardware functionality with some software measures to counter fault attacks.

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

- maintain the integrity and the confidentiality of data stored in the memory of the TOE,

and

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

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

# 4.  Assumptions and Clarification of Scope

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

The 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 [14].

The ST includes multiple objectives for the composite product manufacturer.

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 described in [6] and [9] section 1.5.5, the TOE can be delivered to the composite product manufacturer after phase 3or after phase 4 (as complete modules, plain wafers, bare dies, in any IC case, or in any type of package). However, the single chips are identical in all cases. This means that the test mode is deactivated, and the TOE is locked into 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 must support the authentication and verification mechanism and must know the corresponding authentication reference data. The composite product manufacturer receives sufficient information about the authentication mechanism in [15] chapter 3.

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] section 3.6 / 4.5.1.3.

The objective OE.Secure_Delivery is only applicable in case the TOE is ordered with a (temporarily) deactivated 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 [15] chapter 3:

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

As Infineon has no information about the security requirements of the implemented IC embedded software, it is not possible for the guidance to define any concrete security requirements for the environment of the IC Embedded Software Developer or Composite Product Manufacturer.

The objective OE.Flashing_Secured_Env requires the user to perform flashing and successful TOE authentication using the TOE's Flash Loader in a secure environment. The user is made aware of the presence of this security objective for the operational environment in the user guidance in [PPM, 1.3]. There it is stated that only certain Flash Loader versions claim compliance to the Loader Package 2 as defined in the PP for loading in insecure environments. The user should refer to the applicable certificate and Security Target to identify whether this is the case for the present TOE. The ST of the current TOE does not contain this package claim.

# 5.    Architectural Information

Detailed information in the TOE architecture is to be found in [6] and [9] sections 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.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

# 7.    IT Product Testing

The developers' testing effort can be summarised in the way described in the following:

TOE test configuration: The tests are performed with the TOE and a simulator.

Developer's testing: All TSFs and related security mechanisms, subsystems and modules are tested in order to assure complete coverage of all SFRs.

Different classes of developer tests are performed to test the TOE in a sufficient manner:

- Simulation Tests,
- *Qualification Tests / Software Verification,*
- *Verification Tests,*
- *Security Evaluation Tests,*
- *Production Tests.*

The evaluator's testing effort can be summarized in the way described in the following:

The evaluator's objective regarding this aspect was to test the functionality of the TOE, and to verify the developer's test results by repeating developer's tests and to add independent tests.

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

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

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

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; moreover, no attack scenario with the attack potential high was actually successful.

## 8.    Evaluated Configuration

This certification covers the following configurations of the TOE: Smartcard IC IFX_CCI_001Fh, IFX_CCI_002Fh, IFX_CCI_0030h, IFX_CCI_0033h, IFX_CCI_0035h, IFX_CCI_0036h, IFX_CCI_0038h S11 and M11 (Singapore).

Hardware configuration:

The hardware of the TOE can be ordered with different SOLID FLASH™ and RAM sizes (up to 240 kB SOLID FLASH™ and up to 12 kB RAM). The configuration (as listed in [6] and [9], Table 3) can be done during the manufacturing process of the TOE according to the choice of the user.

Firmware configuration:

The firmware of the TOE comprises the BOS (FW identifier provided in Table 4) and the Flash Loader (version provided in Table 4). The latter can be configured in three different ways as outlined in the following:

- Option 1: The user or/and a subcontractor downloads the software into the SOLID FLASH™ memory. Infineon Technologies does not receive any user software.

  - Flash Loader can be activated or reactivated by the user or subcontractor to download software into the SOLID FLASH™ memory.

- Option 2: The user provides software to download into the SOLID FLASH™ memory to Infineon Technologies AG. The software is loaded into the SOLID FLASH™ memory during chip production.

  - No Flashloader present.

- Option 3: The user provides software to download into the SOLID FLASH™ memory to Infineon Technologies AG. The software is loaded into the NVM memory during chip production.

  - Flash Loader is blocked by Infineon but can be activated or reactivated by the user or subcontractor to download software into the SOLID FLASH™ memory. The user is required to provide a reactivation procedure as part of the software to Infineon Technologies AG

An overview about the different Flash Loader options is also given in [6] and [9] (section 1.4.8).

Optional software libraries:

Based on the library selection, the TOE can be delivered with or without the functionality of the HSL. This is considered in the developer documentation and corresponding notes are added where required.

If the user decides not to use the HSL, it is not delivered to the user and the accompanying additional specific security functionality as listed in Table 9 is not provided by the TOE. Upon deselection of a library, the code implementing the functionality is excluded and thus this functionality is not available to the user.

Excluding the code of the deselected functionality has no impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use this functionality.


# 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,

- 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,

- 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,

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 2013-05-15,

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 20 DEV EV, Developer evidence for the evaluation of a deterministic random number generator, Version 0.9, 2013-02-28,

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 20 EVL-DRNG, Evaluation Report as part of the Evaluation Technical Report, Part B – ETR-Part Deterministic Random Number Generator, Template-Version 0.10, 2013-02-28

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 23, Zusammentragen von Nachweisen der Entwickler, Version 4, 2017-03-15,

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 23 CCDB-CDE, CC Supporting Document Guidance – Collection of Developer Evidence, Version 1.5, 2012-04, CCDB-2012-04-005

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 23 JIL-CDE, Collection of Developer Evidence, Version 1.5, 2012-01, Joint Interpretation Library.

- Application Notes and Interpretation of the Scheme (AIS) – AIS 25, Anwendungen der CC auf integrierte Schaltungen, Version 9, 2017-03-15,

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS25_CCDB-HW-ADV-ARC_App1, CC Supporting Document Mandatory Technical Document – Security Architecture requirements (ADV_ARC) for smart cards and similar devices, Version 2.1, 2014-04, CCDB-2014-04-001,

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS25_CCDB-HW-IC-CC, CC Supporting Document Mandatory Technical Document – The Application of CC to Integrated Circuits, Version 3.0, 2009-03, CCDB-2009-03-002,

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS25_JIL-HW-ADV-ARC_App1, Joint Interpretation Library – Security Architecture requirements (ADV_ARC) for smart cards and similar devices – Appendix 1, Version 2.0, 2012-01

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS25_JIL-HW-IC-CC, Joint Interpretation Library – The Application of CC to Integrated Circuits, Version 4.0, 2024-04,

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS25_JIL-SecReq-CodeLoad, Joint Interpretation Library – Security requirements for post-delivery code loading, Version 1.0, 2016-02, 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,

- Auswahl geeigneter Chips für DPA-Messungen, Version 1.1, 2008-12-07, AIS26_BSI-ADPA-SC,Bundesamt für Sicherheit in der Informationstechnik,

- Special Attack Methods for Smartcards and Similar Devices, Version 1.4, 2011-06-08,

- CC Supporting Document Mandatory Technical Document – Requirements to perform Integrated Circuit Evaluations, Version 1.1, 2013-05, CCDB-2013-05-001

- Joint Interpretation Library – Application of Attack Potential to Smartcards and Similar Devices, Version 3.2.1, 2024-02, AIS26_JIL-AP-SC,Bundesamt für Sicherheit in der Informationstechnik.

- Joint Interpretation Library – Attack Methods for Smartcards and Similar Devices, Version 2.5 (confidential), 2022-05, AIS26_JIL-ATT-SC, Bundesamt für Sicherheit in der Informationstechnik.

- Joint Interpretation Library – Requirements to perform Integrated Circuit Evaluations, Version 1.1, 2013-02, AIS26_JIL-IC-EVL,Bundesamt für Sicherheit in der Informationstechnik.

- Anwendungshinweise und Interpretationen zum Schema (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,

- Developer evidence for the evaluation of a physical true random generator, Version 0.8, 2013-02-28, AIS31_DEV-EV,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, AIS31_EVL-PTRNG, Bundesamt für Sicherheit in der Informationstechnik.

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 32, CC-Interpretationen im deutschen Zertifizierungsschema, Version 7, 2011-06-08,

- 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,

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 35, Öffentliche Fassung eines Security Target (ST-lite), Version 2, 2007-11-12,

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 36, Kompositionsevaluierung, Version 5, 2017-03-15,

- CC Supporting Document Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, Version 1.4, 2015-12, AIS36_CCDB-COMP, CCDB-2015-12-001,

- CC Supporting Document Guidance – ETR template for composite evaluation of Smart Cards and similar devices, Version 1.1, 2015-12, AIS36_CCDB-COMP-ETR, CCDB-2015-12-002,

- Joint Interpretation Library – Composite product evaluation for Smart Cards and similar devices, Version 1.6, 2024-04, AIS36_JIL-COMP, Joint Interpretation Working Group,

- CC Supporting Document Guidance – ETR template for composite evaluation of Smart Cards and similar devices, Version 1.2, 2024-04, AIS36_JIL-COMP-ETR,Joint Interpretation Working Group,

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 37, Terminologie und Vorbereitung von Smartcard-Evaluierungen, Version 3, 2010-05-17,

- CC Supporting Document Guidance – Smartcard Evaluation, Version 2.0, 2010-02, AIS37_CCDB-SC-EVALCCDB-2010-03-001,

- Joint Interpretation Library – Guidance for smartcard evaluation, Version 3.0, 2024-04, AIS37_JIL-SC-EVAL, Joint Interpretation Working Group,

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 38, Reuse of evaluation results, Version 2, 2007-09-28,

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 39, Formal Methods, Version 3, 2008-10-24, Bundesamt für Sicherheit in der Informationstechnik,

- Anwendungshinweise und Interpretationen zum Schema (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,AIS41_PP-ST-2,

- 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,

- Guidelines for Evaluating Machine-Learning based Side-Channel Attack Resistances, Version 2024-01, 2024-02-29, Bundesamt für Sicherheit in der Informationstechnik,

- Review-Protokoll zum (Krypto-)AVA-KickOff, 2019-08-23, Bundesamt für Sicherheit in der Informationstechnik,

- Guidelines for Evaluating Side-Channel and Fault Attack Resistance of Elliptic Curve Implementations, Version 3.0, 2024-02-29, Bundesamt für Sicherheit in der Informationstechnik,

- 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

- Guidance for Site Certification, Version 1.1, 2013-12-04, Bundesamt für Sicherheit in der Informationstechnik, AIS47 SC-GD,

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 48, Anforderungen an die Prüfung von Sicherheitsetiketten, Version 1.0, 2015-04-30, Bundesamt für Sicherheit in der Informationstechnik,

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 48, Anforderungen an die Prüfung von Sicherheitsetiketten, Version 1.0, 2015-04-30, Bundesamt für Sicherheit in der Informationstechnik,

- Joint Interpretation Library – Assurance Continuity - Practical Cases for Smart Cards and similar devices, Version 1.1, 2024-04, Joint Interpretation Working Group, JIL-AssCont,

- Joint Interpretation Library – Assurance Continuity - Practical Cases for Smart Cards and similar devices, Version 1.1, 2024-04, Joint Interpretation Working Group, JIL-MSSR,

- Joint Interpretation Library – Remaining Strength of Asymmetric Cryptographic Mechanisms after Partial Key Leakage, Version 1.0 (confidential), 2020-06, Joint Interpretation Working Group,JIL-SoACM,

- A proposal for: Functionality classes for random number generators, Version 2.0, 2011-09-18, W. Killmann, W. Schindler, T-Systems GEI GmbH and Bundesamt für Sicherheit in der Informationstechnik, KS2011

are considered.

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

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

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

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

- All components of the EAL 5 package including the class ASE as defined in the CC (see also part C of this report)

- The components ALC_DVS.2 and AVA_VAN.5 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-1102-2019, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the transition from CCv3.1 to CC:2022, the scope limitation of software libraries, the changes on the security target and the guidance documentation on HRM[12], PRM[13], SEC[14], PPM[15] and HSL[16] where also within the scope of the evaluation.

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 5 augmented by ALC_DVS.2 and AVA_VAN.5

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. Note that the column "Security Level" given in table 7 refers to the pure cryptographic (mathematical) strength only, and does not take into account whatever exploitable weaknesses induced by side-channel leakage, physical attacks, or implementation flaws of any kind.

| No. | Purpose | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Security Level above 120 Bits | Comments |
|---|---|---|---|---|---|---|
| 1 | Cryptographic Primitive | Physical True RNG PTG.2 | [AIS31] (proprietary) | N/A | N/A | - |

Table 3: TOE cryptographic functionality

## 10. Obligations and Notes for the Usage of the TOE

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

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

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

Some security measures are partly implemented in this certified TOE, but require additional configuration or control or measures to be implemented by a product layer on top, e.g. the 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.

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

● All security hints described in the delivered documents SEC[14], HRM[12], PRM[15], HSL_API [16], and UMSLC_API[17] must be considered.

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

● All security hints described in PPM[15] must be considered.

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

● The IC Embedded Software Developer can deliver their software either to Infineon to let them implement it in the TOE (in the Flash memory) or to the Composite Product Manufacturer to let them download the software into the Flash memory.

● The TOE does not claim conformance to "Package 2: Loader dedicated for usage by authorized users only" of PP [8], section 7.3.2 and must thus be personalized in a secure environment

● The delivery procedure from the IC Embedded Software Developer to the Composite Product Manufacturer is not part of this evaluation. If the flashloader is deactivated a secure delivery is required.

● The delivery procedure from the TOE manufacturer (IFX) to the composite product manufacturer is not part of this evaluation. However, for security reasons, a form of transport protection might be required depending on the order option (see Section 2.1 for details). The applied transport protection mechanisms must be considered during the composite evaluation considering the security needs of any pre-loaded IC Embedded Software that is active during delivery.

# 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

| | |
|---|---|
| **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 |
| **SFP** | Security Function Policy |
| **SFR** | Security Functional Requirement |
| **ST** | Security Target |
| **TOE** | Target of Evaluation |
| **TSF** | TOE Security Functionality |

## 13.2. Glossary

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

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

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

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

**Informal** - Expressed in natural language.

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

**Package** - named set of either security functional or security assurance requirements

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

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

**Semiformal** - Expressed in a restricted syntax language with defined semantics.

**Subject** - An active entity in the TOE that performs operations on objects.

**Target of Evaluation** - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

**TOE Security Functionality** - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

## 14. Bibliography

[1]    Common Criteria for Information Technology Security Evaluation/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.

[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[6]
https://www.bsi.bund.de/AIS

---

[6]specifically

•   see chapter 9.1

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

[6]     Security Target BSI-DSZ-CC-1102-V2-2025, Version 2.9, 2025-01-09, IFX_CCI_001Fh, IFX_CCI_002Fh, IFX_CCI_0030h,IFX_CCI_0033h, IFX_CCI_0035h, IFX_CCI_0036h,IFX_CCI_0038h S11 and M11 Security Target, Infineon Technologies AG e (confidential document)

[7]     Evaluation Technical Report, Version 1, Date 2025-01-14, Document Title, Lab-Name, (confidential document)

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

[9]     Security Target BSI-DSZ-CC-1102-V2-2025, Version 2.9, 2025-01-09, IFX_CCI_001Fh, IFX_CCI_002Fh, IFX_CCI_0030h,IFX_CCI_0033h, IFX_CCI_0035h, IFX_CCI_0036h,IFX_CCI_0038h S11 and M11 Security Target Lite, Infineon Technologies AG (sanitised public document)

[10]    ETR for composite evaluation according to AIS 36 for BSI-DSZ-CC-1102-V2-2025, Version 1, 2025-01-14, EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR_COMP), TÜV Informationstechnik GmbH (confidential document)

[11]     Configuration list for the TOE, Version 1.2, 2024-11-11, Configuration Management Scope (confidential document)

[12]    Hardware Reference Manual, Version 4.3, 2020-02-10, 32-bit Security Controller – V15, Hardware Reference Manual Guidance documentation for the TOE, Infineon Technologies AG

[13]    Programmers Reference Manual, Version 5.8, 2024-05-24, SLx1/SLx3 (40 nm) security controllers, Programmer's Reference Manual, SLCx7_DFP, Infineon Technologies AG

[14]    Security Guidelines, Version 1.00-2689, 2020-11-05, 32-bit Security Controller – V15, Security Guidelines, Infineon Technologies AG

[15]    Production and personalization Manual, Version 3.6, 2024-12-16, Production and personalization, 32-bit Arm-based security controller, Infineon Technologies AG

[16]    HSL Library, Version 02.62.7626, 2020-12-17, HSL library for SLCx7 in 40nm Infineon Technologies AG

[17]    UMSLC Library Manual, Version 1.1, 2018-05-23, UMSLC library for SLCx7 in 40nm, Infineon Technologies AG

# 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-1102-V2-2025

## Evaluation results regarding development and production environment

The IT product IFX_CCI_001Fh, IFX_CCI_002Fh, IFX_CCI_0030h, IFX_CCI_0033h, IFX_CCI_0035h, IFX_CCI_0036h, IFX_CCI_0038h in the design steps S11 and M11 with software libraries: HSL v2.62.7626 (optional) and UMSLC v01.00.0234, with specific IC-dedicated firmware (BOS and Flash Loader) (Target of Evaluation, TOE) 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 for conformance to the Common Criteria for IT Security Evaluation (CC), CC:2022.

As a result of the TOE certification, dated 20 February 2025, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.2)

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

The relevant delivery sites are as follows:

| Site ID | Company name and address |
|---------|--------------------------|
| DHL Singapore | DHL Supply Chain Singapore Pte Ltd., Advanced Regional Center<br>Tampines LogisPark<br>1 Greenwich Drive<br>Singapore 533865 |
| KWE Shanghai | KWE Kintetsu World Express (China) Co., Ltd.<br>Shanghai Pudong Airport Pilot Free Trade Zone<br>No. 530 Zheng Ding Road<br>Shanghai,<br>P.R. China |
| K&N Großostheim | Kühne & Nagel<br>Stockstädter Strasse 10<br>63762 Großostheim<br>Germany |

Tabelle 4: TOE Delivery / Distribution Sites

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