Federal Office
for Information Security

# Certification Report

## BSI-DSZ-CC-1149-V3-2023

for

## NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3)

from

## NXP Semiconductors Germany GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

# Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

**BSI-DSZ-CC-1149-V3-2023** (*)

Smartcard Controller

**NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3)**

| | |
|---|---|
| from | NXP Semiconductors Germany GmbH |
| PP Conformance: | Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014 |
| Functionality: | PP conformant plus product specific extensions Common Criteria Part 2 extended |
| Assurance: | Common Criteria Part 3 conformant EAL 6 augmented by ALC_FLR.1, ASE_TSS.2 |
| valid until: | 12 December 2028 |

SOGIS
Recognition Agreement

Common Criteria

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

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

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

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

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

Bonn, 13 December 2023

For the Federal Office for Information Security

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

Sandro Amendola L.S.
Director-General

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

This page is intentionally left blank.

# Contents

# A. Certification

## 1. Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

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

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

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

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

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

## 2. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs [3]
- Special decrees issued by the Bundesministerium des Innern 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), Version 3.1[4] [1] also published as ISO/IEC 15408

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

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

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

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

# 3. Recognition Agreements

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

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

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

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

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

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

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

## 3.2. International Recognition of CC – Certificates (CCRA)

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

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

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

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

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

# 4. Performance of Evaluation and Certification

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

The product NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3) has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1149-V2-2023. Specific results from the evaluation process BSI-DSZ-CC-1149-V2-2023 were re-used.

The evaluation of the product NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3) was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 6 December 2023. 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: NXP Semiconductors Austria GmbH.

The product was developed by: NXP Semiconductors Germany GmbH.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

# 5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 13 December 2023 is valid until 12 December 2028. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

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 NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3) has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[6] NXP Semiconductors Germany GmbH
Beiersdorfstraße 12
22529 Hamburg

# 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 TOE is the hard macro “NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3)”, or in short “N7122”, which is manufactured by GlobalFoundries 40nm (C40) technology and comprises of hardware, software (security IC Dedicated Software), and documentation. The N7122 is self-sufficient at the boundary of the hard macro and can be instantiated within packaged products. The TOE does not include a customer-specific Security IC Embedded Software, however, it provides secure mechanisms for customers to download and execute their code on the TOE.

The IC Dedicated Software comprises IC Dedicated Test Software for test purposes and IC Dedicated Support Software. The IC Dedicated Support Software consists of the Boot Software, which controls the boot process of the hardware platform, and a Firmware Interface. The IC Dedicated Support Software also comprises the following optional software components:

- a Library Interface, which simplifies the access to the hardware for the Security IC Embedded Software,
- a Flash Loader OS, which supports the download of code and data to the Flash by the Composite Product Manufacturer before Operational Usage (e.g. during development), and
- a Crypto Library, which provides simplified access to the frequently used cryptographic algorithms AES, TDES, RNG, RSA, ECC, hashing and utilities.

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

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 6 augmented by ALC_FLR.1, ASE_TSS.2.

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 |
|---|---|
| TSF.Service | Service functionalities apart from cryptographic operation |
| TSF.Protection | General security measures to protect the TSF |
| TSF.Control | Operating conditions, memory and hardware access control |
| TSF.Crypto | Cryptographic Services |

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [9], chapter 6.1.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 3.1. 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 3.2 to 3.4.

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:

**NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3)**

The following table outlines the TOE deliverables:

| Type | Name | Release | Form of delivery |
|---|---|---|---|
| **TOE components for all configurations** | | | |
| IC Hardware | N7122 | A1 | Hard macro instantiated within a wafer, module and/or package. |
| Document | NXP Secure Smart Card Controller N7122 – Overview, Product data sheet [11] | 0.1 / 2021-03-31 | Electronic document (PDF via NXP DocStore). |
| Document | NXP Secure Smart Card Controller N7122 – Instruction Set Manual, Product data sheet addendum [12] | 0.2 / 2021-03-29 | Electronic document (PDF via NXP DocStore). |
| Document | NXP Secure Smart Card Controller N7122 – Chip health mode, Product data sheet addendum [13] | 0.2 / 2021-03-29 | Electronic document (PDF via NXP DocStore). |
| Document | NXP Secure Smart Card Controller N7122 – Peripheral Configuration and Use Product data sheet addendum [14] | 0.2 / 2021-04-12 | Electronic document (PDF via NXP DocStore). |
| Document | NXP Secure Smart Card Controller N7122 – MMU Configuration and NXP Firmware Interface Specification, Product data sheet addendum [15] | 1.0 / 2023-03-16 | Electronic document (PDF via NXP DocStore). |
| Document | NXP N7122 A1 Hardmacro – Lifecycle Documentation, Report [16] | 0.2 / 2022-02-04 | Electronic document (PDF via NXP DocStore). |
| Document | NXP Secure Smart Card Controller N7122 – Shared OS Libraries [17] | 0.4 / 2022-02-10 | Electronic document (PDF via NXP DocStore). |

| | | | |
|---|---|---|---|
| Document | NXP Secure Smart Card Controller N7122 – Wafer and delivery specification [18] | 1.2 / 2023-05-12 | Electronic document (PDF via NXP DocStore). |
| Document | NXP Secure Smart Card Controller N7122, Information on Guidance and Operation, Guidance and operation manual [19] | 1.3 / 2022-02-08 | Electronic document (PDF via NXP DocStore). |
| **Deliverables specific to COS-ROM configuration** | | | |
| IC Dedicated Test Software | Test Software | 11.6.5 | On-chip software. |
| IC Dedicated Support Software | Boot Software | 11.6.5 | On-chip software. |
| | Firmware | 11.6.5 | On-chip software. |
| | Library Interface | 11.6.5 | On-chip software. |
| | Flashloader OS | 1.3.3 | On-chip software. |
| Library | Communication Library | 7.10.3 | On-chip software. |
| Library | CRC Library | 1.1.8 | On-chip software. |
| Library | Memory Library | 1.2.3.1 | On-chip software. |
| Library | Flash Loader Library | 3.10.0 | On-chip software. |
| Document | NXP Secure Smart Card Controller N7122 – Flashloader OS, Product data sheet addendum [20] | 0.4 / 2022-02-10 | Electronic document (PDF via NXP DocStore). |
| **Deliverables specific to NOS-ROM configuration** | | | |
| IC Dedicated Test Software | Test Software | 11.6.5 | On-chip software. |
| IC Dedicated Support Software | Boot Software | 11.6.5 | On-chip software. |
| | Firmware | 11.6.5 | On-chip software. |
| | Library Interface | 11.6.5 | On-chip software. |
| Library | Communication Library | 7.10.2 | On-chip software. |
| Library | CRC Library | 1.1.8 | On-chip software. |
| Library | Memory Library | 1.2.3.1 | On-chip software. |
| **Deliverables of the Crypto Library** | | | |
| IC Dedicated Support Software | Crypto Library | 1.1.2 | On-chip software. |
| **TOE components required for all packages** | | | |
| Document | N7122 Crypto Library, Information on Guidance and Operation, User manual [21] | 1.5 / 2023-11-23 | Electronic document (PDF via NXP DocStore). |
| **Package Random Number Generation** | | | |
| Library | RNG Lib | 1.1.2 | Electronic files (object files via NXP DocStore). |
| Library | RNG HealthTest Lib | 1.1.2 | Electronic files (object files via NXP DocStore). |

| | | | |
|---|---|---|---|
| Document | N7122 Crypto Library – RNG Library, User manual [22] | 1.1 / 2020-08-24 | Electronic document (PDF via NXP DocStore). |
| **Package Symmetric Ciphers** | | | |
| Library | Sym. Cipher Lib | 1.1.2 | Electronic files (object files via NXP DocStore). |
| Document | N7122 Crypto Library – SymCfg User manual [23] | 1.1 / 2020-08-24 | Electronic document (PDF via NXP DocStore). |
| **Package KeyStore** | | | |
| Library | KeyStoreMgr Lib | 1.1.2 | Electronic files (object files via NXP DocStore). |
| Document | N7122 Crypto Library – KeyStoreMgr, User manual Preliminary user manual [24] | 1.1 / 2020-08-24 | Electronic document (PDF via NXP DocStore). |
| **TOE components required for the packages Random Number Generation and Symmetric Ciphers** | | | |
| Library | Sym. Utilities Lib | 1.1.2 | Electronic files (object files via NXP DocStore). |
| Document | N7122 Crypto Library – Utils, User manual [25] | 1.1 / 2020-08-24 | Electronic document (PDF via NXP DocStore). |
| **Package RSA Encryption / Decryption** | | | |
| Library | RSA Lib | 1.1.2 | Electronic files (object files via NXP DocStore). |
| Document | N7122 Crypto Library – RSA, User manual [26] | 1.2 / 2020-08-24 | Electronic document (PDF via NXP DocStore). |
| **Package RSA Key Generation** | | | |
| Library | RSA Key Generation Lib | 1.1.2 | Electronic files (object files via NXP DocStore). |
| Document | N7122 Crypto Library – RSA Key Generation, User Manual [27] | 1.2 / 2020-08-24 | Electronic document (PDF via NXP DocStore). |
| **Package ECC over GF(p)** | | | |
| Library | ECC Lib | 1.1.2 | Electronic files (object files via NXP DocStore). |
| Document | N7122 Crypto Library – ECC over GF(p), User manual [28] | 1.2 / 2020-08-24 | Electronic document (PDF via NXP DocStore). |
| **Package SHA** | | | |
| Library | SHA Library & Hash Library | 1.1.2 | Electronic files (object files via NXP DocStore). |
| Document | N7122 Crypto Library – SHA, User manual [29] | 1.1 / 2020-08-24 | Electronic document (PDF via NXP DocStore). |

| | | | |
|---|---|---|---|
| Document | N7122 Crypto Library – HASH, User manual [30] | 1.1 / 2020-08-24 | Electronic document (PDF via NXP DocStore). |
| **TOE components required for the packages RSA Encryption / Decryption, RSA Key Generation, ECC over GF(p), and SHA** | | | |
| Library | Asym. Utilities Lib | 1.1.2 | Electronic files (object files via NXP DocStore). |
| Document | N7122 Crypto Library – UtilsAsym, User manual [31] | 1.1 / 2020-08-24 | Electronic document (PDF via NXP DocStore). |
| **Package KoreanSeed (non TSF)** | | | |
| Library | KoreanSeed Lib | 1.1.2 | Electronic files (object files via NXP DocStore). |
| Document | N7122 Crypto Library – KoreanSeed, User Manual [32] | 1.1 / 2020-09-28 | Electronic document (PDF via NXP DocStore). |

Table 2: TOE deliverables

The TOE can be delivered in three different release packages: R1, R2, R3. These are explained in [6] and [9] chapter 1.4.1. The release packages are identical in the hard macro related functionalities of the TOE, but differ in the instantiation specific functionalities which are needed for the packaged product to integrate the hard macro. The differences are only minor functional modifications of the IC Dedicated Software without impact on the security functionalities of the TOE. Release packages R1 and R2 are manufactured at GlobalFoundries Fab 7 in Singapore. Release package R3 is manufactured at GlobalFoundries Fab 1 in Dresden.

The different release packages can be identified by Wafer Test ID, Firmware Extension ID, and Manufacturer ID using the GetVersion firmware command.

| Release Package | Wafer Test ID | Firmware Extension ID | Manufacturer ID |
|---|---|---|---|
| R1 | 0x0F | 0x06 | 0x7A |
| R2 | 0x10 | 0x07 | 0x7A |
| R3 | 0x0F | 0x06 | 0x79 |
| | 0x10 | 0x07 | 0x79 |

Table 3: TOE deliverables

For more information refer to [15] chapter 4.1.3.2.

The hardware version can be identified (optical identification) by its die inscription as described in [18] chapter 2.9. Logical identification of the TOE is done via the firmware function phfwSystem_GetVersion. The same data can be accessed via Chip Health Mode, see [13] chapter 3.3.

# 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 symmetric and asymmetric cryptographic algorithms to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols and it will provide a True Random Number Generator (TRNG) and Deterministic Random Number Generator (DRNG).

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 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 the Security Target [6] and [9] chapter 7.

# 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: OE.Resp-Appl, OE.Process-Sec-IC, OE.Lim_Block_Loader, OE.Loader_Usage and OE.Check_Init. Details can be found in the Security Target [6] and [9], chapter 4.2 and 4.3.

# 5. Architectural Information

The IC hardware is a microcontroller incorporating a central processing unit (CPU), memories accessible via a Memory Management Unit (MMU), cryptographic coprocessors, other security components, contact-based and contactless communication interfaces as well as a general purpose I/O interface which can be used to directly use peripherals of the TOE such as the cryptographic coprocessors. The central processing unit supports a 32-/16-bit instruction set optimized for smart card applications. On-chip memories are ROM, RAM and Flash. The Flash can be used as data or program memory. It consists of highly reliable memory cells, which are designed to provide data integrity. The Flash memory is optimized for applications that require reliable non-volatile data storage for data and program code. Dedicated security functionality protects the contents of all memories. The logical Flash size can be configured in 1kB steps. The IC integrates coprocessors for AES, DES (both within the new Crypto2+ coprocessor) and a new 128 bit Public Key Crypto Coprocessor (Fame3) to support the implementation of asymmetric cryptographic algorithms.

The IC Dedicated Software comprises IC Dedicated Test Software for test purposes and IC Dedicated Support Software. The IC Dedicated Support Software consists of the Boot Software, which controls the boot process of the hardware platform. Furthermore, it provides a Firmware Interface and optionally a Library Interface, simplifying access to the hardware for the Security IC Embedded Software. The IC Dedicated Support Software also comprises optional software components, i.e.,

- a Flash Loader OS which supports download of code and data to Flash by the Composite Product Manufacturer before Operational Usage (e.g. during development), and
- a Crypto Library which provides simplified access to frequently used cryptographic algorithms AES, TDES, RNG, RSA and ECC.

The availability of these software components depends on the different TOE configurations.

# 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

## 7.1. Developer's Test according to ATE_FUN

Testing approach:

- All TSF and related security mechanisms, subsystems and modules are tested in order to assure complete coverage of all SFR.
- Different classes of tests are performed to test the TOE in a sufficient manner:
  - System Verification:

    Test cases that can not be performed at module level are defined and implemented for system verification. This includes mainly the startup behaviour, system interoperability, endurance, and system security.
  - Functional Module Verification:

    This test category is used to verify the correct functionality of each of the individual modules that make up the TOE. It includes the following test groups:
    - Positive Testing: Tests that are based on the requirement specification and the expected usage by the customer.
    - Negative Testing: Tests that extend the scope of the intended usage of the TOE, assuming a misuse by the user.
    - The tests are run with all possible system configurations.
  - Security Verification: This test category addresses the security mechanisms described in the Security Architecture description. Two main categories of security module verification are defined:
    - Integrity Protection Module Verification (fault injection) using whitebox and blackbox testing.
    - DPA module verification (side-channel analysis).
  - Characterization:

This mostly addresses production tests to measure varying parameters in post-silicon verification while all parameters are within the specified limits. The developer performs a Matrix Characterization Run to measure parameters using varying processes (corner material) and different temperatures.

- Qualification:

  This test category ensures that a developed IC is production ready and has the expected quality. This addresses

  - Electrostatic discharge due to electrostatic stress in the field (contactless communication),
  - Fast aging of the device due to high temperatures to guarantee the life time of the product,
  - Flash qualification to ensure that features like anti-tearing and wear levelling work as specified,
  - Package qualification to ensure that the IC can be placed in the final delivery form (package) under industrial environments and the final product quality is achieved, and
  - PUF qualification to ensure that the promised PUF properties hold in field conditions.

- Validation:

  Execution of all customer-visible use cases to ensure that the entire system works as defined for customer-visible operation. This includes

  - on-chip test framework developed to use each officially released product variant and execute each public available API.

## 7.2. Independent Testing according to ATE_IND

Testing approach:

- The evaluator's objective regarding this aspect was to test the functionality of the TOE as described in the ST and to verify the developer‘s test results by repeating developer‘s tests and additionally add independent tests.
- In the course of the evaluation of the TOE the following classes of tests were carried out:
  - Module tests,
  - Simulation tests,
  - Tests in User Mode of logical card B,
  - Tests in System Mode of card B,
  - Tests in Test Mode,
  - Hardware tests, and
  - Cryptographic library tests.

  With this kind of tests the entire security functionality of the TOE was tested.

## 7.3. Penetration Testing according to AVA_VAN

Overview:

- 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.

Penetration testing approach:

- Systematic search for potential vulnerabilities and known attacks in public domain sources, use of a list of vulnerabilities, and from a methodical analysis of the evaluation documents.
- Analysis why these vulnerabilities are unexploitable in the intended environment of the TOE.
- If the rationale is suspect in the opinion of the evaluator penetration tests are devised.

Even if the rational is convincing in the opinion of the evaluator penetration tests are devised for some vulnerabilities, especially to support the argument of non-practicability of exploiting time in case of SPA, DPA and FI attacks.

# 8. Evaluated Configuration

The TOE can be delivered with various configuration options as described in chapter 1.4.1 of [6] and [9] and shown in the following table. Of these, only one option (COS-ROM) is available to external customers. The other option (NOS-ROM) is only available for NXP internal use.

| Configuration Option | Description |
|---|---|
| Customer OS ROM Code (COS-ROM) | The TOE provides the functionality of a Flash Loader such that customers can load their Security IC Embedded Software Code to the NVM memory.<br>If the Flash Loader is available, the Library Interface and the N7122 Crypto Library become mandatory.<br>All libraries given in Table 2 will be stored to ROM.<br>The Security IC Embedded Software will be stored in Flash.<br>Note:<br>The TOE does not provide a NXP System Mode OS. |
| NXP OS ROM Code (NOS-ROM) | The TOE does not provide the functionality of a Flash Loader.<br>The Security IC Embedded Software will be stored in ROM.<br>The Libraries given in Table 2 will be stored to either ROM or Flash.<br>Note:<br>This option is available for NXP internal use only. |

Table 4: : TOE Major Configuration Options

The following table shows the size of the TOE's memories:

| Memory type | Memory size | Description |
|---|---|---|
| NVM | Configurable in 1 KB steps up to 633.5 KB | The size of the Non-Volatile Memory. |
| ROM | Configurable to 0 KB or 219 KB | Size of the Read-Only Memory. |
| RAM | Up to 12.5 KB | Size of the Random-Access Memory. Size available to customer depends on ordered configuration. |

Table 5: TOE memory configuration limits

In chapter 1.4.1 of [6] and [9], the developer describes that TOE configurations can be applied during the ordering process. The following table lists these Ordering configurations.

| Product option | Choices | Description |
|---|---|---|
| NVM size | Configurable in 1KB steps up to 633,5 KB | The Flash memory size is logically configurable, within the given step size. |

Table 6: TOE configuration options

Other TOE configurations are listed in [6] and [9] as well. They address different options for communication interfaces or the availability of the chip health mode, which can be used for TOE identification.

# 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:

*(i) The Application of CC to Integrated Circuits*

*(ii) Application of Attack Potential to Smartcards*

*(iii) Guidance, Smartcard Evaluation*

(see [4], AIS 25, AIS 37).

For RNG assessment the scheme interpretations AIS 31 and AIS 20 were 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.

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, ASE_TSS.2 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-1149-V2-2023, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on penetration tests to reassess the vulnerability analysis and updates in the guidance.

The evaluation has confirmed:

- PP Conformance: Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014 [8]
- for the Functionality: PP conformant plus product specific extensions Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant EAL 6 augmented by ALC_FLR.1, ASE_TSS.2

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 | Security Level above 120 Bits |
|---|---|---|---|---|---|
| TOE Hardware/Firmware | | | | | |
| 1 | Cryptographic primitive | AES | [FIPS197] | 128, 192, 256 | Yes |
| 2 | Confidentiality | AES encryption and decryption in ECB mode | [FIPS197] (AES), [NIST SP800-38A] (ECB) | 128, 192 256 | No |
| 3 | Cryptographic primitive | Triple-DES | [NIST SP800-67] | 168 | No |

| No. | Purpose | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Security Level above 120 Bits |
|---|---|---|---|---|---|
| 4 | Confidentiality | Triple-DES encryption and decryption in ECB mode | [NIST SP800-67] (TDES), [NIST SP800-38A] (ECB) | 168 | No |
| 5 | Confidentiality | AES encryption and decryption in CBC mode using PUF key | [FIPS197] (AES), [NIST SP800-38A] (CBC), [PUF] | 128 | Yes |
| 6 | Integrity | AES MAC generation and verification in CBC-MAC mode | [FIPS197] (AES), Algorithm 1 in [ISO_9797-1] (CBC-MAC), [PUF] | 128 | No |
| 7 | Key Derivation | Proprietary PUF key derivation | [PUF] | 128 | Not rated |
| 8 | Random number generation | PTG.2 | Comformant to [AIS31] | N/A | N/A |
| TOE Software(Crypto Library) | | | | | |
| 9 | Cryptographic primitive | AES | [FIPS197] | 128, 192, 256 | Yes |
| 10 | Confidentiality | AES encryption and decryption in CBC, OFB, and CTR mode | [FIPS197] (AES), [NIST SP800-38A] (CBC, OFB, CTR) | 128, 192, 256 | Yes |
| 11 | Integrity | AES MAC generation in CBC-MAC mode | [FIPS197] (AES), Algorithm 1 in [ISO_9797-1] (CBC-MAC) | 128, 192, 256 | No |
| 12 | Integrity | AES MAC generation in CMAC mode | [FIPS197] (AES), [NIST SP800-38B] (CMAC) | 128, 192, 256 | Yes |
| 13 | Cryptographic primitive | Triple-DES | [NIST SP800-67] | 168 | No |
| 14 | Confidentiality | Triple-DES encryption and decryption in CBC and OFB mode | [NIST SP800-67] (TDES), [NIST SP800-38A] (CBC, OFB) | 168 | No |
| 15 | Integrity | Triple-DES MAC generation in CBC-MAC and Retail-MAC | [NIST SP800-67] (TDES), Algorithm 1 in [ISO_9797-1] (CBC-MAC), Algorithm 3 in [ISO_9797-1] (CBC-MAC) | 168 | No |
| 16 | Integrity | Triple-DES MAC generation in CMAC mode | [NIST SP800-67] (TDES), [NIST SP800-38B] (CMAC) | 168 | No |
| 17 | Cryptographic primitive | RSAEP, RSADP, RSASP1, RSAVP1 | [PKCS #1] | 512-1999 | No |
| 18 | Cryptographic | RSAEP, RSADP, | [PKCS #1] | 2000 - 2799 | > 100 bits |

| No. | Purpose | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Security Level above 120 Bits |
|---|---|---|---|---|---|
| | primitive | RSASP1, RSAVP1 | | | |
| 19 | Cryptographic primitive | RSAEP, RSADP, RSASP1, RSAVP1 | [PKCS #1] | 2800 - 4096 | Yes |
| 20 | Confidentiality | RSA encryption and decryption with EME-OAEP encoding | [PKCS #1] | 512 - 1999 | No |
| 21 | Confidentiality | RSA encryption and decryption with EME-OAEP encoding | [PKCS #1] | 2000 - 2799 | > 100 bits |
| 22 | Confidentiality | RSA encryption and decryption with EME-OAEP encoding | [PKCS #1] | 2800 - 4096 | Yes |
| 23 | Cryptographic primitive | RSA signature generation and verification with EMSA-PSS encoding | [PKCS #1] | 512 - 1999 | No |
| 24 | Cryptographic primitive | RSA signature generation and verification with EMSA-PSS encoding | [PKCS #1] | 2000 - 2799 | > 100 bits |
| 25 | Cryptographic primitive | RSA signature generation and verification with EMSA-PSS encoding | [PKCS #1] | 2800 - 4096 | Yes |
| 26 | Key generation | RSA key generation | [ALGO] | 512 - 1999 | No |
| 27 | Key generation | RSA key generation[7] | [ALGO], [FIPS 186-4] | 2000 - 2799 | > 100 bits |
| 28 | Key generation | RSA key generation[7] | [ALGO], [FIPS 186-4] | 2800- 4096 | Yes |
| 29 | Cryptographic primitive | ECDSA signature generation and verification | [ISO_14888-3], [ANS X9.62], [FIPS186-4], [IEEE_P1363] | 224 | No |
| 30 | Cryptographic primitive | ECDSA signature generation and verification | [ISO_14888-3], [ANS X9.62], [FIPS186-4], [IEEE_P1363] | 256, 320, 384, 512, 521 | Yes |
| 31 | Key Exchange | ECDH | [ISO_11770-3], [ANS X9.62], [IEEE_P1363] | 224 | No |
| 32 | Key | ECDH | [ISO_11770-3], | 256, 320, | Yes |

[7]For the modulus n (n = p*q) the prime numbers p and q generated by the key generator are congruent to 3 modulo 4

| No. | Purpose | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Security Level above 120 Bits |
|---|---|---|---|---|---|
| | Exchange | | [ANS X9.62], [IEEE_P1363] | 384, 512, 521 | |
| 33 | Key generation | ECDSA Key Generation | [ISO_14888-3], [ANS X9.62], [FIPS186-4] | 224 | No |
| 34 | Key generation | ECDSA Key Generation | [ISO_14888-3], [ANS X9.62], [FIPS186-4] | 256, 320, 384, 512, 521 | Yes |
| 35 | Cryptographic primitive | SHA-1 | [FIPS180-4] | N/A | No |
| 36 | Cryptographic primitive | SHA-224, SHA-256, SHA-384, SHA-512 | [FIPS180-4] | N/A | Yes |
| 37 | Random number generation | PTG.3 based AES or TDES in CTR mode | [FIPS197] (AES), [NIST SP800-67] (TDES), [NIST SP800-38A] (CTR), [NIST SP800-90A] (CTR_DRBG)<br>Conformant to [AIS20] | N/A | N/A |
| 38 | Random number generation | DRG.4 based AES or TDES in CTR mode | [FIPS197] (AES), [NIST SP800-67] (TDES), [NIST SP800-38A] (CTR), [NIST SP800-90A] (CTR_DRBG)<br>Conformant to [AIS20] | N/A | N/A |
| TOE Software (Flash Loader) | | | | | |
| 39 | Authenticity | MAC verification with AES in CMAC mode | [FIPS197] (AES), [NIST SP800-38B] (CMAC) | 128 | Not rated |
| 40 | Authentication | MAC generation and verification with AES in CMAC mode | [FIPS197] (AES), [NIST SP800-38B] (CMAC) | 128 | Not rated |
| 41 | Key derivation | Key derivation using AES in CMAC mode as pseudo-random function | [FIPS197] (AES), [NIST SP800-38B] (CMAC), [NIST SP800-108] (KBKDF) | 128 | Not rated |
| 42 | Confidentiality | Decryption with AES in CBC mode | [FIPS197] (AES), [NIST SP800-38A] (CBC) | 128 | Not rated |

Table 7: TOE cryptographic functionality

Please note that the IC Embedded Software is responsible for key handling. In this context, the key requirements of [NIST SP800-67] have to be considered.

[AGD_CL_RSA] N7122 Crypto Library RSA, Version 1.2, 2020-08-24, NXP Germany.

[AIS20] Anwendungsweise und Interpretationen zum Schema (AIS) – AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 2013-05-15, Zertifizierungsstelle des BSI im Rahmen des Zertifizierungsschemas, Bundesamt für Sicherheit in der Informationstechnik.

| | |
|---|---|
| [ANS X9.62] | Public Key Cryptography for the Financial Service Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005-11-16, American National Standards Institute |
| [FIPS180-4] | Federal Information Processing Standard Publication 180-4, Secure Hash Standards (SHS), August 2015, National Institute of Standards and Technology.. |
| [FIPS186-4] | Federal Information Processing Standard Publication 186-4, Digital Signature Standards (DSS), July 2013, National Institute of Standards and Technology. |
| [FIPS197] | Federal Information Processing Standards Publication 197, Announcing the ADVANCED ENCRYPTION STANDARD (AES), 2001-11-26, National Institute of Standards and Technology (NIST). |
| [IEEE_P1363] | IEEE P1363. Standard specifications for public key cryptography. IEEE, 2000. |
| [ISO_9797-1] | ISO 9797-1: Information technology – Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, 1999-12, ISO/IEC |
| [ISO_11770-3] | ISO 11770-3: Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques, August 2015, ISO/IEC |
| [ISO_14888-3] | ISO/IEC 14888-3, IT Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms, November 2018. |
| [NIST SP800-38A] | NIST Special Publication 800-38A 2001 Edition Recommendation for BlockCipher Modes of Operation Method and Techniques, National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce. |
| [NIST SP800-38B] | NIST Special Publication 800-38B, Recommendation for BlockCipher Modes of Operation: The CMAC Mode for Authentication, May 2005 National Institute of Standards and Technology. |
| [NIST SP800-67] | NIST Special Publication 800-67 –Revision 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher – Revised July 2017, National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce |
| [NIST SP800-90A] | NIST SP 800-90A, A Deterministic Random Bit Generator Validation System (DRBGVS), 2015-10-29, National Institute of Standards and Technology. |
| [NIST SP800-108] | NIST SP 800-108, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), October 2009, National Institute of Standards and Technology. |
| [PKCS #1] | PKCS #1: RSA Cryptography Standard, Version 2.1, 2002-06-14, RSA Laboratories. |
| [PUF] | PUF Key derivation function specification, 2014, NXP Semiconductors |


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

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

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and

techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

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

Some security measures are partly implemented in this certified TOE, but require additional configuration or control or measures to be implemented by a product layer on top, e.g. the IC Dedicated Support Software and/or Embedded Software using the TOE. For this reason the TOE includes guidance documentation (see table 2) which contains obligations and guidelines for the developer of the product layer on top on how to securely use this certified TOE and which measures have to be implemented in order to fulfil the security requirements of the Security Target of the TOE. In the course of the evaluation of the composite product or system it must be examined if the required measures have been correctly and effectively implemented by the product layer on top. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the documents "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.

# 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, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8] https://www.bsi.bund.de/AIS

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

[6] Security Target BSI-DSZ-CC-1149-V3-2023, NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3), Version 1.8, 2023-12-01, NXP Semiconductors (confidential document)

[7] Evaluation Technical Report (ETR) for NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3), BSI-DSZ-CC-1149-V3, Version 2, 2023-12-01, TÜV Informationstechnik GmbH.

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

[8] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluation nach CC (Common Criteria)
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2, Reuse of evaluation results
- AIS 39, Version 3, Formal Methods
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren
- AIS 47, Version 1.1, Regelungen zu Site Certification

[9] Security Target Lite BSI-DSZ-CC-1149-V3-2023, NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2R3), Version 1.8, 2023-12-01, NXP Semiconductors (sanitised public document)

[10] Evaluation Technical Report for Composite Evaluation (ETR COMP) for NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3), Version 2, 2023-12-01, TÜV Informationstechnik GmbH. (confidential document)

[11] NXP Secure Smart Card Controller N7122 Overview Product data sheet, Version 0.1, 2021-03-31, NXP Semiconductors

[12] NXP Secure Smart Card Controller N7122 – Instruction Set Manual, Product data sheet addendum, Version 0.2, 2021-03-29, NXP Semiconductors

[13] NXP Secure Smart Card Controller N7122 – Chip health mode, Product data sheet addendum, Version 0.2, 2021-03-29, NXP Semiconductors

[14] NXP Secure Smart Card Controller N7122 – Peripheral Configuration and Use Product data sheet addendum, Version 0.2, 2021-04-12, NXP Semiconductors

[15] NXP Secure Smart Card Controller N7122 – MMU Configuration and NXP Firmware Interface Specification, Product data sheet addendum, Version 1.0, 2023-03-16, NXP Semiconductors

[16] NXP N7122 A1 Hardmacro – Lifecycle Documentation, Report, Version 0.2, 2022-02-04, NXP Semiconductors

[17] NXP Secure Smart Card Controller N7122 – Shared OS Libraries, Version 0.4, 2022-02-10, NXP Semiconductors

[18] NXP Secure Smart Card Controller N7122 – Wafer and delivery specification, Version 1.2, 2023-05-12, NXP Semiconductors

[19] NXP Secure Smart Card Controller N7122, Information on Guidance and Operation, Guidance and operation manual, Version 1.3, 2022-02-08, NXP Semiconductors

[20] NXP Secure Smart Card Controller N7122 – Flashloader OS, Product data sheet addendum,Version 0.4, 2022-02-10, NXP Semiconductors

[21] N7122 Crypto Library, Information on Guidance and Operation, User manual, Version 1.5, 2022-11-23, NXP Semiconductors

[22] N7122 Crypto Library – RNG Library, User manual, Version 1.1, 2020-08-24, NXP Semiconductors

[23] N7122 Crypto Library – SymCfg User manual, Version 1.1, 2020-08-24, NXP Semiconductors

[24] N7122 Crypto Library – KeyStoreMgr, User manual Preliminary user manual, Version 1.1, 2020-08-24, NXP Semiconductors

[25] N7122 Crypto Library – Utils, User manual, Version 1.1, 2020-08-24, NXP Semiconductors

[26] N7122 Crypto Library – Rsa, User manual, Version 1.2, 2020-08-24, NXP Semiconductors

[27] N7122 Crypto Library – RSA Key Generation, User Manual, Version 1.2, 2020-08-24, NXP Semiconductors

[28] N7122 Crypto Library – ECC over GF(p), User manual, Version 1.2, 2020-08-24, NXP Semiconductors

[29] N7122 Crypto Library – SHA, User manual, Version 1.1, 2020-08-24, NXP Semiconductors

[30] N7122 Crypto Library – HASH, User manual, Version 1.1, 2020-08-24, NXP Semiconductors

[31] N7122 Crypto Library – UtilsAsym, User manual, Version 1.1, 2020-08-24, NXP Semiconductors

[32] N7122 Crypto Library – KoreanSeed, User Manual,Version 1.1, 2020-09-28, NXP

# C. Excerpts from the Criteria

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

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

# D. Annexes

## List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment

# Annex B of Certification Report BSI-DSZ-CC-1149-V3-2023

## Evaluation results regarding development and production environment

The IT product NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3) (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 13 December 2023, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.5, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_FLR.1 and ALC_TAT.3) are fulfilled for the development and production sites of the TOE listed below:

| Name of site / Company name | Address | Function |
|---|---|---|
| **Development Sites** | | |
| NXP Hamburg | NXP Semiconductors Germany GmbH<br>Troplowitzstr. 20<br>22529 Hamburg<br>Germany | Project management, central design database, HW/FW/SW development and verification, security architecture and evaluation, flaw remediation, trust provisioning, customer support, IT support, IC test and pre-personalization, key generation and delivery, reliability test & failure analysis and warehousing incl. scrapping, shipment and delivery. |
| NXP Gratkorn | NXP Semiconductors Austria GmbH<br>Mikronweg 1<br>8101 Gratkorn<br>Austria | Project management, HW/FW/SW development and verification, security architecture and evaluation, and document control system (DocStore). |
| NXP Eindhoven | NXP Semiconductors<br>Eindhoven<br>HTC-46.3-west (Development Center)<br>Building 46, High Tech Campus<br>HTC-46.3-west<br>5656 AE5656AE, Eindhoven<br>The Netherlands | HW/FW/SW development, security architecture. IT engineering and generic support. |
| NXP Nijmegen | NXP Semiconductors Nijmegen B.V.<br>Gerstweg 2<br>6534AE Nijmegen<br>The Netherlands | Verification of design data and mask data, sample preparation. |
| NXP Glasgow 2 | NXP Glasgow EK | Hardware development, security |

| | | |
|---|---|---|
| | Pegasus House, Scottish Enterprise Technology Park, Bramah Ave<br>East Kilbride, Glasgow G75 0RD<br>Scotland, UK | architecture and reviews. |
| NXP Leuven | NXP Semiconductors<br>Interleuvenlaan 80<br>B-3001 Leuven<br>Belgium | Hardware development, security reviews. |
| Sii Gdansk 2 | SII<br>Olivia Prime Building, 10th floor, Grunwaldzka 472E<br>80-309 Gdansk<br>Poland | SW development and verification. |
| NXP IT Eindhoven | NXP Master IT | NXP Master IT |
| Akquinet Datacenter Hamburg | Akquinet Datacenter Hamburg<br>Ulzburger Strasse 201<br>22850 Norderstedt<br>Germany | Data center. |
| Colt Datacenter Hamburg | Colt Datacenter Hamburg<br>Obenhauptstrasse<br>22335 Hamburg<br>Germany | Data center. |
| Digital Realty Phoenix | Digital Realty Data Center<br>120 E Van Buren St, Phoenix<br>AZ 85004<br>U.S.A. | Data center. |
| Equinix Singapore | EQUINIX<br>20 Ayer Rajah Crescent, IBX SG1, Level 5 Unit 5, Ayer Rajah Industrial Park<br>139964 Singapore | Data center. |
| NXP Bangalore | NXP India Private Limited<br>Manyata Technology Park, Nagawara Village, Kasaba Hobli<br>Bangalore 560 045<br>India | Data center. |
| NXP Bucharest | NXP Semiconductors Romania<br>Campus 6, Bulevardul Iuliu Maniu 6L, 061103 Bucureşti<br>Romania | IT engineering and support. |
| NXP Guadalajara | NXP Guadalajara<br>Periferico Sur #8110 Col. El Mante JALISCO, 45609 Tlaquepaque<br>Mexico | IT engineering and support. |
| NXP Master IT | NXP Semiconductors<br>HTC Building 60<br>High Tech Campus | Virtual IT Network and Administration site. |

| | | |
|---|---|---|
| | 5656 Eindhoven<br>Netherlands | |
| **Production Sites** | | |
| Global Foundries Singapore (Fab 7) | GlobalFoundries Singapore Pte Ltd<br>60 Woodlands Industrial Park D, Street 2<br>Singapore, 738406 | Mask and wafer production. |
| Global Foundries Dresden (Fab 1) | GlobalFoundries Fab 1 Dresden<br>Wilschdorfer Landstrasse 101<br>01109 Dresden<br>Germany | Mask and wafer production. |
| AMTC Dresden | Advanced Mask Technology Center GmbH & Co KG (AMTC)<br>Rähnitzer Allee 9<br>01109 Dresden<br>Germany | Wafer mask production. |
| | Toppan Photomasks Inc.<br>400 Texas Avenue<br>Round Rock, TX 78664<br>USA | IT administration for AMTC Dresden. |
| Chipbond Hsinchu | Chipbond Technology Corporation<br>No. 3, Li-Hsin Rd. V<br>Science Based Industrial Park<br>Hsin-Chu City<br>Taiwan, R.O.C. | Bumping. |
| NXP Hamburg TC | See NXP Hamburg | See NXP Hamburg. |
| NXP ATBK | NXP Semiconductors Thailand (ATBK)<br>303 Moo 3 Chaengwattana Rd., Laksi<br>Bangkok 10210<br>Thailand | Test centre, wafer treatment, module assembly, (pre-) personalization, delivery, and test program engineering (TPE). |
| NXP ATKH | NXP Semiconductors Taiwan Ltd (ATKH)<br>#10, Chin 5th Road, N.E.P.Z<br>Kaohsiung 81170<br>Taiwan, R.O.C. | Test centre, wafer treatment, module assembly, (pre-) personalization, and delivery. |
| Linxens Thailand | Linxens Co., Ltd.<br>142 Moo, Hi-Tech Industrial Estate, Tambon Ban Laean, Amphor Bang Pa-In<br>13160 Ayutthaya<br>Thailand | Inlay production. |
| HID Malaysia | HID Global Sdn. Bhd.<br>No. 2, Jalan i-Park 1/1<br>Kawasan Perindustrian i-Park<br>Bandar Indahpura<br>81000 Kulai, Johor<br>Malaysia | Inlay production. |

| | | |
|---|---|---|
| SIPI Chicago | Sipi Metals & Materials<br>1720 N. Elston Avenue Chicago, Illinois 60642-1579<br>United States | Secure Scapping. |

Table 8: Relevant development/production 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