Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1136-V2-2022

for

NXP Secure Smart Card Controller N7121 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-1136-V2-2022 (*)

Smartcard Controller

NXP Secure Smart Card Controller N7121 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 ASE_TSS.2, ALC_FLR.1

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations by advice of the Certification Body for components beyond 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, 7 June 2022

For the Federal Office for Information Security

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

Sandro Amendola
Head of Division

L.S.

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

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

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

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

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

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

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

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

2. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs [3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]

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

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

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

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

3. Recognition Agreements

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

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

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

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

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

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

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

3.2. International Recognition of CC – Certificates (CCRA)

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

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

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

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

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

4. Performance of Evaluation and Certification

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

The product NXP Secure Smart Card Controller N7121 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-1136-2021. The new certificate BSI-DSZ-CC-1136-V2-2022 replaces the certificate BSI-DSZ-CC-1136-2021. Specific results from the evaluation process BSI-DSZ-CC-1136-2021 were re-used only as of dated by the baseline certificate BSI-DSZ-CC-1136-2021. The evaluation resulted in a scope change outlined in a change to the Security Target and addressed in the Guidance Documentation and the new ETR-for Composition addendum.

The evaluation of the product NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3) was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 17 May 2022. 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 Germany 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.

[5] Information Technology Security Evaluation Facility

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.

As specific results from the evaluation process BSI-DSZ-CC-1136-2021 were re-used only as of dated by the baseline certificate BSI-DSZ-CC-1136-2021, this new certificate issued on 7 June 2022 has the same formal validity as the baseline certificate: 9 February 2026. Validity can be re-newed by a full re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.
4. to provide the ETR-for-Composition [10], the new addendum [36] and all related guidance documentation (see table 2 below) to any evaluator making reuse of the certification result, e.g. in a composite evaluation process.

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 N7121 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
Troplowitzstrasse 20
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 N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3)”, or in short “N7121”, which is manufactured by Globalfoundries 40nm (C40) technology and comprises of hardware, software (security IC Dedicated Software), and documentation. The N7121 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. 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:

- two logical cards (A and B),
- a System Mode OS which offers ready-to-use resource and access management for customer applications that do not want to be exposed to the more low-level features of the TOE, the System Mode OS also provides a Secure User Mode Box, which further restricts the access of code executed in User Mode (UM),
- 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, 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 ASE_TSS.2 and ALC_FLR.1.

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 (AES, TDES, RNG, RSA, ECC, Hashing, Utilities)

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 N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3)

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
TOE components for all configurations				
1	IC Hardware	N7121	B1	Hard macro instantiated within a wafer, modules or package.
2	IC Dedicated Test Software	Test Software	9.2.3.0	On-chip software.
3	IC Dedicated Software	Boot Software	9.2.3.0	On-chip software.
		Firmware	9.2.3.0	On-chip software
4	Document	NXP Secure Smart Card Controller N7121, Overview, Product data sheet [13]	3.3 / 2020-04-15	Electronic document (PDF via NXP DocStore).
5	Document	SmartMX3 family N7121, Wafer and delivery, specification [11]	3.3 / 2021-08-27	Electronic document (PDF via NXP DocStore).
6	Document	SmartMX3 family P71D321, Dedicated type creation [14]	3.1 / 2019-03-21	Electronic document (PDF via NXP DocStore).
7	Document	NXP Secure Smart Card Controller N7121, Instruction Set Manual, Product data sheet addendum [15]	3.0 / 2018-11-23	Electronic document (PDF via NXP DocStore).
8	Document	NXP Secure Smart Card Controller N7121, Chip Health Mode, Product data sheet addendum [16]	3.1 / 2020-06-30	Electronic document (PDF via NXP DocStore).

No	Type	Identifier	Release	Form of Delivery
9	Document	NXP Secure Smart Card Controller N7121, Peripheral Configuration and Use, Product data sheet addendum [17]	3.2 / 2020-02-18	Electronic document (PDF via NXP DocStore).
10	Document	NXP Secure Smart Card Controller N7121, MMU Configuration and NXP Firmware Interface Specification, Product data sheet addendum [18]	3.7 / 2021-09-10	Electronic document (PDF via NXP DocStore).
11	Document	NXP Secure Smart Card Controller N7121, Information on Guidance and Operation, Guidance and operation manual [12]	3.2 / 2019-05-28	Electronic document (PDF via NXP DocStore).
12	Document	NXP N7121 B1 Hardmacro, Lifecycle Documentation [19]	1.30 / 2020-06-18	Electronic document (PDF via NXP DocStore).
Deliverables of the Flash Loader OS				
13	IC Dedicated Support Software	Flashloader OS	1.2.5	On-chip software
14	Document	NXP Secure Smart Card Controller N7121, Flashloader OS, Product data sheet addendum [20]	3.0 / 2018-11-01	Electronic document (PDF via NXP DocStore).
Deliverables of the Library Interface				
15	IC Dedicated Support Software	Library Interface	9.2.3.0	On-chip software
16	Library	Communication Library	6.0.0	Electronic files (object files via NXP DocStore).
17	Library	CRC Library	1.1.8	Electronic files (object files via NXP DocStore).
18	Library	Memory Library	1.2.3	Electronic files (object files via NXP DocStore).
19	Library	Flash Loader Library	3.6.0	Electronic files (object files via NXP DocStore).
20	Documentation[7]	NXP Secure Smart Card Controller N7121, Shared OS Libraries, Product data sheet addendum [21]	3.2 / 2019-10-30	Electronic files (PDF via NXP DocStore).
Deliverables of the System Mode OS (for UM customers)				

[7]This guidance is available for NXP designers responsible for designing IO sidecar of a derived product only.

No	Type	Identifier	Release	Form of Delivery
21	IC Dedicated Support Software	System Mode OS	13.2.3.0	On-chip software.
22	Document	NXP Secure Smart Card Controller N7121, NXP System Mode OS, Product data sheet addendum [22]	3.6 / 2021-09-10	Electronic document (PDF via NXP DocStore).
Deliverables for Card-A Developer (NXP)[8]				
23	Document	NXP Secure Smart Card Controller N7121, Specification and Design Documentation [23]	1.0 / 2018-03-30	Electronic document (PDF via internal NXP network).
Deliverables of the Crypto Library				
24	IC Dedicated Support Software	Crypto Library	0.7.6	On-chip software.
Package Random Number Generation				
25	Library	RNG Lib	0.7.6	Electronic files (object files via NXP DocStore).
26	Library	RNG HealthTest Lib	0.7.6	Electronic files (object files via NXP DocStore).
27	Document	N7121 Crypto Library, RNG Library, Preliminary user manual [24]	1.2 / 2018-11-09	Electronic files (PDF via NXP DocStore).
Package Symmetric Ciphers				
28	Library	Sym. Cipher Lib	0.7.6	Electronic files (object files via NXP DocStore).
29	Document	N7121 Crypto Library, Symmetric Cipher Library (SymCfg), Preliminary user manual [25]	1.4 / 2018-09-19	Electronic files (PDF via NXP DocStore).
Package KeyStore				
30	Library	KeyStoreMgr	0.7.6	Electronic files (object files via NXP DocStore).
31	Document	N7121 Crypto Library, KeyStoreMgr Library, Preliminary user manual [26]	1.1 / 2018-09-19	Electronic files (PDF via NXP DocStore).
TOE components required for the packages Random Number Generation and Symmetric Ciphers				
32	Library	Sym. Utilities Lib	0.7.6	Electronic files (object files via NXP DocStore).
33	Document	N7121 Crypto Library, Utils Library, Preliminary user manual [27]	1.1 / 2018-02-02	Electronic files (PDF via NXP DocStore).
Package RSA Encryption / Decryption				

[8]NXP develops and owns all code for Card-A. These deliverables are available for NXP only.

No	Type	Identifier	Release	Form of Delivery
34	Library	RSA Lib	0.7.6	Electronic files (object files via NXP DocStore).
35	Document	N7121 Crypto Library, RSA Library, Preliminary user manual [28]	1.4 / 2019-03-28	Electronic files (PDF via NXP DocStore).
Package RSA Key Generation				
36	Library	RSA Key Generation Lib	0.7.6	Electronic files (object files via NXP DocStore).
37	Document	N7121 Crypto Library, RSA Key Generation Library, Preliminary user manual [29]	1.3 / 2018-10-11	Electronic files (PDF via NXP DocStore).
Package ECC over GF(p)				
38	Library	ECC Lib	0.7.6	Electronic files (object files via NXP DocStore).
39	Document	N7121 Crypto Library, ECC over GF(p) Library, Preliminary user manual [30]	2.3 / 2022-05-04	Electronic files (PDF via NXP DocStore).
Package SHA				
40	Library	SHA Library & Hash Library	0.7.6	Electronic files (object files via NXP DocStore).
41	Document	N7121 Crypto Library, SHA Library, Preliminary user manual [31]	1.1 / 2018-03-20	Electronic files (PDF via NXP DocStore).
42	Document	N7121 Crypto Library, HASH Library, Preliminary user manual [32]	1.2 / 2018-03-20	Electronic files (PDF via NXP DocStore).
TOE components required for the packages RSA Encryption / Decryption, RSA Key Generation, ECC over GF(p), and SHA				
43	Library	Asym. Utilities Lib	0.7.6	Electronic files (object files via NXP DocStore).
44	Document	N7121 Crypto Library, UtilsAsym Library, Preliminary user manual [33]	1.3 / 2018-04-13	Electronic files (PDF via NXP DocStore).
Package KoreanSeed (non-TSF)				
45	Library	KoreanSeed Lib	0.7.6	Electronic files (object files via NXP DocStore).
46	Document	N7121 Crypto Library, Korean Seed Library, User Manual [34]	1.1 / 2018-03-20	Electronic files (PDF via NXP DocStore).
TOE components required for all packages				
47	Document	N7121 Crypto Library, Information on Guidance and Operation, Product user manual [35]	3.4 / 2022-05-04	Electronic files (PDF via NXP DocStore).

Table 2: Deliverables of the TOE

Release packages R1 and R2 are manufactured at Globalfoundries Singapore (Fab 7) and consist of the deliverables given in Table 2 plus the instantiation specific IC Dedicated Software given in Table 3. The release packages R1 and R2 differ only in some functional improvements of the IC Dedicated Software. There is no impact on the security functionalities of the TOE. Release package R3 is used to identify devices manufactured at Globalfoundries Dresden (Fab 1). The instantiation specific IC Dedicated Software for R3 devices is equal to either R1 or R2.

Release Package	ID of Wafer Test Version	ID of the IC Dedicated Firmware Extensions
R1 or R3	0x83	0x0
	0x84	0x0
	0x90	0x50
R2 or R3	0x85	0x0
	0x87	0x1
	0x92	0x51

Table 3: Release Packages R1/R2/R3 and corresponding IDs

The requirements for the delivery of the TOE are described in chapter 3 of the Wafer and Delivery Specification [11]. The TOE documentation and related software (items are marked in Table 2) are delivered in electronic form by the document control centre by NXP Semiconductors with special protective measures.

The hardware version can be identified (optical identification) by its die inscription as described in [11] chapter 2.9.2.

The logical identification of the TOE is done via the firmware function call phfwSystem_GetVersion (in case of SM customers) or phosSystem_GetVersion (in case of UM customers, i.e., the NXP SM OS is present in System Mode of Logical Card B (SM-B). For more information refer to [16] chapter 3.3 and [19] chapter 4.1.3.2.

The global version number of the optional crypto library will be returned by calling the library function phCl_getVersion as describe in chapter 2.1 of [35]. Furthermore, [35], chapter 2 describes the integrity and confidentiality check of files associated with the crypto library. It lists SHA values for each library file for identification purposes.

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 specific 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, OE.Check_Init. Details can be found in the Security Target [6] and [9], chapter 4.2 and 4.3.

Note in particular the scope for the ECC point multiplication, see the ST-Lite [9] (Application Note in 6.1.4.4), and Guidance Document [30] (Chapter 2.8).

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. Onchip 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.,

- two logical cards (A and B),
- a System Mode OS which offers ready-to-use resource and access management for

- customer applications that do not want to be exposed to the more low-level features of the TOE,
- the System Mode OS also provides a Secure User Mode Box, which further restricts the access of code executed in User Mode (UM), 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, ECC, hashing and Utilities.

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.
    - Version of the DUT: 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,
  - a Java Card OS is used to execute reference transactions for banking and eGov, and
  - MIFARE tests.

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 A and B,
  - Tests in System Mode of card A and B,
  - 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].

The following table shows the size of the TOE's memories: (some are configurable to the customer others are fixed):

Memory type	Memory size	Description
NVM	Configurable up to 344 KBytes	The size of the Non-Volatile Memory.
ROM	Configurable to 0 KBytes or 150 KBytes	Size of the Read-Only Memory.
RAM	12 KBytes	Size of the Random-Access Memory. Size available to customer depends on ordered configuration (e.g., availability of MIFARE).

Table 4: TOE memory configuration limits

In chapter 1.4.1 of [6] and [9], the developer describes that TOE configurations can be applied either during the ordering process or even after delivery as a post-delivery configuration. The ST describes configuration options with security impact in detail while other configuration options are only listed to provide a full picture. Table 5 shows TOE configurations with security impact as described in chapter 1.4.1 of [6] and [9].

Other TOE configurations without security impact (following ST) are listed in chapter 1.4.1 of [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.

Product option	Choices	Description
NVM Size	Configurable in 1 kByte steps up to 344 kBytes	The Flash memory size is logically configurable, within the given step size. Note: If utilized, the Flashloader occupies 16 kB of storage, which are freed up after its usage.
Customer Type	• System Mode Customer • User Mode Customer	Depending on this choice, the customer has access to the System Mode of the logical card B (System Mode customer) or not (User Mode customer). In the first case, customers can store the Security IC Embedded Software in the System Mode of the logical card B. Otherwise, the NXP System Mode OS is placed on each available logical card in System Mode, while the customer can only access the less privileged User Mode.
Use Flash Loader	• Yes • No	Depending on this choice, the TOE provides the functionality of a Flash Loader such that customers can load their code to the NVM memory. If the Flash Loader is available, the Library Interface and the N7121 Crypto Library become mandatory. If the Flash Loader is not available, the customer can still decide whether the Security IC Embedded Software will be stored in ROM or Flash during the development process. The Security IC Embedded Software is then programmed to Flash by NXP and using the Flash Loader which will be removed afterwards.

Table 5: TOE configuration options

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 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.

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 ASE_TSS.2, ALC_FLR.1 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-1136-2021, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the changes in manufacturing sites of the TOE and changes to the user guidance of the TOE and the Security Target [6] and [9]. The Globalfoundries Fab1 Dresden (GF1) site was added to the production flow as a second site for wafer production. The new release package R3 is used to identify devices produced at this site. The equivalency of devices produced at both manufacturing sites is ensured by using the same test flow and test data. *The application note of SFR FCS_COP.1/ECC_DHKE was changed, for more details refer to chapter 6.1.4.4 of [6] and [9], as well as the Guidance Document [30] (Chapter 2.8).*

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 ASE_TSS.2, ALC_FLR.1

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

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

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The 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 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context) only.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 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	Yes
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	Yes
8	Random number generation	PTG.2	Comformant to [AIS31]	N/A	Yes
TOE Software(Crypto Library)					
9	Cryptographic primitive	AES	[FIPS197]	128, 192, 256	Yes
10	Confidentiality	AES encryption and decryption in CBC mode or CTR mode	[FIPS197] (AES), [NIST SP800-38A] (CBC, 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	Yes
14	Confidentiality	Triple-DES encryption and decryption in CBC mode	[NIST SP800-67] (TDES), [NIST SP800-38A] (CBC)	168	Yes

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
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	Yes
17	Cryptographic primitive	RSAEP, RSADP, RSASP1, RSAVP1	[PKCS #1]	512-1975	No
18	Cryptographic primitive	RSAEP, RSADP, RSASP1, RSAVP1	[PKCS #1]	1976 - 4096	Yes
19	Confidentiality	RSA encryption and decryption with EME-OAEP encoding	[PKCS #1]	512 - 1975	No
20	Confidentiality	RSA encryption and decryption with EME-OAEP encoding	[PKCS #1]	1976 - 4096	Yes
21	Cryptographic primitive	RSA signature generation and verification with EMSA-PSS encoding	[PKCS #1]	512 - 1975	No
22	Cryptographic primitive	RSA signature generation and verification with EMSA-PSS encoding	[PKCS #1]	1976 - 4096	Yes
23	Key derivation	RSA derivation of public key from private key	[AGD_CL_RSA, 4.4]	512 - 4096	N/A
24	Key generation	RSA key generation	[ALGO]	512 - 2047	No
25	Key generation	RSA key generation[9]	[ALGO], [FIPS 186-4]	2048 - 4096	Yes
26	Cryptographic primitive	ECDSA signature generation and verification	[ISO_14888-3], [ANS X9.62], [FIPS186-4], [IEEE_P1363]	224, 256, 320, 384, 512, 521	Yes
27	Key Exchange	ECDH	[ISO_11770-3], [ANS X9.62], [IEEE_P1363]	224, 256, 320, 384, 512, 521	Yes
28	Key generation	ECDSA Key Generation	[ISO_14888-3], [ANS X9.62], [FIPS186-4]	224, 256, 320, 384, 512, 521	Yes

[9]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 100 Bits
29	Cryptographic primitive	SHA-1	[FIPS180-4]	N/A	No
30	Cryptographic primitive	SHA-224, SHA-256, SHA-384, SHA-512	[FIPS180-4]	N/A	Yes
31	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) Conformant to [AIS20]	N/A	Yes
32	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) Conformant to [AIS20]	N/A	Yes
TOE Software (Flash Loader)					
33	Authenticity	MAC verification with AES in CMAC mode	[FIPS197] (AES), [NIST SP800-38B] (CMAC)	128	Yes
34	Authentication	MAC generation and verification with AES in CMAC mode	[FIPS197] (AES), [NIST SP800-38B] (CMAC)	128	Yes
35	Key derivation	Key derivation using AES in CMAC mode as pseudo-random function	[FIPS197] (AES), [NIST SP800-38B] (CMAC), [NIST SP800-108] (KBKDF)	128	Yes
36	Confidentiality	Decryption with AES in CBC mode	[FIPS197] (AES), [NIST SP800-38A] (CBC)	128	Yes

Table 6: TOE cryptographic functionality

[AGD_CL_RSA] N7121 Crypto Library, RSA Library, Preliminary user manual, Version 1.4, 2019-03-28, NXP Semiconductors.

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

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

[ALGO]	Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 07.12.2016 Veröffentlicht: BAnz AT 2016-12-30 B5, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen.
[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 11770-3: Information technology – Security techniques – Digital signatures with appendix Part 3: Discrete logarithm based mechanisms, August 2015, ISO/IEC
[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 January 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 document "ETR for composite evaluation" [10] and the Addendum to the ETR for Composition [36].

At the point in time when evaluation and certification results are reused there might be an update of the document "ETR for composite evaluation" available. Therefore, the certified products list on the BSI website has to be checked for latest information on reassessments, recertifications or maintenance result available for the product.

In addition, the following aspects need to be fulfilled when using the TOE:

Please note that for this re-evaluation, no full re-assessment of the TOE's security features has been conducted. An addendum to the ETR for Composition [36] has been created to update only those parts which have been reviewed and analysed. When using ECC point multiplication, in particular Chapter 2.8 of Guidance Document [30] should be observed, as well as VUL_P.28 in [36] which affects contact-based as well as contactless operation. The ETR for Composition [10] is only valid in combination with the Addendum to the ETR for Composition [36]. Therefore, for composite evaluations the creation date of the ETR for Composition [10] of the base evaluation is valid.

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

SM System Mode

ST Security Target

TOE Target of Evaluation

TSF TOE Security Functionality

UM User Mode

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[10] 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-1136-V2-2022, Version 2.5, 2022-05-04, NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3) Security Target, NXP Semiconductors (confidential document)

[7] Evaluation Technical Report NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3) B1, BSI-DSZ-CC-1136-V2-2022, Version 2, 2022-05-05, Evaluation Technical Report Summary, TÜV Informationstechnik GmbH (confidential document)

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

[9] Security Target Lite BSI-DSZ-CC-1136-V2-2022, Version 2.5, 2022-05-04, NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3) Security Target Lite, NXP Semiconductors

[10] ETR for composite evaluation according to AIS 36 for the Product 7121, BSI-DSZ-CC-1136-2021, Version 3, 2021-02-05, Evaluation Technical Report For Composite Evaluation (ETR Comp), TÜV Informationstechnik GmbH (confidential document)

[10] 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 37, Version 3, Terminologie und Verbreitung von Smartcard-Evaluierungen
- 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

[11] SmartMX3 family N7121, Wafer and delivery specification, Version 3.3, 2021-08-27, NXP Semiconductors (confidential document)

[12] NXP Secure Smart Card Controller N7121, Information on Guidance and Operation, Version 3.2, 2019-05-28, NXP Semiconductors (confidential document)

[13] NXP Secure Smart Card Controller N7121, Overview Product data sheet, Version 3.3, 2020-04-15, NXP Semiconductors

[14] SmartMX3 family P71D321, Dedicated type creation, Version 3.1, 2019-03-21, NXP Semiconductors

[15] NXP Secure Smart Card Controller N7121, Instruction Set Manual, Product data sheet addendum, Version 3.0, 2018-11-23, NXP Semiconductors

[16] NXP Secure Smart Card Controller N7121, Chip Health Mode, Product data sheet addendum, Version 3.1, 2020-06-30, NXP Semiconductors

[17] NXP Secure Smart Card Controller N7121, Peripheral Configuration and Use, Product data sheet addendum, Version 3.2, 2020-02-18, NXP Semiconductors

[18] NXP Secure Smart Card Controller N7121, MMU Configuration and NXP Firmware Interface Specification, Product data sheet addendum, Version 3.7, 2021-09-10, NXP Semiconductors

[19] NXP N7121 B1 Hardmacro, Lifecycle Documentation, Version 1.30, 2020-06-18, NXP Semiconductors

[20] NXP Secure Smart Card Controller N7121, Flashloader OS, Product data sheet addendum, Version 3.0, 2018-11-01, NXP Semiconductors

[21] NXP Secure Smart Card Controller N7121, Shared OS Libraries, Product data sheet addendum, Version 3.2, 2019-10-30, NXP Semiconductors

[22] NXP Secure Smart Card Controller N7121, NXP System Mode OS, Product data sheet addendum, Version 3.6, 2021-09-10, NXP Semiconductors

[23] NXP Secure Smart Card Controller N7121, Specification and Design Documentation, Version 1.0, 2018-03-30, NXP Semiconductors

[24] N7121 Crypto Library, RNG Library, Preliminary user manual, Version 1.2, 2018-11-09, NXP Semiconductors

[25] N7121 Crypto Library, Symmetric Cipher Library (SymCfg), Preliminary user manual, Version 1.4, 2018-09-19, NXP Semiconductors

[26] N7121 Crypto Library, KeyStoreMgr Library, Preliminary user manual, Version 1.1, 2018-09-19, NXP Semiconductors

[27] N7121 Crypto Library, Utils Library, Preliminary user manual, Version 1.1, 2018-02-02, NXP Semiconducors

[28] N7121 Crypto Library, RSA Library, Preliminary user manual, Version 1.4, 2019-03-28, NXP Semiconductors

[29] N7121 Crypto Library, RSA Key Generation Library, Preliminary user manual, Version 1.3, 2018-10-11, NXP Semiconductors

[30] N7121 Crypto Library, ECC over GF(p) Library, Preliminary user manual, Version 2.3, 2022-05-04, NXP Semiconductors

[31] N7121 Crypto Library, SHA Library, Preliminary user manual, Version 1.1, 2018-03-20, NXP Semiconductors

[32] N7121 Crypto Library, HASH Library, Preliminary user manual, Version 1.2, 2018-03-20, NXP Semiconductors

[33] N7121 Crypto Library, UtilsAsym Library, Preliminary user manual, Version 1.3, 2018-04-13, NXP Semiconductors

[34] N7121 Crypto Library, Korean Seed Library, User Manual, Version 1.1, 2018-03-20, NXP Semiconductors

[35] N7121 Crypto Library, Information on Guidance and Operation, Product user manual, Version 3.4, 2022-05-04, NXP Semiconductor

[36] Addendum to the Evaluation Technical for Composite Evaluation (ETR COMP) for the N7121 B1, version 2, 2022-05-05, TÜV Informationstechnik GmbH.

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-1136-V2-2022

Evaluation results regarding development and production environment

The IT product NXP Secure Smart Card Controller N7121 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 7 June 2022, 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 Troplowitzstr. 20 22529 Hamburg Germany	Project management, central design database, HW/FW/SW development and verification, security architecture and evaluation, flaw remediation, trust provisioning, and customer support.
NXP Master IT	NXP Semiconductors HTC Building 60 High Tech Campus 5656 Eindhoven Netherlands	Virtual IT Network and Administration site
NXP Gratkorn	NXP Semiconductors Austria GmbH Mikronweg 1 8101 Gratkorn Austria	Project management, HW/FW/SW development and verification, security architecture and evaluation, trust provisioning, and document control system (DocStore).
NXP Eindhoven Development	NXP Semiconductors Building 46, High Tech Campus HTC-46.3-west 5656 AE Eindhoven	HW/FW/SW development, security architecture.

	The Netherlands	
NXP Glasgow 2	NXP Glasgow EK Pegasus House, Scottish Enterprise Technology Park, 3 Bramah Ave East Kilbride, Glasgow G75 0RD Scotland, UK	Hardware development, security architecture and reviews.
NXP Leuven	NXP Semiconductors Interleuvenlaan 80 3001 Leuven Belgium	Hardware development, security reviews.
NXP Nijmegen	NXP Semiconductors Nijmegen B.V. Gerstweg 2 6534AE Nijmegen The Netherlands	Verification of design data and mask data, sample preparation.
GlobalLogic Wroclaw	GlobalLogic, Ul. Strzegomska 48A, 53-611 Wroclaw, Poland	SW development and verification.
Sii Gdansk 2	SII Olivia Prime Building, 10th floor, Grunwaldzka 472E 80-309 Gdansk Poland	SW development and verification.
NXP Eindhoven IT	NXP Semiconductors Netherlands B.V. Building 60, High Tech Campus HTC60, Secure Room (rooms 131, 133) 5656 AG Eindhoven The Netherlands	IT engineering and generic support.

NXP Bangalore	NXP India Private Limited Manyata Technology Park, Nagawara Village, Kasaba Hobli Bangalore 560 045 India	Data center
Colt Datacenter Hamburg	Colt Datacenter Hamburg Obenhauptstrasse 1C 22335 Hamburg Germany	Data center.
Akquinet Datacenter Hamburg	Akquinet Datacenter Hamburg Ulzburger Strasse 201 22850 Norderstedt Germany	Data center.
Digital Realty Phoenix	Digital Realty Data Center 120 E Van Buren St, Phoenix AZ 85004, U.S.A.	Data center.
Equinix Singapore	EQUINIX 20 Ayer Rajah Crescent, I BX SG1, Level 5 Unit 5, Ayer Rajah Industrial Park 139964 Singapore	Data center.
NXP Bucharest	NXP Semiconductors Romania Campus 6, Bulevardul Iuliu Maniu 6L, 061103 Bucureşti Romania	IT engineering and support.
NXP Guadalajara	NXP Guadalajara Periferico Sur #8110 Col. El Mante JALISCO, 45609 Tlaquepaque Mexico	IT engineering and support.

Chipbond Hsinchu	Chipbond Technology Corporation No. 3, Li-Hsin Rd. V Science Based Industrial Park Hsin-Chu City Taiwan, R.O.C.	Bumping.
NXP Hamburg TC	See NXP Hamburg.	Test Centre, personalization, and delivery.
NXP ATBK	NXP Semiconductors Thailand (ATBK) 303 Moo 3 Chaengwattana Rd., Laksi Bangkok 10210 Thailand	Test centre, wafer treatment, module assembly, (pre-) personalization, delivery, and test program engineering (TPE).
NXP ATKH	NXP Semiconductors Taiwan Ltd (ATKH) #10, Chin 5th Road, N.E.P.Z Kaohsiung 81170 Taiwan, R.O.C.	Test centre, wafer treatment, module assembly, (pre-) personalization, and delivery.
Global Foundries Dresden (Fab1)	GlobalFoundries Fab 1 Dresden, Wilschdorfer Landstrasse 101, 01109 Dresden, Germany	Mask and wafer production
Global Foundries Singapore (Fab 7)	GLOBALFOUNDRIES Singapore Pte Ltd 60 Woodlands Industrial Park D, Street 2 Singapore, 738406	Mask and wafer production.
AMTC Dresden	Advanced Mask Technology Center GmbH & Co KG (AMTC) Rähnitzer Allee 9 01109 Dresden Germany	Wafer mask production.
Linxens Thailand	Linxens Co., Ltd. 142 Moo, Hi-Tech Industrial Estate, Tambon Ban Laean, Amphor Bang Pa-In 13160 Ayutthaya Thailand	Inlay production.

HID Malaysia	HID Global Sdn. Bhd. No. 2, Jalan i-Park 1/1 Kawasan Perindustrian i-Park Bandar Indahpura 81000 Kulai, Johor Malaysia	Inlay production.

Table 7: 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