Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1040-2019

for

NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library

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-1040-2019 (*)

Smartcard Controller

NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library

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 and ASE_TSS.2

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, 14 June 2019

For the Federal Office for Information Security

Bernd Kowalski
Head of Division

L.S.

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

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

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

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

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

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

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

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

2. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.

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

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

[3] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

- 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.sogisportal.eu.

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

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

3.2. International Recognition of CC – Certificates (CCRA)

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

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

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

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

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

4. Performance of Evaluation and Certification

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

The product NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library has undergone the certification procedure at BSI.

The evaluation of the product NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library was conducted by Brightsight BV. The evaluation was completed on 31 May 2019.

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.

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 14 June 2019 is valid until 13 June 2024. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

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

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

6. Publication

The product NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[5] 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 Target of Evaluation (TOE) is the hard macro NXP Secure Smart Card Controller N7121, with IC Dedicated Software and an optional crypto Library (Crypto Library on N7121) and documentation describing instruction set and usage of the TOE. N7121 provides high security for smartcard applications and in particular for being used in the banking and finance market, in electronic commerce, or in governmental applications. 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. An optional System Mode OS is available, offering implemented functionality for customers that do not want to be exposed to the more low-level features of the TOE. The optional Flashloader OS supports download of code and data to Flash by the Composite Product Manufacturer before Operational Usage (e.g. during development). The optional Symmetric Crypto Library provides simplified access to cryptographic algorithms and basic functions.

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 and ASE_TSS.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
TSF.Service	This portion of the TSF comprises random number generation, reconfiguration of the TOE features, self-test functionality, as well as a secure channel for using the Flash Loader. It further provides mechanisms to store initialization, pre-personalization, and/or other data on the TOE.
TSF.Protection	This portion of the TSF comprises physical and logical protection to avoid information leakage and detect fault injection. It defines resets in case an error or attack was detected and guarantees that memories used by the optional available cryptographic libraries are cleared before other applications can access these memories.
TSF.Control	This portion of the TSF controls the operating conditions and manages the access rights to memories and peripherals for the

TOE Security Functionality	Addressed issue
	different TOE modes.
TSF.Crypto	This portion of the TSF provides cryptographic functionality such as TDES and AES in different modes depending on the availability of the N7121 Crypto Library. Furthermore, based on the availability of the N7121 Crypto Library, TSF.Crypto also covers asymmetric cryptography (RSA and ECC over GF(p)) and hashing.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [9], chapter 7.

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

The following table outlines the TOE deliverables:

No	Type	Identifier	Release / Date	Form of Delivery
TOE components for all configurations				
1	IC Hardware	N7121	B1	Hard macro instantiated within a wafer, modules and package.
2	IC Dedicated Test Software	Test Software	9.2.3	On-chip software
3	IC Dedicated Support Software	Boot Software	9.2.3	On-chip software
4		Firmware	9.2.3	On-chip software
5	Document	NXP Secure Smart Card Controller N7121 - Overview, Product data sheet	3.2 31-05-2019	Electronic document (PDF via NXP DocStore)

No	Type	Identifier	Release / Date	Form of Delivery
6	Document	NXP Secure Smart Card Controller N7121 – Instruction Set Manual, Objective data sheet addendum	3.0 23-11-2018	Electronic document (PDF via NXP DocStore)
7	Document	NXP Secure Smart Card Controller N7121 – Chip Health Mode, Objective data sheet addendum	3.0 23-11-2018	Electronic document (PDF via NXP DocStore)
8	Document	NXP Secure Smart Card Controller N7121 – Peripheral Configuration and Use, Objective data sheet addendum	3.1 20-12-2018	Electronic document (PDF via NXP DocStore)
9	Document	NXP Secure Smart Card Controller N7121 – MMU Configuration and NXP Firmware Interface Specification, Objective data sheet addendum	3.2 08-02-2019	Electronic document (PDF via NXP DocStore)
10	Document	NXP Secure Smart Card Controller N7121, Information on Guidance and Operation, Guidance and operation manual	3.2 28-05-2019	Electronic document (PDF via NXP DocStore)
Deliverables of the Flash Loader OS				
11	IC Dedicated Support Software	Flashloader OS	1.2.5	On-chip software
12	Document	NXP Secure Smart Card Controller N7121 – Flashloader OS, Objective data sheet addendum	3.0 01-11-2018	Electronic document (PDF via NXP DocStore)
Deliverables of the Library Interface				
13	IC Dedicated Support Software	Library Interface	9.2.3	On-chip software
14	Library	Communication Library	6.0.0	Electronic files (object files via NXP DocStore)
15	Library	CRC Library	1.1.8	Electronic files (object files via NXP DocStore)
16	Library	Memory Library	1.2.3	Electronic files (object files via NXP DocStore)
17	Library	Flash Loader Library	3.6.0	Electronic files (object files via NXP DocStore)
18	Document	NXP Secure Smart Card Controller N7121 – Shared OS Libraries, Objective data sheet addendum	3.0 01-11-2018	Electronic document (PDF via NXP DocStore)
Deliverables of the System Mode OS (for UM customers)				
19	IC Dedicated Support Software	System Mode OS	13.2.3	On-chip software
20	Document	NXP Secure Smart Card Controller N7121 – NXP System Mode OS, Objective data sheet addendum	3.2 08-02-2019	Electronic document (PDF via NXP DocStore)
Deliverables of the crypto library				

No	Type	Identifier	Release / Date	Form of Delivery
21	IC Dedicated Support Software	Crypto Library	0.7.6	Electronic files (object files via NXP DocStore)
Package Random Number Generation				
22	Library	RNG Lib	0.7.6	Electronic files (object files via NXP DocStore)
23	Library	RNG HealthTest Lib	0.7.6	Electronic files (object files via NXP DocStore)
24	Document	N7121 Crypto Library – RNG Library, Preliminary user manual	1.2 09-11-2018	Electronic document (PDF via NXP DocStore)
Package Symmetric Ciphers				
25	Library	Sym. Cipher Lib	0.7.6	Electronic files (object files via NXP DocStore)
26	Document	N7121 Crypto Library – Symmetric Cipher Library (SymCfg), Preliminary user manual	1.4 19-09-2018	Electronic document (PDF via NXP DocStore)
Package KeyStore				
27	Library	KeyStoreMgr Lib	0.7.6	Electronic files (object files via NXP DocStore)
28	Document	N7121 Crypto Library – KeyStoreMgr Library, Preliminary user manual	1.1 19-09-2018	Electronic document (PDF via NXP DocStore)
TOE components required for the packages Random Number Generation and Symmetric Ciphers				
29	Library	Sym. Utilities Lib	0.7.6	Electronic files (object files via NXP DocStore)
30	Document	N7121 Crypto Library – Utils Library, Preliminary user manual	1.1 02-02-2018	Electronic document (PDF via NXP DocStore)
Package RSA Encryption / Decryption				
31	Library	RSA Lib	0.7.6	Electronic files (object files via NXP DocStore)
32	Document	N7121 Crypto Library – RSA Library, Preliminary user manual	1.4 28-03-2019	Electronic document (PDF via NXP DocStore)
Package RSA Key Generation				
33	Library	RSA Key Generation Lib	0.7.6	Electronic files (object files via NXP DocStore)
34	Document	N7121 Crypto Library – RSA Key Generation Library, Preliminary user manual	1.3 11-10-2018	Electronic document (PDF via NXP DocStore)
Package ECC over GF(p)				
35	Library	ECC Lib	0.7.6	Electronic files (object files via NXP DocStore)
36	Document	N7121 Crypto Library – ECC over GF(p) Library, Preliminary user manual	2.1 28-03-2019	Electronic document (PDF via NXP DocStore)
Package SHA				

No	Type	Identifier	Release / Date	Form of Delivery
37	Library	SHA Library & Hash Library	0.7.6	Electronic files (object files via NXP DocStore)
38	Document	N7121 Crypto Library – SHA Library, Preliminary user manual	1.1 20-03-2018	Electronic document (PDF via NXP DocStore)
39	Document	N7121 Crypto Library – HASH Library, Preliminary user manual	1.2 20-03-2018	Electronic document (PDF via NXP DocStore)
TOE components required for the packages RSA Encryption / Decryption, RSA Key Generation, ECC over GF(p), and SHA				
40	Library	Asym. Utilities Lib	0.7.6	Electronic files (object files via NXP DocStore)
41	Document	N7121 Crypto Library – UtilsAsym Library, Preliminary user manual	1.3 13-04-2018	Electronic document (PDF via NXP DocStore)
TOE components required for all packages				
42	Document	N7121 Crypto Library, Information on Guidance and Operation, Product user manual	3.0 29-05-2019	Electronic document (PDF via NXP DocStore)

Table 2: Deliverables of the TOE

At the end of phase 3 or 4 the TOE is delivered to the customer in the form of a hardware wafer or module or package and a set of documents and electronic files.

- The hardware is delivered in parcels sealed with special tape;
- The guidance documents are delivered as pdf files from NXP DocStore;
- Library objects are delivered as electronic documents from NXP DocStore;

For a detailed description of the secure acceptance procedure of the TOE is referred to Chapter 2 and 3 of [18] for the hardware plus firmware, and Chapter 2 of [30] for the Crypto Library.

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 TOE implements physical and logical security functionality in order to protect user data stored and operated on the smartcard when used in a hostile environment. Hence the TOE maintains integrity and confidentiality of code and data stored in its memories and the different CPU modes with the related capabilities for configuration and memory access and for integrity, the correct operation and the confidentiality of security functionality provided by the TOE. Therefore the TOEs policy is to protect against malfunction, leakage, physical manipulation and probing. Besides, the TOE's life-cycle is supported as well as the user Identification whereas the abuse of functionality is prevented. Furthermore, random numbers generation as well as specific cryptographic services are being provided to be securely used by the smartcard embedded software.

Additionally, there is a hardware access control policy that regulates the access to memory areas and special function registers, as well as a access control policy for the Flash Loader.

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 4.3.

5. Architectural Information

The TOE is the hard macro NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library, which comprises hardware, software (security IC Dedicated Software).

- Hardware:

  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.

- Sofware:

  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

The Security Target specifies several configuration options. However, the actual hardware is always the same. The hardware differences are in the enabling and disabling of memory sections. The differences in software are in the delivery of software components in the form of object files or in access to on-chip firmware components.

7.1. Developer testing of the TOE (ATE_FUN):

The developer used a variety of test tools and test strategies to test the TOE Hardware, Firmware and Crypto Library.

The TOE Hardware/Firmware was tested with different strategies for ‘system testing’ and ‘module testing’. System testing includes the following test strategies:

- Power Verification
- Performance Verification
- Characterization
- Qualification
- Security Analysis
- Contactless Compliance Verification
- Contact Compliance Verification

There are three configuration options that affect the Crypto Library: presence or absence of the two parts of the Crypto Library and their location. All combinations thereof comprise a different configuration. The Crypto Library is primarily tested in FLASH, but configurations with a subset of the Crypto Library in ROM are also tested.

The tests cover all security functions and aspects of the TSF. The majority of the tests are performed by NXP through execution of test scripts. The testing is largely automated using a TestOS Operating System that allows convenient access to the Crypto Library functions from the outside. TestOS verifies that the functions return the expected values, and additionally it verifies that registers are cleared or restored (as specified by the Crypto Library function), that the CPU stack and workspace areas are properly cleared, that the Security Counter is correctly updated, and optionally that the CRC of the input parameter structure is correct. Thus, the protection of residual information has been verified for all functions where appropriate.

Besides TestOS, a fault injection simulator is used to indirectly test the responses to errors during operation. The fault injection simulator creates an interrupt after every instruction and increments the program counter when a target instruction has been performed to simulate the skipping of code lines. Finally, code inspection is performed to assess the presence of countermeasures that cannot adequately be tested using direct testing. Thus, the protection against side channel analysis and perturbation attacks has been verified by performing code inspection on the countermeasures in the implementation representations of all components whose side channel protection is not provided by the hardware.

The developer has performed extensive testing on FSP, subsystem, module and module interface level. To aid in the analysis of test coverage and depth, a simulator has been used that assesses which lines of the code have been hit during particular tests, and which branches have been taken.

All parameter choices have been addressed at least once and cryptographic operations with keys of all key sizes have been tested at least once. All boundary cases identified have been tested explicitly, and negative testing is performed where appropriate. The code coverage analysis shows that indeed all different behaviour of the (module) interfaces has been tested.

The test results provided by the developer show that all tests of hardware and firmware and Crypto Library functionality have concluded positively and that no deviations from the expected values have been found.

7.2. Independent testing (ATE_IND)

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

During the evaluation of the TOE the following types of tests were performed.

- Simulation tests
- Wafer test
- Tests in System mode of logical card A and B
- Tests in test mode
- Hardware tests
- Cryptographic library tests

With these tests the entire security functionality of the TOE was tested. The functional testing results of the evaluator showed that the TOE exhibited the expected behaviour. No deviations were found.

7.3. Penetration testing (AVA_VAN)

Penetration tests were devised after performing a public search for potential vulnerabilities and after performing a methodical vulnerability analysis. Intensive penetration testing was planned based on the analysis results and performed for the underlying mechanisms of security functionalities. All penetration tests concluded as expected. The overall conclusion is that the N7121 is protected against attackers with high attack potential when the user guidance is followed. The user of the TOE (the embedded software developer) must implement the advices of the user guidances [11] - [30].

8. Evaluated Configuration

The N7121 can be delivered with various configuration options as described in section 1.4.1 of [6] and [9]. The configuration options are divided into two groups: major configuration options and minor configuration options.

The major configuration is provided with several minor configuration options. These minor configuration options (and all others) for NXP Secure Smart Card Controller N7121 can be selected by the customer via electronic Order Entry Form. The Order Entry Form identifies all the minor configuration options, which are supported by the major configuration.

The N7121 hardware platform was tested including all minor configuration options that can be selected based on Table 3 in chapter 1.4.1 of [6] and [9]. All minor configurations were available to the evaluator. The major configuration does not have dependencies to security features. All minor configuration options that are part of the evaluation were tested. The minor configuration options behave as specified and therefore the results described in this document are applicable for all minor configurations described in [6] and [9].

The TOE does not include a customer-specific Security IC Embedded Software.

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

The evaluation has confirmed:

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

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].

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

AES	Advanced Encryption Standard
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
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ECB	Electronic Code Book
ECDH	Elliptic Curve Diffie-Hellman protocol
ECDSA	Elliptic Curve Digital Signature Algorithm
EEC	Elliptic Curve Cryptography
EEPROM	Electrically Erasable Read Only Memory
ES	Embedded Software
ETR	Evaluation Technical Report
HW	Hardware
IC	Integrated Circuit

ISO	International Organization for Standardization
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MMU	Memory Management Unit
NIST	National Institute of Standards and Technology
OS	Operating system
PP	Protection Profile
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
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[6] 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] specifically

- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) – (Requirements for the structure and contents of a CC-evaluation Intermediate Report)
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC
- 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 39, Formal Method, Version 3.0, 24.10.2008
- AIS 46, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, Version 3, 04.12.2013.
- AIS 47, Version 1.1, Regelungen zu Site Certification

[6] NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library Security Target, BSI-DSZ-CC-1040-2019, Rev. 1.5, 31 May 2019, NXP Semiconductors (confidential document)

[7] Evaluation Technical Report NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (N7121), BSI-DSZ-CC-1040-2019, Version 8.0, 31 May 2019, Brightsight (confidential document)

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

[9] NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library Security Target Lite, BSI-DSZ-CC-1040-2019, Rev. 1.1, 31 May 2019, NXP Semiconductors (sanitised public document)

[10] ETR for Composition NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (N7121), BSI-DSZ-CC-1040-2019, Version 8.0, 31 May 2019, Brightsight (confidential document)

[11] NXP Secure Smart Card Controller N7121 Overview, Product data sheet, Revision 3.2, 31 May 2019, NXP Semiconductors (confidential document)

[12] NXP Secure Smart Card Controller N7121 Platform Instruction Set Manual, Revision 3.0, 23 November 2018, NXP Semiconductors (confidential document)

[13] NXP Secure Smart Card Controller N7121 Chip Health Mode, Revision 3.0, 23 November 2018, NXP Semiconductors (confidential document)

[14] NXP Secure Smart Card Controller N7121 Peripheral Configuration and Use, Revision 3.1, 20 December 2018, NXP Semiconductors (confidential document)

[15] NXP Secure Smart Card Controller N7121 MMU Configuration and NXP Firmware Interface Specification, Revision 3.2, 8 February 2019, NXP Semiconductors (confidential document)

[16] NXP Secure Smart Card Controller N7121 Flashloader OS, Revision 3.0, 1 November 2018, NXP Semiconductors (confidential document)

[17] NXP Secure Smart Card Controller N7121 Shared OS Libraries, Revision 3.0, 1 November 2018, NXP Semiconductors (confidential document)

[18] NXP Secure Smart Card Controller N7121 Information on Guidance and Operation, Revision 3.2, 28 May 2019, NXP Semiconductors (confidential document)

[19] NXP Secure Smart Card Controller N7121 NXP System Mode OS, Revision 3.2, 8 February 2019, NXP Semiconductors (confidential document)

[20] N7121 Crypto Library. ECC over GF(p). Revision 2.1, 28 March 2019, NXP Semiconductors (confidential document)

[21] N7121 Crypto Library. Hash Library. Revision 1.2, 20 March 2018, NXP Semiconductors (confidential document)

[22] N7121 Crypto Library. RNG Library. Revision 1.2, 09 November 2018, NXP Semiconductors (confidential document)

[23] N7121 Crypto Library, KeyStoreMgr Library. Revision 1.1, 19 September 2018, NXP Semiconductors (confidential document)

[24] N7121 Crypto Library. RSA Library. Revision 1.4, 28 March 2019, NXP Semiconductors (confidential document)

[25] N7121 Crypto Library. RSA Key Generation Library. Revision 1.3, 11 October 2018, NXP Semiconductors (confidential document)

[26] N7121 Crypto Library. SHA Library. Revision 1.1, 20 March 2018, NXP Semiconductors (confidential document)

[27] N7121 Crypto Library. Symmetric Cipher Library (SymCfg). Revision 1.4, 19 September 2018, NXP Semiconductors (confidential document)

[28] N7121 Crypto Library. Utils Library. Revision 1.1, 02 February 2018, NXP Semiconductors (confidential document)

[29] N7121 Crypto Library. UtilsAsym Library. Revision 1.3, 13 April 2018, NXP Semiconductors (confidential document)

[30] N7121 Crypto Library. Information on Guidance and Operation. Revision 3.0, 29 May 2019, NXP Semiconductors (confidential document)

[31] N7121_Firmware_Sources_CW1810_MRA_FM_x413B_r140220.csv, 21 June 2018, NXP Semiconductors (confidential document)

[32] N7121_Digital_Design_Source_CW1810_MRA_FM_x413B_r43732.csv, 21 June 2018, NXP Semiconductors (confidential document)

[33] NXP Secure Smart Card, Controller N7121, Common Criteria CIL, 6 July, 2018, NXP Semiconductors (confidential document)

[34] N7121 Crypto Library, Configuration Item List, 07 April 2018, NXP Semiconductors (confidential document)

[35] Evaluation Reference List, v1.3, 31 May 2019, NXP Semiconductors (confidential document)

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 detailled 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 C: Overview and rating of cryptographic functionalities implemented in the TOE

Annex B of Certification Report BSI-DSZ-CC-1040-2019

Evaluation results regarding development and production environment

The IT product NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (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 14 June 2019, 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_TAT.3, ALC_FLR.1)

are fulfilled for the development and production sites of the TOE listed below:

Site	Role in the life-cycle
NXP Hamburg Troplowitzstr. 20 22529 Hamburg Germany	• Software Development Software Test • Simulation Hardware Development Hardware Test • Simulation Silicon Prototype Tests Order Fulfillment ROM • Flash Coding Center Data Center • IT Management Configuration Mgmt Trust Provisioning Flaw Remediation Documentation • Testing • Personalization • Packaging Engineering / Customer Samples • Warehouse & Delivery • Shipping • Distribution Of Tools & Documentation
NXP Munich North Schatzbogen 7, 81829 Munich Germany	• Software Development
NXP Gratkorn Mikron-Weg 1 8108 Gratkorn Austria	• Software Development Software Test • Simulation Hardware Development Hardware Test • Simulation Silicon Prototype Tests Documentation • Tools & Documentation
NXP Leuven Interleuvenlaan 80 B-3001 Leuven Belgium	• IP Development Security Reviews NXP
NXP High Tech Campus Building 60 Secure RoomNXP Nijmegen Gerstweg 2, 6534AE Nijmegen, Netherlands	• Hardware Testing

Site	Role in the life-cycle
NXP Glasgow Phoenix House, 3 Bramah Avenue, Scottish Enterprise Technology Park, East Kilbride, G75 0RD UK	• Hardware Development • Security Reviews
NXP Eindhoven (DevWing) HTC-46.3-west Building 46, High Tech Campus, 5656AE Eindhoven The Netherlands	• Hardware Development • Hardware Test • Simulation Software Development
NXP Eindhoven (HTC60) Building 60, Secure Room 131 and 133, 5656AE Eindhoven, The Netherlands	• IT Management
NXP ATBK 303 Moo 3 Chaengwattana Rd. Laksi, Bangkok 10210 Thailand	• Testing • Personalization • Packaging
NXP ATKH #10, Chin 5th Road, N.E.P.Z, Kaohsiung 81170 Taiwan, R.O.C	• Testing • Personalization • Packaging
GlobalLogic Zilina Antona Bernoláka 334/72 010 01 Žilina Slovakia	• Software Development
GlobalLogic Wroclaw Strzegomska 56B Street, 53-611 Wroclaw, Poland	• Software Development
SII Gdansk Olivia Star Sii Sp. z o. o. Grunwaldzka 472C 80-309 Gdansk Poland	• Software Development
AMTC AMAdvanced Mask Technology Center GmbH & Co KG Rähnitzer Allee 9 01109 Dresden Germany	• Mask Manufacturing
GLOBALFOUNDRIES Woodlands Campus 60 Woodlands Industrial Park D, Street 2 Singapore, 738406	• Manufacturing
Chipbond Hsinchu Chipbond Technology Corporation No. 3, Li-Hsin Rd. V, Science Based Industrial Park, Hsin-Chu City, Taiwan, R.O.C.	• Bumping

Site	Role in the life-cycle
SMARTRAC Technology Ltd. (= Linxens) 142 Moo 1 Hi-Tech Industrial Estate Tambon Ban Laean, Amphor Bang-Pa-In 13160 Ayutthaya Thailand	• Assembly
HID Global Ireland Teoranta Paic Tionscail na Tulaigh Balle na hAbhann Co. Galway Ireland	• Assembly
HCL Gothenburg Gunnar Engellaus väg 3, Gothenburg 418 78 Sweden	• IT Management
Datacenter Akquinet Hamburg Ulsburger Strasse 201, 22850 Norderstedt Germany	• Provision of remote access to data
Datacenter Colt Hamburg Obenhauptstrasse 22335 Hamburg Germany	• Provision of remote access to data

Table 3: Relevant development/production sites for the respective TOE configurations

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.

Annex C of Certification Report BSI-DSZ-CC-1040-2019

Overview and rating of cryptographic functionalities implemented in the TOE

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key size in bits	Security Level Above 100 bits	Comments
1	Cryptographic Primitive	AES	[FIPS 197] (AES)	128, 192, 256	Yes	FCS_COP.1/AES in the AES co-processor
2	Confidentiality	AES encryption and decryption in ECB mode	[FIPS 197] (AES), [NIST SP 800-38A] (ECB),	128, 192, 256	No	FCS_COP.1/AES_LIB optionally in the Crypto Library
3	Confidentiality	AES encryption and decryption in CBC mode or CTR mode	[FIPS 197] (AES), [NIST SP 800-38A] (CBC and CTR mode),	128, 192, 256	Yes	FCS_COP.1/AES_LIB optionally in the Crypto Library
4	Integrity	AES MAC generation in CBC-MAC mode	[FIPS 197] (AES), [ISO/IEC 9797-1] and Algorithm 1 (CBC-MAC mode).	128, 192, 256	No	FCS_COP.1/AES_LIB optionally in the Crypto Library
5	Integrity	AES MAC generation in CMAC mode	[FIPS 197] (AES), And [NIST SP 800-38B] (CMAC mode).	128, 192, 256	Yes	FCS_COP.1/AES_LIB optionally in the Crypto Library
6	Cryptographic Primitive	Triple-DES	[NIST SP 800-67], [NIST SP 800-38A].	112	No	FCS_COP.1/TDES In the TDES coprocessor
7	Cryptographic Primitive	Triple-DES	[NIST SP 800-67], [NIST SP 800-38A].	168	Yes	FCS_COP.1/TDES In the TDES coprocessor
8	Confidentiality	Triple-DES encryption and decryption in ECB mode	[NIST SP 800-67] (TDES), [NIST SP 800-38A] (ECB mode)	112, 168	No	Optionally in the Crypto Library: FCS_COP.1/TDES_LIB

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key size in bits	Security Level Above 100 bits	Comments
9	Confidentiality	Triple-DES encryption and decryption in CBC mode	[NIST SP 800-67] (TDES), [NIST SP 800-38A] (ECB mode)	112	No	Optionally in the Crypto Library: FCS_COP.1/TDES_LIB
10	Confidentiality	Triple-DES encryption and decryption in CBC mode	[NIST SP 800-67] (TDES), [NIST SP 800-38A] (CBC mode)	168	Yes	Optionally in the Crypto Library: FCS_COP.1/TDES_LIB
11	Integrity	Triple-DES MAC generation in the modes CBC-MAC, Retail-MAC, CMAC	[NIST SP 800-67] (TDES), [ISO/IEC 9797-1], Algorithm 1 (CBC-MAC mode), [ISO/IEC 9797-1], Algorithm 3 (Retail-MAC mode), and [NIST SP 800-38B] (CMAC mode).	112	No	Optionally in the Crypto Library: FCS_COP.1/TDES_LIB
12	Integrity	Triple-DES MAC generation in CBC-MAC mode	[NIST SP 800-67] (TDES), [ISO/IEC 9797-1], Algorithm 1 (CBC-MAC mode)	168	No	Optionally in the Crypto Library: FCS_COP.1/TDES_LIB
13	Integrity	Triple-DES MAC generation in CMAC mode	[NIST SP 800-67] (TDES), [NIST SP 800-38B] (CMAC mode).	168	Yes	Optionally in the Crypto Library: FCS_COP.1/TDES_LIB
14	Cryptographic Primitive	RSAEP, RSADP, RSASP1, RSAVP1	[PKCS #1]	512 to 1975	No	Optionally in the Crypto Library: FCS_COP.1/RSA
15	Cryptographic Primitive	RSAEP, RSADP, RSASP1, RSAVP1	[PKCS #1]	1976 to 4096	Yes	Optionally in the Crypto Library: FCS_COP.1/RSA
16	Confidentiality	RSA encryption and decryption with EME-OAEP encoding	[PKCS #1], [CryptoLib-UM-RSA]	512 to 1975	No	Optionally in the Crypto Library FCS_COP.1/RSA_PAD combined with FCS_COP.1/RSA
17	Confidentiality	RSA encryption and decryption with EME-OAEP encoding	[PKCS #1], [CryptoLib-UM-RSA]	1976 to 4096	Yes	Optionally in the Crypto Library FCS_COP.1/RSA_PAD combined with FCS_COP.1/RSA
18	Cryptographic Primitive	RSA signature generation and verification with EMSA-PSS encoding	[PKCS #1]	512 to 1975	No	Optionally in the Crypto Library FCS_COP.1/RSA_PAD combined with FCS_COP.1/RSA
19	Cryptographic Primitive	RSA signature generation and verification with EMSA-PSS encoding	[PKCS #1]	1976 to 4096	Yes	Optionally in the Crypto Library FCS_COP.1/RSA_PAD combined with FCS_COP.1/RSA
20	Key derivation	RSA derivation of public key from private key	[CryptoLib-UM-RSAKG]	512 bits to 4096	N/a	Optionally in the Crypto Library FCS_COP.1/RSA_PubExp
21	Key generation	RSA key generation	[BSSS], [CryptoLib-UM-RSAKG]	512 to 1975	No	Optionally in the Crypto Library FCS_CKM.1/RSA
22	Key generation	RSA Key Generation	[FIPS 186-4] B.3.3, [BSSS], [CryptoLib-UM-RSAKG]	1976 to 4096	Yes	Optionally in the Crypto Library FCS_CKM.1/RSA
23	Cryptographic primitive	ECDSA signature generation and verification	[ISO/IEC 14888-3], [ANSI X9.62-2005], [FIPS 186-4], [IEEE Std 1363], [CryptoLib-UM-ECC]	224, 256, 320, 384, 512, 521 bits	Yes	Optionally in Crypto Library: FCS_COP.1/ECDSA

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key size in bits	Security Level Above 100 bits	Comments
24	Key Exchange	ECDH	[ISO/IEC 11770-3], [ANSI X9.63], [IEEE Std 1363].	224, 256, 320, 384, 512, 521 bits	Yes	Optionally in Crypto Library: FCS_COP.1/ECC_DHK E
25	Key generation	ECDSA Key Generation	[ISO/IEC 14888-3], [ANSI X9.62-2005], [FIPS 186-4]	224, 256, 320, 384, 512, 521 bits	Yes	Optionally in the Crypto Library FCS_CKM.1/ECDSA
26	Cryptographic Primitive	SHA-1,	[FIPS 180-4].	N/A	No	Optionally in Crypto Library: FCS_COP.1/SHA
27	Cryptographic Primitive	SHA-224, SHA-256, SHA-384, and SHA-512	[FIPS 180-4].	N/A	Yes	Optionally in Crypto Library: FCS_COP.1/SHA
28	Confidentiality	AES encryption and decryption in CBC mode	[FIPS 197], [NIST SP 800-38A], [PUF]	128 bits	Yes	Optionally in Crypto Library: FCS_COP.1/AES_PUF
29	Integrity	AES MAC generation and verification in CBC-MAC mode	[FIPS 197], [ISO/IEC 9797-1] (CBC-MAC) [PUF]	128 bits	No	Optionally in Crypto Library: FCS_COP.1/MAC_PUF
30	Key Derivation	Proprietary PUF Key Derivation	[PUF]	128 bits	Yes	Optionally in Crypto Library: FCS_CKM.1/PUF
31	Cryptographic Primitive	PTG.2	[HW-UM] Conformant to [AIS20/31]	N/a	Yes	FCS_RNG.1/PTG.2
32	Cryptographic Primitive	PTG.3 with counter with AES or TDES	[FIPS 197] [NIST SP 800-67] [NIST SP800-90A] [CryptoLib-UM], [CryptoLib-UM-RNG] Conformant to [AIS20/31]	N/a	Yes	FCS_RNG.1/PTG.3 TDES is three-key
33	Cryptographic Primitive	DRG.4 with counter with AES or TDES	[FIPS 197] [NIST SP 800-67] [NIST SP800-90A] [CryptoLib-UM], [CryptoLib-UM-RNG] Conformant to [AIS20/31]	N/a	Yes	FCS_RNG.1/DRG.4 TDES is three-key
34	Authenticity	MAC verification With AES in CMAC mode	[FIPS 197] (AES), [NIST SP 800-38B] (CMAC mode).	128	Yes	FlashLoader FL_Auth Authenticity of flash contents to be loaded FDP_UIT.1/Loader FlashLoader FL_Auth Integrity of Secure Messaging
35	Authentication	MAC generation and verification With AES in CMAC mode	[FIPS 197] (AES), [NIST SP 800-38B] (CMAC mode), [HW-TDS], table 1841 (Authentication).	128	Yes	FlashLoader FL_Auth Mutual Authentication
36	Key derivation	Key derivation using pseudo-random function based on AES in CMAC mode as PRF.	[FIPS 197] (AES), [NIST SP 800-38B] (CMAC mode). [NIST SP800-108] [DSheet_FL]	128	Yes	FlashLoader FL_Auth Key derivation
37	Confidentiality	Decryption with AES in CBC mode	[FIPS 197] (AES), [NIST SP 800-38A] (CBC mode). [DSheet_FL]	128	Yes	FTP_UCT.1/Loader FlashLoader FL_Auth Confidentiality of Secure Messaging

Table 4: TOE cryptographic functionality

[CryptoLib-UM] N7121 Crypto Library. Information on Guidance and Operation. Revision 3.0, 29 May 2019

[CryptoLib-UM-ECC] N7121 Crypto Library. ECC over GF(p). Revision 2.1, 28 March 2019

[CryptoLib-UM-RSA] N7121 Crypto Library. RSA Library. Revision 1.4, 28 March 2019

[CryptoLib-UM-RSAKG] N7121 Crypto Library. RSA Key Generation Library. Revision 1.3, 11 October 2018

[HW-TDS] NXP Secure Smart Card Controller N7121 Specification and Design Documentation, Revision 1.0, 30 March 2018

[HW-UM] NXP Secure Smart Card Controller N7121 Information on Guidance and Operation, Revision 3.2, 28 May 2019

[PUF] PUF Key derivation function specification, NXP Semiconductors, BUID, 2014

[ANSI X9.62-1999] ANSI X9.62-1999: Public Key Cryptography for the Financial Services Industry: the Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standards Institute (ANSI), 1999

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

[ANSI X9.63] ANSI X9.63: Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve cryptography, American National Standard, January 2011

[ANSSI 2011] ANSSI 2011: http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000024668816, American National Standards Institute (ANSI), 1999.

[BSSS] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), German “Bundesanzeiger“, BAnz AT 30.01.2015 B3

[FIPS 180-4] FIPS PUB 180-4 Federal Information Processing Standards Publication Secure Hash Standard (SHS), August 2015, Information Technology Laboratory National Institute of Standards and Technology.

[FIPS 186-4] FIPS PUB 186-4 Federal Information Processing Standards Publication Digital Signature Standard (DSS), July 2013, Information Technology Laboratory National Institute of Standards and Technology.

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

[IEEE Std 1363] "IEEE Standard Specifications for Public-Key Cryptography", IEEE Computer Society, IEEE Std 1363™-2000, December 2005

[ISO/IEC 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/IEC 11770-3] ISO/IEC 11770-3-2015: Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques, 2015

[ISO/IEC 14888-3] ISO/IEC 14888-3:2015: Information technology – Security techniques – Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms, 2016

[NIST SP 800-38A] NIST Special Publication 800-38A, Recommendation for BlockCipher Modes of Operation , National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce

[NIST SP 800-38B] NIST Special Publication 800-38B, Recommendation for BlockCipher Modes of Operation: The CMAC Mode for Authentication, National Institute of Standards and Technology

[NIST SP 800-67] NIST Special Publication 800-67 –Revision 1, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher – Revised January 2012, National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce

[NIST SP 800-90a] NIST SP 800-90A, Revision 1: Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015, Elaine Barker and John Kelsey, Special Publication, National Institute of Standards and Technology [PKCS #1] PKCS #1: RSA Cryptography Standard, Version 2.2, October 27, 2012, RSA Laboratories

[NIST SP800-108] NIST SP 800-108, Recommendation for Key Derivation using Pseudorandom Functions, October 2009

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

[RFC 5639] RFC 5639: J. Merkle, ECC Brainpool Standard Curves and Curve Generation, BSI, March 2010

Note: End of report