Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0977-V2-2019

for

NXP Secure Smart Card Controller N7021 VA including IC Dedicated Software

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

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 N7021 VA including IC Dedicated Software has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0977-2017. Specific results from the evaluation process BSI-DSZ-CC-0977-2017 were re-used.

The evaluation of the product NXP Secure Smart Card Controller N7021 VA including IC Dedicated Software was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 18 July 2019. 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.

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 31 July 2019 is valid until 31 July 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

[5] Information Technology Security Evaluation Facility

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 N7021 VA including IC Dedicated Software 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 Target of Evaluation (TOE) is the IC hardware platform “NXP Secure Smart Card Controller N7021 VA including IC Dedicated Software” and documentation describing instruction set and usage of the TOE. The TOE does not include a customer-specific Security IC Embedded Software.

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. A System Mode OS is available (optional), offering 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 Flashloader OS (optional) supports download of code and data to Flash by the Composite Product Manufacturer before Operational Usage (e.g. during development). The Symmetric Crypto Library (optional) provides simplified access to frequently used symmetric cryptography algorithms.

The N7021 VA supports two logical cards (Card A and Card B). Both logical cards are divided into a User Mode and a System Mode. The logical location of the Security IC Embedded Software depends on the usage of the IC hardware platform. Card A is reserved for Security IC Embedded Software developed by NXP. Card B is available for Security IC Embedded Software developed by the customer. If a customer did not order any NXP developed Security IC Embedded Software product, then User Mode Card A is not present.

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, 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**
Security Services	
SS.RNG	Random Number Generator
SS.SW_RNG	Hybrid Deterministic/Hybrid Physical Random Number Generator
SS.HW_TDES	Triple-DES coprocessor
SS.SW_DES	Triple-DES Software Support
SS.HW_AES	AES coprocessor
SS.SW_AES	AES Software Support

TOE Security Functionality	Addressed issue
SS.Loader	Loader
SS.SELF_TEST	Self Test
SS.RESET	Reset Functionality
SS.RECONFIG	Post Delivery Configuration
Security Features	
SF.OPC	Control of Operating Conditions
SF.PHY	Protection against Physical Manipulation
SF.LOG	Logical Protection
SF.COMP	Protection of Mode Control
SF.MEM_ACC	Memory Access Control
SF.SFR_ACC	Special Function Register Access Control
SF.MEM_SUB	Secure User Mode Box Firewall
SF.Object_Reuse	Reuse of Memory
SF.PUF	PUF

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 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 N7021 VA including IC Dedicated Software

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
Deliverables for all configurations of the TOE				
1	IC Hardware	N7021 VA	VA	Wafer, modules and package

No	Type	Identifier	Release	Form of Delivery
2	IC Dedicated Test Software	Test software	20.0	On-chip software
3	IC Dedicated Support Software	Boot software	20.0	Part of SuperSystemMode.dat
4	IC Dedicated Support Software	Firmware interface	20.0	On-chip software
5	Document	SmartMX3 family P71D320 Overview, pinning and electrical characteristics, Product data sheet [11]	3.1 / 2019-06-04	PDF via NXP DocStore
6	Document	SmartMX3 N7021 Instruction Set Manual, Objective data sheet addendum [12]	1.4 / 2016-09-29	PDF via NXP DocStore
7	Document	SmartMX3 family N7021 Wafer and delivery specification, Objective wafer specification [13]	1.3 / 2018-05-15	PDF via NXP DocStore
8	Document	SmartMX3 N7021 Post Delivery Configuration Post Delivery Configuration, Objective data sheet addendum [14]	1.1 / 2017-03-22	PDF via NXP DocStore
9	Document	SmartMX3 N7021 Chip Health Mode, Chip Health Mode, Objective data sheet addendum [15]	1.0 / 2016-12-06	PDF via NXP DocStore
10	Document	SmartMX3 N7021 Peripheral Configuration and Use, Objective data sheet addendum [16]	1.4 / 2017-11-03	PDF via NXP DocStore
11	Document	SmartMX3 N7021 MMU configuration & FW interface, Data Sheet addendum [17]	1.5 / 2017-11-03	PDF via NXP DocStore
12	Document	SmartMX3 N7021, Inter-Card Communication Functionality and additional APIs, Objective data sheet addendum [18]	1.1 / 2017-03-09	PDF via NXP DocStore
13	Document	SmartMX3 N7021 NVM Operate Function, Data Sheet addendum [19]	1.0 / 2017-01-13	PDF via NXP DocStore
14	Document	NXP Secure Smart Card Controller N7021 Information on Guidance and Operation, Guidance and Operation Manual [20]	1.4 / 2019-06-04	PDF via NXP DocStore
Deliverables of the Flashloader OS				
15	IC Dedicated Support Software	Flashloader OS	20.0	On-chip software
16	Document	SmartMX3 N7021 FlashLoader, Objective data sheet addendum [21]	1.3 / 2018-08-24	PDF via NXP DocStore
Deliverables of the Library Interface				
17	IC Dedicated Support Software	Library Interface	20.0	On-chip software
18	Library File	libComm		SDK installer via NXP DocStore

No	Type	Identifier	Release	Form of Delivery
19	Library File	libCrc		SDK installer via NXP DocStore
20	Library File	libMem		SDK installer via NXP DocStoreSDK installer via NXP DocStore
21	Library File	libFL		SDK installer via NXP DocStoreSDK installer via NXP DocStore
22	Document	SmartMX3 N7021 Shared OS Libraries Memory, communication and CRC, including guidance and operation, Objective data sheet addendum [22]	1.2 / 2017-11-03	PDF via NXP DocStore
Deliverables of the System Mode OS				
23	IC Dedicated Support Software	System Mode OS	20.0	On-chip software
24	Document	SmartMX3 N7021 NXP System Mode OS Interface, Objective data sheet addendum [23]	1.6 / 2017-11-03	PDF via NXP DocStore
Deliverables of the Crypto Library Iron				
25	IC Dedicated Support Software	Crypto Library Iron	2.0.6-01	On-chip software
26	Library Files	Crypto Library Iron	2.0.6-01	SDK installer via NXP DocStoreSDK installer via NXP DocStore
27	Document	Crypto Library V1.0 on N7021 VA, Symmetric Cipher Library (SymCfg), User manual [24]	1.2 / 2017-02-13	PDF via NXP DocStore
28	Document	N7021 Crypto Library, RNG Library, User manual [25]	1.3 / 2017-03-27	PDF via NXP DocStore
29	Document	N7021 Crypto Library, Utils Library, User manual [26]	1.1 / 2016-11-28	PDF via NXP DocStore
30	Document	Crypto Library Iron on N7021 VA, Information on Guidance and Operation, Guidance and Operation Manual [27]	2.0 / 2018-11-15	PDF via NXP DocStore

Table 2: Deliverables of the TOE

The requirements for the delivery of the TOE are described in chapter 31 of the “Product Data Sheet” [11]. For each delivery form of the hardware platform NXP offers two ways of delivery of the TOE:

1. The customer collects the product himself at the NXP site.

2. The product is sent to the customer by NXP with special protective measures.

The TOE documentation and related software (items are marked in Table 5) are delivered in electronic form by the document control centre of NXP.

The hardware version can be identified by a coded nameplate as described in [13] chapters 2.9.2 and 3.2.

The TOE further provides the FabKey which can be configured by the customer to hold 128 bytes for batch, wafer or die individual data and can be read out by the configuration interface (see GetFabKey API in [17], chapter 5 and [23], chapter 5.2). The process of FabKey submission is described in [11], chapter 26.

Only the configurations defined in [17], chapter 5.6.3.2, Tab. 5.40 and in [23], chapter 5.8.3.2, Tab. 5.57 are evaluated options.

The ST references the version of the Crypto Library. This version number is also noted in the [27], chapter 2 thus the TOE components listed in the guidance are traceable to the reference given in the Security Target [6] and [9]. Furthermore, [27], chapter 2 describes the integrity and confidentiality check of files associated with the crypto library. It lists SHA-256 values for each library file for identification purposes. In addition to identifying the delivered components, the library identifies itself via its “GetVersion” command.

3. Security Policy

The security policy enforced is defined by the selected 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 the symmetric cryptographic block cipher algorithm 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 chapter 7 of the Security Target [6] and [9].

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE Environment. The following topics are of relevance: 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 4.3.

5. Architectural Information

The IC hardware is a microcontroller incorporating a central processing unit (CPU), memories accessible via a Memory Management Unit (MMU), cryptographic coprocessors, other security components and several electrical communication interfaces. The central processing unit supports a 32-/16-bit instruction set optimized for smart card applications. The first and in some cases the second byte of an instruction are used for operation encoding. On-chip memories are ROM, RAM and Flash. The Flash can be used as data or program memory. It consists of highly reliable memory cells, which are designed to provide data integrity. Flash 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 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. A System Mode OS is available (optional), offering 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 Flashloader OS (optional) supports download of code and data to Flash by the Composite Product Manufacturer before Operational Usage (e.g. during development). The Symmetric Crypto Library (optional) provides simplified access to frequently used symmetric cryptography algorithms.

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 developer’s testing effort can be summarised in the following aspects.

TOE test configuration and Developer’s 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
  - Functional Module verification: For the functional verification, black-box testing and white-box testing is performed to ensure the correct functionality as specified in the functional specification and customer specifications (ordering options).
  - Security Verification: This test category addresses the security mechanisms described in the Security Architecture description. Two main categories of security module verification are defined, i.e., integrity protection module

verification (fault injection) and DPA module verification (side-channel analysis). This also includes black-box and white-box testing.

- 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.

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,
  - Tests in test mode
  - Hardware tests and
  - Cryptographic library tests.

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

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 N7021 VA can be delivered with various configuration options as described in chapter 1.4.2 of [6] and [9]. The configuration options are divided into two groups: major configuration options and minor configuration options.

Three major configurations can be chosen by the customer during the ordering process:

- Configuration based on 320 kBytes of Flash memory as code space,
- Configuration based on 240 kBytes of Flash memory as code space,
- Configuration based on 144 kBytes of ROM memory as code space.

Each major configuration is provided with several minor configuration options. These minor configuration options (and all others) for NXP Secure Smart Card Controller N7021 VA can be selected by the customer via Order Entry Form (see [28]). The Order Entry Form identifies all the minor configuration options, which are supported by the major configuration.

The N7021 VA hardware platform was tested including all minor configuration options that can be selected based on Table 1.2 in chapter 1.4.2.2 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 described in [11] and [20]. 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 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-0977-2017, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the life cycle and updates in the documentation of the TOE.

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
Hardware					
1.	Cryptographic primitive	3-key Triple DES	[NIST SP800-67]	|k| = 168	Yes
2.	Cryptographic primitive	AES	[FIPS197]	|k| = 128 / 192 / 256	Yes
3.	Cryptographic primitive	Physical RNG PTG.2	[AIS31]	-	Yes
4.	Confidentiality	3-key Triple DES in ECB mode without padding	[NIST SP800-67] [NIST SP800-38A]	|k| = 168	No
5.	Confidentiality	AES in ECB mode without padding	[FIPS197], [NIST SP800-38A]	|k| = 128 / 192 / 256	No
6.	Confidentiality	AES encryption and decryption in CBC mode	[FIPS 197] [NIST SP 800-38A] [ADV_ATE, 6.8.3.7.1]	|k| = 128	Yes
7.	Integrity	AES MAC generation and verification in CBC-MAC mode	[FIPS 197] [ISO 9797-1] [ADV_ATE, 6.8.3.7.1]	|k| = 128	No
8.	Key Derivation	Proprietary PUF Key Derivation	[ADV_ATE, 6.8.3.7.1]	|k| = 128	Yes
Crypto Library (optional)					
9.	Cryptographic primitive	3-key Triple DES	[NIST SP800-67]	|k| = 168	Yes
10.	Cryptographic primitive	AES	[FIPS197]	|k| = 128 / 192 / 256	Yes
11.	Confidentiality	3-key Triple DES in CBC mode	[NIST SP 800-67] [NIST SP 800-38A]	|k| = 168	Yes

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
12.	Confidentiality	AES in CBC mode	[FIPS197] [NIST SP 800-38A]	|k| = 128 / 192 / 256	Yes
13.	Integrity	3-key Triple DES in CBC-MAC mode	[NIST SP 800-67] [ISO_9797-1]	|k| = 168	No
14.	Integrity	3-key Triple DES in Retail-MAC mode	[NIST SP 800-67] [ISO_9797-1]	|k| = 168	Yes
15.	Integrity	3-key Triple DES in CMAC mode	[NIST SP 800-67] [NIST SP800-38B]	|k| = 168	Yes
16.	Integrity	AES in CBC-MAC mode	[FIPS197] [ISO_9797-1]	|k| = 128 / 192 / 256	No
17.	Integrity	AES in CMAC mode	[FIPS197] [NIST SP800-38B]	|k| = 128 / 192 / 256	Yes
18.	Cryptographic primitive	Hybrid-Physical PTG.3 based on CTR_DRBG with AES-128/192/256	[AIS31] [FIPS 197] [NIST SP800-90A] [AGD_CL_RNG]	N/A	Yes
19.	Cryptographic primitive	Hybrid-Physical PTG.3 based on CTR_DRBG with 3-key TDES	[AIS31] [NIST SP 800-67] [NIST SP800-90A] [AGD_CL_RNG]	N/A	Yes
20.	Cryptographic primitive	Hybrid-Deterministic DRG.4 based on CTR_DRBG with AES-128/192/256	[AIS31] [FIPS 197] [NIST SP800-90A] [AGD_CL_RNG]	N/A	Yes
21.	Cryptographic primitive	Hybrid-Deterministic DRG.4 based on CTR_DRBG with 3-key TDES	[AIS31] [NIST SP 800-67] [NIST SP800-90A] [AGD_CL_RNG]	N/A	Yes
Flash Loader (optional, depends on crypto library)					
22.	Confidentiality	AES in CBC mode with constant IV	[FIPS197] [NIST SP800-38A]	|k| = 128	Yes
23.	Authenticity	MAC verification with AES in CMAC mode	[FIPS197] [NIST SP800-38B]	|k| = 128	Yes
24.	Key derivation	KBKDF based on AES in CMAC mode	[NIST SP800-108] [FIPS197] [NIST SP800-38B] [ADV_ATE, 6.12.3.4.1.2.6]	|k| = 128	Yes

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
25.	Authentication	Mutual Authentication Protocol based on MAC generation and verification With AES in CMAC mode	[FIPS 197] [NIST SP 800-38B] [ADV_ATE, 6.12.3.4.1.2.8]	|k| = 128	Yes

Table 3: TOE cryptographic functionality

[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.

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

[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

[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

[ADV_ATE] NXP Secure Smart Card Controller N7021 Classes ADV and ATE – Sys.P4, Version 1.6, 2017-03-30, NXP Semiconductors

[AGD_CL_RNG] N7021 Crypto Library RNG Library, Product user manual, Version 1.3, 2017-03-27, 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].

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

11. Security Target

For the purpose of publishing, the Security Target [9] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement

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

13.2. Glossary

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

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

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

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7] 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] NXP Secure Smart Card Controller N7021 VA Security Target, BSI-DSZ-CC-0977-V2-2019, Version 2.3, 2019-06-04, NXP Semiconductors (confidential document)

[7] Evaluation Technical Report N7021 VA, BSI-DSZ-CC-0977-V2, Version 4, 2019-07-17, 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] NXP Secure Smart Card Controller N7021 VA Security Target Lite, BSI-DSZ-CC-0977-V2-2019, Version 2.3, 2019-06-04, NXP Semiconductors (sanitised public document)

[10] Evaluation Technical for Composite Evaluation for the N7021 VA, BSI-DSZ-CC-0977-V2 version 4, 2019-07-17, TÜV Informationstechnik GmbH (confidential document)

[7] specifically

- AIS1, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers, Version 13, 14.08.2008,
- AIS14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 03.08.2010,
- AIS19, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC, Version 9, 03.11.2014,
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 8, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 9, 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 4, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2, Reuse of evaluation results
- AIS39, Formal Method, Version 3.0, 24.10.2008
- AIS46, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, Version 3, 04.12.2013.

[11] SmartMX3 family P71D320 Overview, pinning and electrical characteristics, Product data sheet, Version 3.1, 2019-06-04, NXP Semiconductors (confidential document)

[12] SmartMX3 N7021 Instruction Set Manual, Objective data sheet addendum, Version 1.4, 2016-09-29, NXP Semiconductors (confidential document)

[13] SmartMX3 family N7021 Wafer and delivery specification, Objective wafer specification, Version 1.3, 2018-05-15, NXP Semiconductors (confidential document)

[14] SmartMX3 N7021 Post Delivery Configuration Post Delivery Configuration, Objective data sheet addendum, Version 1.1, 2017-03-22, NXP Semiconductors (confidential document)

[15] SmartMX3 N7021 Chip Health Mode Chip Health Mode, Objective data sheet addendum, Version 1.0, 2016-12-06, NXP Semiconductors (confidential document)

[16] SmartMX3 N7021 Peripheral Configuration and Use Peripheral Configuration and Use on the N7021, Objective data sheet addendum, Version 1.4, 2017-11-03, NXP Semiconductors (confidential document)

[17] SmartMX3 N7021 MMU configuration & FW interface Access / resource management and security configuration, Data Sheet addendum, Version 1.5, 2017-11-03, NXP Semiconductors (confidential document)

[18] SmartMX3 N7021, Inter-Card Communication Functionality and additional APIs, Objective data sheet addendum, Version 1.1, 2017-03-09, NXP Semiconductors (confidential document)

[19] SmartMX3 N7021 NVM Operate Function, Data Sheet addendum, Version 1.0, 2017-01-13, NXP Semiconductors (confidential document)

[20] NXP Secure Smart Card Controller N7021 Information on Guidance and Operation, Guidance and Operation Manual, Version 1.4, 2019-06-04, NXP Semiconductors (confidential document)

[21] SmartMX3 N7021 FlashLoader, Product Data Sheet addendum, Version 1.3, 2018-08-24, NXP Semiconductors (confidential document)

[22] SmartMX3 N7021 Shared OS Libraries Memory, communication and CRC, including guidance and operation, Objective data sheet addendum, Version 1.2, 2017-11-03, NXP Semiconductors (confidential document)

[23] SmartMX3 N7021 NXP System Mode OS Interface UM configuration and applications, Objective data sheet addendum, Version 1.6, 2017-11-03, NXP Semiconductors (confidential document)

[24] Crypto Library V1.0 on N7021 VA Symmetric Cipher Library (SymCfg), User manual, Version 1.2, 2017-02-13, NXP Semiconductors (confidential document)

[25] N7021 Crypto Library RNG Library, Product user manual, Version 1.3, 2017-03-27, NXP Semiconductors (confidential document)

[26] N7021 Crypto Library Utils Library, User manual, Version 1.1, 2016-11-28, NXP Semiconductors (confidential document)

[27] Crypto Library Iron on N7021 VA Information on Guidance and Operation, User manual, Version 2.0, 2018-11-15, NXP Semiconductors (confidential document)

[28] Order Entry Form, Version 1.9, 2017-03-27, NXP Semiconductors

[29] Crypto Library Iron / Cobalt V1.0 on N7021 VA, Life Cycle, Version 1.3, 2017-03-07, NXP Semiconductors (confidential document)

[30] P71D320 Crypto Library, Configuration Item List, Evaluation documentation, Version 1.0, 2017-03-07, NXP Semiconductors (confidential document)

[31] NXP Secure Smart Card Controller 7021 VA Evaluation Reference List, Version 2.2, 2019-07-17, NXP Semiconductors (confidential document)

[32] NXP Secure Smart Card Controller N7021, Common Criteria CIL, Version 0.5, 2017-04-06, 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 B of Certification Report BSI-DSZ-CC-0977-V2-2019

Evaluation results regarding development and production environment

The IT product NXP Secure Smart Card Controller N7021 VA including IC Dedicated Software (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 31 July 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_FLR.1, ALC_LCD.1, ALC_TAT.3)

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

Name of site / Company name	Address	Function
NXP Hamburg	NXP Semiconductors Germany GmbH Troplowitzstr. 20 22529 Hamburg Germany	SW/HW Development, Delivery, central design database, ROM/Flash code handling, configuration of the Fabkey, and customer support, CM and Tooling
NXP Gratkorn	NXP Semiconductors Austria GmbH Mikronweg 1 8101 Gratkorn Austria	SW/HW development, testing and documentation
NXP Eindhoven Development	NXP Semiconductors Building 46, High Tech Campus HTC-46.3-west 5656 AE Eindhoven The Netherlands	Development centre
NXP Glasgow 2	NXP Glasgow EK. 3 Bramah Avenue, Phoenix House, Scottish Enterprise Technology Park East Kilbride G75 0RD Scotland	Hardware development, security reviews
NXP Leuven	NXP Semiconductors Interleuvenlaan 80 B-3001 Leuven Belgium	Hardware development, security reviews
NXP Munich North	NXP Semiconductors Germany GmbH Schatzbogen 7 81829 Munich Germany	SW development
NXP Nijmegen	NXP Semiconductors Nijmegen B.V. Gerstweg 2 6534AE Nijmegen The Netherlands	Development and Manufacturing, Regional Quality Centre – Europe

Name of site / Company name	Address	Function
GlobalLogic Wroclaw	GLOBALLOGIC REC sp. z o.o. Strzegomska 56B Street 53-611 Wroclaw Poland	SW development
Sii Gdansk 2	Sii Sp. z o. o./Branch in Gdansk Olivia Star, 17th floor Grunwaldzka 472C 80-309 Gdansk Poland	SW development
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
HCL Gothenburg	HCL Gothenburg Gunnar Engellaus väg 3 Gothenburg 418 78 Sweden	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 Hamburg Obenhauptstrasse 22335 Hamburg Germany	Data center
Akquniet Datacenter Hamburg	AKQUINET Hamburg Ulzburger Strasse 201 22850 Norderstedt Germany	Data center
TSMC Hsinchu	Taiwan Semiconductor Manufacturing Company Limited Fab 2/5, Fab 8, Fab 14A	Mask data preparation, Mask and wafer production
Chipbond Hsinchu	No. 3, Li-Hsin Rd. V Science Based Industrial Park Hsin-Chu City Taiwan, R.O.C.	Bumping
TCE-H (part of NXP Hamburg)	NXP Semiconductors Germany GmbH Troplowitzstr. 20 22529 Hamburg Germany	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

Table 4: 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.

Note: End of report