

# Certification Report

**BSI-DSZ-CC-1019-V2-2019**

for

**Crypto Library Cobalt on N7021 VA**

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-1019-V2-2019 (\*)**

Smartcard Controller

**Crypto Library Cobalt on N7021 VA**

from NXP Semiconductors Germany GmbH

PP Conformance: Security IC Platform Protection Profile with  
Augmentation Packages Version 1.0, 13 January  
2014, BSI-CC-PP-0084-2014

Functionality: PP conformant plus product specific extensions  
Common Criteria Part 2 extended

Assurance: Common Criteria Part 3 conformant  
EAL 6 augmented by ASE\_TSS.2, ALC\_FLR.1



SOGIS  
Recognition Agreement



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.

Bonn, 29 October 2019

For the Federal Office for Information Security



Common Criteria  
Recognition Arrangement  
recognition for components  
up to EAL 2 and ALC\_FLR  
only

Joachim Weber  
Head of Branch

L.S.



Bundesamt für Sicherheit in der Informationstechnik

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

This page is intentionally left blank.

## Contents

A. Certification.....	6
1. Preliminary Remarks.....	6
2. Specifications of the Certification Procedure.....	6
3. Recognition Agreements.....	7
4. Performance of Evaluation and Certification.....	8
5. Validity of the Certification Result.....	8
6. Publication.....	9
B. Certification Results.....	10
1. Executive Summary.....	11
2. Identification of the TOE.....	12
3. Security Policy.....	14
4. Assumptions and Clarification of Scope.....	14
5. Architectural Information.....	14
6. Documentation.....	15
7. IT Product Testing.....	15
8. Evaluated Configuration.....	17
9. Results of the Evaluation.....	18
10. Obligations and Notes for the Usage of the TOE.....	21
11. Security Target.....	22
12. Regulation specific aspects (eIDAS, QES).....	22
13. Definitions.....	22
14. Bibliography.....	24
C. Excerpts from the Criteria.....	27
D. Annexes.....	28

## 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<sup>1</sup>
- BSI Certification and Approval Ordinance<sup>2</sup>
- BSI Schedule of Costs<sup>3</sup>
- 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<sup>4</sup> [1] also published as ISO/IEC 15408.

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

<sup>2</sup> 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

<sup>3</sup> 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.sogis.eu>.

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

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

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

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

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

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

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

<sup>4</sup> 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 Crypto Library Cobalt on N7021 VA has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1019-2017. Specific results from the evaluation process BSI-DSZ-CC-1019-2017 were re-used.

The evaluation of the product Crypto Library Cobalt on N7021 VA was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 16 October 2019. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)<sup>5</sup> 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 29 October 2019 is valid until 28 October 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

<sup>5</sup> 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 Crypto Library Cobalt on N7021 VA 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<sup>6</sup> of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

<sup>6</sup> 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), Crypto Library Cobalt on N7021 VA, comprises 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. It further comprises the Crypto Library Cobalt on N7021 VA 2.0.8 which provides additional functionality for asymmetric cryptography and hashing. The composite TOE does not include a customer-specific Security IC Embedded Software. This report mainly concentrates on the description of the additional features and tests for the library part introduced by the composite evaluation. For more information see the certification report of the hardware platform [13].

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 Crypto Library Cobalt on N7021 VA provides access to RSA encryption and decryption, RSA key-pair generation, RSA public-key computation, ECDSA (ECC over GF(p)) for signature generation, ECDSA (ECC over GF(p)) key pair generation, ECDH (ECC Diffie-Hellmann) key exchange, as well as SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512.

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 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The security functionality of the hardware platform for the N7021 is described in the Hardware Security Target [15]. They entirely apply to this Security Target.

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

TOE Security Functionality	Addressed issue
SS.RSA	The TOE provides functions that implement the RSA algorithm and the RSA-CRT algorithm for data encryption, decryption, signature and verification.
SS.RSA_Pad	The TOE provides functions that implement the RSA algorithm and the

TOE Security Functionality	Addressed issue
	RSA-CRT algorithm for message and signature encoding.
SS.RSA_PublicExp	The TOE provides functions that implement computation of an RSA public key from a private CRT key.
SS.ECDSA	The TOE provides functions to perform ECDSA Signature Generation and Signature Verification.
SS.ECC_DHKE	The TOE provides functions to perform Diffie-Hellman Key Exchange.
SS.RSA_KeyGen	The TOE provides functions to generate RSA key pairs.
SS.SHA	The TOE implements functions to compute the Secure Hash Algorithms SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512.
SF.LOG	Logical Protection
SF.OPC	Control of Operating Conditions
SF.PHY	Protection against Physical Manipulation

Table 1: Additional TOE Security Functionalities

For more details please refer to the Security Target [6] and [9], chapter 7 and the hardware platform Security Target [15].

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 3.4, 3.2 and 3.3.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

## 2. Identification of the TOE

The Target of Evaluation (TOE) is called:

### Crypto Library Cobalt on N7021 VA

The following table outlines the additional TOE deliverables to the hardware platform [13]:

#	Type	Name	Release	Form of delivery
<b>RSA</b>				
1	Library	RSA Library	2.0.8	Electronic files
2	Document	N7021 Crypto Library: User Manual – RSA	1.4	Electronic document

<b>RSA Key Generation</b>				
3	Library	RSA Key Generation Library	2.0.8	Electronic files
4	Document	N7021 Crypto Library: User Manual - RSA Key Generation	1.0	Electronic document
<b>ECC over GF(p)</b>				
5	Library	ECC Library	2.0.8	Electronic files
6	Document	N7021 Crypto Library: User Manual - ECC over GF(p)	1.2	Electronic document
<b>Package SHA</b>				
7	Library	SHA Library	2.0.8	Electronic files
8	Document	N7021 Crypto Library: User Manual – SHA	1.0	Electronic document
9	Document	N7021 Crypto Library: User Manual - Hash Library	1.0	Electronic document
<b>Required for all packages</b>				
10	Library	Asymmetric Utilities Library	2.0.8	Electronic files
11	Document	N7021 Crypto Library: User Manual – UtilsAsym	1.0	Electronic document
12	Document	N7021 Crypto Library: User Guidance Manual - Crypto Library Cobalt on N7021 VA	1.8	Electronic document

Table 2: Deliverables of the TOE

The TOE, its version, its commercial type name, the major-, minor-, post-delivery configurations and its components are all identified in [9], [15] and the Guidance and Operation Manual [12].

Furthermore, the evaluator reviewed the respective guidance documentation and reviewed the identification process as described by the developer.

The hardware version can be identified by unique coded nameplate, as described in the Product Data Sheet [16].

Within the evaluation of this TOE the developer made full reuse of previously audited and evaluated sites.

The requirements for the delivery of TOE are described in the Product Data Sheet. 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 are delivered in electronic form by the document control centre of NXP.

The delivery of the Crypto Library is addressed in [12 a] chapter 2. Here, identification of a certified product, and the different forms and ways of delivery are given. The description covers delivery of the guidance and libraries, identification of the TOE and related measures to avoid masquerade attacks.

### 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.

### 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 security objective for the “Security Objectives for the Operational environment” defined in the Protection Profile, and given in the Hardware Security Target are entirely valid for this evaluation. No new objectives for the TOE-Environment were defined.

Details can be found in the Security Target [6] and [9], chapter 4.3 and the hardware platform Security Target [15].

### 5. Architectural Information

The TOE consists of the IC hardware and IC Dedicated Software. The IC Dedicated Software is composed of IC Dedicated Test Software for test purposes and IC Dedicated Support Software. The IC Dedicated Test Software contains the Test Software, the IC Dedicated Support Software is composed of the Boot Software, the Firmware Interface, the Library Interface, the Symmetric Crypto Library, the System Mode OS and the

Flashloader OS. All other software is called Security IC Embedded Software. The Security IC Embedded Software is not part of the TOE.

## 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

### Developer's Test according to ATE\_FUN

TOE test configuration:

- The tests are performed with the TOE and a simulator.

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 sufficiently test the TOE.
  - 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 ageing of the device due to high temperatures to guarantee the lifetime of the product,
    - Flash qualification to ensure that features like anti-tearing and wear levelling work as specified,

- Package qualification to ensure that the IC can be placed in the final delivery form (package) under industrial environments and the final product quality is achieved, and
- PUF qualification to ensure that the promised PUF properties hold in field conditions.
- Validation: Execution of all customer-visible use cases to ensure that the entire system works as defined for customer-visible operation. This includes
  - on-chip test framework developed to use each officially released product variant and execute each public available API,
  - a Java Card OS is used to execute reference transactions for banking and egov, and

Amount of developer testing performed:

- The tests are performed on security mechanisms on subsystem and module level.
- As demonstrated by ATE\_COV.3 the developer has tested all security mechanisms and TSFIs.
- As demonstrated by ATE\_DPT.3 the developer has tested all the TSF subsystems and modules against the TOE design and against the security architecture description.

### **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 STs, the Functional Specification and the TOE Design, 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.

Selection criteria:

- All security mechanisms and security features (portions of the TSF) and related interfaces were tested, therefore no selection criteria are applied. All security mechanisms and related interfaces are tested regarding their functional behaviour. The tests were chosen to perform at minimum one test for each security mechanism of TSF and related interfaces.



## 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 not exploitable 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 rationale 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.

### Attack scenarios having been tested:

- Effectiveness of the TOE security functionality,
- Effectiveness of filters and detectors,
- Effectiveness of bus and memory encryption,
- Differential Fault Analysis,
- Simple and Differential Power Analysis,
- EMA / SEMA / DEMA Attacks,
- Effectiveness of deactivation of test functions,
- Effectiveness of the horizontal and vertical firewalls, and
- Statistical tests of TOE generated random numbers.

## 8. Evaluated Configuration

The composite TOE consists of the IC hardware platform N7021 VA with IC Dedicated Software and documentation describing instruction set and usage of the TOE and the Crypto Library Cobalt on N7021 VA. The composite TOE does not include a customer-specific Security IC Embedded Software.

The N7021 VA hardware platform was tested in the context of its evaluation (BSI-DSZ-CC-0977-V2-2019) including all minor configuration options that can be selected based on the information found in chapter 1.4.2 of the hardware Security Target [15]. All minor configurations are 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. Therefore, the results described in this document are applicable for all minor configurations described in the hardware Security Target [15].

## 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) *Composite product evaluation for Smart Cards and similar devices (see AIS 36). According to this concept the relevant guidance documents of the underlying platform and the documents ETR for Composition from the platform evaluations have been applied in the TOE evaluation.*

(see [4], AIS 25, AIS 26, AIS 37).

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-1019-2017, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on a reassessment of the security functionality provided by the Crypto Library Cobalt on N7021 VA as well as an updated production flow.

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.

In addition to the cryptographic functionalities of the HW platform listed in [13], the composite TOE provides the following additional cryptographic services:

No.	Purpose	Cryptographic Mechanism	Implementation Standard	Key Size in Bits	Security Level above 100 Bits
1	Confidentiality	RSAEP encryption	[PKCS #1, 5.1.1]	k  = 512 - 4096	Yes for  k  ≥ 1976 bit
		RSADP decryption	[PKCS #1, 5.1.2]	k  = 512 - 4096	Yes for  k  ≥ 1976 bit
		RSA encryption and decryption with EME-OAEP encoding	[PKCS #1, 7.1.1 / Step 2] (see [12 d])	k  = 512 - 4096	Yes for  k  ≥ 1976 bit
2	Cryptographic Primitive	RSASP1 signature generation	[PKCS #1, 5.2.1]	k  = 512 - 4096	Yes for  k  ≥ 1976 bit
		RSAPV1 signature verification	[PKCS #1, 5.2.2]	k  = 512 - 4096	Yes for  k  ≥ 1976 bit
		RSA signature generation and verification in EMSA-PSS encoding	[PKCS #1, 9.1] (see [12 d])	k  = 512 - 4096	Yes for  k  ≥ 1976 bit
3	Key generation	RSA public key computation	[PKCS #1] (see [12 d])	k  = 512 - 4096	Yes for  k  ≥ 1976 bit
		RSA key-pair generation <sup>7</sup>	[PKCS #1] and [FIPS186-4] (see [12 d])	k  = 512 - 4096	Yes for  k  ≥ 1976 bit

<sup>7</sup> For the modulus  $n$  ( $n = p \cdot q$ ) the prime numbers  $p$  and  $q$  generated by the Crypto Library Cobalt on N7021 VA are congruent to 3 modulo 4.

No.	Purpose	Cryptographic Mechanism	Implementation Standard	Key Size in Bits	Security Level above 100 Bits
4	Cryptographic Primitive	ECDSA signature generation and verification	[ISO_14888-3], [IEEE_P1363], [ANSI X9.62] and [FIPS 186-4]. Supported curves: <ul style="list-style-type: none"> <li>• brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1 and brainpoolP512t1 defined in [Brainpool],</li> <li>• ansix9p224r1, ansix9p256r1, ansix9p384r1 and ansix9p521r1 defined in [ANSI X9.62], and</li> <li>• ANSSI FRP256v1 defined in [ANSSI_EC].</li> </ul> See [12 b].	k  = 224, 256, 320, 384, 512	Yes for  k  ≥ 250 bit
5	Key Agreement	Diffie-Hellman Key Exchange based on ECC over GF(p)	[ISO_11770-3], [ANSI X9.63], and [IEEE_P1363] Supported curves: see row 4	see row 4	Yes for  k  ≥ 250 bit
6	Key generation	ECDSA (ECC over GF(p)) key generation	[ISO_14888-3], [ANSI X9.62], and [FIPS168-4] Supported curves: see row 4	see row 4	Yes for  k  ≥ 250 bit
7	Cryptographic Primitive	Hashing based on SHA-1	[FIPS180-4]	N/A	No
		Hashing based on SHA- {224, 256, 384, 512}	[FIPS180-4]	N/A	Yes

Table 3: TOE cryptographic functionality

[ANSSI_EC]	Avis relatif aux paramètres de courbes elliptiques définis par l'Etat français, JORF n°0241 du 16 octobre 2011 page 17533 texte n° 30, <a href="https://www.legifrance.gouv.fr/affichTexte.do?sessionId=?cidTexte=JORFTEXT000024668816">https://www.legifrance.gouv.fr/affichTexte.do?sessionId=?cidTexte=JORFTEXT000024668816</a> .
[ANSI X9.62]	American National Standard for Financial Services ANS X9.62-2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), November 16, 2005, American National Standards Institute.
[ANSI X9.63]	American National Standard for Financial Services X9.63-2001, Public Key Cryptography for the Financial Services Industry - Key Agreement and Key Transport Using Elliptic Curve Cryptography, November 20, 2001, American National Standards Institute.
[Brainpool]	ECC Brainpool Standard Curves and Curve Generation, M. Lochter, Version 1.0, 2005 (available online at <a href="http://www.ecc-brainpool.org/ecc-standard.htm">http://www.ecc-brainpool.org/ecc-standard.htm</a> ).
[FIPS180-4]	FIPS PUB 180-4 Federal Information Processing Standards Publication Secure Hash Standard (SHS), August 2015, Information Technology Laboratory National Institute of Standards and Technology.
[FIPS186-4]	Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013, U.S. department of Commerce / National Institute of Standards and Technology (NIST).
[IEEE_P1363]	IEEE P1363. Standard specifications for public key cryptography. IEEE, 2000.
[ISO_11770-3]	ISO/IEC 11770-3-2015: Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques, 2015
[ISO_14888-3]	ISO/IEC 14888-3:2015: Information technology – Security techniques – Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms, 2016
[PKCS #1]	PKCS #1: RSA Cryptography Standard, Version 2.2, October 27, 2012, RSA Laboratories.

## 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

<b>AIS</b>	Application Notes and Interpretations of the Scheme
<b>BSI</b>	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
<b>BSIG</b>	BSI-Gesetz / Act on the Federal Office for Information Security
<b>CCRA</b>	Common Criteria Recognition Arrangement
<b>CC</b>	Common Criteria for IT Security Evaluation
<b>CEM</b>	Common Methodology for Information Technology Security Evaluation
<b>cPP</b>	Collaborative Protection Profile
<b>EAL</b>	Evaluation Assurance Level
<b>ECC</b>	Elliptic Curve Cryptography
<b>ECDH</b>	Elliptic Curve Diffie-Hellman
<b>ECDSA</b>	Elliptic Curve Digital Signature Algorithm
<b>EME</b>	Encoding Methods for Encryption
<b>EMSA</b>	Encoding Methods for Signatures with Appendix

<b>ETR</b>	Evaluation Technical Report
<b>FIPS</b>	Federal Information Processing Standard
<b>GF</b>	Galois field
<b>ISO</b>	International Organization for Standardization
<b>IT</b>	Information Technology
<b>ITSEF</b>	Information Technology Security Evaluation Facility
<b>OAEP</b>	Optimal Asymmetric Encryption Padding
<b>PKCS</b>	Public Key Cryptography Standards
<b>PP</b>	Protection Profile
<b>PSS</b>	Probabilistic Signature Scheme
<b>RSA</b>	Rivest-Shamir-Adleman (Crypto Algorithm)
<b>RSADP</b>	RSA Decryption Primitive
<b>RSAEP</b>	RSA Encryption Primitive
<b>RSASP1</b>	RSA Signature Primitive 1
<b>RSASSA</b>	RSA Signature Scheme with Appendix
<b>RSVP1</b>	RSA Verification Primitive 1
<b>SAR</b>	Security Assurance Requirement
<b>SFP</b>	Security Function Policy
<b>SFR</b>	Security Functional Requirement
<b>SHA</b>	Secure Hash Algorithm
<b>ST</b>	Security Target
<b>TOE</b>	Target of Evaluation
<b>TSF</b>	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<sup>8</sup>  
<https://www.bsi.bund.de/AIS>

<sup>8</sup>specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2, Reuse of evaluation results
- AIS 47, Version 1.1 Regelungen zu Site Certification



- [5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, <https://www.bsi.bund.de/zertifizierungsberichte>
- [6] Crypto Library Cobalt on N7021 VA Security Target, BSI-DSZ-CC-1019-V2, Version 2.3, 05.06.2019, NXP Semiconductors (confidential document)
- [7] EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY), Crypto Library Cobalt on N7021 VA 2.0.8, BSI-DSZ-CC-1019-V2, Version 4, 17.09.2019, 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] Crypto Library Cobalt on N7021 VA Security Target Lite, BSI-DSZ-CC-1019-V2, Version 2.3, 05.06.2019, NXP Semiconductors (sanitised public document)
- [10] Evaluation Technical Report for Composite Evaluation (ETR COMP), Crypto Library Cobalt on N7021 VA 2.0.8, BSI-DSZ-CC-1019-V2, Version 4, 17.09.2019, TÜV Informationstechnik GmbH – Evaluation Body for IT Security.(confidential document)
- [11] Configuration lists for the TOE:
  - (a) Crypto Library Iron / Cobalt V1.0 on N7021 VA, Life Cycle, Version 1.3, 07.03.2017, (confidential document)
  - (b) P71D320 Crypto Library, Configuration Item List, Version 1.0, 07.03.2017 Evaluation documentation
  - (c) Crypto Library Cobalt on N7021 VA Evaluation Reference List, Version 2.2, 11.09.2019, NXP Semiconductors (confidential document)
- [12] Guidance documentation for the TOE:
  - (a) Crypto Library Cobalt V1.0 on N7021 VA Information on Guidance and Operation, Version 1.8, 06.06.2019 (confidential document)
  - (b) N7021 Crypto Library ECC over GF(p) Library, Version 1.2, 19.01.2017, (confidential document)
  - (c) N7021 Crypto Library HASH Library, Version 1.0, 29.09.2016 (confidential document)
  - (d) N7021 Crypto Library RSA Library, Version 1.4, 03.09.2019 (confidential document)
  - (e) N7021 Crypto Library RSA Key Generation Library, Version 1.0, 16.09.2016 (confidential document)
  - (f) N7021 Crypto Library SHA Library, Version 1.0, 29.09.2016 (confidential document)
  - (g) N7021 Crypto Library UtilsAsym Library, Version 1.0, 28.11.2016 (confidential document)
- [13] Certification Report BSI-DSZ-CC-0977-V2-2019, 31.07.2019, BSI
- [14] EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP), BSI-DSZ-CC-0977-V2, Version 4, 17.07.2019, TÜV Informationstechnik GmbH (confidential document)

- [15] NXP Secure Smart Card Controller N7021 VA Security Target Lite, BSI-DSZ-CC-0977-V2, Version 2.3, 04.06.2019, NXP Semiconductors (sanitised public document)
- [16] SmartMX3 family N7021 Wafer and delivery specification, Objective wafer specification, Version 1.3, 15.05.2018, 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 detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

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

## **D. Annexes**

### **List of annexes of this certification report**

- Annex A: Security Target provided within a separate document.
- Annex B: Evaluation results regarding development and production environment

## Annex B of Certification Report BSI-DSZ-CC-1019-V2-2019

### Evaluation results regarding development and production environment



The IT product Crypto Library Cobalt on N7021 VA (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 29 October 2019, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (ALC\_CMC.5, ALC\_CMS.5, ALC\_DEL.1, ALC\_DVS.2, ALC\_LCD.1 and ALC\_TAT.3)

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

Name of site / Company name	Address	Function
<b>Development Sites</b>		
NXP Hamburg	NXP Semiconductors Germany GmbH Tropplowitzstr. 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.

Name of site / Company name	Address	Function
NXP Nijmegen	NXP Semiconductors Nijmegen B.V. Gerstweg 2 6534AE Nijmegen The Netherlands	Development and Manufacturing, Regional Quality Centre – Europe.
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.
Akquinet Datacenter Hamburg	AKQUINET Hamburg Ulzburger Strasse 201 22850 Norderstedt Germany	Data center.
<b>Production Sites</b>		
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 Tropowitzstr. 20 22529 Hamburg Germany	Test Centre, personalization, and delivery.

Name of site / Company name	Address	Function
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: Developer and Production Sites

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and [9]) are fulfilled by the procedures of these sites.

Note: End of report