Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1019-2017

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-1019-2017 (*)

Smart Cards and similar devices: IC, Cryptolib

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 Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 6 augmented by ASE_TSS.2 and ALC_FLR.1

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations and 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 4.

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

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

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

Bonn, 24 November 2017

For the Federal Office for Information Security

Bernd Kowalski
Head of Division

L.S.

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

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

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the 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: http://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 Crypto Library Cobalt on N7021 VA has undergone the certification procedure at BSI.

The evaluation of the product Crypto Library Cobalt on N7021 VA was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 6 November 2017. 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 24 November 2017 is valid until 23 November 2022. Validity can be renewed 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 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[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), 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 and ALC_FLR.1.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 6.1. 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 RSA-CRT algorithm for message and signature encoding.

TOE Security Functionality	Addressed issue
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
RSA				
1	Library	RSA Library	2.0.8	Electronic files
2	Document	N7021 Crypto Library: User Manual – RSA [12]	1.3	Electronic document
RSA Key Generation				

3	Library	RSA Key Generation Library	2.0.8	Electronic files
4	Document	N7021 Crypto Library: User Manual - RSA Key Generation [12]	1.0	Electronic document
ECC over GF(p)				
5	Library	ECC Library	2.0.8	Electronic files
6	Document	N7021 Crypto Library: User Manual - ECC over GF(p) [12]	1.2	Electronic document
Package SHA				
7	Library	SHA Library	2.0.8	Electronic files
8	Document	N7021 Crypto Library: User Manual – SHA [12]	1.0	Electronic document
9	Document	N7021 Crypto Library: User Manual - Hash Library [12]	1.0	Electronic document
Required for all packages				
10	Library	Asymmetric Utilities Library	2.0.8	Electronic files
11	Document	N7021 Crypto Library: User Manual – UtilsAsym [12]	1.0	Electronic document
12	Document	N7021 Crypto Library: User Guidance Manual - Crypto Library Cobalt on N7021 VA [12]	1.7	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 [14].

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.

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 chapter 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
  - MIFARE tests.

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 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.

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-0977-2017) 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 and ALC_FLR.1 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014 [8]
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 6 augmented by ASE_TSS.2 and 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 additional cryptographic functionalities of the composite 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	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Crypto. Primitives	RSAEP encryption / decryption	[16, 5.1.1]	|k| = 512 - 4096	Yes for |k| ≥ 1976 bit	See [17, 3.1]
2		RSADP encryption / decryption	[16, 5.1.2]	|k| = 512 - 4096	Yes for |k| ≥ 1976 bit	
3		RSASP1 signature generation and verification	[16, 5.2.1]	|k| = 512 - 4096	Yes for |k| ≥ 1976 bit	
4		RSAVP1 signature generation and verification	[16, 5.2.2]	|k| = 512 - 4096	Yes for |k| ≥ 1976 bit	
5		EME-OAEP message and signature encoding	[16, 7.1.1 / Step 2]	|k| = 512 - 4096	Yes for |k| ≥ 1976 bit	
6		EMSA-PSS message and signature encoding	[16, 9.1]	|k| = 512 - 4096	Yes for |k| ≥ 1976 bit	
7		RSA key pair generation in FIPS mode	[16]; [21] probable prime generation (Algorithm according to Section B3.3 with restriction to primes congruent to 3 mod 4)	|k| = 2048, 3072	Yes	-
8		RSA key pair generation in	[16], [17]; [21] probable prime generation (Algorithm	|k| = 512 -	Yes for |k| ≥	-

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
		non-FIPS mode	according Section B3.3 of [21] with restriction to primes congruent to 3 mod 4) with the following modifications: 1) Step 5.4 of B3.3 is omitted. 2) The most significant byte (MSB) of prime candidates p and q respectively is generated randomly to ensure their size restriction of [17]. These MSBs are then used for all tested prime candidates.	4096	1976 bit	
9		RSA public key computation	[16]	|k| = 512 - 4096	Yes for |k| ≥ 1976 bit	-
10		ECDSA signature generation and verification	[18]	|k| = 128 - 640	Yes for |k| ≥ 250 bit	The following elliptic curves are supported: [21] and [Brainpool]. See also [17, 3.2].
11		Diffie-Hellman Key Exchange based on ECC over GF(p)	[19]	|k| = 128 - 640	Yes for |k| ≥ 250 bit	
12		Hashing based on SHA-1	[22]	N/A	No	-
13		Hashing based on SHA-224	[22]	N/A	Yes	-
14		Hashing based on SHA-256	[22]	N/A	Yes	-
15		Hashing based on SHA-384	[22]	N/A	Yes	-
16		Hashing based on SHA-512	[22]	N/A	Yes	-

Table 3: Additional TOE cryptographic functionality

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 chapter 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. Definitions

12.1. 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
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm

EME	Encoding Methods for Encryption
EMSA	Encoding Methods for Signatures with Appendix
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
GF	Galois field
ISO	International Organization for Standardization
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
OAEP	Optimal Asymmetric Encryption Padding
PKCS	Public Key Cryptography Standards
PP	Protection Profile
PSS	Probabilistic Signature Scheme
RSA	Rivest-Shamir-Adleman (Crypto Algorithm)
RSADP	RSA Decryption Primitive
RSAEP	RSA Encryption Primitive
RSASP1	RSA Signature Primitive 1
RSASSA	RSA Signature Scheme with Appendix
RSAVP1	RSA Verification Primitive 1
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2. 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.

13. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 4, September 2012
http://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

[7] specifically

- AIS 1, Version 13, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 23, Version 3, Zusammentragen von Nachweisen der Entwickler
- AIS 25, Version 9, 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

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

[6] Crypto Library Cobalt on N7021 VA Security Target, BSI-DSZ-CC-1019, Version 1.2, 5 July 2017, NXP Semiconductors (confidential document)

[7] Evaluation Technical Report, Version 2, 20 October 2017, EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY), TÜV Informationstechnik GmbH (confidential document)

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

[9] Crypto Library Cobalt on N7021 VA Security Target Lite, BSI-DSZ-CC-1019, Version 1.1, 5 July 2017, NXP Semiconductors (sanitised public document)

[10] ETR for composite evaluation according to AIS 36 for the Crypto Library Cobalt on N7021 VA, Version 2, 20 October 2017, EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP), TÜV Informationstechnik GmbH (confidential document)

[11] Configuration lists for the TOE:

- Version 1.3, 07 March 2017, Crypto Library Iron / Cobalt V1.0 on N7021 VA, Life Cycle (confidential document)
- Version 1.0, 07 March 2017, P71D320 Crypto Library, Configuration Item List, Evaluation documentation (confidential document)

[12] Guidance documentation for the TOE:

- Version 1.7, 19 April 2017, Crypto Library Cobalt V1.0 on N7021 VA Information on Guidance and Operation (confidential document)
- Version 1.2, 19 January 2017, N7021 Crypto Library ECC over GF(p) Library (confidential document)
- Version 1.0, 29 September 2016, N7021 Crypto Library HASH Library (confidential document)
- Version 1.3, 12 April 2017, N7021 Crypto Library RSA Library (confidential document)
- Version 1.0, 16 September 2016, N7021 Crypto Library RSA Key Generation Library (confidential document)

- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluierungen
- AIS 38, Version 2, Reuse of evaluation results
- AIS 41, Version 2, Guidelines for PPs and STs
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren
- AIS 47, Version 1.1 Regelungen zu Site Certification

- Version 1.0, 29 September 2016, N7021 Crypto Library SHA Library (confidential document)
- Version 1.0, 28 November 2016, N7021 Crypto Library UtilsAsym Library (confidential document)

[13] Certification Report BSI-DSZ-CC-0977-2017, 24 July 2017, BSI

[14] Evaluation Technical Report for Composite Evaluation for the N7021 VA, Version 2, 30 June 2017, TÜV Informationstechnik GmbH (confidential document)

[15] NXP Secure Smart Card Controller N7021 VA Security Target Lite, BSI-DSZ-CC-0977-2017, Version 1.1, 31 May 2017, NXP Semiconductors (sanitised public document)

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

[17] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 07.12.2016 Veröffentlicht: BAnz AT 30.12.2016 B5, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen.

[18] Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 2: Digital signatures, 2002-12, ISO/IEC.

[19] Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 3: Key establishment, 2002-12, ISO/IEC.

[20] Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 1: General, 2008-04, ISO/IEC

[21] 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).

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

[23] SmartMX3 family N7021 Wafer and delivery specification, Version 1.1, 05 August 2016, 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 10.4
- 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 11
- On the detailled definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 12 to 16
- 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 http://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-1019-2017

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, and 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 24 November 2017, 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	Type of site
Development Sites		
NXP Semiconductors Hamburg	Business Unit Identification Troplowitzstrasse 20 22529 Hamburg, Germany	SW/HW Development, Delivery, order fulfillment, ROM/Flash code handling, and customer support, CM and Tooling.
NXP Semiconductors Austria GmbH Styria	Business Unit Identification Mikron-Weg 1 8101 Gratkorn, Austria	SW / HW development, testing and documentation
NXP Semiconductors Development Center Eindhoven HTC-46.3 West	Building 46, High Tech Campus 5656AE, Eindhoven, Netherlands	Development center
NXP Glasgow	151 West George Street Glasgow G2 2JJ, Scotland, UK	Hardware development, security reviews
NXP Semiconductors Leuven	Interleuvenlaan 80 B-3001 Leuven, Belgium	Security reviews
NXP Munich	NXP Semiconductors Germany GmbH Business Unit S&C Bayerwaldstr. 11 81737 Munich, Germany	Software development

Name of site / Company name	Address	Type of site
NXP Semiconductors RQC & NPIT & MM	NXP Semiconductors Netherlands B.V. Gerstweg 2 6534AE Nijmegen, Netherlands	Development and Manufacturing, Regional Quality Center - Europe
GlobalLogic REC Slovakia, s.r.o	Vysokoškolákov 1757/1 010 01 Žilina, Slovakia	Software development
GlobalLogic REC Wroclaw	Strzegomska 56B Street 53-611 Wroclaw, Poland	Software development
SII Gdansk	Olivia Gate, al. Grunwaldzka 472, 80-309 Gdansk, Poland	Software development
NXP High Tech Campus	Building 60, High Tech Campus Secure Room 131 5656AE, Eindhoven, Netherlands	IT Engineering and generic Support
Atos Bydgoszcz	Building BETA Secure Room B20S1 Biznes Park ul. Kraszewskiego 1 85-240 Bydgoszcz, Poland	IT Engineering and generic Support
Production sites		
TSMC, Fab 5	No. 121 Park Ave. III Hsinchu Science Park Hsinchu, Taiwan 300-77, R.O.C.	Mask data preparation,and wafer production Mask
TSMC, Fab 7	No. 6, Creation Rd. II Hsinchu Science Park Hsinchu, Taiwan 300-77, R.O.C.	Mask data preparation, and wafer production Mask
TSMC, Fab 14A	No. 1, Nan-Ke North Rd. Tainan Science Park Tainan, Taiwan 741-44, R.O.C.	Mask data preparation,and wafer production Mask
Chipbond Technology Corporation	No. 3, Li-Hsin Rd. V Science Based Industrial Park Hsin-Chu City Taiwan, R.O.C.	Bumping
NXP Semiconductors GmbH Hamburg Test Center Europe - Hamburg (TCE-H)	Stresemannallee 101 22569 Hamburg, Germany	Test center, configuration of the Fabkey, and delivery

Name of site / Company name	Address	Type of site
Assembly & Test Bangkok (ATBK) (former APB)	303 Moo 3 Chaengwattana Rd. Laksi, Bangkok 10210, Thailand	Test center, wafer treatment, module assembly and delivery
Assembly & Test Kaohsiung (APKH)(former APK)	#10, Jing 5th Road, N.E.P.Z, Kaohsiung 81170 Taiwan, R.O.C	Test center, wafer treatment, module assembly and delivery
SPIL CS	SPIL, Siliconware Precision Industries Co., Ltd., Chung Shan Facility and Da Fong Facility Chung Shan Facility: No. 153, Sec. 3, Chung Shan Rd., Tantzu, Taichung, Taiwan, R.O.C.	Test center, wafer treatment, module assembly

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