Crypto Library Cobalt on N7021 VA

Security Target Lite

Rev. 2.3 — 5 June 2019 Product evaluation document

BSI-DSZ-CC-1019-V2 PUBLIC

Document information

Information	Content
Keywords	Security Target Lite, Crypto Library, N7021 VA
Abstract	Security Target Lite for the N7021 VA Crypto Library according to the Common Criteria for Information Technology Evaluation (CC) at Level EAL6 augmented. The Crypto Library is developed and provided by NXP Semiconductors, Business Line Security & Connectivity.

Revision history

Revision number	Date	Description
2.3	2019-06-05	Derived from full Security Target v2.3

1 ST Introduction

This chapter is divided into the following sections: ST Identification, TOE Overview and TOE Description.

1.1 ST Reference

“Crypto Library Cobalt on N7021 VA, Security Target, Revision 2.3, NXP Semiconductors, 5 June 2019"

1.2 TOE Reference

The TOE is named "Crypto Library Cobalt on N7021 VA". The TOE is a composite TOE, consisting of:

- The hardware “NXP Secure Smart Card Controller N7021 VA” which is used as evaluated platform,
- The software “Crypto Library Cobalt on N7021 VA” which is built upon this platform.

This Security Target builds on the Hardware Security Target [13], which refers to the “N7021 VA”, provided by NXP Semiconductors.

The NXP Secure Smart Card Controller N7021 VA is named "N7021" in short. The Crypto Library Cobalt on N7021 VA is named "Crypto Library" in short.

1.3 TOE Overview

1.3.1 Introduction

The Hardware Security Target [13] contains, in section 1.3 “TOE Overview”, an introduction about the N7021 hardware TOE that is considered in the evaluation. The Hardware Security Target includes IC Dedicated Software provided with the N7021 hardware platform.

The “Crypto Library Cobalt on N7021 VA“ is a cryptographic library that can be used by the Security IC Embedded Software. The cryptographic library consists of several binary packages that are intended to be linked to the Security IC Embedded Software. The Security IC Embedded Software developer links the binary packages that he needs to his Embedded Software and the whole is subsequently implemented in arbitrary memory of the hardware platform.

The NXP N7021 provides the computing platform and cryptographic support by means of co-processors for the Crypto Library Cobalt on N7021 VA.

The Crypto Library Cobalt on N7021 VA provides the security functionality described below in addition to the functionality described in the Hardware Security Target [13] for the hardware platform:

The Crypto Library provides RSA, RSA key generation, RSA public key computation, ECDSA (ECC over GF(p)) signature generation and verification, ECDSA (ECC over GF(p)) key generation, ECDH (ECC Diffie-Hellmann) key-exchange, standard security level SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512.

1.3.2 Life-Cycle

The life cycle of the hardware platform as part of the TOE is described in section 1.4.4 "Security During Development and Production" of the Hardware Security Target [13]. The delivery process or the hardware platform is independent from the Crypto Library Cobalt on N7021 VA.

The Crypto Library Cobalt on N7021 VA is delivered in Phase 1 (for a definition of the Phases refer to Section 1.2.3 'TOE life cycle' of the Protection Profile [5]) as a software package (a set of binary files) to the developers of Security IC Embedded Software. The Security IC Embedded Software may comprise in this case an operating system and/or other smart card software (applications). The Software developer can incorporate the Crypto Library into their product.

The subsequent use of the Crypto Library Cobalt on N7021 VA by Security IC Embedded Software Developers is out of the control of the developer NXP Semiconductors; the integration of the Crypto Library Cobalt on N7021 VA into Security IC Embedded Software is not part of this evaluation.

Security during Development and Production

The development process of the Crypto Library Cobalt on N7021 VA is part of the evaluation. The access to the implementation documentation, test bench and the source code is restricted to the development team of the Crypto Library Cobalt on N7021 VA. The security measures installed within NXP, including a secure delivery process, ensure the integrity and quality of the delivered Crypto Library Cobalt on N7021 VA binary files.

1.3.3 Specific Issues of Hardware and the Common Criteria

Regarding the Application Note 2 of the Protection Profile [5] the TOE provides additional functionality which is not covered in the Protection profile [5] and the Hardware Security Target [13]. This additional functionality is added using the policy “P.Add-CryptoLib-Func” (see Section 3.3 of this Security Target).

1.4 TOE Description

The Target of Evaluation (TOE) consists of a hardware part and a software part:

- The hardware part consists of the N7021 with IC Dedicated Software. The hardware part of the TOE includes dedicated guidance documentation.
- The software part consists of the IC Dedicated Support Software “Crypto Library Cobalt on N7021 VA” which consists of a software library and associated documentation. The Crypto Library Cobalt on N7021 VA is an additional part that provides cryptographic functions that can be operated on the hardware platform as described in this Security Target.

The hardware part of the TOE is not described in detail in this document. Details are included in the Hardware Security Target [13] and therefore this latter document will be cited wherever appropriate.

The TOE components consist of all the TOE components listed in Table 1 of the Hardware Security Target [13] plus all TOE components listed in the table below:

Table 1. Components of the TOE that are additional to the Hardware Security Target

Type	Name	Release	Form of Delivery
Package RSA Encryption / Decryption			

Type	Name	Release	Form of Delivery
Library	RSA Library	2.0.8	SDK add-on installer via NXP DocStore
Document	N7021 Crypto Library: User Manual - RSA [9]	1.4	PDF via NXP DocStore
Package RSA Key Generation			
Library	RSA Key Generation Library	2.0.8	SDK add-on installer via NXP DocStore
Document	N7021 Crypto Library: User Manual - RSA Key Generation [10]	1.0	PDF via NXP DocStore
Package ECC over GF(p)			
Library	ECC Library	2.0.8	SDK add-on installer via NXP DocStore
Document	N7021 Crypto Library: User Manual - ECC over GF(p) [11]	1.2	PDF via NXP DocStore
Package SHA			
Library	SHA Library	2.0.8	SDK add-on installer via NXP DocStore
Document	N7021 Crypto Library: User Manual - SHA [8]	1.0	PDF via NXP DocStore
Document	N7021 Crypto Library: User Manual - Hash Library [7]	1.0	PDF via NXP DocStore
Required for all packages			
Library	Asymmetric Utilities Library	2.0.8	SDK add-on installer via NXP DocStore
Document	N7021 Crypto Library: User Manual - UtilsAsym [12]	1.0	PDF via NXP DocStore
Document	N7021 Crypto Library: User Guidance Manual - Crypto Library Cobalt on N7021 VA [6]	1.8	PDF via NXP DocStore

The documentation can be downloaded by the customer from the NXP DocStore website after registration. Library files (object files, header files and linker scripts) are also made available to the customer via NXP DocStore, as part of a downloadable and installable SDK add-on.

1.4.1 Hardware Description

The NXP N7021 hardware is described in section 1.4.3.1 “Hardware Description” of the Hardware Security Target [13]. The IC Dedicated Software delivered with the hardware platform is described in section 1.4.3.2 “Software Description” of the Hardware Security Target [13].

As described in the Hardware Security Target [13], the N7021 hardware provides the customer with a configuration option to disable the PKCC coprocessor. When the PKCC is disabled using this option, it is no longer possible to make use of the packages 'RSA Encryption / Decryption', 'RSA Key Generation' and 'ECC over GF(p)' provided by this Crypto Library.

1.4.2 Software Description

A Security IC Embedded Software developer may create Security IC Embedded Software to execute on the NXP N7021 hardware. This software is stored in arbitrary

memory of the hardware and is not part of the TOE, with one exception: the Security IC Embedded Software may contain the “Crypto Library Cobalt on N7021 VA“ (or parts thereof[1]) and this Crypto Library is part of the TOE.

RSA

- The RSA algorithm can be used for encryption and decryption as well as for signature generation, signature verification, message encoding and signature encoding.
- The RSA key generation can be used to generate RSA key pairs.
- The RSA public key computation can be used to compute the public key that belongs to a given private CRT key.

The TOE supports various key sizes for RSA up to a limit of 4096 bits.

RSA functionality is not available in case the customer disabled the PKCC coprocessor as part of the hardware configuration. See the Hardware Security Target [13] for more information.

ECDSA (ECC over GF(p))

- The ECDSA (ECC over GF(p)) algorithm can be used for signature generation and signature verification.
- The ECDSA (ECC over GF(p)) key generation algorithm can be used to generate ECC over GF(p) key pairs for ECDSA.
- The ECDH (ECC Diffie-Hellman) key exchange algorithm can be used to establish cryptographic keys. It can be also used as secure point multiplication.

The TOE supports various key sizes for ECC over GF(p) up to a limit of 640 bits for signature generation, key pair generation and key exchange. For signature verification the TOE supports key sizes up to a limit of 640 bits.

Supported curves are any Weierstrass curves from size 128 bits to size 640 bits with co-factor equal 1.

ECC functionality is not available in case the customer disabled the PKCC coprocessor as part of the hardware configuration. See the Hardware Security Target [13] for more information.

SHA

- The SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 algorithms can be used for different purposes such as computing hash values in the course of digital signature creation or key derivation.

Resistance of cryptographic algorithms against attacks

The cryptographic algorithms are designed taking into account the attacks described in JIL-ATT-SC: Attack Methods for Smartcards and Similar Devices [19].

Further security functionality

- The TOE includes internal security measures for residual information protection.

Note that the TOE does not restrict access to the functions provided by the hardware: these functions are still directly accessible to the Security IC Embedded Software.

1 These crypto functions are supplied as a library rather than as a monolithic program, and hence a user of the library may include only those functions that are actually required – it is not necessary to include all cryptographic functions of the library in every Security IC Embedded Software. For example, it is possible to omit the RSA or the ECC components. However, some dependencies exist; details are described in the User Guidance [6].

1.4.3 Documentation

The documentation for the NXP N7021 hardware is listed in section 1.4.3.3 “Documentation” of the Hardware Security Target [13].

The Crypto Library has associated user manuals and one user guidance documentation (see [6]). The user manuals contain:

- the specification of the functions provided by the Crypto Library,
- details of the parameters and options required to call the Crypto Library by the Security IC Embedded Software

and the user guidance document contains:

- Guidelines on the secure usage of the Crypto Library, including the requirements on the environment (the Security IC Embedded Software calling the Crypto Library is considered to be part of the environment).

1.4.4 Interface of the TOE

The interface to the NXP N7021 hardware is described in section 1.4.5 “Interface of the TOE” of the Hardware Security Target [13]. The use of this interface is not restricted by the use of the Crypto Library Cobalt on N7021 VA.

The interface to the TOE additionally consists of software function calls, as detailed in the “User Manual” documents of the Crypto Library Cobalt on N7021 VA. The developer of the Security IC Embedded Software will link the required functionality of the Crypto Library Cobalt on N7021 VA into the Security IC Embedded Software as required for his Application.

1.4.5 Life Cycle and Delivery of the TOE

The life cycle and delivery for the NXP N7021 hardware is described in section 1.4.4 “Security during development and production” of the Hardware Security Target [13].

The Crypto Library Cobalt on N7021 VA is delivered as part of Phase 1 (for a definition of the Phases refer to section ‘1.2.3 TOE life cycle’ of the Protection Profile [5]) to the Security IC Embedded Software developer. The Crypto Library Cobalt on N7021 VA may be delivered by e-mail or by Document Control (DocuControl or DocStore) or by delivering physical media such as compact disks by mail or courier. To protect the Crypto Library Cobalt on N7021 VA during the delivery process, the Crypto Library Cobalt on N7021 VA is encrypted and digitally signed. The Security IC Embedded Software developer then integrates the Crypto Library Cobalt on N7021 VA in the Security IC Embedded Software.

1.4.6 TOE Intended Usage

Regarding to Phase 7 (for a definition of the Phases refer to section ‘1.2.3 TOE life cycle’ of the Protection Profile [5]), the combination of the hardware and the Security IC Embedded Software is used by the end-user. The method of use of the product in this phase depends on the application. The TOE is intended to be used in an unsecured environment, that is, the TOE does not rely on the Phase 7 environment to counter any threat.

For details on the usage of the hardware platform refer to section 1.4.5 “TOE Intended Usage” in the Hardware Security Target [13].

The Crypto Library Cobalt on N7021 VA is intended to support the development of the Security IC Embedded Software since the cryptographic functions provided by the Crypto Library Cobalt on N7021 VA include countermeasures against the threats described in this Security Target. The used modules of the Crypto Library Cobalt on N7021 VA are linked to the other parts of the Security IC Embedded Software and they are implemented as an extention of the Security IC Dedicated Software in arbitrary memory of the hardware platform.

1.4.7 TOE User Environment

The user environment for the Crypto Library Cobalt on N7021 VA is the Security IC Embedded Software, developed by customers of NXP, to run on the NXP N7021 hardware.

1.4.8 General IT features of the TOE

The general features of the NXP N7021 hardware are described in section 1.3 “TOE overview” of the Hardware Security Target [13]. These are supplemented for the TOE by the functions listed in Section 1.3.1 of this Security Target.

2 CC Conformance and Evaluation Assurance Level

The evaluation is based upon:

- "Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001" [1]
- "Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002" [2]
- "Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003" [3]

For the evaluation the following methodology will be used:

- "Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004" [4]

The chosen level of assurance is **EAL6 + augmented**.

The augmentations to EAL6 are ASE_TSS.2 and ALC_FLR.1.

This Security Target claims the following CC conformances:

- CC 3.1 Part 2 extended, Part 3 conformant, EAL6 augmented
- Strict Conformance to the Protection Profile [5]

The assurance level for evaluation and the functionality of the TOE are chosen in order to allow the confirmation that the TOE is suitable for use within devices compliant with the German Digital Signature Law.

Note 1. The hardware platform is evaluated according to the assurance level EAL 6 augmented. The evaluation of the hardware platform is appropriate for the composite evaluation since both the EAL level and the augmentations claimed in this Security Target are identical to those claimed for the hardware platform (refer to the Hardware Security Target [13]).

2.1 Conformance claim rationale

According to chapter 2 this Security Target claims strict conformance to the Protection Profile [5]. As shown in 1.3 the composed TOE consists of hardware (Secure Controller IC) and software (IC Dedicated Software). This is identical to the TOE as defined in [5] and therefore the TOE type is consistent.

3 Security Problem Definition

3.1 Description of Assets

Since this Security Target claims strict conformance to a PP [5], the assets defined in section 3.1 of the Protection Profile apply to this Security Target. User Data and TSF data are defined as part of assets in [13]. Since the data computed by the Crypto Library contains keys, plain text and cipher text that are considered as User Data and e.g. blinding vectors that are considered as TSF data the assets are considered as complete for this Security Target.

3.2 Threats

Since this Security Target claims strict conformance to the PP [5], the threats defined in section 3.2 of the Protection Profile, and which are described in section 3.2 “Threats” of the Hardware Security Target [13] are valid for this Security Target. No additional threats are defined for this Security Target.

3.3 Organizational Security Policies

In addition to the security functionality provided by the hardware and defined in the hardware security target [13], the following additional security functionality is provided by the Crypto Library for use by the Security IC Embedded Software:

P.Add-CryptoLib-Func: Additional Specific Security Functionality

The TOE provides the following additional security functionality to the Security IC Embedded Software:

- RSA encryption, decryption, signature generation, signature verification, message encoding and signature encoding.
- RSA public key computation
- RSA key generation,
- ECDSA (ECC over GF(p)) signature generation and verification,
- ECC over GF(p) key generation,
- ECDH (ECC Diffie-Hellman) key exchange,
- SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 Hash Algorithms.

In addition, the TOE shall provide resistance against attacks as described in Note 4 and in Security architectural information.

Regarding the Application Note 5 of the Protection Profile [5] there are no other additional policies defined in this Security Target.

3.4 Assumptions

The assumptions are described in the Hardware Security Target [13]. No additional assumptions are defined for this Security Target.

4 Security Objectives

This chapter contains the following sections: “Security Objectives for the TOE”, “Security Objectives for the Security IC Embedded Software”, “Security Objectives for the Operational Environment”, and “Security Objectives Rationale”.

4.1 Security Objectives for the TOE

The security objectives for the TOE defined in the Protection Profile [5] and the Hardware Security Target [13] are entirely applied to this Security Target.

The following additional security objectives for the Crypto Library are defined by this ST, and are provided by the software part of the TOE:

O.RSA	The TOE includes functionality to provide encryption, decryption, signature creation, signature verification, message encoding and signature encoding using the RSA algorithm, see Note 4.
O.RSA_PubExp	The TOE includes functionality to compute an RSA public key from an RSA private key, see Note 4.
O.RSA_KeyGen	The TOE includes functionality to generate RSA key pairs, see Note 4.
O.ECDSA	The TOE includes functionality to provide signature creation and signature verification using the ECC over GF(p) algorithm, see Note 4.
O.ECC_DHKE	The TOE includes functionality to provide Diffie-Hellman key exchange based on ECC over GF(p), see Note 4.
O.ECC_KeyGen	The TOE includes functionality to generate ECC over GF(p) key pairs, see Note 4.
O.SHA	The TOE includes functionality to provide electronic hashing facilities using the SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 algorithms.

Note 4. All introduced security objectives claiming cryptographic functionality are protected against attacks as described in JIL-ATT-SC: Attack Methods for Smartcards and Similar Devices [19], which include Side Channel Attacks, Perturbation attacks, Differential Fault Analysis (DFA) and timing attacks. The following exceptions apply:

1. RSA Public Key computation and RSA Key generation do not contain protective measures against DPA
2. ECDSA (ECC over GF(p)) Key Generation does not contain protective measures against DPA
3. SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 do not contain protective measures against DPA, DFA and timing attacks. It provides countermeasures against template attacks targeting the input message and the output digest.

This does not mean that the algorithm is insecure; rather at the time of this security target no promising attacks were found. More details about conditions and restrictions for resistance against attacks are given in the user documentation of the Crypto Library.

4.2 Security Objectives for the IC Embedded Software

The security objectives for the Security IC Embedded Software defined in section 4.2 of the Protection Profile [5] and additional refinements in the Hardware Security Target [13] entirely apply to this Security Target.

The TOE assumes that the Security IC Embedded Software abides by the provisions detailed in “Clarification of Treatment of user data of the Composite TOE (OE.Resp-Appl)” contained within section 4.2 “Security Objectives for the Security IC Embedded Software” of the Hardware Security Target [13].

4.3 Security Objectives for the Operational Environment

The security objective for the “Security Objectives for the Operational environment” defined in the PP [5], and given in the Hardware Security Target [13] are entirely valid for this Security Target.

4.4 Security Objectives Rationale

Section 4.4 of the Protection Profile [5] and Section 4.4 of the Hardware Security Target [13] provide a rationale how the threats, organisational security policies and assumptions are addressed by the objectives that are subject of the PP. They entirely apply to this Security Target. The justification for the additional security objectives for the Crypto Library on N7021 are listed in the table below:

Table 2. Additional Security Objectives versus threats, assumptions or policies for Crypto Library on Crypto Library Cobalt on N7021 VA

Threat, Assumption/Policy	Security Objective
P.Add-CryptoLib-Func	O.RSA O.RSA_PubExp O.RSA_KeyGen O.ECDSA O.ECC_DHKE O.ECC_KeyGen O.SHA

They are in line with the security objectives of the Protection Profile and supplement these according to the additional assumptions and organisational security policy.

The rationale for all item defined in the Security Target is given below.

Since the objectives O.RSA, O.RSA_PubExp, O.RSA_KeyGen, O.ECDSA, O.ECC_DHKE, O.ECC_KeyGen and O.SHA require the TOE to implement exactly the same specific security functionality as required by P.Add-CryptoLib-Func, the organizational security policy P.Add-CryptoLib-Func is covered by the security objectives. Additionally, the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced define how to implement the specific security functionality required by P.Add-CryptoLib-Func and therefore support P.Add-CryptoLib-Func. These security objectives are also valid for the additional specific security functionality since they must also avert the related threats for the components added to the organisational security policy.

The justification of the additional policy and the additional assumptions show that they do not contradict with the rationale already given in the Protection Profile [5] for the assumptions, policy and threats defined there.

5 Extended Components Definition

This Security Target does not define extended components.

6 Security Requirements

6.1 Security Functional Requirements

To support a better understanding of the combination Protection Profile and Security Target of the hardware platform (N7021) vs. this Security Target (Crypto Library Cobalt on N7021 VA), the TOE SFRs are presented in the following sections.

6.1.1 SFRs from the Protection Profile and the Security Target of the platform

The Security Functional Requirements (SFRs) for this TOE (Crypto Library Cobalt on N7021 VA) are specified based on the Smart Card IC Platform Protection Profile [5], and are defined in the Common Criteria [2] or in the Protection Profile [5]. They entirely apply to this Security Target.

Note 5. These requirements have already been stated in the Hardware Security Target [13] and are fulfilled by the chip hardware, if not indicated otherwise in this Section.

The additional SFRs shown in this Section are defined in the Common Criteria, described in sections 6.1.3 “Security Functional Requirements added in this Security Target” of the Hardware Security Target [13]. They entirely apply to this Security Target.

6.1.2 Security Functional Requirements added in this Security Target

The SFRs in Section 6.1.1 are further supplemented by the additional SFRs described in the following subsections of this Security Target.

The SFRs described in Table 3 are added for the Crypto Library. The composite TOE, consisting of chip hardware N7021 and Crypto Library, fulfils all requirements from Section 6.1.1 and Table 3.

Table 3. SFRs defined in this Security Target for Crypto Library

Name	Title	Defined in
FCS_COP.1/RSA	Cryptographic operation (RSA encryption, decryption, signature and verification)	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1/RSA_PAD	Cryptographic operation (RSA message and signature encoding)	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1/RSA_PubExp	Cryptographic operation (RSA public key computation)	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1/ECDSA	ECDSA Cryptographic operation (ECC over GF(p) signature generation and verification)	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1/ECC_DHKE	ECDH Cryptographic operation (ECC Diffie-Hellman key exchange)	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1/SHA	Cryptographic operation (SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512)	CC Part 2 [2]; specified in this ST, see below.
FCS_CKM.1/RSA	Cryptographic key generation (RSA key generation)	CC Part 2 [2]; specified in this ST, see below.
FCS_CKM.1/ECC	ECC Cryptographic key generation (ECC over GF(p) key generation)	CC Part 2 [2]; specified in this ST, see below.

Name	Title	Defined in
FCS_CKM.4	Cryptographic Key Destruction	CC Part 2 [2]; specified in this ST, see below.

The requirements listed in Table 3 are detailed in the following sub-sections.

Additional SFR regarding cryptographic functionality

The TSF provides cryptographic functionality to help satisfy several high-level security objectives. In order for a cryptographic operation to function correctly, the operation must be performed in accordance with a specified algorithm and with a cryptographic key of a specified size. The following Functional Requirements to the TOE can be derived from this CC component:

FCS_COP.1/RSA	**Cryptographic operation**
Hierarchical to:	No other components.
FCS_COP.1.1/RSA	The TSF shall perform *encryption, decryption, signature generation and verification*[2] in accordance with the specified cryptographic algorithm *RSA*[3] and cryptographic key sizes *512 bits to 4096 bits*[4] that meet the following: *PKCS #1, v2.2: RSAEP, RSADP, RSASP1, RSAVP1*[5].
Application Notes:	The cryptographic algorithms are designed taking into account the attacks described in JIL-ATT-SC: Attack Methods for Smartcards and Similar Devices [19].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1/RSA_PAD	**Cryptographic operation**
Hierarchical to:	No other components.
FCS_COP.1.1/RSA_PAD	The TSF shall perform *message and signature encoding methods*[6] in accordance with the specified cryptographic algorithm *EME-OAEP and EMSA-PSS*[7] and cryptographic key sizes *512 bits to 4096 bits*[8] that meet the following: *PKCS #1, v2.2: EME-OAEP and EMSA-PSS*[9].
Application Notes:	Regarding OAEP the input of encode as well as the input and output of decode are considered sensitive values. Regarding PSS the input of the encoding and verify operations are considered sensitive values. In both cases the length of the sensitive values is assumed to be public.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with

2 [assignment: *list of cryptographic operations*]
3 [assignment: *cryptographic algorithm*]
4 [assignment: *cryptographic key sizes*]
5 [assignment: *list of standards*]
6 [assignment: *list of cryptographic operations*]
7 [assignment: *cryptographic algorithm*]
8 [assignment: *cryptographic key sizes*]
9 [assignment: *list of standards*]

	security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1/RSA_PubExp	**Cryptographic operation**
Hierarchical to:	No other components.
FCS_COP.1.1/RSA_PubExp	The TSF shall perform *public key computation*[10] in accordance with the specified cryptographic algorithm *RSA*[11] and cryptographic key sizes *512 bits to 4096 bits*[12] that meet the following: *PKCS #1, v2.2*[13].
Application Notes:	(1) The cryptographic algorithms are designed taking into account the attacks described in JIL-ATT-SC: Attack Methods for Smartcards and Similar Devices [19]. (2) The computation will result in the generation of a public RSA key from the private key (in CRT format). As this key is implied by the private key, this is not true key generation, and, to prevent duplication in this ST, this has not been included as a separate FCS_CKM.1 SFR.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1/ECDSA	**Cryptographic operation**
Hierarchical to:	No other components.
FCS_COP.1.1/ECDSA	The TSF shall perform *signature generation and verification*[14] in accordance with the specified cryptographic algorithm *ECDSA / ECC over GF(p)*[15] and cryptographic key sizes *224, 256, 320, 384, 512 and 521 bits*[16] that meet the following: *ISO/IEC 14888-3, ANSI X9.62, FIPS PUB 186-4 and IEEE Std 1363™-2000*[17].
Application Notes:	The cryptographic algorithms are designed taking into account the attacks described in JIL-ATT-SC: Attack Methods for Smartcards and Similar Devices [19].
Note:	Due to BSI regulations the certification covers the standard curves ansix9p224r1, ansix9p256r1, ansix9p384r1 and ansix9p521r1 from ANSI X9.62 [21], brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1 and brainpoolP512t1 from RFC 5639 [23], and ANSSI FRP256v1 [24] curves.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with

10 [assignment: *list of cryptographic operations*]
11 [assignment: *cryptographic algorithm*]
12 [assignment: *cryptographic key sizes*]
13 [assignment: *list of standards*]
14 [assignment: *list of cryptographic operations*]
15 [assignment: *cryptographic algorithm*]
16 [assignment: *cryptographic key sizes*]
17 [assignment: *list of standards*]

	security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1/ECC_DHKE	**Cryptographic operation**
Hierarchical to:	No other components.
FCS_COP.1.1/ECC_DHKE	The TSF shall perform *Diffie-Hellman Key Exchange*[18] in accordance with the specified cryptographic algorithm *ECC over GF(p)*[19] and cryptographic key sizes *224, 256, 320, 384, 512 and 521 bits*[20] that meet the following: *ISO/IEC 11770-3:2015, ANSI X9.63, IEEE Std 1363™-2000*[21].
Application Notes:	(1) The cryptographic algorithms are designed taking into account the attacks described in JIL-ATT-SC: Attack Methods for Smartcards and Similar Devices [19]. (2) The security functionality does not provide the complete key exchange procedure, but only the point multiplication which is used for the multiplication of the private key with the communication partner's public key. Therefore this function can be used as part of a Diffie-Hellman key exchange as well pure point multiplication.
Notes:	Due to BSI regulations the certification covers the standard curves ansix9p224r1, ansix9p256r1, ansix9p384r1 and ansix9p521r1 from ANSI X9.62 [21], brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1 and brainpoolP512t1 from RFC 5639 [23], and ANSSI FRP256v1 [24] curves.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1/SHA	**Cryptographic operation**
Hierarchical to:	No other components.
FCS_COP.1.1/SHA	The TSF shall perform *hashing*[22] in accordance with a specified cryptographic algorithm *SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512*[23] and cryptographic key size *none*[24] that meet the following: *FIPS 180-4* [16][25].

18 [assignment: *list of cryptographic operations*]
19 [assignment: *cryptographic algorithm*]
20 [assignment: *cryptographic key sizes*]
21 [assignment: *list of standards*]
22 [assignment: *list of cryptographic operations*]
23 [assignment: *cryptographic algorithm*]
24 [assignment: *cryptographic key sizes*]
25 [assignment: *list of standards*]

Application Notes:	1) The security functionality is resistant against template attacks targeting the input message and the output digest. (2) The length of the data to hash has to be a multiple of one byte. Arbitrary bit lengths are not supported.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.

The TSF provides functionality to generate a variety of key pairs. In order for the key generation to function correctly, the operation must be performed in accordance with a specified standard and with cryptographic key sizes out of a specified range. The following Security Functional Requirements to the TOE can be derived from this CC component:

FCS_CKM.1/RSA	**Cryptographic Key Generation**
Hierarchical to:	No other components.
FCS_CKM.1.1/RSA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *RSA*[26] and specified cryptographic key sizes *512-4096 bits*[27] that meet the following: *PKCS #1, v2.2 and FIPS 186-4*[28].
Application Notes:	For the modulus n (n = p*q) the prime numbers p and q generated by the key generator are congruent to 3 modulo 4. The cryptographic algorithms are designed taking into account the attacks described in JIL-ATT-SC: Attack Methods for Smartcards and Similar Devices [19].
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1/ECC	**Cryptographic Key Generation**
Hierarchical to:	No other components.
FCS_CKM.1.1/ECC	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDSA (ECC over GF(p))*[29] and specified cryptographic key sizes *224, 256, 320, 384, 512 and 521 bits*[30] that meet the following: *ISO/IEC 14888-3:2015, ANSI X9.62 and FIPS PUB 186-4*[31].

26 [assignment: *cryptographic key generation algorithm*]
27 [assignment: *cryptographic key sizes*]
28 [assignment: *list of standards*]
29 [assignment: *cryptographic algorithm*]
30 [assignment: *cryptographic key sizes*]
31 [assignment: *list of standards*]

Application Notes:	The cryptographic algorithms are designed taking into account the attacks described in JIL-ATT-SC: Attack Methods for Smartcards and Similar Devices [19].
Note:	Due to BSI regulations the certification covers the standard curves ansix9p224r1, ansix9p256r1, ansix9p384r1 and ansix9p521r1 from ANSI X9.62 [21], brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1 and brainpoolP512t1 from RFC 5639 [23], and ANSSI FRP256v1 [24] curves.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.4	**Cryptographic Key Destruction**
Hierarchical to:	No other components.
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwrite*[32] that meets the following: *ISO 11568-4:2007* [14][33]
Application Notes:	The Crypto Library provides the smartcard embedded software with library calls to perform various cryptographic algorithms that involve keys (e.g., AES, DES, RSA, etc.). Through the parameters of the library calls the smartcard embedded software provides keys for the cryptographic algorithms. To perform its cryptographic algorithms the library copies these keys, or a transformation thereof, to the working-buffer (supplied by the smartcard embedded software) and/or the memory/special function registers of the Crypto Library on N7021 VA. Depending upon the algorithm the library either overwrites these keys before returning control to the smartcard embedded software or provides a library call to through which the smartcard embedded software can clear these keys. In the case of a separate library call to clear keys the guidance instructs the smartcard embedded software when/how this call should be used.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
Note:	Clearing of keys that are provided by the smartcard embedded software to the Crypto Library is the responsibility of the smartcard embedded software.

32 [assignment: *cryptographic key destruction method*]
33 [assignment: *list of standards*]

6.2 Security Assurance Requirements

Table 4 below lists all security assurance components that are valid for Crypto Library Cobalt on N7021 VA. These security assurance components are required by EAL6 or by the Protection Profile [5]. Augmentations by the Security Target are marked with ST.

Table 4. Security Assurance Requirements EAL6+ and PP augmentations for Crypto Library Cobalt on N7021 VA

SAR	Title	Required by
ADV_ARC.1	Security architecture description	PP / EAL6
ADV_FSP.5	Complete semi-formal functional specification with additional error information	EAL6
ADV_IMP.2	Complete mapping of implementation representation of the TSF	EAL6
ADV_INT.3	Minimally complex internals	EAL6
ADV_TDS.5	Complete Semiformal modular design	EAL6
ADV_SPM.1	Security Policy Modelling	EAL6
AGD_OPE.1	Operational user guidance	PP / EAL6
AGD_PRE.1	Preparative procedures	PP / EAL6
ALC_CMC.5	Advanced support	PP / EAL6
ALC_CMS.5	Development tools CM coverage	EAL6
ALC_DEL.1	Delivery procedures	PP / EAL6
ALC_DVS.2	Sufficiency of security measures	PP / EAL6
ALC_FLR.1	Flaw remediation	ST
ALC_LCD.1	Developer defined life-cycle model	PP / EAL6
ALC_TAT.3	Compliance with implementation standards – all parts	EAL6
ASE_CCL.1	Conformance claims	PP / EAL6
ASE_ECD.1	Extended components definition	PP / EAL6
ASE_INT.1	ST introduction	PP / EAL6
ASE_OBJ.2	Security objectives	PP / EAL6
ASE_REQ.2	Derived security requirements	PP / EAL6
ASE_SPD.1	Security problem definition	PP / EAL6
ASE_TSS.2	TOE summary specification	ST
ATE_COV.3	Rigorous analysis of coverage	EAL6
ATE_DPT.3	Testing: modular design	EAL6
ATE_FUN.2	Ordered functional testing	EAL6
ATE_IND.2	Independent testing - sample	PP / EAL6
AVA_VAN.5	Advanced methodical vulnerability analysis	PP / EAL6

Security Assurance Requirement ADV_SPM.1 requires the developer to provide a Security Policy Model for the Crypto Library. However, the N7021 hardware already provides a Security Policy Model (see [13] for details), which also applies unchanged to the composite product. As the SFRs introduced in this ST do not add a new Security Policy or change the rules of existing Security Policies of the hardware, there is no need for an additional Security Policy Model for the Crypto Library.

6.2.1 Refinements of the Security Assurance Requirements for EAL6+

The Security Target claims strict conformance to the Protection Profile [5], and therefore it has to be conform to the refinements of the TOE security assurance requirements (see Application Note 23 of the PP [5]).

The Hardware Security Target [13] for N7021 has chosen the evaluation assurance level EAL6+. The Security Target of the hardware platform with IC Dedicated Software including cryptographic library is based on the Protection Profile [5], which requires the lower level EAL4+. This implies that the refinements made in the Protection Profile [5], section 6.2.1 Refinements of the TOE Assurance Requirements, for EAL4+ had to be refined again in order to ensure EAL6+ in the Hardware Security Target (this was necessary for ALC_CMS.5, ALC_CMC.5, ADV_IMP.2, ATE_COV.3, and ADV_FSP.5).

Since these refinements explain and interpret the CC for hardware, these refinements do not affect the additional software in this composite TOE. Therefore all refinements made in the PP [5] are valid without change for the composite TOE.

6.3 Security Requirements Rationale

6.3.1 Rationale for the Security Functional Requirements

Section 6.3.1 of the PP [5] and Section 6.3.1 of the Hardware Security Target [13] provide the mapping between security functional requirements and security objectives of the TOE. This mapping entirely apply to this Security Target.

This ST lists a number of security objectives and SFRs for Crypto Library, which are additional to both the PP and the Hardware ST. These are listed in the following table.

Table 5. Mapping of SFRs to Security Objectives for Crypto Library in this ST

Objective	TOE Security Functional Requirements
O.RSA	FCS_COP.1/RSA FCS_COP.1/RSA_Pad FDP_IFC.1 FDP_ITT.1[HW] FPT_ITT.1[HW] FPT_FLS.1 FRU_FLT.2 FDP_RIP.1[SW] FCS_CKM.4
O.RSA_PubExp	FCS_COP.1/RSA_PubExp FDP_IFC.1 FDP_ITT.1[HW] FPT_ITT.1[HW] FPT_FLS.1 FRU_FLT.2 FDP_RIP.1[SW]

Objective	TOE Security Functional Requirements
O.RSA_KeyGen	FCS_CKM.1/RSA FDP_IFC.1 FDP_ITT.1[HW] FPT_ITT.1[HW] FPT_FLS.1 FRU_FLT.2 FDP_RIP.1[SW]
O.ECDSA	FCS_COP.1/ECDSA FDP_IFC.1 FDP_ITT.1[HW] FPT_ITT.1[HW] FPT_FLS.1 FRU_FLT.2 FDP_RIP.1[SW] FCS_CKM.4
O.ECC_DHKE	FCS_COP.1/ECC_DHKE FDP_IFC.1 FDP_ITT.1[HW] FPT_ITT.1[HW] FPT_FLS.1 FRU_FLT.2 FDP_RIP.1[SW]
O.ECC_KeyGen	FCS_CKM.1/ECC FDP_IFC.1 FDP_ITT.1[HW] FPT_ITT.1[HW] FPT_FLS.1 FRU_FLT.2 FDP_RIP.1[SW]
O.SHA	FCS_COP.1/SHA FDP_IFC.1 FDP_ITT.1[HW] FPT_ITT.1[HW] FPT_FLS.1 FRU_FLT.2 FDP_RIP.1[SW]

The justification of the security objectives O.RSA, O.RSA_PubExp, O.RSA_KeyGen, O.ECDSA, O.ECC_DHKE, O.ECC_KeyGen and O.SHA are all as follows:

- Each objective is directly implemented by a single SFR specifying the (cryptographic) service that the objective wishes to achieve (see the above table for the mapping).
- The requirements and architectural measures that originally were taken from the Protection Profile [5] and thus were also part of the Security Target of the hardware (chip) evaluation support the security objectives:
  - FRU_FLT.2 and FPT_FLS.1 supports the objective by ensuring that the TOE works correctly (i.e., all of the TOE's capabilities are ensured) within the specified operating conditions and maintains a secure state when the TOE is outside the specified

operating conditions. A secure state is also entered when perturbation or DFA attacks are detected.

- FDP_ITT.1[HW] (for User Data) and FPT_ITT.1[HW] (for TSF Data) ensure that no User Data (plain text data, keys) or TSF Data is disclosed when they are transmitted between different functional units of the TOE (i.e., the different memories, the CPU, cryptographic co-processors), thereby supporting the objective in keeping confidential data secret.
- FDP_IFC.1 also supports the aspects of confidentiality by ensuring that User Data and TSF Data are not accessible from the TOE except when the Security IC Embedded Software decides to communicate them via an external interface.
- FDP_RIP.1[SW] and FCS_CKM.4 ensures that the TOE provides procedural measures to prevent disclosure of memory contents that was used by the TOE. The Crypto Library supports FDP_RIP.1[SW] and FCS_CKM.4 by making all memory contents used by the library no longer available. Note that the requirement for residual information protection applies to all functionality of the Crypto Library.

6.3.2 Extended requirements

This Security Target does not define extended requirements.

6.3.3 Dependencies of security requirements

SFRs [FDP_ITC.1, or FDP_ITC.2 or FCS_CKM.1] are not included in this Security Target for FCS_COP.1/SHA since the TOE only provides a pure engine for these algorithms without additional features like the handling of keys or importing data from outside the TOE. Therefore the Security IC Embedded Software must fulfil these requirements related to the needs of the realized application.

6.3.4 Rationale for the Assurance Requirements

The selection of assurance components and augmentations of Crypto Library on N7021 is generally based on EAL6, the underlying Protection Profile [5], and the Security Target of the hardware [13] of the N7021.

EAL6 was chosen to provide an even stronger baseline of assurance than the EAL4 in the Protection Profile. The augmentations ALC_FLR.1 and ASE_TSS.2 were chosen to extend the level of assurance even further.

7 TOE Summary Specification

This chapter describes the "IT Security Functionality".

7.1 IT Security Functionality

The evaluation of this cryptographic library is performed as a composite evaluation, where the TOE comprises both the underlying hardware and the embedded software (Crypto Library). The TOE of this composite evaluation therefore extends the security functionality already available in the chip platform (see section 7.1 "Portions of the TOE Security Functionality" of the Hardware Security [13]).

The security functionality of N7021

The security functionality of the hardware platform for the N7021 is described in the Hardware Security Target [13]. They entirely apply to this Security Target.

Note 8. The security functionality SF.LOG is extended by the Crypto Library as described in Security Features of the TOE.

The additional security functionality provided by the TOE is described in the following sub-sections.

The IT security functionalities directly correspond to the TOE security functional requirements defined in Section 6.1. The definitions of the IT security functionalities refer to the corresponding security functional requirements.

7.1.1 Security Services of the TOE

7.1.1.1 SS.RSA

The TOE provides functions that implement the RSA algorithm and the RSA-CRT algorithm for data encryption, decryption, signature and verification. All algorithms are defined in PKCS #1, v2.2 (RSAEP, RSADP, RSAP1, RSAVP1)

This routine supports various key lengths from 512 bits to 4096 bits.

The TOE contains modular exponentiation functions, which, together with other functions in the TOE, perform the operations required for RSA encryption or decryption. Two different RSA algorithms are supported by the TOE, namely the "Simple Straight Forward Method" (called RSA "straight forward", the key consists of the pair n and d) and RSA using the "Chinese Remainder Theorem" (RSA CRT, the key consists of the quintuple p, q, dp, dq, qInv).

Attack resistance for this security functionality is discussed in Security architectural information.

This security functionality covers:

- FCS_COP.1/RSA

7.1.1.2 SS.RSA_Pad

The TOE provides functions that implement the RSA algorithm and the RSA-CRT algorithm for message and signature encoding. This IT security functionality supports the EME-OAEP and EMSA-PSS signature scheme. All algorithms are defined in PKCS #1, v2.2 (EME-OAEP, EMSA-PSS)

This routine supports various key lengths from 512 bits to 4096 bits.

Attack resistance for this security functionality is discussed in Security architectural information.

This security functionality covers:

- FCS_COP.1/RSA_PAD

7.1.1.3 SS.RSA_PublicExp

The TOE provides functions that implement computation of an RSA public key from a private CRT key. All algorithms are defined in PKCS #1, v2.2.

This routine supports various key lengths from 512 bits to 4096 bits (CRT).

Attack resistance for this security functionality is discussed in Security architectural information.

This security functionality covers:

- FCS_COP.1/RSA_PubExp

7.1.1.4 SS.ECDSA

The TOE provides functions to perform ECDSA Signature Generation and Signature Verification according to ISO/IEC 14888-3:2015 [18], ANSI X9.62 [21], FIPS PUB 186-4 [17] and IEEE Std 1363™-2000 [20]

Note that hashing of the message must be done beforehand and is not provided by this security functionality, but could be provided by SS.SHA.

The supported key length are 224, 256, 320, 384, 512 and 521 bits.

SS.ECDSA supports the following standard curves: ansix9p224r1, ansix9p256r1, ansix9p384r1 and ansix9p521r1 from ANSI X9.62 [21], brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1 and brainpoolP512t1 from RFC 5639 [23], and ANSSI FRP256v1 [24] curves.

Attack resistance for this security functionality is discussed in Security architectural information.

This security functionality covers:

- FCS_COP.1/ECDSA

The TOE further provides functions to perform a full ECC point addition as well as a basic curve parameter check for EC domain parameter. These functionalities are additionally assessed by the ITSEF performing the evaluation.

7.1.1.5 SS.ECC_DHKE

The TOE provides functions to perform Diffie-Hellman Key Exchange according to ISO/IEC 11770-3:2015 [15], ANSI X9.63 [22] and IEEE Std 1363™-2000 [20]

The supported key length are 224, 256, 320, 384, 512 and 521 bits.

SS.ECC_DHKE supports the following standard curves: ansix9p224r1, ansix9p256r1, ansix9p384r1 and ansix9p521r1 from ANSI X9.62 [21], brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1,

brainpoolP384r1, brainpoolP384t1, brainpoolP512r1 and brainpoolP512t1 from RFC 5639 [23], and ANSSI FRP256v1 [24] curves.

Attack resistance for this security functionality is discussed in Security architectural information.

This security functionality covers:

- FCS_COP.1/ECC_DHKE

7.1.1.6 SS.RSA_KeyGen

The TOE provides functions to generate RSA key pairs as described in PKCS #1, v2.2, and FIPS 186-4 [17].

It supports various key lengths from 512 bits to 4096 bits.

Two different output formats for the key parameters are supported by the TOE, namely the "Simple Straight Forward Method" (RSA "straight forward") and RSA using the "Chinese Remainder Theorem" (RSA CRT).

Attack resistance for this security functionality is discussed in Security architectural information.

This security functionality covers:

- FCS_CKM.1/RSA

7.1.1.7 SS.ECC_KeyGen

The TOE provides functions to perform ECC over GF(p) Key Generation according to ISO/IEC 14888-3:2015 [18], ANSI X9.62 [21] and FIPS PUB 186-4 [17].

The supported key length are 224, 256, 320, 384, 512 and 521 bits.

SS.ECC_KeyGen supports the following standard curves: ansix9p224r1, ansix9p256r1, ansix9p384r1 and ansix9p521r1 from ANSI X9.62 [21], brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1 and brainpoolP512t1 from RFC 5639 [23], and ANSSI FRP256v1 [24] curves.

Attack resistance for this security functionality is discussed in Security architectural information.

This security functionality covers:

- FCS_CKM.1/ECC

7.1.1.8 SS.SHA

The TOE implements functions to compute the Secure Hash Algorithms SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 according to the standard FIPS 180-4 [16]

Attack resistance for this security functionality is discussed in Security architectural information.

This security functionality covers:

- FCS_COP.1/SHA

8 Annexes

8.1 Further Information contained in the PP

The Annex of the Protection Profile ([5], chapter 7) provides further information. Section 7.1 of the PP describes the development and production process of smartcards, containing a detailed life-cycle description and a description of the assets of the Integrated Circuits Designer/Manufacturer. Section 7.6 of the PP gives examples of Attack Scenarios.

8.2 Glossary and Vocabulary

Note: To ease understanding of the used terms the glossary of the Protection Profile [5] is included here.

Application Data	All data managed by the Security IC Embedded Software in the application context. Application data comprise all data in the final Security IC.
Authentication reference data	Data used to verify the claimed identity in an authentication procedure.
Authentication verification data	Data used to prove the claimed identity in an authentication procedure.
Composite Product Integrator	Role installing or finalizing the IC Security IC Embedded Software and the applications on platform transforming the TOE into the unpersonalized Composite Product after TOE delivery. The TOE Manufacturer may implement IC Security IC Embedded Software delivered by the Security IC Embedded Software Developer before TOE delivery (e.g. if the IC Security IC Embedded Software is implemented in ROM or is stored in the non-volatile memory as service provided by the IC Manufacturer or IC Packaging Manufacturer).
Composite Product Manufacturer	The Composite Product Manufacturer has the following roles (i) the Security IC Embedded Software Developer (Phase 1), (ii) the Composite Product Integrator (Phase 5) and (iii) the Personalizer (Phase 6). If the TOE is delivered after Phase 3 in form of wafers or sawn wafers (dice) he has the role of the IC Packaging Manufacturer (Phase 4) in addition. The customer of the TOE Manufacturer who receives the TOE during TOE Delivery. The Composite Product Manufacturer includes the Security IC Embedded Software developer and all roles after TOE Delivery up to Phase 6 (refer to Figure 2 on page 10 and Section 7.1.1).
End-consumer	User of the Composite Product in Phase 7.
IC Dedicated Software	IC proprietary software embedded in a Security IC (also known as IC firmware) and developed by the IC Developer. Such software is required for testing purpose (IC Dedicated Test Software) but may provide additional

	services to facilitate usage of the hardware and/or to provide additional services (IC Dedicated Support Software).
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
Initialization Data	Initialization Data defined by the TOE Manufacturer to identify the TOE and to keep track of the Security IC's production and further life-cycle phases are considered as belonging to the TSF data. These data are for instance used for traceability and for TOE identification (identification data).
Integrated Circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions.
Memory	The memory comprises of the RAM, ROM and the Flash of the TOE.
Memory Management Unit	The MMU maps the virtual addresses used by the CPU into the physical addresses of RAM, ROM and Flash. This mapping is done based on memory partitioning. Memory partitioning is fixed.
Pre-personalization Data	Any data supplied by the Card Manufacturer that is injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 3). These data are for instance used for traceability and/or to secure shipment between phases.
Security IC	(as used in this Protection Profile) Composition of the TOE, the Security IC Embedded Software, user data of the Composite TOE and the package (the Security IC carrier).
Security IC Embedded Software	Software embedded in a Security IC and normally not being developed by the IC Designer. The Security IC Embedded Software is designed in Phase 1 and embedded into the Security IC in Phase 3 or in later phases of the Security IC product life-cycle. Some part of that software may actually implement a Security IC application others may provide standard services. Nevertheless, this distinction doesn't matter here so that the Security IC Embedded Software can be considered as being application dependent whereas the IC Dedicated Software is definitely not.
Security IC Product	Composite product which includes the Security Integrated Circuit (i.e. the TOE) and the Security IC Embedded Software and is evaluated as composite

	target of evaluation in the sense of the Supporting Document
Secured Environment	Operational environment maintains the confidentiality and integrity of the TOE as addressed by OE.Process-Sec-IC and the confidentiality and integrity of the IC Security IC Embedded Software, TSF data or user data associated with the product by security procedures of the product manufacturer, personaliser and other actors before delivery to the end-user depending on the life-cycle.
Test Features	All features and functions (implemented by the IC Dedicated Test Software and/or hardware) which are designed to be used before TOE Delivery only and delivered as part of the TOE.
TOE Delivery	The period when the TOE is delivered which is (refer to Figure 2 on page 10) either (i) after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or (ii) after Phase 4 (or before Phase 5) if the TOE is delivered in form of packaged products.
TOE Manufacturer	The TOE Manufacturer must ensure that all requirements for the TOE (as defined in Section 1.2.2) and its development and production environment are fulfilled (refer to Figure 2 on page 10). The TOE Manufacturer has the following roles: (i) IC Developer (Phase 2) and (ii) IC Manufacturer (Phase 3). If the TOE is delivered after Phase 4 in form of packaged products, he has the role of the (iii) IC Packaging Manufacturer (Phase 4) in addition.
TSF data	DataData for the operation of the TOE upon which the enforcement of the SFR relies. They are created by and for the TOE, that might affect the operation of the TOE. This includes information about the TOE's configuration, if any is coded in non-volatile non-programmable memories (ROM), in non-volatile programmable memories (for instance E2PROM or flash memory), in specific circuitry or a combination thereof.
User data of the Composite TOE	All data managed by the Security IC Embedded Software in the application context.
User data of the TOE	Data for the user of the TOE, that does not affect the operation of the TSF. From the point of view of TOE defined in this PP the user data comprises the Security IC Embedded Software and the user data of the Composite TOE.

9 Bibliography

9.1 Evaluation documents

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004

[5] Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, registered and certified by Bundesamt fuer Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0084-2014

9.2 Developer documents

[6] N7021 Crypto Library: User Guidance – N7021 Crypto Library

[7] N7021 Crypto Library: User Manual – Hash

[8] N7021 Crypto Library: User Manual – SHA

[9] N7021 Crypto Library: User Manual – RSA

[10] N7021 Crypto Library: User Manual – RSA Key Generation

[11] N7021 Crypto Library: User Manual – ECC over GF(p)

[12] N7021 Crypto Library: User Manual – UtilsAsym

[13] NXP Secure Smart Card Controller N7021 VA: Security Target, NXP Semiconductors

9.3 Standards

[14] ISO 11568-4-2007: Banking – Key management (retail) – Part 4: Asymmetric cryptosystems – Key management and life cycle, 2007

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

[16] FIPS PUB 180-4: Secure Hash Standard, Federal Information Processing Standards Publication, February 2011, US Department of Commerce/National Institute of Standards and Technology

[17] FIPS PUB 186-4: Digital Signature Standard, Federal Information Processing Standards Publication, 2013, July, National Institute of Standards and Technology

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

[19] JIL-ATT-SC: Attack Methods for Smartcards and Similar Devices, Joint Interpretation Library, Version 2.2, January 2013

[20] IEEE Std 1363™-2000: IEEE Standard Specifications for Public-Key Cryptography, IEEE Computer Society, 2005-12-12

[21] ANSI X9.62: Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Standard (ECDSA), American National Standard, November 16th, 2005

[22] ANSI X9.63: Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve cryptography, American National Standard, January 2011
[23] RFC 5639: Elliptic Curve Cryptography (ECC) Brainpool Standard - Curves and Curve Generation, IETF, March 2010
[24] ANSSI 2011:http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000024668816

10 Legal information

10.1 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

10.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the *Terms and conditions of commercial sale* of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

10.3 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

Adelante, **Bitport**, **Bitsound**, **CoolFlux**, **CoReUse**, **DESFire**, **EZ-HV**, **FabKey**, **GreenChip**, **HiPerSmart**, **HITAG**, **I²C-bus** logo, **ICODE**, **I-CODE**, **ITEC**, **Labelution**, **MIFARE**, **MIFARE Plus**, **MIFARE Ultralight**, **MoReUse**, **QLPAK**, **Silicon Tuner**, **SiliconMAX**, **SmartXA**, **STARplug**, **TOPFET**, **TrenchMOS**, **TriMedia** and **UCODE** — are trademarks of NXP B.V.

HD Radio and **HD Radio** logo — are trademarks of iBiquity Digital Corporation.

Tables

Contents

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 5 June 2019