Crypto Library V3.1.x on P6022y VB

Security Target

Rev. 2.1 — 12 December 2022 **Evaluation document**

NSCIB-CC-15-67206 **PUBLIC**

Document information

Information	Content
Keywords	Security Target, Crypto Library, P6022y VB
Abstract	Security Target for the Crypto Library V3.1.x on P6022y VB 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
0.6	2015-04-02	Derived from ST for Crypto Library V3.0 on P6021y VB, Rev. 0.6, and updated the whole chapters for P6022y VB
0.7	2015-04-22	Updated Table 1, changed the reference of P.Crypto-Service to HW-ST, replaced O.AES and O.DES by O.SW_AES and O.SW_DES, replaced O.HW_TDES and O.HW_AES by O.TDES and O.AES, changed the reference of O.TDES and O.AES to HW-ST, removed O.INTEGRITY_CHK and FDP_ITT.5, updated FDP_SOP.1.1, and updated Bibliography
0.8	2015-05-19	Updated the certification ID
0.9	2015-09-10	Updated Table 1
1.0	2015-09-24	Changed TOE name and updated UM versions
1.1	2015-10-15	Updated the UGM version and date in Table 1
1.2	2015-11-26	Updated Table 1 to cover CL V3.1.2
1.3	2016-02-24	Changed TOE name and Title, and updated Section 1.1
1.4	2016-03-18	Updated Table 1
1.5	2016-06-27	Updated Table 1
1.6	2017-08-08	Removed ECC over GF(p) curve parameter verification, updated UGM reference
1.7	2017-10-19	EAL increased to EAL 6 augmented for all configurations. Added missing header file to Table 1
1.8	2017-12-14	Removed MIFARE-related functionality from scope. Updated documentation format in Table 1.
1.9	2018-02-22	Updated CC references to CC v3.1 r5
2.0	2018-03-22	Updated UGM reference in Table 1.
2.1	2022-12-12	Updated reference to HW platform Security Target

1 ST Introduction

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

1.1 ST Identification

This Security Target is for the Common Criteria evaluation of the “Crypto Library V3.1.x on P6022y VB” provided by NXP Semiconductors.

ST Identification: Crypto Library V3.1.x on P6022y VB Security Target, Rev. 2.1 – 12 December 2022 NSCIB-CC-15-67206

The TOE is a composite TOE, consisting of:

- The hardware “NXP Secure Smart Card Controller P6022y VB” which is used as evaluated platform,
- The “Crypto Library V3.1.x on P6022y VB” which is built upon this platform.

This Security Target builds on the Hardware Security Target [10], which refers to the “NXP Secure Smart Card Controller P6022y VB”, provided by NXP Semiconductors.

The Crypto Library V3.1.x covers Crypto Library V3.1.2. In this Security Target, the Crypto Library V3.1.x represents Crypto Library V3.1.2. In case of a composite evaluation the used minor version of the CL should be explicitly mentioned.

To unify documents derivative independent identification “Crypto Library on SmartMX2“ is used where possible. Derivative dependent information is emphasized as such.

1.2 TOE Overview

1.2.1 Introduction

The Hardware Security Target [10] contains, in section 1.3 “TOE Overview”, an introduction about the SmartMX2 P6022y VB hardware TOE that is considered in the evaluation. The Hardware Security Target includes IC Dedicated Software stored in the ROM provided with the SmartMX2 P6022y VB hardware platform.

The “Crypto Library V3.1.x on P6022y VB“ is a cryptographic library, which provides a set of cryptographic functions that can be used by the Smartcard Embedded Software. The cryptographic library consists of several binary packages that are intended to be linked to the Smartcard Embedded Software. The Smartcard Embedded Software developer links the binary packages that he needs to his Smartcard Embedded Software and the whole is subsequently implemented in arbitrary memory (ROM or EEPROM) of the hardware platform.

The NXP SmartMX2 P6022y VB provides the computing platform and cryptographic support by means of co-processors for the Crypto Library V3.1.x on P6022y VB.

The Crypto Library V3.1.x on P6022y VB provides the security functionality described below in addition to the functionality described in the Hardware Security Target [10] for the hardware platform.

The Crypto Library provides AES[1], DES[1], Triple-DES (3DES)[1], 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, full point addition (ECC over GF(p)), standard security level SHA 1, SHA-224, SHA-256, SHA-384, SHA-512 algorithms.[2]

Most algorithms are resistant against attacks as described in the JIL attack methods for smartcard and similar devices [31].

In addition, the Crypto Library implements a software (pseudo) random number generator which is initialized (seeded) by the hardware random number generator of the SmartMX2.

Finally, the TOE provides a secure copy routine, a secure memory compare routine, a secure modular multiply routine, a secure modular add and subtract routine and includes internal security measures for residual information protection.

1.2.2 Life-Cycle

The life cycle of the hardware platform as part of the TOE is described in section 1.4.5 “TOE Intended Usage” of the Hardware Security Target [10]. The delivery process or the hardware platform is independent from the Crypto Library V3.1.x on P6022y VB.

The Crypto Library 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 Smartcard Embedded Software. The Smartcard 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 by Smartcard Embedded Software Developers is out of the control of the developer NXP Semiconductors; the integration of the Crypto Library into Smartcard Embedded Software is not part of this evaluation.

Security during Development and Production

The development process of the Crypto Library 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 V3.1.x on P6022y VB. The security measures installed within NXP, including a secure delivery process, ensure the integrity and quality of the delivered Crypto Library binary files.

1.2.3 Specific Issues of Smartcard 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 [10]. This additional functionality is added using the policy “P.Add-Func” (see Section 3.3 of this Security Target).

1 AES, DES, and Triple-DES can be used in ECB, CBC, CBC-MAC, or CMAC mode.

2 To fend off attackers with high attack potential an adequate security level must be used (references can be found in national and international documents and standards). In particular this means that SHA-1, Single-DES and short key lengths for RSA, ECC shall not be used.

1.3 TOE Description

The Target of Evaluation (TOE) consists of a hardware part (incl. IC Dedicated Software) and the Smartcard Embedded Software part:

- The hardware part consists of the NXP Secure Smart Card Controller P6022y VB with IC Dedicated Software. The P6022y VB is configurable to P6022P VB, P6022X VB, P6022M VB, P6022D VB, or P6022J VB.
  - **P6022P VB / P6022X VB:** The IC Dedicated Software of P6022P VB / P6022X VB is composed of IC Dedicated Test Software and IC Dedicated Support Software. The IC Dedicated Test Software contains the Test-ROM Software; the IC Dedicated Support Software is composed of the Boot-ROM Software, and the Plain Firmware Operating System (FOS-Plain). FOS-Plain does not include any MIFARE Emulation.
  - **P6022M VB / P6022D VB / P6022J VB:** The IC Dedicated Software of P6022M VB / P6022D VB / P6022J VB is composed of IC Dedicated Test Software and IC Dedicated Support Software. The IC Dedicated Test Software contains the Test-ROM Software; the IC Dedicated Support Software is composed of the Boot-ROM Software, and the Emulation Firmware Operating System (FOS-Emu). In the FOS-Emu, P6022M VB includes Emulation MIFARE Plus MF1PLUSx0, P6022D VB includes Emulation MIFARE DESFire EV1, and P6022J VB includes both Emulation MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1.
- All other software is called Smartcard Embedded Software. The hardware part of the TOE includes dedicated guidance documentation. The Smartcard Embedded Software “Crypto Library V3.1.x on P6022y VB” consists of a software library and associated documentation. The Crypto Library V3.1.x on P6022y VB is an additional part that provides cryptographic functions that can be operated on the hardware platform as described in this Security Target. The rest of the Smartcard Embedded Software is not part of the TOE.

The hardware part of the TOE is not described in detail in this document. Details are included in the Hardware Security Target [10] and therefore this latter document will be cited wherever appropriate. However the assets, assumptions, threats, objectives and security functional requirements are tracked in this Security Target.

The TOE components consist of all the TOE components listed in Table 1 of the Hardware Security Target [10] 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	Date	Form of Delivery
Library File	phSmx2ClDes.lib	1.5	2015-09-14	Electronic file
	phSmx2ClAes.lib	1.6	2015-09-14	Electronic file
	phSmx2ClRsa.lib	1.10	2015-09-14	Electronic file
	phSmx2ClRsaKg.lib	2.7	2015-09-14	Electronic file
	phSmx2ClEccGfp.lib	2.7	2015-09-14	Electronic file
	phSmx2ClSha.lib	1.7	2015-09-14	Electronic file
	phSmx2ClSha512.lib	1.8	2015-09-14	Electronic file
	phSmx2ClRng.lib	2.8	2015-09-14	Electronic file
	phSmx2ClUtils.lib	2.2	2015-09-14	Electronic file
	phSmx2ClSymCfg.lib	1.8	2015-09-14	Electronic file
Header File	phSmx2ClDes.h	1.4	2015-03-26	Electronic file

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

Type	Name	Release	Date	Form of Delivery
	phSmx2ClAes.h	1.5	2015-03-26	Electronic file
	phSmx2ClRsa.h	1.9	2015-04-28	Electronic file
	phSmx2ClRsaKg.h	2.6	2015-04-28	Electronic file
	phSmx2ClEccGfp.h	2.6	2015-04-28	Electronic file
	phSmx2ClSha.h	1.6	2015-03-26	Electronic file
	phSmx2ClSha512.h	1.7	2015-03-26	Electronic file
	phSmx2ClRng.h	2.7	2015-04-28	Electronic file
	phSmx2ClUtils.h	2.0	2015-04-28	Electronic file
	phSmx2ClUtils_ImportExportFcts.h	2.0	2015-04-28	Electronic file
	phSmx2ClUtils_RngAccess.h	2.0	2015-04-28	Electronic file
	phSmx2ClTypes.h	1.1	2013-11-15	Electronic file
	phSmx2ClSymCfg.h	1.7	2015-03-26	Electronic file
	phSmx2ClSymCfg_Aes.h	1.7	2015-03-26	Electronic file
	phSmx2ClSymCfg_Des.h	1.7	2015-03-26	Electronic file
Source Code	phSmx2ClUtils_ ImportExportFcts.a51	2.0	2015-04-28	Electronic file
	phSmx2ClUtils_RngAccess.a51	2.0	2015-04-28	Electronic file
Documents	User Guidance Manual [11]	1.6	2018-02-28	PDF via DocStore
	User Guidance: DES [13]	1.0	2015-11-23	PDF via DocStore
	User Guidance: AES [14]	1.0	2015-11-23	PDF via DocStore
	User Guidance: RSA [17]	1.0	2015-11-23	PDF via DocStore
	User Guidance: RSA Key Generation [18]	1.0	2015-11-23	PDF via DocStore
	User Guidance: ECC over GF(p) [19]	1.0	2015-11-23	PDF via DocStore
	User Guidance: SHA [15]	1.0	2015-11-23	PDF via DocStore
	User Guidance: SHA512 [16]	1.0	2015-11-23	PDF via DocStore
	User Guidance: RNG [12]	1.0	2015-11-23	PDF via DocStore
	User Guidance: Utils [20]	1.0	2015-11-23	PDF via DocStore
	User Guidance: SymCfg [21]	1.1	2016-03-16	PDF via DocStore

1.3.1 Hardware description

The NXP SmartMX2 P6022y VB hardware is described in section 1.4.4.1 “Hardware Description” of the Hardware Security Target [10]. The IC Dedicated Support Software stored in the Test-ROM and delivered with the hardware platform is described in section 1.4.4.2 “Software Description” of the Hardware Security Target [10].

1.3.2 Software description

A Smartcard embedded Software developer may create Smartcard embedded Software to execute on the NXP SmartMX2 hardware. This software is stored in arbitrary memory of the NXP SmartMX2 hardware and is not part of the TOE, with one exception: the Smartcard embedded Software may contain the “Crypto Library V3.1.x on P6022y VB“ (or parts thereof) and this Crypto Library (or parts thereof [3]) is part of the TOE.

AES

- The AES algorithm is intended to provide encryption and decryption functionality.
- The Crypto Library implements two library versions for AES algorithm (phSmx2ClAes library and part of phSmx2ClSymCfg library) with different security configurations. For more details on those different configurations please refer the user guidance documentation of the Crypto Library [11].
- The following modes of operation are supported for AES: ECB, CBC, CBC-MAC and CMAC.

DES/3DES

- The DES and Triple-DES (3DES) algorithm are intended to provide encryption and decryption functionality.
- The Crypto Library implements two library versions for DES algorithm (phSmx2ClDes library and part of phSmx2ClSymCfg library) with different security configurations. For more details on those different configurations please refer the user guidance documentation of the Crypto Library [11].
- The following modes of operation are supported for DES and Triple-DES: ECB, CBC, CBC-MAC, and CMAC

To fend off attackers with high attack potential an adequate security level must be used (references can be found in national and international documents and standards). In particular this means that Single-DES shall not be used.

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. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

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.

3 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 Smartcard Embedded Software. For example, it is possible to omit the RSA or the SHA 1 components. However, some dependencies exist; details are described in the User Guidance [11].

- The ECDH (ECC Diffie-Hellman) key exchange algorithm can be used to establish cryptographic keys. It can be also used as secure point multiplication.
- Provide secure point addition for Elliptic Curves over GF(p).

The TOE supports various key sizes for ECC over GF(p) up to a limit of 576 bits for signature generation, key pair generation and key exchange. For signature verification the TOE supports key sizes up to a limit of 576 bits . To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

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.

To fend off attackers with high attack potential an adequate security level must be used (references can be found in national and international documents and standards). In particular this means that SHA-1 shall not be used.

Resistance of cryptographic algorithms against attacks

The cryptographic algorithms are resistant against attacks as described in JIL, Attack Methods for Smartcards and Similar Devices [31], which include Side Channel Attacks, Perturbation attacks, Differential Fault Analysis (DFA) and timing attacks, except for SHA, which is only resistant against Side Channel Attacks and timing attacks.

More details about conditions and restrictions for resistance against attacks are given in the user documentation of the Crypto Library [11].

Random number generation

- The TOE provides access to random numbers generated by a software (pseudo) random number generator and functions to perform a test of the hardware (true) random number generator at initialisation.

Other security functionality

- The TOE includes internal security measures for residual information protection.
- The TOE provides a secure copy routine.
- The TOE provides a secure compare routine
- The TOE provides a secure modular multiply routine
- The TOE provides a secure modular add and subtract routine

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

1.3.3 Documentation

The documentation for the NXP SmartMX2 P6022y VB hardware is listed in section 1.4.3.3 “Documentation” of the Hardware Security Target [10].

The Crypto Library has associated user manuals and one user guidance documentation (see [11]). 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 Smartcard Embedded Software and

The user guidance document contains:

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

1.3.4 Interface of the TOE

The interface to the NXP SmartMX2 P6022y VB hardware is described in section 1.4.6 “Interface of the TOE” of the Hardware Security Target [10].

The use of this interface is not restricted by the use of the Crypto Library V3.1.x on P6022y VB.

The interface to the TOE additionally consists of software function calls, as detailed in the “User Manual” documents of the Crypto Library V3.1.x on P6022y VB. The developer of the Smartcard Embedded Software will link the required functionality of the Crypto Library V3.1.x on P6022y VB into the Smartcard Embedded Software as required for his Application.

1.3.5 Life Cycle and Delivery of the TOE

The life cycle and delivery for the NXP SmartMX2 P6022y VB hardware is described in section 1.4.4 “Security during development and production” of the Hardware Security Target [10].

The crypto library is encrypted and signed for delivery. The actual delivery of the signed, encrypted file may be by e-mail or on physical media such as compact disks.

The Crypto Library 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 Smartcard Embedded Software developer. The Crypto Library may be delivered by e-mail or by delivering physical media such as compact disks by mail or courier. To protect the Crypto Library during the delivery process, the Crypto Library is encrypted and digitally signed. The Smartcard Embedded Software developer then integrates the Crypto Library in the Smartcard Embedded Software.

1.3.6 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 smartcard hardware and the Smartcard 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 [10].

The Crypto Library V3.1.x on P6022y VB is intended to support the development of the Smartcard Embedded Software since the cryptographic functions provided by the Crypto Library V3.1.x on P6022y VB include countermeasures against the threats described in this Security Target. The used modules of the Crypto Library V3.1.x on P6022y VB are linked to the other parts of the Smartcard Embedded Software and they are implemented as part of the Smartcard Embedded Software in arbitrary memory of the hardware platform.

1.3.7 TOE User Environment

The user environment for the crypto library is the Smartcard Embedded Software, developed by customers of NXP, to run on the NXP P6022y VB hardware.

1.3.8 General IT features of the TOE

The general features of the NXP SmartMX2 P6022y VB hardware are described in section 1.3 “TOE overview” of the Hardware Security Target [10]. These are supplemented for the TOE by the functions listed in section 1.2.1 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** for all configurations. 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, EAL 6 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 [10]).

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 Smart Card Controller IC) and software (Dedicated Test and Support Software). This is identical to the TOE as defined in [5] and therefore the TOE type is consistent.

3 Security Problem Definition

This Security Target claims strict conformance to the Security IC Platform protection profile [5]. The Assets, Assumptions, Threats and Organizational Security Policies of the Protection Profile are assumed here, together with extensions defined in chapter 3 “Security Problem Definition” of the Hardware Security Target [10]. In the following sub-sections, only extensions to the different sections are listed. The titles of the chapters that are not extended are cited here for completeness.

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 mentioned as assets in [10]. 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 described in section 3.2 “Threats” of the Hardware Security Target [10] are valid for this Security Target. The threats are listed in the table below.

Table 2. Threats for Crypto Library V3.1.x on P6022y VB

Name	Title	Defined in
T.Leak-Inherent	Inherent Information Leakage	PP [5]
T.Phys-Probing	Physical Probing	PP [5]
T.Malfunction	Malfunction due to Environmental Stress	PP [5]
T.Phys-Manipulation	Physical Manipulation	PP [5]
T.Leak-Forced	Forced Information Leakage	PP [5]
T.Abuse-Func	Abuse of Functionality	PP [5]
T.RND	Deficiency of Random Numbers	PP [5]
T.Unauthorised-Access	Unauthorized Memory or Hardware Access	HW ST [10]

Note 2. Within the Hardware Security Target [10], the threat T.RND has been used in a context where the hardware (true) random number generator is threatened. The TOE consists of both hardware (NXP SmartMX2 P6022y VB) and software (Crypto Library V3.1.x on P6022y VB). The Crypto Library provides random numbers generated by a software (pseudo) random number generator. Therefore the threat T.RND explicitly includes both deficiencies of hardware random numbers as well as deficiency of software random numbers.

3.3 Organizational Security Policies

Since this Security Target claims strict conformance to the PP [5], the Policy P.Process-TOE “Identification during TOE Development and Production” of the Protection Profile is

applied here also. The hardware security target [10] defines additional security policies. The policies valid for the TOE are listed in the table below.

Table 3. Organisational security policies for Crypto Library V3.1.x on P6022y VB

Name	Title	Defined in
P.Process-TOE	Identification during TOE Development and Production	PP [5]
P.Crypto-Service	Cryptographic services of the TOE	HW-ST [10]
P.Add-Components-Plain	Additional Specific Security Components	HW-ST [10]

The Crypto Library part of the TOE uses the AES co-processor hardware to provide AES security functionality, and the DES co-processor hardware to provide DES security functionality as listed below in P.Add-Func: Additional Specific Security Functionality. In addition to the security functionality provided by the hardware and defined in the Security Target of the P6022y VB the following additional security functionality is provided by the Crypto Library for use by the Smart Card Embedded Software:

P.Add-Func: Additional Specific Security Functionality

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

- AES encryption and decryption,
- DES and Triple-DES encryption and decryption,
- 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,
- ECC over GF(p) point addition,
- SHA 1, SHA-224, SHA-256, SHA-384 and SHA-512 Hash Algorithms,
- access to the RNG (implementation of a software RNG),
- secure copy routine,
- secure compare routine,
- secure modular multiply routine,
- secure modular add and subtract routine;

In addition, the TOE shall

- provide protection of residual information, and
- provide resistance against attacks as described in Note 4 and in Section 7.2.

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

3.4 Assumptions

Since this Security Target claims strict conformance to the PP [5], the assumptions defined in section 3.4 of the Protection Profile, and described in section 3.4 “Assumptions” of the Hardware Security Target [10] are valid for this Security Target. The assumptions valid for the TOE are listed below.

Table 4. Assumptions for Crypto Library V3.1.x on P6022y VB

Name	Title	Defined in
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalization	PP [5]
A.Resp-Appl	Treatment of user Data of the Composite TOE	PP [5]
A.Check-Init-Plain	Check of initialisation data by the Security IC Embedded Software	HW-ST [10]

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 following tables list the security objectives of the Protection Profile [5] and the Hardware Security Target [10]. The security objectives for the TOE are listed in the table below:

Table 5. Security Objectives for Crypto Library on Crypto Library V3.1.x on P6022y VB

Name	Title	Defined in
O.Leak-Inherent	Protection against Inherent Information Leakage	PP [5]
O.Phys-Probing	Protection against Physical Probing	PP [5]
O.Malfunction	Protection against Malfunctions	PP [5]
O.Phys-Manipulation	Protection against Physical Manipulation	PP [5]
O.Leak-Forced	Protection against Forced Information Leakage	PP [5]
O.Abuse-Func	Protection against Abuse of Functionality	PP [5]
O.Identification	TOE Identification	PP [5]
O.RND	Random Numbers	PP [5]
O.TDES	Cryptographic service Triple-DES	HW-ST [10]
O.AES	Cryptographic service AES	HW-ST [10]
O.CUST_RECONF_PLAIN	Post Delivery Configuration of Hardware	HW-ST [10]
O.EEPROM_INTEGRITY	Integrity support of data stored to EEPROM	HW-ST [10]
O.FM_FW	Firmware Mode Firewall	HW-ST [10]
O.MEM_ACCESS	Area based Memory Access Control	HW-ST [10]
O.SFR_ACCESS	Special Function Register Access Control	HW-ST [10]
O.PUF	Sealing/Unsealing user data	HW-ST [10]

Note 3. Within the Hardware Security Target [10], the objective O.RND has been used in context with the hardware (true) random number generator (RNG). In addition to this, the TOE also provides a software (pseudo) RNG. Therefore the objective O.RND is extended to comprise also the quality of random numbers generated by the software (pseudo) RNG. See also Note 2 in Section 3.2, which extends T.RND in a similar way.

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

O.SW_AES The TOE includes functionality to provide encryption and decryption facilities of the AES algorithm, see Note 4

O.SW_DES The TOE includes functionality to provide encryption and decryption facilities of the DES & Triple-DES algorithm, see Note 4

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.ECC_Add	The TOE includes functionality to provide a point addition based on ECC over GF(p), 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.
O.Copy	The TOE includes functionality to copy memory content, see Note 4.
O.Compare	The TOE includes functionality to compare memory content, see Note 4.
O.ModMultiply	The TOE includes functionality to modular multiply memory content, see Note 4.
O.ModAddSubtract	The TOE includes functionality to modular add and subtract memory content, see Note 4.
O.REUSE	The TOE includes measures to ensure that the memory resources being used by the TOE cannot be disclosed to subsequent users of the same memory resource.

Note 4. All introduced security objectives claiming cryptographic functionality and the security objectives for copy and compare are protected against attacks as described in the JIL, Attack Methods for Smartcards and Similar Devices [31], which include Side Channel Attacks, Perturbation attacks, Differential Fault Analysis (DFA) and timing attack. 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 and DFA.

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.

To fend off attackers with high attack potential an adequate security level must be used (references can be found in national and international documents and standards). In particular this means that SHA-1, Single-DES, and short key lengths for RSA and ECC shall not be used.

4.2 Security Objectives for the Security IC Embedded Software

The security objectives for the security IC Embedded software, listed in the following Table 6, are taken from the PP [5]. Additional refinements in the Hardware Security Target [10] are also valid in the ST for the Crypto Library (the “IC Dedicated Support Software”).

Table 6. Security Objectives for the Security IC Embedded Software

Name	Title	Applies to phase
OE.Resp-Appl	Treatment of user data of the Composite TOE	Phase 1

The crypto library TOE assumes that the Smartcard 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 [10].

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 [10] are valid for this Security Target. They are listed in the table below:

Table 7. Security Objectives for the operational environment for Crypto Library V3.1.x on P6022y VB

Name	Title	Applies to phase
OE.Process-Sec-IC	Protection during composite product manufacturing	TOE delivery up to the end of phase 6
OE.Check-Init	Check of initialisation data by the Security Card Embedded Software	

4.4 Security Objectives Rationale

Section 4.4 of the Protection Profile provides a rationale how the assumptions, threats, and organisational security policies are addressed by the objectives that are subject of the PP [5]. The following table reproduces the table in section 4.4 of the PP [5].

Table 8. Security Objectives versus Assumptions, Threats or Policies , taken from PP

Assumption, Threat or OSP	Security Objective	Note
A.Resp-Appl	OE.Resp Appl	
P.Process-TOE	O.Identification	Phase 2 – 3
A.Process-Sec-IC	OE.Process Sec-IC	Phase 4 – 6
T.Leak-Inherent	O.Leak Inherent	
T.Phys-Probing	O.Phys Probing	
T.Malfunction	O.Malfunction	
T.Phys-Manipulation	O.Phys Manipulation	
T.Leak-Forced	O.Leak Forced	
T.Abuse-Func	O.Abuse Func	
T.RND	O.RND	

The justification for the additional security objectives for Crypto Library V3.1.x on P6022y VB are listed in the table below:

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

Table 9. Additional Security Objectives versus threats, assumptions or policies for Crypto Library V3.1.x on P6022y VB

Threat, Assumption/Policy	Security Objective	Note
T.Unauthorised-Access	O.FM_FW O.MEM_ACCESS O.SFR_ACCESS	
P.Crypto-Service	O.TDES, O.AES	
P.Add-Components-Plain	O.EEPROM_INTEGRITY O.CUST_RECONF_PLAIN O.PUF	
P.Add-Func	O.SW_AES O.SW_DES O.RSA O.RSA_PubExp O.RSA_KeyGen O.ECDSAO.ECC_DHKE O.ECC_KeyGen O.ECC_Add O.SHA O.RND O.REUSE O.Copy O.Compare O.ModMultiply O.ModAddSub	
A.Check-Init-Plain	OE.Check-Init	(Phase 1) and (Phase 4 – 6)

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

T.Unauthorised-Access

According to security objectives O.FM_FW, O.MEM_ACCESS and O.SFR_ACCESS the TOE must enforce memory partitioning with address mapping and control of access to memories and Special Function Registers in Firmware Mode, System Mode and User Mode and must enforce a memory management scheme in User Mode so that access to memories and Special Function Registers is under control. Access rights in Firmware Mode and User Mode must be explicitly granted by Security IC Embedded Software running in System Mode. Thus, security violations caused by accidental or deliberate access to restricted data, code and shared hardware resources can be prevented. Threat T.Unauthorised-Access is therewith covered by these security objectives.

In addition, the definition of security objective OE.Resp-Appl in the PP [5] is further clarified in this Security Target. The clarification for OE.Resp-Appl makes clear that the Security IC Embedded Software must separate User Data of different applications and is not allowed to undermine the restrictions of the TOE. Therefore, this clarification contributes to coverage of threat T.Unauthorised-Access.

T.Malfunction

Since the objective provides the functionality to check the integrity of user data and TSF data during the transfer between different parts of the TOE the objective implements specific security functionality to detect the manipulation of user data or TSF data.
The detection of manipulated TSF data supports the prevention of malfunction due to modified security services of the TOE. Thereby the threat T.Malfunction is removed.
Therefore the threat is countered if the objective holds.

P.Crypto-Service

Since the objectives O.TDES and O.AES require the TOE to implement exactly the same specific security functionality as required by P.Crypto-Service, the organisational security policy is covered by the objectives.

P.Add-Components-Plain

Since the objectives O.EEPROM_INTEGRITY, O.CUST_RECONF_PLAIN, and

O.PUF require the TOE to implement exactly the same specific security functionality as required by P.Add-Components-Plain, the organisational security policy is covered by the objectives.

Nevertheless 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-Components-Plain. These security objectives are also valid for the additional specific security functionality since they must avert the related threats also for the components added related to the policy.

P.Add-Func

Since the objectives O.SW_AES, O.SW_DES, O.RSA, O.RSA_PubExp, O.RSA_KeyGen, O.ECDSA, O.ECC_DHKE, O.ECC_KeyGen, O.ECC_Add, O.SHA, O.RND, O.Copy, O.Compare, O.ModMultiply, O.ModAddSubt and O.REUSE require the TOE to implement exactly the same specific security functionality as required by P.Add-Func, the organizational security policy P.Add-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-Func and therefore support P.Add-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.

A.Check-Init-Plain

Security objective OE.Check-Init requires the Security IC Embedded Software to implement a function assumed in assumption A.Check-Init-Plain, so that the assumption is covered by the security objective.

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

To define the IT security functional requirements of the TOE an additional component of the family FDP_ITT (User data protection, internal TOE transfer) is defined in Hardware ST [10] and an additional family (FDP_SOP) of the Class FDP (user data protection) is defined here. This family describes the functional requirements for basic operations on data in the TOE.

Note that the PP “Security IC Platform Protection Profile [5] also defines extended security functional requirements in chapter 5, which are included in this Security Target.

As defined in CC Part 2, FDP class addresses user data protection. Secure basic operations (FDP_SOP) address protection of user data when it is processed by Copy or Compare function, respectively. Therefore, it is judged that FDP class is suitable for FDP_SOP family.

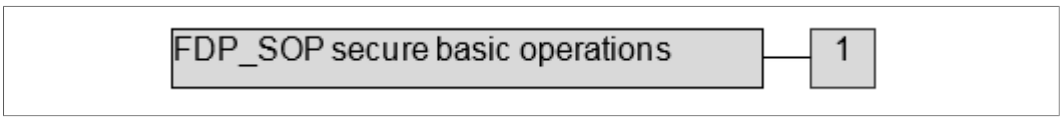
The reason for adding an extra family to FDP class is that existing families do not address protection of user data against all relevant attacks. In particular, FDP_IFC and FDP_ITT (as well as FPT_ITT) are associated with protection against side-channel attacks.

5.1 Secure basic operations (FDP_SOP)

Family Behaviour

This family defines requirements for the TOE to perform basic operations on data, which could be user data but also key data.

Component levelling



FDP_SOP.1 Requires the TOE to provide the possibility to perform basic secure operations on data

Management: FDP_SOP.1

There are no management activities foreseen.

Audit: FDP_SOP.1

There are no actions defined to be auditable.

FDP_SOP.1 Secure basic operations

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_SOP.1.1 The TSF shall provide a [selection: Copy, Compare, ModMultiply, ModAddSub] function on data [Selection: from source [assignment: list of objects] to destination [assignment: list of objects], residing in [assignment: list of objects].

Application note: The different memories, are seen as possible objects

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 (P6022y VB) vs. this Security Target (Crypto Library V3.1.x on P6022y VB), the TOE SFRs are presented in the following sections.

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

The Security Functional Requirements (SFRs) for this TOE (Crypto Library V3.1.x on P6022y VB) are specified based on the Smart Card IC Platform Protection Profile [5], and are defined in the Common Criteria or in the Protection Profile, as is shown by the third column of the following table:

Table 10. SFRs defined in the Protection Profile or the Common Criteria

SFR	Title	Defined in
FAU_SAS.1	Audit storage	PP Section 5.3 [5] (provided by chip HW)
FCS_RNG.1	Generation of random numbers	PP Section 5.1 [5] (provided by chip HW).
FDP_IFC.1	Subset information flow control	CC Part 2 [2] (provided by chip HW)
FDP_ITT.1	Basic internal transfer protection	CC Part 2 [2] (provided by chip HW)
FMT_LIM.1	Limited capabilities	PP Section 5.2 [5] (provided by chip HW)
FMT_LIM.2	Limited availability	PP Section 5.2 [5] (provided by chip HW)
FPT_FLS.1	Failure with preservation of secure state	CC Part 2 [2] (provided by chip HW)
FPT_ITT.1	Basic internal TSF data transfer protection	CC Part 2 [2] (provided by chip HW)
FPT_PHP.3	Resistance to physical attack	CC Part 2 [2] (provided by chip HW)
FRU_FLT.2	Limited fault tolerance	CC Part 2 [2] (provided by chip HW)
FDP_SDC.1	Stored data confidentiality	PP, Section 5.4 [5] (provided by chip HW)
FDP_SDI.2	Stored data integrity monitoring and action	CC, Part 2 [2] (provided by chip HW)
FCS_COP.1[TDES]	Cryptographic operation - TDES	PP, Section 7.4.1 [5] (provided by chip HW)
FCS_CKM.4[TDES]	Cryptographic key destruction - TDES	PP, Section 7.4.1 [5] (provided by chip HW)
FCS_COP.1[AES]	Cryptographic operation - AES	PP, Section 7.4.2 [5] (provided by chip HW)
FCS_CKM.4[AES]	Cryptographic key destruction	PP, Section 7.4.2 [5] (provided by chip HW)

Note 5. These requirements have already been stated in the hardware ST [10] and are fulfilled by the chip hardware, if not indicated otherwise in Table 10.

The TOE shall meet the requirements “Random number generation” as specified below.

The hardware part of the TOE (NXP SmartMX2 P6022y VB) provides a physical random number generator (RNG) that fulfils FCS_RNG.1 as already mentioned above in Table 10. The additional software part of the TOE (Crypto Library) implements a software (pseudo) RNG that fulfils FCS_RNG.1[HYB-DET] (see below). This software RNG obtains its seed from the hardware RNG, after the TOE (Crypto Library) has performed a self test of the hardware RNG.

FCS_RNG.1[HYB-DET]	**Random number generation**
Hierarchical to:	No other components.
FCS_RNG.1.1[HYB-DET]	The TSF shall provide a hybrid deterministic random number generator that implements: (K.4.1) a chi-squared test on the seed generator. (DRG.4.1) The internal state of the RNG shall use PTRNG of class PTG.2 (as defined in [7]) as random source. (DRG.4.2) The RNG provides forward secrecy (as defined in [7]). (DRG.4.3) The RNG provides backward secrecy even if the current internal state is known (as defined in [7]). (DRG.4.4) The RNG provides enhanced forward secrecy on demand (as defined in [7]). (DRG.4.5) The internal state of the RNG is seeded by an PTRNG of class PTG.2 (as defined in [7]).
FCS_RNG.1.2[HYB-DET]	The TSF shall provide random numbers that meet: (K.4.2) class K.4 of AIS20 [8]. (DRG.4.6) The RNG generates output for which 2^{48} strings of bit length 128 are mutually different with probability at least $1 – 2^{-24}$. (DRG.4.7) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A (as defined in [7]).
Application Notes:	(1) The security functionality is resistant against side channel analysis and similar techniques. (2) The Crypto Library V3.1.x on P6022y VB provides the smartcard embedded software with separate library calls to initialise the random number generator (which includes the chi-squared test) and to generate random data. The user can call an initialisation function upon use of the random number generator.
Dependencies:	No dependencies.

Note:	Only if the chi-squared test succeeds the hardware RNG seeds the software RNG implemented as part of the Crypto Library on SmartMX2 (as part of security functionality SS.SW_RNG).
Note:	The Crypto Library does not prevent the operating system from accessing the hardware RNG. If the hardware RNG is used by the operating system directly, it has to be decided based on the Smartcard Embedded Software's security needs, what kind of test has to be performed and what requirements will have to be applied for this test. In this case the developer of the Smartcard Embedded Software must ensure that the conditions prescribed in the Guidance, Delivery and Operation Manual for the NXP SmartMX2 Secure Smart Card Controller P6022y VB are met.

The software (pseudo) RNG, which is implemented in the software part of the TOE (Crypto Library), fulfils FCS_RNG.1[HYB-PHY] (see below) with a certain limitation. This limitation can be given by the Smartcard Embedded Software. For details on the limitation please refer the user guidance documentation of the Crypto Library [11].

FCS_RNG.1[HYB-PHY]	**Random number generation**
Hierarchical to:	No other components.
FCS_RNG.1.1[HYB-PHY]	The TSF shall provide a hybrid physical random number generator that implements: (PTG.3.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure has been detected no random numbers will be output. (PTG.3.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source. (PTG.3.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG is started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test and the seeding of the DRG.3 postprocessing algorithm have been finished successfully or when a defect has been detected. (PTG.3.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon. (PTG.3.5) The online test procedure checks the raw random number sequence. It is triggered continuously. The online test is suitable for detecting nontolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.

	(PTG.3.6) The algorithmic post-processing algorithm belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function, and the output data rate of the post-processing algorithm shall not exceed its input data rate.
FCS_RNG.1.2[HYB-PHY]	The TSF shall provide random numbers that meet: (PTG.3.7) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A (as defined in [7]). (PTG.3.8) The internal random numbers shall use PTRNG of class PTG.2 as random source for the post-processing.
Dependencies:	No dependencies.

The SFRs for Crypto Library V3.1.x on P6022y VB include the SFRs from Table 10, the SFR FCS_RNG.1[HYB-DET], FCS_RNG.1[HYB-PHY], and the additional SFRs listed in Table 11.

The additional SFRs shown in Table 11 are defined in the Common Criteria, described in sections 6.1.1.3 “Additional SFRs regarding cryptographic functionality” and 6.1.1.4 “Additional SFRs regarding access control”, and 6.1.1.2 “Additional SFR defined in Extended Components Definition” of the Hardware Security Target [10].

Table 11. SFRs defined in the Hardware Security Target for Crypto Library V3.1.x on P6022y VB

Name	Title	Defined in
FCS_CKM.1[PUF]	Cryptographic key generation	CC Part 2 [2], and added to PP in the Hardware [10] section 6.1.1.3 “Additional SFRs regarding cryptographic functionality”.
FCS_CKM.4[PUF]	Cryptographic key destruction	CC Part 2 [2], and added to PP in the Hardware [10] section 6.1.1.3 “Additional SFRs regarding cryptographic functionality”.
FCS_COP.1[PUF_AES]	Cryptographic operation	CC Part 2 [2], and added to PP in the Hardware [10] section 6.1.1.3 “Additional SFRs regarding cryptographic functionality”.
FCS_COP.1[PUF_MAC]	Cryptographic operation	CC Part 2 [2], and added to PP in the Hardware [10] section 6.1.1.3 “Additional SFRs regarding cryptographic functionality”.
FDP_ACC.1[MEM]	Subset access control	CC Part 2 [2], and added to PP in the Hardware [10] section 6.1.1.4 “Additional SFRs regarding access control”.
FDP_ACC.1[SFR]	Subset access control	CC Part 2 [2], and added to PP in the Hardware [10] section 6.1.1.4 “Additional SFRs regarding access control”.
FDP_ACF.1[MEM]	Security attribute based access control	CC Part 2 [2], and added to PP in the Hardware [10] section 6.1.1.4 “Additional SFRs regarding access control”.”.
FDP_ACF.1[SFR]	Security attribute based access control	CC Part 2 [2], and added to PP in the Hardware [10] section 6.1.1.4 “Additional SFRs regarding access control”.”.
FMT_MSA.3[MEM]	Static attribute initialization	CC Part 2 [2], and added to PP in the Hardware [10] section 6.1.1.4 “Additional SFRs regarding access control”.

Table 11. SFRs defined in the Hardware Security Target for Crypto Library V3.1.x on P6022y VB*...continued*

Name	Title	Defined in
FMT_MSA.3[SFR]	Static attribute initialization	CC Part 2 [2], and added to PP in the Hardware ST [10]section 6.1.1.4 “Additional SFRs regarding access control”.
FMT_MSA.1[MEM]	Management of security attributes	CC Part 2 [2], and added to PP in the Hardware [10] section 6.1.1.4 “Additional SFRs regarding access control”.
FMT_MSA.1[SFR]	Management of security attributes	CC Part 2 [2], and added to PP in the Hardware [10] section 6.1.1.4 “Additional SFRs regarding access control”.
FMT_SMF.1[HW]	Specification of management functions	CC Part 2 [2], and added to PP in the Hardware [10] section 6.1.1.4 “Additional SFRs regarding access control”.

Like the requirements already listed in Table 10, the requirements listed in Table 11 have already been stated in the Hardware Security Target [10] and are fulfilled by the chip hardware.

6.1.2 SFRs added by Crypto Library

The SFRs defined in the previous section are further supplemented by the additional SFRs described in the following subsections of this Security Target, as listed in Table 12. The SFRs described in Table 12 are new for the crypto library.

Table 12. SFRs defined in this Security Target

Name	Title	Defined in
FCS_COP.1[SW_AES]	Cryptographic operation - AES	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1[SW_DES]	Cryptographic operation - DES and TDES	CC Part 2 [2]; specified in this ST, see below.
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[ECC_Additional]	ECC point addition	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1[SHA]	Cryptographic operation (SHA-1[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.

Table 12. SFRs defined in this Security Target...*continued*

Name	Title	Defined in
FCS_CKM.4	Cryptographic Key Destruction	CC Part 2 [2]; specified in this ST, see below.
FDP_RIP.1	Subset Residual Information Protection	CC Part 2 [2]; specified in this ST, see below.

[1] Due to the AVA_VAN.5 requirement SHA-1 shall not be used.

The requirements listed in Table 12 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[SW_AES]	**Cryptographic operation - AES**
Hierarchical to:	No other components.
FCS_COP.1.1[SW_AES]	The TSF shall perform *decryption and encryption* [4] in accordance with a specified cryptographic algorithm AES in *ECB, CBC, CBC-MAC or CMAC* [5] and cryptographic key sizes *128, 192 or 256 bit* [6] that meet the following: *FIPS 197* [22], *NIST SP 800-38A* [26], *ISO 9797-1, Algorithm 1 (CBC-MAC mode)* [28], *and NIST SP 800-38B (CMAC mode)* [27] [7].
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [31].
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[SW_DES]	**Cryptographic operation - DES and TDES**
Hierarchical to:	No other components.
FCS_COP.1.1[SW_DES]	The TSF shall perform *encryption and decryption* [8] in accordance with a specified cryptographic algorithm DES and Triple-DES in *ECB, CBC CBC-MAC or CMAC* [9] and cryptographic key sizes *1-key DES (56 bit), 2-key TDES (112 bit) or 3-key TDES (168 bit)* [10] that meet the following FIPS Publication 46-3 (DES and TDES) [24] and NIST Special Publication 800-38A, 2001 (ECB and CBC mode) [26], ISO 9797-1, Algorithm 1 (CBC-

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

	MAC mode) [28], and NIST Special Publication 800-38B (CMAC mode) [27] [11].
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [31]. To fend off attackers with high attack potential an adequate security level must be used (references can be found in national and international documents and standards). In particular this means that Single-DES shall not 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], FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1[RSA]	**Cryptographic operation**
Hierarchical to:	No other components.
FCS_COP.1.1[RSA]	The TSF shall perform encryption, decryption, signature and verification in accordance with the specified cryptographic algorithm RSA and cryptographic key sizes 512 bits to 4096 bits that meet the following: PKCS #1, v2.1: RSAEP, RSADP, RSASP1, RSAVP1.
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [31]. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).
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 in accordance with the specified cryptographic algorithm EME-OAEP and EMSA-PSS and cryptographic key sizes 512 bits to 4096 bits that meet the following: PKCS #1, v2.1: EME-OAEP and EMSA-PSS.
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [31]. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).
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_PubExp]	**Cryptographic operation**
Hierarchical to:	No other components.

11 [assignment: *list of standards*]

FCS_COP.1.1[RSA_PubExp]	The TSF shall perform public key computation in accordance with the specified cryptographic algorithm RSA and cryptographic key sizes 512 bits to 4096 bits that meet the following: PKCS #1, v2.1.
Application Notes:	(1) The security functionality is resistant against side channel analysis and other attacks described in [31]. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards). (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 in accordance with the specified cryptographic algorithm ECDSA / ECC over GF(p) and cryptographic key sizes 129 to 576 bits that meet the following:ISO/IEC 15946-2.
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [31]. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).
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[ECC_DHKE]	**Cryptographic operation**
Hierarchical to:	No other components.
FCS_COP.1.1[ECC_DHKE]	The TSF shall perform Diffie-Hellman Key Exchange in accordance with the specified cryptographic algorithm ECC over GF(p) and cryptographic key sizes 129 to 576 bits that meet the following: ISO/IEC 15946-3.
Application Notes:	(1) The security functionality is resistant against side channel analysis and other attacks described in [31]. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards). (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.
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[ECC_Additional]	**Cryptographic operation**
Hierarchical to:	No other components.
FCS_COP.1.1[ECC_Additional]	The TSF shall perform a full point addition in accordance with the specified cryptographic algorithm ECC over GF(p) and cryptographic key sizes 129 to 576 bits that meet the following: ISO/IEC 15946-1.
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [31]. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).
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 in accordance with the specified cryptographic algorithm SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 and cryptographic key size none that meet the following: FIPS 180-4.
Application Notes:	1) The security functionality is resistant against side channel analysis and timing attacks as described in [31]. To fend off attackers with high attack potential an adequate security level must be used (references can be found in national and international documents and standards). In particular this means that SHA-1 shall not be used. (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 and specified cryptographic key sizes 512-4096 bits that meet the following: PKCS #1, v2.1 and "Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), German “Bundesanzeiger Nr. 85“, p. 2034, June 7th, 2011".
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [31]. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
Note:	The standard “Geeignete Algorithmen” sets up requirements for RSA key generation, if the generated RSA key pair is used in a signature application according to the German Signature Act. This standard is also accepted by the German Bundesamt für Sicherheit in der Informationstechnik (BSI) for Common Criteria evaluations that include the assurance requirements AVA_VAN.5 with high attack potential.
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)) and specified cryptographic key sizes 129 to 576 bits that meet the following: ISO/IEC 15946-1 and “Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), German “Bundesanzeiger Nr. 85“, p. 2034, June 7th, 2011” [30].
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [31]. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

Note:	The standard “Geeignete Algorithmen” sets up requirements for ECDSA key generation, if the generated ECDSA key pair is used in a signature application according to the German Signature Act. This standard is also accepted by the German Bundesamt für Sicherheit in der Informationstechnik (BSI) for Common Criteria evaluations that include the assurance requirements AVA_VAN.5 with high attack potential.
FDP_RIP.1	**Subset Residual Information Protection**
Hierarchical to:	No other components.

This family addresses the need to ensure that information in a resource is no longer accessible when the resource is deallocated, and that therefore newly created objects do not contain information that was accidentally left behind in the resources used to create the objects. The following Functional Requirement to the TOE can be derived from the CC component FDP_RIP.1:

FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from the following objects: all objects (variables) used by the Crypto Library as specified in the user guidance documentation.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

Note 6. The TSF ensures that, upon exit from each function, with the exception of input parameters, return values or locations where it is explicitly documented that values remain at specific addresses, any memory resources used by that function that contained temporary or secret values are cleared

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 that meets the following: ISO11568
Application Notes:	The Crypto Library V3.1.x on P6022y VB 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 P6022y VB. 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 V3.1.x on P6022y VB is the responsibility of the smartcard embedded software.

6.1.3 Extended TOE security functional requirements

The SFRs from the previous sections are further supplemented by four iterations of an extended SFR introduced in the following subsections of this Security Target, as listed in Table 13.

Table 13. SFRs defined in this Security Target

Name	Title	Defined in
FDP_SOP.1[Copy]	Secure basic operations (secure copy)	Specified in this ST, see below.
FDP_SOP.1[Compare]	Secure basic operations (secure compare)	Specified in this ST, see below.
FDP_SOP.1[ModMultiply]	Secure basic operations (secure modular multiply)	Specified in this ST, see below.
FDP_SOP.1[ModAddSub]	Secure basic operations (secure modular add and subtract)	Specified in this ST, see below.

The FDP_SOP.1 (secure basic operations) is introduced as a new component within a new family FDP_SOP consisting only of that new component

FDP_SOP.1[Copy]	**Secure Basic Operations**
Hierarchical to:	No other components.
FDP_SOP.1.1[Copy]	The TSF shall provide a Copy function on data from source ROM, RAM and EEPROM to destination RAM.
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [31].

FDP_SOP.1[Compare]	**Secure Basic Operations**
Hierarchical to:	No other components.
FDP_SOP.1.1[Compare]	The TSF shall provide a Compare function on data residing in ROM, RAM and EEPROM.
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [31].

FDP_SOP.1[ModMultiply]	**Secure Basic Operations**
Hierarchical to:	No other components.
FDP_SOP.1.1[ModMultiply]	The TSF shall provide a Modular Multiply function on data residing in ROM, RAM and EEPROM.
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [31].

FDP_SOP.1[ModAddSub]	**Secure Basic Operations**
Hierarchical to:	No other components.
FDP_SOP.1.1[ModAddSub]	The TSF shall provide a Modular Add and Subtract function on data residing in ROM, RAM and EEPROM.
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [31].

6.2 Security Assurance Requirements

Table 14 below lists all security assurance components that are valid for the TOE. These security assurance components are required by EAL6 or by the Protection Profile [5]. Augmentations by the Security Target are marked with ST.

Table 14. Security Assurance Requirements EAL6+ and PP augmentations

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

Table 14. Security Assurance Requirements EAL6+ and PP augmentations...*continued*

SAR	Title	Required by
ATE_IND.2	Independent testing - sample	PP / EAL6
AVA_VAN.5	Advanced methodical vulnerability analysis	PP / EAL6

6.2.1 Refinements of the Security Assurance Requirements for EAL6+

The ST 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 [10] has chosen the evaluation assurance level EAL6+. This Hardware Security Target bases 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] provides a rationale for the mapping between security functional requirements and security objectives defined in the Protection Profile. The mapping is reproduced in the following table.

Table 15. Mapping of Security Requirements to Security Objectives in the PP

Objective	TOE Security Functional Requirements
O.Leak Inherent	FDP_ITT.1 “Basic internal transfer protection” FPT_ITT.1 “Basic internal TSF data transfer protection” FDP_IFC.1 “Subset information flow control”
O.Phys Probing	FDP_SDC.1 “Stored data confidentiality” FPT_PHP.3 “Resistance to physical attack”
O.Malfunction	FRU_FLT.2 “Limited fault tolerance FPT_FLS.1 “Failure with preservation of secure state”
O.Phys Manipulation	FDP_SDI.2 “Stored data integrity monitoring and action” FPT_PHP.3 “Resistance to physical attack”
O.Leak Forced	All requirements listed for O.Leak Inherent FDP_ITT.1, FPT_ITT.1, FDP_IFC.1 plus those listed for O.Malfunction and O.Phys Manipulation FRU_FLT.2, FPT_FLS.1, FPT_PHP.3
O.Abuse Func	FMT_LIM.1 “Limited capabilities” FMT_LIM.2 “Limited availability” plus those for O.Leak Inherent, O.Phys Probing, O.Malfunction, O.Phys Manipulation, O.Leak Forced FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1
O.Identification	FAU_SAS.1 “Audit storage”
O.RND	FCS_RNG.1 “Quality metric for random numbers” for the hardware RNG plus those for O.Leak Inherent, O.Phys Probing, O.Malfunction, O.Phys Manipulation, O.Leak Forced FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1 plus: see [12] (for aspects concerning the software RNG)

Note 7. O.RND has been extended if compared to the PP [5] to include also a software RNG (see also Note 3). The rationale given in the PP only covers the part of O.RND dealing with the hardware RNG. For O.RND additional functionality (software RNG) and additional requirements (FCS_RNG.1[HYB-DET], and FCS_RNG.1[HYB-PHY]) have been added. The explanation following Table 17 describe this in more detail.

The Hardware Security Target [10] lists a number of security objectives and SFRs that are additional to the Security Objectives and SFRs in the Protection Profile. These are listed in the following table.

Table 16. Mapping of SFRs to Security Objectives in the Hardware ST

Objective	TOE Security Functional Requirements
O.TDES	FCS_COP.1[TDES], FCS_CKM.4[TDES]
O.AES	FCS_COP.1[AES], FCS_CKM.4[AES]
O.FM_FW	FDP_ACC.1[MEM] FDP_ACF.1[MEM] FMT_MSA.3[MEM]
O.MEM_ACCESS	FDP_ACC.1[MEM] FDP_ACF.1[MEM] FMT_MSA.3[MEM] FMT_MSA.1[MEM] FMT_MSA.1[SFR] FMT_SMF.1[HW]
O.SFR_ACCESS	FDP_ACC.1[SFR] FDP_ACF.1[SFR] FMT_MSA.3[SFR] FMT_MSA.1[SFR] FMT_SMF.1[HW]
O.CUST_RECONF_PLAIN	FMT_SMF.1[HW]
O.EEPROM_INTEGRITY	FDP_SDI.2[HW]
O.PUF	FCS_CKM.1[PUF], FCS_CKM.4[PUF], FCS_COP.1[PUF_AES], FCS_COP.1[PUF_MAC]

The rationales for the mappings in Table 16 may be found in the Hardware ST [10].

Finally, this ST lists a number of security objectives and SFRs additional to both the PP and the Hardware ST. These are listed in the following table.

Table 17. Mapping of SFRs to Security Objectives in this ST

Objective	TOE Security Functional Requirements
O.SW_AES	FCS_COP.1[SW AES] ADV.ARC.1 (and underlying platform SFRs)
O.SW_DES	FCS_COP.1[SW DES] ADV.ARC.1 (and underlying platform SFRs)
O.RSA	FCS_COP.1[RSA] FCS_COP.1[RSA_Pad] ADV.ARC.1 (and underlying platform SFRs)
O.RSA_PubExp	FCS_COP.1[RSA_PubExp] ADV.ARC.1 (and underlying platform SFRs)
O.RSA_KeyGen	FCS_CKM.1[RSA] ADV.ARC.1 (and underlying platform SFRs)
O.ECDSA	FCS_COP.1[ECDSA] ADV.ARC.1 (and underlying platform SFRs)
O.ECC_DHKE	FCS_COP.1[ECC_DHKE] ADV.ARC.1 (and underlying platform SFRs)
O.ECC_Add	FCS_COP.1[ECC_Additional] ADV.ARC.1 (and underlying platform SFRs)
O.ECC_KeyGen	FCS_CKM.1[ECC] ADV.ARC.1 (and underlying platform SFRs)
O.SHA	FCS_COP.1[SHA] ADV.ARC.1 (and underlying platform SFRs)
O.Copy	FDP_SOP.1[Copy] ADV.ARC.1 (and underlying platform SFRs)
O.REUSE	FDP_RIP.1 FCS_CKM.4
O.Compare	FDP_SOP.1[Compare] ADV.ARC.1 (and underlying platform SFRs)
O.ModMultiply	FDP_SOP.1[ModMultiply] ADV.ARC.1 (and underlying platform SFRs)
O.ModAddSub	FDP_SOP.1[ModAddSub] ADV.ARC.1 (and underlying platform SFRs)

Table 17. Mapping of SFRs to Security Objectives in this ST*...continued*

Objective	TOE Security Functional Requirements
O.RND	FCS_RNG.1[HYB-DET] FCS_RNG.1[HYB-PHY] ADV.ARC.1 (and underlying platform SFRs)
OE.Resp Appl	Not applicable
OE.Process-Sec-IC	Not applicable

The justification of the security objectives O.SW_AES, O.SW_DES, O.RSA, O.RSA_PubExp, O.RSA_KeyGen, O.ECDSA, O.ECC_DHKE, O.ECC_Add, O.ECC_KeyGen, O.SHA, O.COPY, O.COMPARE, O.ModMultiply, and O.ModAddSub 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 objective:
  - ADV.ARC.1 (and underlying platform SFRs) 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.
  - ADV.ARC.1 (and underlying platform SFRs) ensures 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.
- ADV.ARC.1 (and underlying platform SFRs) by ensuring that User Data and TSF Data are not accessible from the TOE except when the Smartcard Embedded Software decides to communicate them via an external interface.

The justification of the security objective O.REUSE is as follows:

- O.REUSE requires the TOE to provide procedural measures to prevent disclosure of memory contents that was used by the TOE. This applies to the Crypto Library V3.1.x on P6022y VB and is met by the SFR FDP_RIP.1 and FCS_CKM.4, which requires the library to make unavailable all memory contents that has been used by it. Note that the requirement for residual information protection applies to all functionality of the Cryptographic Library.

The justification of the security objective O.RND is as follows:

- O.RND requires the TOE to generate random numbers with (a) ensured cryptographic quality (i.e. not predictable and with sufficient entropy) such that (b) information about the generated random numbers is not available to an attacker.
  1. Ensured cryptographic quality (sufficient entropy part) of generated random numbers is met by FCS_RNG.1.1[HYB-DET] through the characteristic 'hybrid deterministic', by FCS_RNG.1.1[HYB-PHY] through the characteristic 'hybrid physical', and by the random number generator meeting NIST SP 800-90A. Ensured cryptographic quality (not predictable part) of generated random numbers is met by FCS_RNG.1[HYB-DET] through the characteristic 'chi-squared test of the seed generator', by FCS_RNG.1[HYB-PHY] through the characteristic

'cryptographic post-processing algorithm', and FCS_RNG.1 from the certified hardware platform.

2. Information about the generated random numbers is not available to an attacker is met through ADV.ARC.1, which prevent physical manipulation and malfunction of the TOE and support this objective because they prevent attackers from manipulating or otherwise affecting the random number generator.

6.3.2 Extended requirements

This Security Target does define extended requirements, because there are no existing SFRs available that cover the claimed functionality. The PP [5] contains extended functional requirements, which are explained in the rationale of the PP (see [5], section 5).

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[SW_AES], FCS_COP.1[SW_DES] and 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 Smartcard 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 the TOE is generally based on EAL6, the underlying Protection Profile [5], and the Security Target of the hardware [10] of the TOE.

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 (cryptographic 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 [10]).

The security functionality of the hardware platform is listed in the following table;

Table 18. IT security functionalities defined in the Hardware Security Target

Name	Title
SS.RNG	Random Number Generator
SS.TDES	Triple-DES coprocessor
SS.AES	AES coprocessor
SS.RECONFIG	Post Delivery Configuration
SF.OPC	Control of Operating Conditions
SF.PHY	Protection against Physical Manipulation
SF.LOG	Logical Protection
SF.COMP	Protection of Mode Control
SF.MEM_ACC	Memory Access Control
SF.SFR_ACC	Special Function Register Access Control
SF.FFW	Firmware Firewall
SF.FIRMWARE	Firmware Support
SF.PUF	User Data Protection using PUF

Note 8. The security functionality SS.RNG implements the hardware RNG. The TOE also implements software RNG as part of security functionality SS.SW_RNG; for details see Section 7.1.1.12. The hardware RNG is not externally visible through the interfaces of the Crypto Library; instead users of the Crypto Library are intended to use the software RNG (SS.SW_RNG).

Note 9. The security functionality SF.LOG is extended by the crypto library TOE as described in Section 7.1.2.

Note 10. The following TSF are not used by the Crypto Library:

- SF.COMP (no special mode required)
- SF.MEM_ACC (only access to own code and workspace needed, no further assumptions about memory access are made)
- SF.SFR_ACC (only access to used SFRs needed, no further assumptions about SFR access are made)
- SF.FFW (no firmware used)
- SF.FIRMWARE (no firmware used)
- SS.RECONFIG (no reconfiguration possible when Crypto Library runs)

The additional security functionality provided by the cryptographic library 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.SW_AES

.

The TOE uses the SmartMX2 AES hardware coprocessor to provide AES encryption and decryption facility using 128, 192 or 256 bit keys.

The TOE implements two library versions for the AES (phSmx2ClAes library and part of phSmx2ClSymCfg library) with different security configurations.

The supported modes are ECB, “outer” CBC and CMAC (i.e. the CBC mode applied to the block cipher algorithm AES).

In addition, the TOE provides the ability to compute a CBC-MAC. The CBC-MAC mode of operation is rather similar to the CBC mode of operation, but returns only the last cipher text (see also [28], Algorithm 1)

SS.SW_AES is a basic cryptographic function which provides the AES algorithm as defined by the standard [22].

The interface to SS.SW_AES allows AES operations independent from prior key loading. The user has to take care that adequate keys of the correct size are loaded before the cryptographic operation is performed. Details are described in the user guidance [11] and the user manual [14].

Attack resistance for this security functionality is discussed in Section 7.2.

This security functionality covers:

- FCS_COP.1[SW_AES]

7.1.1.2 SS.SW_DES

.

The TOE uses the SmartMX2 Triple-DES hardware coprocessor to provide a DES encryption and decryption facility using 56-bit keys, and to provide Triple-DES encryption and decryption. The Triple-DES function uses double-length or triple-length keys with sizes of 112 or 168 bits respectively.

The TOE implements two library versions for the DES (phSmx2ClDes library and part of phSmx2ClSymCfg library) with different security configurations.

The supported modes are ECB, CBC and CMAC (i.e. the CBC mode applied to the block cipher algorithm 3DES or DES).

In addition, the TOE provides the ability to compute a CBC-MAC. The CBC-MAC mode of operation is rather similar to the CBC mode of operation, but returns only the last cipher text (see also [28], Algorithm 1, or [25], Appendix F). Like ECB and CBC, the CBC-MAC mode of operation can also be applied to both DES and 3DES as underlying block cipher algorithm.

To fend off attackers with high attack potential an adequate security level must be used (references can be found in national and international documents and standards). In particular this means that Single-DES shall not be used.

SS.SW_DES is a modular basic cryptographic function which provides the DES and Triple-DES algorithm (with two and three keys) as defined by the standard [24]

The interface to SS.SW_DES allows performing Single-DES or 2-key and 3-key Triple-DES operations independent from prior key loading. The user has to take care that adequate keys of the correct size are loaded before the cryptographic operation is performed. Details are described in the user manual [13]. All modes of operation (ECB, CBC, CBC MAC) can be applied to DES, two-key 3DES and three-key 3DES for a total of nine possible combinations.

Attack resistance for this security functionality is discussed in Section 7.2.

This security functionality covers:

- FCS_COP.1[SW_DES]

7.1.1.3 SS.RSA

.

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

This routine supports various key lengths from 512 bits to 4096 bits. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

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 Section 7.2.

This security functionality covers:

- FCS_COP.1[RSA]

7.1.1.4 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, v2.1 (EME-OAEP, EMSA-PSS)

This routine supports various key lengths from 512 bits to 4096 bits. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

Attack resistance for this security functionality is discussed in Section 7.2.

This security functionality covers:

- FCS_COP.1[RSA_PAD]

7.1.1.5 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, v2.1.

This routine supports various key lengths from 512 bits to 4096 bits (CRT). To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

Attack resistance for this security functionality is discussed in Section 7.2.

This security functionality covers:

- FCS_COP.1[RSA_PubExp]

7.1.1.6 SS.ECDSA

.

The TOE provides functions to perform ECDSA Signature Generation and Signature Verification according to ISO/IEC 15946-2.

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 is 129 to 576 bits for signature generation and 129 to 576 bits for signature verification. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

Attack resistance for this security functionality is discussed in Section 7.2.

This security functionality covers:

- FCS_COP.1[ECDSA]

7.1.1.7 SS.ECC_DHKE

.

The TOE provides functions to perform Diffie-Hellman Key Exchange according to ISO/IEC 15946-3.

The supported key length is 129 to 576 bits. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

Attack resistance for this security functionality is discussed in Section 7.2.

This security functionality covers:

- FCS_COP.1[ECC_DHKE]

7.1.1.8 SS.ECC_Additional

.

The TOE provides functionality to perform a full ECC point addition according to ISO/IEC 15946-1.

The supported key length is 129 to 576 bits. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

Attack resistance for this security functionality is discussed in Section 7.2.

This security functionality covers:

- FCS_COP.1[ECC_Additional]

7.1.1.9 SS.RSA_KeyGen

.

The TOE provides functions to generate RSA key pairs as described in PKCS #1, v2.1 and „Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), German “Bundesanzeiger Nr. 85“, p. 2034, June 7th, 2011“.

It supports various key lengths from 512 bits to 4096 bits. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

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).

Attach resistance for this security functionality is discussed in Section 7.2.

This security functionality covers:

- FCS_CKM.1[RSA]

7.1.1.10 SS.ECC_KeyGen

.

The TOE provides functions to perform ECC over GF(p) Key Generation according to ISO/IEC 15946-1 section 6.1 and “Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), German “Bundesanzeiger Nr. 85“, p. 2034, June 7th, 2011”

It supports key length from 129 to 576 bits. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

Attack resistance for this security functionality is discussed in Section 7.2.

This security functionality covers:

- FCS_CKM.1[ECC]

7.1.1.11 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 [23].

To fend off attackers with high attack potential an adequate security level must be used (references can be found in national and international documents and standards). In particular this means that SHA-1 shall not be used.

This security functionality covers:

- FCS_COP.1[SHA]

7.1.1.12 SS.SW_RNG

.

The TOE contains both a hardware Random Number Generator (RNG) and a software RNG; for the hardware RNG (SS.RNG) see the Note 8. SS.SW_RNG consists of the implementation of the software RNG and of appropriate online tests for the hardware RNG (as required for FCS_RNG.1[HYB-DET] and FCS_RNG.1[HYB-PHY] taken from the Protection Profile [5] and the proposal for AIS20/31 [7]):

The Crypto Library implements a software (pseudo) RNG that can be used as a general purpose random source. This software RNG has to be seeded by random numbers taken from the hardware RNG implemented in the SmartMX2 processor. The implementation of the software RNG is based on the standard NIST SP 800-90A as described in [29].

In addition, the Crypto Library implements appropriate online tests according to the Hardware User Guidance Manual [9] for the hardware RNG, which fulfils the functionality class P2 defined by the AIS31 [6] and class PTG.2 defined by the proposal for AIS20/31 [7], as required by SFR FCS_RNG.1[HYB-DET] and SFR FCS_RNG.1[HYB-PHY]. The interface of SS.SW_RNG allows to test the hardware RNG and to seed the software RNG after successful testing.

This security functionality covers:

- FCS_RNG.1[HYB-DET]
- FCS_RNG.1[HYB-PHY]

7.1.1.13 SS.COPY

.

The security service SS.COPY implements functionality to copy memory content in a secure manner protected against attacks.

This resistance against attacks is described in Section 7.2.

This security functionality covers:

- FDP_SOP.1[Copy]

7.1.1.14 SS.COMPARE

.

The security service SS.COMPARE implements functionality to compare different blocks of memory content in a manner protected against attacks.

This resistance against attacks is described in Section 7.2.

This security functionality covers:

- FDP_SOP.1[Compare]

7.1.1.15 SS.ModMultiply

.

The security service SS.ModMultiply implements functionality to modular multiply different blocks of memory content in a manner protected against attacks.

This resistance against attacks is described in Section 7.2.

This security functionality covers:

- FDP_SOP.1[ModMultiply]

7.1.1.16 SS.ModAddSub

.

The security service SS.ModAddSub implements functionality to modular add and subtract different blocks of memory content in a manner protected against attacks.

This resistance against attacks is described in Section 7.2.

This security functionality covers:

- FDP_SOP.1[ModAddSub]

7.1.2 Security Functions

7.1.2.1 SF.Object_Reuse

.

The TOE provides internal security measures which clear memory areas used by the Crypto Library after usage. This functionality is required by the security functional component FDP_RIP.1 taken from the Common Criteria Part 2 [2].

These measures ensure that a subsequent process may not gain access to cryptographic assets stored temporarily in memory used by the TOE.

This security functionality covers:

- FDP_RIP.1
- FCS_CKM.4

7.2 Security architectural information

Since this Security Target claims the assurance requirement ASE_TSS.2 security architectural information on a very high level is supposed to be included in the TSS to inform potential customers on how the TOE protects itself against interference, logical tampering and bypass. In the security architecture context, this covers the aspects selfprotection and non-bypassability.

SF.COMP

The protection of mode control is completely covered by the underlying hardware platform [10]

SF.LOG

The logical protection relates to the SFRs FDP_ITT.1, FPT_ITT.1 and FDP_IFC.1. The underlying hardware platform contains a number of hardware countermeasures, and for details is referred to the Security Target of the hardware platform [10].

For AES, the resistance against SPA, DPA and timing attacks is provided by the co-processors in the hardware part of the TOE. In addition, the TOE implements two library versions for the AES algorithm (phSmx2ClAes library and part of phSmx2ClSymCfg library) with different security configurations. For more details on those different configurations please refer the user guidance documentation of the Crypto Library [11].

For DES, the resistance against SPA, DPA and timing attacks is provided by the Triple-DES co-processor (which supports single DES and Triple-DES operations) in the hardware part of the TOE. In addition, the TOE implements two library versions for the DES algorithm (phSmx2ClDes library and part of phSmx2ClSymCfg library) with different security configurations. For more details on those different configurations please refer the user guidance documentation of the Crypto Library [11].

The TOE adds a number of countermeasures to protect RSA calculations, secure exponentiation, and RSA key generation, modulus and exponent blinding is used. Furthermore, are timing attacks prevented using careful coding and timing resistance of the underlying co-processor.

For all ECC related calculations, randomized projective coordinates are used. Timing attacks are prevented using careful coding and timing resistance of the underlying co-processor.

For the key generation algorithms, there is no interface available to force the key generation to repeat the previous calculation with the same parameters.

For RSA also the number of times that the key generation and public key computation can be performed is limited.

For the secure compare and secure copy function measures randomizing the program flow are implemented.

For the secure modular multiply and secure add and subtract function blinding on the data is performed.

SF.OPC

The control of operation conditions relates to the security requirements FRU_FLT.2 and FPT_FLS.1. The underlying hardware platform contains a number of hardware countermeasures. For the details is referred to the Security Target of the hardware platform [10]

The TOE implements a number of software sensors that detect DFA attacks on AES, DES, RSA and ECC. Also software sensors are implemented to detect perturbation attacks in the secure copy, the secure compare, the secure modular multiply, and the secure modular add and subtract functions.

SF.PHY

Protection against physical manipulation and probing is completely covered by the underlying hardware platform [10].

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.
Boot Mode	CPU mode of the TOE dedicated to the start-up of the TOE after every reset. This mode is not accessible for the Smartcard Embedded Software.
Composite Product Integrator	Role installing or finalizing the 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 Embedded Software delivered by the Security IC Embedded Software Developer before TOE delivery (e.g. if the 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).
CPU mode	Mode in which the CPU operates. The TOE supports four modes, the Boot Mode, Test Mode, Firmware Mode

	andSystem Mode. The Smartcard Embedded Software can only run in System Mode. The other three modes (Boot, Test, and Firmware) are not accessible for the Smartcard Embedded Software.
DocStore	https://www.docstore.nxp.com/
End-consumer	User of the Composite Product in Phase 7.
Exception interrupts	Non-maskable interrupt of program execution starting from fixed (depending on exception source) addressees and enabling the System Mode. The source of exceptions are: hardware breakpoints, single fault injection detection, illegal instructions, stack overflow and unauthorised system calls.
FabKey Area	A memory area in the EEPROM that contains data that is programmed during testing by the IC Manufacturer. The amount of data and the type of information can be selected by the customer.
Firmware Mode	CPU mode of the TOE dedicated to execution of the Emulation Framework, MIFARE DESFire and MIFARE Plus Operating System, which is part of the Security IC Dedicated Support Software. This mode is not accessible for the Security IC Embedded Software.
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 EEPROM of the TOE.

Memory Management Unit	The MMU maps the virtual addresses used by the CPU into the physical addresses of RAM, ROM and EEPROM. This mapping is done based on memory partitioning. Memory partitioning is fixed.
MIFARE	Contact-less smart card interface standard, complying with ISO14443A.
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 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 Embedded Software, TSF data or user data associated with the smartcard product by security procedures of the smartcard product manufacturer, personaliser and other actors before delivery to the smartcard end-user depending on the smartcard life-cycle.
Special Function Registers	Registers used to access and configure the functions for the communication with an external interface device, the cryptographic co-processor for Triple-DES, the Fame2 co-processor for basic arithmetic functions to perform asymmetric cryptographic algorithms, the random numbers generator and chip configuration.
Security Row	Top-most 512 bytes of the EEPROM memory reserved for configuration purposes as well as dedicated memory area for the Smartcard Embedded Software to store life-cycle information about the TOE.

Super System Mode	This mode represents either the Boot Mode, Test Mode or Firmware Mode.
System Mode	The System Mode has unlimited access to the hardware resources (with respect to the memory partition). The Memory Management Unit can be configured in this mode.
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.
Test Mode	CPU mode for configuration of the TOE executing the IC Dedicated Test Software. The Test Mode is permanently and irreversible disabled after production testing. In the Test Mode specific Special Function Registers are accessible for test purposes.
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 Smartcard 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

[6] Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitaetsklassen und Evaluationsmethodologie fuer physikalische Zufallszahlengeneratoren, Version 2.1, 02.12.2011, Bundesamt fuer Sicherheit in der Informationstechnik

[7] A proposal for: Functionality classes for random number generators, Version 2.0, 18 September 2011

[8] Anwendungshinweise und Interpretationen zum Schema, AIS20: Funktionalitaetsklassen und Evaluationsmethodologie fuer deterministiche Zufallszahlengeneratoren, Version 3, 15.05.2013, Bundesamt fuer Sicherheit in der Informationstechnik

9 . 2 Developer documents

[9] Information on Guidance and Operation, NXP Secure Smart Card Controller P6022y VB, NXP Semiconductors

[10] Security Target, NXP Secure Smart Card Controller P6022y VB, NXP Semiconductors, Revision 2.8, 09 March 2021

[11] SmartMX2 Crypto Library V3.1.2: User Guidance – Crypto Library V3.1.2 on SmartMX2

[12] SmartMX2 Crypto Library V3: User Manual – Random Number Generator

[13] SmartMX2 Crypto Library V3: User Manual – DES

[14] SmartMX2 Crypto Library V3: User Manual – AES

[15] SmartMX2 Crypto Library V3: User Manual – SHA

[16] SmartMX2 Crypto Library V3: User Manual – SHA-512

[17] SmartMX2 Crypto Library V3: User Manual – RSA

[18] SmartMX2 Crypto Library V3: User Manual – RSA Key Generation

[19] SmartMX2 Crypto Library V3: User Manual – ECC over GF(p)

[20] SmartMX2 Crypto Library V3: User Manual – Utils

[21] SmartMX2 Crypto Library V3: User Manual – SymCfg

9 . 3 Other documents

[22] FIPS PUB 197 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, ADVANCED ENCRYPTION STANDARD (AES), National Institute of Standards and Technology, 2001 November 26

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

[24] FIPS PUB 46-3 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION DATA ENCRYPTION STANDARD (DES) Reaffirmed 1999 October 25

[25] FIPS PUB 81: DES modes of operation, Federal Information Processing Standards Publication, December 2nd, 1980, US Department of Commerce/National Institute of Standards and Technology

[26] NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques, December 2001, Morris Dworkin, National Institute of Standards and Technology

[27] NIST Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005, Morris Dworkin, National Institute of Standards and Technology

[28] ISO/IEC 9797-1: 2011 Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher

[29] NIST Special Publication 800-90A: Recommendation for Random Number Generation Using Deterministic Random Bit Generators, January 2012, Elaine Barker and John Kelsey, National Institute of Standards and Technology

[30] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), German “Bundesanzeiger Nr. 85“, p. 2034, June 7th, 2011

[31] JIL-ATT-SC: Attack Methods for Smartcards and. Similar Devices, Joint Interpretation Library, Version 1.5, February 2009

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: 12 December 2022
Document number: