Crypto Library V2.7 on P5CD145V0A, MSO / P5CC145V0A, MSO / P5CD128V0A, MSO / P5CC128V0A, MSO

Security Target Lite

Rev. 1.1 — 17 February 2011 **Evaluation documentation**

accepted **PUBLIC**

BSI-DSZ-CC-0750

Document information

Info	Content
Keywords	Security Target Lite, Crypto Library, P5CD145V0A, MSO / P5CC145V0A, MSO / P5CD128V0A, MSO / P5CC128V0A, MSO
Abstract	Security Target Lite for the Crypto Library V2.7 on P5CD145V0A, MSO / P5CC145V0A, MSO / P5CD128V0A, MSO / P5CC128V0A, MSO according to the Common Criteria for Information Technology Evaluation (CC) at Level EAL5 augmented. The Crypto Library is developed and provided by NXP Semiconductors, Business Unit Identification.

Revision history

Rev	Date	Description
0.9	16-Nov-2010	First version derived from Security Target
1.0	03-Feb-2011	- Added limitations for ECC curves to all related SFRs - Updated references
1.1	17-Feb-2011	- Corrected Table 7 - Updated all FCS_COP.1 and FCS_CKM.1 SFRs with respect to supported key lengths - FCS_COP.1.1 [ECC_ADD]: Rephrased Application Notes - FCS_COP.1.1 [ECC_DHKE] : Rephrased Application Notes - Updated used Common Criteria version

Contact information

For additional information, please visit: http://www.nxp.com

For sales office addresses, please send an email to: salesaddresses@nxp.com

Glossary

CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
CC	Common Criteria Version 3.1
CPU	Central Processing Unit
DEA	Data Encryption Algorithm.
DES	Data Encryption Standard.
DRNG	Deterministic Random Number Generator
EAL	Evaluation Assurance Level.
ECB	Electronic Code Book (a block cipher mode of operation)
ECC	Elliptic Curve Cryptography
IC	Integrated circuit.
IT	Information Technology.
MMU	Memory Management Unit
MX	Memory eXtension
n/a	not applicable
NDA	Non Disclosure Agreement.
PKC	Public Key Cryptography
PP	Protection Profile.
PSW(H)	Program Status Word (High byte)
SAR	Security Assurance Requirement.
SFR	as abbreviation of the CC term: Security Functional Requirement, as abbreviation of the technical term of the SmartMX-family: Special Function Register
SIM	Subscriber Identity Module.
ST	Security Target.
TOE	Target of Evaluation.
TRNG	True Random Number Generator
TSF	Part of the TOE that realises the security functionality
TSFI	TSF Interface, a means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF. .
UART	Universal Asynchronous Receiver and Transmitter.

1. ST Introduction

This chapter is divided into the following sections: “ST Identification”, “TOE overview”, “CC Conformance and Evaluation Assurance Level”, “TOE Description”and “Further Definitions and Explanations”.

1.1 ST Identification

This Security Target is for the Common Criteria evaluation of the “Crypto Library V2.7 on P5CD145V0A, MSO / P5CC145V0A, MSO / P5CD128V0A, MSO / P5CC128V0A, MSO” provided by NXP Semiconductors, Business Unit Identification.

For ease of reading during this Security Target the TOE is often called Crypto Library on SmartMX.

ST Identification: Crypto Library V2.7 on P5CD145V0A, MSO / P5CC145V0A, MSO / P5CD128V0A, MSO / P5CC128V0A, MSO, Rev. 1.1 - 17 February 2011

The TOE is a composite TOE, consisting of:

- The hardware “NXP SmartMX P5CD145V0A, MSO / P5CC145V0A, MSO / P5CD128V0A, MSO / P5CC128V0A, MSO Secure Smart Card Controller”, which is used as evaluated platform, and all its Major Configurations (see [10] for details):
  - P5CD145V0A, MSO
  - P5CC145V0A, MSO
  - P5CD128V0A, MSO
  - P5CC128V0A, MSO
- The “Crypto Library V2.7 on P5CD145V0A, MSO / P5CC145V0A, MSO / P5CD128V0A, MSO / P5CC128V0A, MSO”, which is built upon this platform.

This Security Target builds on the Hardware Security Target [10], which refers to the “NXP P5CD145V0A, MSO / P5CC145V0A, MSO / P5CD128V0A, MSO / P5CC128V0A, MSO Secure Smart Card Controller” provided by NXP Semiconductors, Business Unit Identification.

1.2 TOE overview

1.2.1 Introduction

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

The Crypto Library on SmartMX 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 the User ROM.

The NXP SmartMX smart card processor provides the computing platform and cryptographic support by means of co-processors for the Crypto Library on SmartMX.

The TOE provides the security functionality listed below in addition to the functionality described in the Hardware Security Target [10] for the hardware platform:

AES

- The AES algorithm is intended to provide encryption and decryption functionality.
- The following modes of operation are supported for AES: ECB, CBC, CBC-MAC.

DES/3DES

- The Single-DES algorithm can be used as a building block, e.g. to implement a Retail-MAC. However, the Single-DES algorithm alone is not considered to be resistant against attacks with a high attack potential, therefore Single-DES alone must not be used for encryption. See also Note 7 in section 4.1.1.
- The Triple-DES (3DES) algorithm is intended to provide encryption and decryption functionality.
- The following modes of operation are supported for DES and Triple-DES: ECB, CBC, CBC-MAC.

RSA

- The RSA algorithm can be used for encryption and decryption as well as for signature generation and signature verification.
- 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 key.

ECC over GF(p)

- The ECC over GF(p) algorithm can be used for signature generation and signature verification
- The ECC over GF(p) key generation algorithm can be used to generate ECC over GF(p) key pairs.
- The 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)

SHA

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

Resistance of cryptographic algorithms against side-channel attacks

The cryptographic algorithms (except SHA) are resistant against Side Channel Attacks, including Simple Power Analysis (SPA), Differential Power Analysis (DPA), Differential Fault Analysis (DFA) and timing attacks. More detail may be found in Table 7.

Random number generation

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

Other security functionality

- The TOE includes internal security measures for residual information protection.
- The TOE provides a secure copy 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.

1.2.2 Life-Cycle

The life cycle of the hardware platform as part of the TOE is described in section 1.4.4 “TOE Intended Usage” of the Hardware Security Target [10]. The delivery process or the hardware platform is independent from the Crypto Library on SmartMX.

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 for a definition of the Phases refer to section ‘1.2.3 TOE life cycle’ of the Protection Profile [9]) 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, Business Unit Identification; 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 on SmartMX. 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 [9] the TOE provides additional functionality which is not covered in the Protection Profile and the Hardware Security Target [10]. This additional functionality is added using the policy “P.Add-Func” (see section 2.4 of this Security Target).

1.3 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 3, July 2009, CCMB-2009-07-001, [1]
- **Common Criteria for Information Technology Security Evaluation** – Part 2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002, [2]
- **Common Criteria for Information Technology Security Evaluation** – Part 3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003, [3]

For the evaluation the following methodology will be used:

- **Common Criteria for Information Technology Security Evaluation** – Evaluation methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004, [4]

The chosen level of assurance is **EAL 5 augmented**.

The augmentations chosen are:

- ALC_DVS.2 and
- AVA_VAN.5.

This Security Target claims the following CC conformances:

- CC 3.1 Part 2 extended, Part 3 conformant, EAL 5 augmented
- Conformance to the Protection Profile "**Bundesamt für Sicherheit in der Informationstechnik (BSI):** Security IC Platform Protection Profile, Version 1.0, 15.06.2007; Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035", [9]

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 5 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]).

1.4 TOE Description

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

- The hardware part consists of the NXP P5CD145V0A, MSO / P5CC145V0A, MSO / P5CD128V0A, MSO / P5CC128V0A, MSO Secure Smart Card Controller with IC Dedicated Software stored in the Test-ROM that is not accessible in the System Mode or the User Mode after Phase 3. The hardware part of the TOE includes dedicated guidance documentation.
- The software part consists of the IC Dedicated Support Software "Crypto Library V2.7 on P5CD145V0A, MSO / P5CC145V0A, MSO / P5CD128V0A, MSO / P5CC128V0A, MSO" which consists of a software library and associated documentation. The Crypto Library on SmartMX is an additional part that provides cryptographic functions that can be operated on the hardware platform as described in this Security Target.

Fig 1 describes the scope of this Security Target. The TOE is described in three layers:

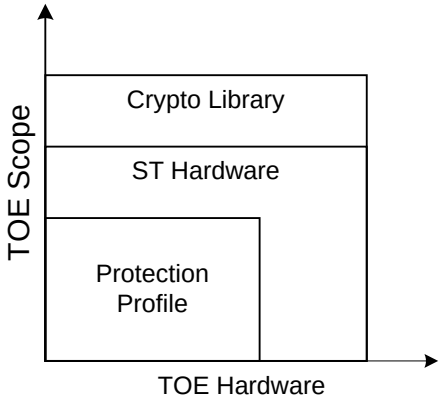

Fig 1. Scope of the Security Target

1. The Protection Profile [9] describes general requirements for smart card controllers and their support software. It is a common basis for smart card platform evaluations

and defines the minimum requirements for the TOE hardware and its associated functionality.

2. The Hardware Security Target [10] defines the functionality of the platform provided by the SmartMX Smart Card Controller.
3. The Crypto Library on SmartMX provides additional functionality to the developer of Smartcard Embedded Software. It is a supplement of the basic cryptographic features provided by the hardware platform. The Crypto Library on SmartMX implements cryptographic algorithms with countermeasures against the attacks described in this Security Target using the co-processors of the SmartMX to provide a software programming interface for the developer of the Smartcard Embedded Software.

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 Table 1 in [10]

Type	Name	Release	Date	Form of Delivery
Software	Crypto Library	2.7	26 March 2010	Electronic file
Documents	Guidance Documents [14]-[22]	See reference list	See reference list	Electronic Document

1.4.1 Hardware Description

The NXP SmartMX hardware is described in section 1.4.2.1 “Hardware Description” of the Hardware Security Target [10]. The IC Dedicated Test Software and IC Dedicated Support Software stored in the Test-ROM and delivered with the hardware platform is described in section 1.4.2.2 “Software Description” of the Hardware Security Target [10].

1.4.2 Software Description

A Smartcard embedded Software developer may create Smartcard embedded Software to execute on the NXP SmartMX hardware. This software is stored in the User ROM of the NXP SmartMX hardware and is not part of the TOE, with one exception: the Smartcard embedded Software may contain theCrypto Library on SmartMX (or parts thereof[1]) and this Crypto Library (or parts thereof) is part of the TOE.

The TOE provides AES[2], DES, Triple-DES (3DES), RSA, RSA key generation, RSA public key computation, ECC over GF(p) signature generation and verification, ECC over GF(p) key generation, ECC Diffie-Helmann key-exchange , SHA-1, SHA-224 and SHA-256 algorithms.

Many of these algorithms are resistant against side-channel attacks: more information may be found in Table 7.

1. These crypto functions are supplied as a library rather than as a monolithic program, and hence a user of the library may include only those functions that are actually required – it is not necessary to include all cryptographic functions of the library in every 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 [14].
2. AES, DES and Triple-Des can be used in ECB, CBC or CBC-MAC mode.

The TOE supports various key sizes for RSA up to a limit of 5024 bits and for ECC over GF(p) up to a limit of 544 bits.

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

Finally, the TOE provides a secure copy routine and includes internal security measures for residual information protection.

1.4.3 Documentation

The documentation for the NXP SmartMX hardware is listed in section 1.4.2.3 “Documentation” of the Hardware Security Target [10].

The Crypto Library has associated user guidance documentation (see Table 1). This contains:

- 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
- user 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).

1.4.4 Interface of the TOE

The interface to the NXP SmartMX hardware is described in section 1.4.5 “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 on SmartMX.

The interface to the TOE additionally consists of software function calls, as detailed in the “User Guide and Reference” document of the Crypto Library on SmartMX. The developer of the Smartcard Embedded Software will link the required functionality of the Crypto Library on SmartMX into the Smartcard Embedded Software as required for his Application.

1.4.5 Life Cycle and Delivery of the TOE

The life cycle and delivery for the NXP SmartMX hardware is described in section 1.4.4 “TOE Intended Usage” 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 [9]) to the Smartcard Embedded Software developer. The Smartcard Embedded Software developer then integrates the Crypto Library in the Smartcard Embedded Software.

Delivery of the Crypto Library to the Smartcard Embedded Software developer may be 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.

1.4.6 TOE Intended Usage

Regarding to phase 7 (for a definition of the Phases refer to section ‘1.2.3 TOE life cycle’ of the Protection Profile [9]), 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 1.4.4 “TOE Intended Usage” in the Hardware Security Target [10].

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

1.4.7 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 SmartMX hardware.

1.4.8 General IT features of the TOE

The general features of the NXP SmartMX 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.

1.5 Further Definitions and Explanations

Since the Security Target claims conformance to the Protection Profile [9], the concepts are used in the same sense. For the definition of terms refer to the Protection Profile [9]. This chapter does not need any supplement in the Security Target.

2. Security Problem Definition

This Security Target claims conformance to the Protection Profile [9]. 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.

2.1 Description of Assets

Since this Security Target claims conformance to the Protection Profile [9], 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.

2.2 Assumptions

Since this Security Target claims conformance to the Protection Profile [9], the assumptions defined in section 3.2 of the Protection Profile, described in section 3.4 “Assumptions” of the Hardware Security Target [10], and shown in Table 2, are valid for this Security Target.

Table 2. Assumptions defined in the PP [9] and the Hardware Security Target [10]

Name	Title	Defined in
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalization	PP [9]
A.Plat-Appl	Usage of Hardware Platform	PP [9]
A.Resp-Appl	Treatment of User Data	PP [9]
A.Check-Init	Check of initialisation data by the Smartcard Embedded Software	HW-ST [10]
A.Key-Function	Usage of Key-dependent Functions	HW-ST [10]

This Security Target defines one additional assumption:

A.RSA-Key-Gen Operational Environment for RSA Key Generation function

The RSA Key Generation provides two different modes. The insecure mode is not secured against side-channel attacks. Therefore the execution speed is faster than in the secure mode. When this version is executed the environment has to avoid side-channel attacks.

2.3 Threats

Since this Security Target claims conformance to the Protection Profile [9], the threats defined in section 3.2 of the Protection Profile, described in section 3.2 “Threats” of the Hardware Security Target [10], and shown in Table 3, are valid for this Security Target.

Table 3. Threats defined in the Protection Profile

Name	Title	Defined in
T.Leak-Inherent	Inherent Information Leakage	PP [9]
T.Phys-Probing	Physical Probing	PP [9]
T.Malfunction	Malfunction due to Environmental Stress	PP [9]
T.Phys-Manipulation	Physical Manipulation	PP [9]
T.Leak-Forced	Forced Information Leakage	PP [9]
T.Abuse-Func	Abuse of Functionality	PP [9]
T.RND	Deficiency of Random Numbers	PP [9]

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 SmartMX) and software (Crypto Library on SmartMX). 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.

2.4 Organisational Security Policies

Since this Security Target claims conformance to the Protection Profile [9], the Policy P.Process-TOE “Protection during TOE Development and Production” of the Protection Profile is applied here also.

The hardware security target defines the following additional security policies:

P.Add-Components: Additional Specific Security Components

The SmartMX processor part of the TOE provides the following additional security functionality to the Smartcard Embedded Software:

- Triple-DES encryption and decryption
- AES encryption and decryption
- Area based Memory Access Control
- Memory separation for different software parts (including IC Dedicated Software and Security IC Embedded Software)
- Special Function Register Access Control

The Crypto Library part of the TOE uses the Triple-DES co-processor hardware to provide DES security functionality, as listed below in P.Add-Func: Additional Specific Security Functionality.

The Crypto Library makes no use of either the Area based Memory Access Control or the Special Function Register Access Control. These features are for the use and control of the Smartcard Embedded Software that includes the Crypto Library.

In addition to the security functionality provided by the hardware mentioned above and defined in the Security Target of the SmartMX, 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
- Triple-DES[3] encryption and decryption,
- RSA encryption, decryption, signature generation and verification,
- RSA public key computation
- RSA key generation,
- ECC over GF(p) signature generation and encryption,
- ECC over GF(p) key generation,
- ECC Diffie-Hellman key exchange
- ECC Secure Point Addition
- SHA-1, SHA-224 and SHA-256 Hash Algorithms,
- access to the RNG (implementation of a software RNG and tests for the hardware RNG),
- secure copy routine.

In addition, the TOE shall

- provide protection of residual information, and
- provide resistance against side channel attacks as described in Table 7 and in section 5.1.13 F.COPY.

Regarding the Application Note 12 of the Protection Profile [9] there are no other additional policies defined in this Security Target.

3. See also Note 7 in section 4.1.1.

3. Security Objectives

This chapter contains the following sections: “Security Objectives for the TOE” and “Security Objectives for the Operational environment”.

3.1 Security Objectives for the TOE

The following table lists the security objectives of the Protection Profile [9] and the Hardware Security Target [10].

Table 4. Security Objectives defined in the Protection Profile and the Hardware Security Target

Name	Title	Defined in
O.Leak-Inherent	Protection against Inherent Information Leakage	PP [9]
O.Phys-Probing	Protection against Physical Probing	PP [9]
O.Malfunction	Protection against Malfunctions	PP [9]
O.Phys-Manipulation	Protection against Physical Manipulation	PP [9]
O.Leak-Forced	Protection against Forced Information Leakage	PP [9]
O.Abuse-Func	Protection against Abuse of Functionality	PP [9]
O.Identification	TOE Identification	PP [9]
O.RND	Random Numbers	PP [9]
O.HW_DES3	Triple DES Functionality	HW-ST [10]
O.HW_AES	AES Functionality	HW-ST [10]
O.MF_FW	MIFARE 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]

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 (Crypto Library on SmartMX) also provides a software (pseudo) RNG and implements test routines for the hardware 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 2.3, 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.AES — The TOE includes functionality to provide encryption and decryption facilities of the AES algorithm, resistant to attack as listed in Table 7.

O.DES3 — The TOE includes functionality to provide encryption and decryption facilities of the Triple-DES algorithm, resistant to attack as listed in. (see also Note 7 in section 4.1.1).

O.RSA	The TOE includes functionality to provide encryption, decryption, signature creation and signature verification using the RSA algorithm, resistant to attack as listed in Table 7.
O.RSA_PubKey	The TOE includes functionality to compute an RSA public key from an RSA private key, resistant to attack as listed in Table 7.
O.RSA_KeyGen	The TOE includes functionality to generate RSA key pairs, resistant to attack as listed in Table 7.
O.ECC	The TOE includes functionality to provide signature creation and signature verification as well as secure point addition using the ECC over GF(p) algorithm, resistant to attack as listed in Table 7.
O.ECC_DHKE	The TOE includes functionality to provide Diffie-Hellman key exchange based on ECC over GF(p), resistant to attack as listed in Table 7.
O.ECC_KeyGen	The TOE includes functionality to generate ECC over GF(p) key pairs, resistant to attack as listed in Table 7.
O.SHA	The TOE includes functionality to provide electronic hashing facilities using the SHA-1, SHA-224 and SHA-256 algorithms.
O.COPY	The TOE includes functionality to copy memory content using a routine that implements countermeasures against side channel attacks.
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.

3.2 Security Objectives for the Operational environment

The security objectives for the operational environment, listed in the following Table 5, are taken from the PP [9]. Additional refinements in the Hardware Security Target [10] are also valid in the ST for the Crypto Library (the “IC Dedicated Support Software”).

Table 5. Security Objectives for the operational environment

Name	Title	Applies to phase
OE.Plat-Appl	Usage of Hardware Platform	Phase 1
OE.Resp-Appl	Treatment of User Data	Phase 1
OE.Process-Sec-IC	Protection during Packaging, Finishing and Personalization	Phase 4 through delivery to phase 7

The crypto library TOE assumes that the Smartcard Embedded Software abides by the provisions detailed in “Clarification of “Usage of Hardware Platform (OE.Plat-Appl)” and “Clarification of Treatment of User Data (OE.Resp-Appl)” contained within section 4.2 “Security Objectives for the Operational environment” of the Hardware Security Target [10].

The Hardware Security Target [10] defines, in section 4.3 “Security Objectives for the Operational environment”, the following additional security objective for the Smart Card Embedded Software:

OE.Check-Init	Check of initialization data by the Smart Card Embedded Software.

This Security Target defines additional security objectives for the operational environment:

OE.RSA-Key-Gen	In case that resistance of the fast, but insecure mode of the RSA Key Generation against side channel attacks is needed, the operational environment shall ensure that side-channel attacks can not be performed.

4. Security Requirements

4.1 Security Functional Requirements

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

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

The Security Functional Requirements (SFRs) for this TOE (Crypto Library on SmartMX) are specified based on the Smart Card IC Platform Protection Profile [9], and are defined in the Common Criteria or in the Protection Profile, as is shown by the third column of the following table:

Table 6. SFRs defined in the Protection Profile or the Common Criteria

Name	Title	Defined in
FAU_SAS.1	Audit storage	PP Section 5.3 [9] (provided by chip HW)
FCS_RNG.1	Generation of random numbers	PP [9] Section 5.1
FDP_IFC.1	Subset information flow control	CC Part 2 [2] (provided partly by chip HW and partly by crypto library SW, see the following Note 4)
FDP_ITT.1	Basic internal transfer protection	CC Part 2 [2] (provided partly by chip HW and partly by crypto library SW, see the following Note 4)
FMT_LIM.1	Limited capabilities	PP Section 5.2 [9] (provided by chip HW)
FMT_LIM.2	Limited availability	PP Section 5.2 [9] (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 partly by chip HW and partly by crypto library SW, see the following Note 4)
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)

These requirements have already been stated in the hardware ST [10] and are fulfilled by the chip hardware, if not indicated otherwise in Table 6. See also the following Note 4.

Note 4. Refinement: The functional requirements FDP_ITT.1, FPT_ITT.1 and FDP_IFC.1 are refined for this composite evaluation to also include resistance

against leakage (SPA, DPA, Timing attacks)[4] of secret information during the application of: AES, DES, 3DES, RSA, RSA key generation, RSA public key computation, ECC over GF(p), ECC Point Addition, ECC Diffie-Hellman Key Exchange and ECC over GF(p) key generation. Compared to the Hardware Security Target [10], the text of these requirements remains unchanged, but these requirements now apply to a more comprehensive TOE (including hardware and software). See also the following Note 6 for a discussion of DFA resistance. – FDP_IFC.1 is again refined to include also resistance against leakage for the secure copy routine (see also section 5.1.13 F.COPY as well as the requirements FDP_ITT.1[COPY] and FPT_ITT.1[COPY] in section 4.1.2)[5].

Note 5. Refinement: FPT_FLS.1 is refined as compared to its first definition in the PP [9] and its instantiation in the hardware ST [10] to include not only the hardware sensors but also “software sensors” that detect DFA attacks on AES, DES, 3DES, RSA and ECC over GF(p) computations. Therefore the requirement is repeated here together with the extended refinement. FPT_FLS.1 now includes also DFA protection for AES, DES, 3DES, RSA and ECC over GF(p). Note, that FRU_FLT.2, which is not modified, works closely together with FPT_FLS.1.

The TOE shall meet the requirements “Random number generation” and “Failure with preservation of secure state (FPT_FLS.1)” as specified below.

FCS_RNG.1[DET] Random number generation

The hardware part of the TOE (NXP SmartMX) provides a physical random number generator (RNG) that fulfils FCS_RNG.1 as already mentioned above in Table 6. The additional software part of the TOE (Crypto Library) implements a software (pseudo) RNG that fulfils FCS_RNG.1[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.

Hierarchical to:	No other components.
FCS_RNG.1.1[DET]	The TSF shall provide a *deterministic*[6] random number generator that implements a *chi-squared test on the seed generator.*
FCS_RNG.1.2[DET]	The TSF shall provide random numbers that meet class K.4 of AIS20 [5].
Application Notes:	The Crypto Library on SmartMX provides the smartcard embedded software with seperate library calls to initialise the random number generator (which includes the chi-squared test) and to generate random data. It is the responsibility of the user to initialise the random number generator before generating random data
Dependencies:	No dependencies.

4. see also Table 7 Algorithm Resistance Overview
5. FDP_ITT.1 and FPT_ITT.1 are iterated in order to allow more exact mappings (see FDP_ITT.1[COPY] and FPT_ITT.1[COPY] in section 4.1.2), but they still refer to the same information flow control policy, i.e. FDP_IFC.1 is not iterated.

[6] Implemented through a recursive call of 2-key triple-DES

Note: Only if the chi-squared test succeeds the hardware RNG seeds the software RNG implemented as part of the Crypto Library on SmartMX (as part of security functionality F.RNG_Access).

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 SmartMX Secure Smart Card Controller are met.

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: *(i) exposure to operating conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur and (ii) DFA attacks on AES, DES, 3DES, RSA and ECC over GF(p).*

Dependencies: No dependencies

Refinement: The term “failure” above also covers “circumstances”. The TOE prevents failures for the “circumstances” defined above.

Note 6. This refinement should be understood with the following implementation details in mind: The TOE contains both hardware sensors (implemented in the chip card hardware) and software sensors (implemented in the Crypto Library software). The software sensors detect DFA attacks in AES, DES, 3DES, RSA and ECC over GF(p) computations and this detection leads to a secure state (no computation results are output and an exception is thrown) in case such an attack occurs. The Smartcard Embedded Software is expected to handle this exception and further ensure a secure state.

The properties of the cryptographic algorithms in respect to their resistance[7] against Side Channel Analysis (FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_FLS.1) can be summarized as follows:

Table 7. Algorithm Resistance Overview

Algorithm	Resistant against			
AES	Timing	SPA	DPA	DFA
DES	Timing	SPA	DPA	DFA
3DES	Timing	SPA	DPA	DFA
RSA decryption and signature generation	Timing	SPA	DPA	DFA

7. SPA = Simple Power Analysis, DPA = Differential Power Analysis, DFA = Differential Fault Analysis

Algorithm	Resistant against			
RSA Public Key Computation	Timing	SPA	n/a	n/a
RSA Key Generation	Timing	SPA	n/a	n/a
ECC over GF(p)	Timing	SPA	DPA	DFA
ECC Diffie-Hellman Key Exchange	Timing	SPA	DPA	n/a
ECC over GF(p) Key Generation	Timing	SPA	n/a	n/a
SHA-1, SHA-224 and SHA-256	-	-	-	n/a

The abbreviation “n/a” in Table 7 Algorithm Resistance Overview means “not applicable”, i.e. the TOE does not provide countermeasures here. This does not mean that the algorithm is insecure; rather at the time of writing this Security Target no promising attacks were known.

Note 7. The countermeasures that protect 3DES against side channel attacks also protect the Single-DES algorithm against these kinds of attacks. Therefore side channel resistance is also claimed for Single-DES. However, it must be noted that Single-DES is no longer considered to be resistant against attackers with a high attack potential, therefore Single-DES must not be used as an encryption algorithm without any additional protection. For the evaluated TOE, Single-DES does not constitute a security functionality on its own. – The resistance of Single-DES and Triple-DES against side channel attacks protects the confidentiality of the keys used in all modes of operation (ECB, CBC, CBC-MAC).

Note 8. The protection of the RSA Key Generation against attacks is only given if the secure mode is executed or if the insecure mode is executed in a secure environment.

Note 9. DPA resistance for ECC Diffie-Hellman Key Exchange is only given with respect to the private key, not for the public key. This is of interest when using the function for a secure point multiplication. In this case only the scalar is protected against DPA like attacks, but not the point.

The SFRs from Table 6 are supplemented by additional SFRs, defined in the Common Criteria, as described in sections 6.1.2 “Additional SFRs regarding cryptographic functionality” and 6.1.3 “Additional SFRs regarding access control” of the Hardware Security Target [10] and shown in the following table.

Table 8. SFRs defined in the Hardware Security Target

Name	Title	Defined in
FCS_COP.1[AES]	Cryptographic operation	CC Part 2 [2], and added to PP in the Hardware ST [10] section 6.1.2 “Additional SFRs regarding cryptographic functionality”.
FCS_COP.1[DES]	Cryptographic operation	CC Part 2 [2], and added to PP in the Hardware ST [10] section 6.1.2 “Additional SFRs regarding cryptographic functionality”.
FDP_ACC.1[MEM]	Subset access control	CC Part 2 [2], and added to PP in the Hardware ST [10] section 6.1.3 “Additional

Name	Title	Defined in
		SFRs regarding access control”.
FDP_ACC.1[SFR]	Subset access control	CC Part 2 [2], and added to PP in the Hardware ST [10] section 6.1.3 “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 ST [10] section 6.1.3 “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 ST [10] section 6.1.3 “Additional SFRs regarding access control”.
FMT_MSA.3[MEM]	Static attribute initialization	CC Part 2 [2], and added to PP in the Hardware ST [10] section 6.1.3 “Additional SFRs regarding access control”.
FMT_MSA.3[SFR]	Static attribute initialization	CC Part 2 [2], and added to PP in the Hardware ST [10] section 6.1.3 “Additional SFRs regarding access control”.
FMT_MSA.1[MEM]	Management of security attributes	CC Part 2 [2], and added to PP in the Hardware ST [10] section 6.1.3 “Additional SFRs regarding access control”.
FMT_MSA.1[SFR]	Management of security attributes	CC Part 2 [2], and added to PP in the Hardware ST [10] section 6.1.3 “Additional SFRs regarding access control”.
FMT_SMF.1	Specification of management functions	CC Part 2 [2], and added to PP in the Hardware ST [10] section 6.1.3 “Additional SFRs regarding access control”.

Like the requirements already listed in Table 6, the requirements listed in Table 8 have already been stated in the Hardware Security Target [10] and are fulfilled by the chip hardware.

4.1.2 Additional SFRs

The SFRs in Table 6 and Table 8 are further supplemented by the additional SFRs described in the following subsections of this Security Target, as listed in Table 9. The SFRs described in Table 9 together with the extensions of FDP_ITT.1, FPT_ITT.1, FDP_IFC.1 and FPT_FLS.1 form the set of SFRs that are new for the crypto library. The composite TOE, consisting of chip hardware and crypto library software, fulfils all requirements from Table 6, Table 8 and Table 9.

Table 9. 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 (TDES)	CC Part 2 [2]; specified in this ST, see below.

Name	Title	Defined in
FCS_COP.1[RSA_encrypt]	Cryptographic operation (RSA encryption and decryption)	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1[RSA_public]	Cryptographic operation (RSA public key computation)	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1[RSA_sign]	Cryptographic operation (RSA signature generation and verification)	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1[ECC_GF_p]	Cryptographic operation (ECC over GF(p) signature generation and verification)	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1[ECC_ADD]	Cryptographic operation (ECC over GF(p) point addition)	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1[ECC_DHKE]	Cryptographic operation (ECC Diffie-Hellman key exchange)	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1[SHA]	Cryptographic operation (SHA-1, SHA-224 and SHA-256)	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_GF_p]	Cryptographic key generation (ECC over GF(p) key generation)	CC Part 2 [2]; specified in this ST, see below.
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.
FDP_ITT.1[COPY]	Basic internal (user data) transfer protection	CC Part 2 [2]; specified in this ST, see below.
FPT_ITT.1[COPY]	Basic internal TSF data transfer protection	CC Part 2 [2]; specified in this ST, see below.

The requirements listed in Table 9 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

Hierarchical to:	No other components.
FCS_COP.1.1[SW-AES]	The TSF shall perform *encryption and decryption* in accordance with the specified cryptographic algorithm *AES in one of the following modes of operation: ECB, CBC or CBC-*

	MAC and cryptographic key sizes *128, 192 and 256 bit* that meet the following: *FIPS Publication 197, Advanced Encryption Standard (AES), NIST Special Publication 800-38A, 2001 (ECB and CBC mode) and ISO 9797-1, Algorithm 1 (CBC-MAC mode)*.
Application Notes:	The security functionality is resistant against side channel analysis and similar techniques.
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

Hierarchical to:	No other components.
FCS_COP.1.1[SW-DES]	The TSF shall perform *encryption and decryption* in accordance with the specified cryptographic algorithm *DES and Triple-DES in one of the following modes of operation: ECB, CBC or CBC-MAC* and cryptographic key sizes 1-*key DES (56 bit), 2-key TDES (112 bit) or 3-key TDES (168 bit)* that meet the following: *ANSI X9.52-1998 [32] (ECB and CBC mode) and FIPS PUB 81 [31] (ECB and CBC mode) and ISO 9797-1 [26], Algorithm 1 (CBC-MAC mode)*.
Application Notes:	(1) The security functionality is resistant against side channel analysis and similar techniques. To fend off attackers with high attack potential a security level of at least 80 Bits must be used. (2) The CBC mode is to be understood as “outer” CBC mode, i.e. CBC mode as defined in [31] and [32] applied to the block cipher algorithm (either DES or Triple-DES). The CBC-MAC mode of operation as defined in ISO 9797-1 [26], Algorithm 1, and also described in Appendix F of [31] is similar to CBC mode, but the output of the CBC-MAC is restricted to the output of the last Triple-DES operation, i.e. only the last block of the ciphertext is returned.
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_encrypt] Cryptographic operation

Hierarchical to:	No other components.
FCS_COP.1.1[RSA_encrypt]	The TSF shall perform *encryption and decryption* in accordance with the specified cryptographic algorithm *RSA without or with EME-OAEP encoding method* and cryptographic key sizes *256 bits to 5024 bits* that meet the following: *PKCS #1, v2.1 (RSAEP, RSADP, RSAES-OAEP)*.
Application Notes:	The security functionality is resistant against side channel analysis and similar techniques. To fend off attackers with

	high attack potential a security level of at least 80 Bits must 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_sign] Cryptographic operation

Hierarchical to:	No other components.
FCS_COP.1.1[RSA_sign]	The TSF shall perform *signature generation and verification* in accordance with the specified cryptographic algorithm *RSA without or with EMSA-PSS encoding method* and cryptographic key sizes *256 bits to 5024 bits* that meet the following: *PKCS #1, v2.1 (RSASP1, RSAVP1, RSASSA-PSS)*.
Application Notes:	The security functionality is resistant against side channel analysis and similar techniques. To fend off attackers with high attack potential a security level of at least 80 Bits must 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_public] Cryptographic operation

Hierarchical to:	No other components.
FCS_COP.1.1[RSA_public]	The TSF shall perform *public key computation* in accordance with the specified cryptographic algorithm *RSA* and cryptographic key sizes *256 bits to 2048 bits (Straight Forward) or 256 to 4096 bits (CRT)* that meet the following: *PKCS #1, v2.1 (RSAEP, RSAVP1)*.
Application Notes:	(1) The security functionality is resistant against side channel analysis and similar techniques. To fend off attackers with high attack potential a security level of at least 80 Bits must be used. (2) The computation will result in the generation of a public RSA key from the private key. 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[ECC_GF_p] Cryptographic operation

Hierarchical to:	No other components.
FCS_COP.1.1[ECC_GF_p]	The TSF shall perform *signature generation and verification* in accordance with the specified cryptographic algorithm *ECC*

over GF(p) and cryptographic key sizes *128 to 544 bits* that meet the following: *ISO 14888-3 [28]*.

Application Notes: The security functionality is resistant against side channel analysis and similar techniques. It is demonstrated for curves defined by NIST [36] and Brainpool [37] only. To fend off attackers with high attack potential a security level of at least 80 Bits must 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[ECC_ADD] Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1[ECC_ADD] The TSF shall perform *secure point addition* in accordance with the specified cryptographic algorithm *ECC over GF(p)* and cryptographic key sizes *128 to 544 bits* that meet the following: *ISO 14888-3 [28]*.

Application Notes: (1) The input and output values of this function have to be treated as secret values.

(2) The security functionality can be used to implement the PACE protocol.

(3) The security functionality is resistant against side channel analysis and similar techniques. It is demonstrated for curves defined by NIST [36] and Brainpool [37] only. To fend off attackers with high attack potential a security level of at least 80 Bits must 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[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 *128 to 544 bits* that meet the following: *ISO 11770-3 [29].*

Application Notes: (1) The security functionality is resistant against side channel analysis and similar techniques. It is demonstrated for curves defined by NIST [36] and Brainpool [37] only. To fend off attackers with high attack potential a security level of at least 80 Bits must be used.

(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. (3) The input value pulic key is also treated as secret value. Therefore it can be used as a secure 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[SHA] Cryptographic operation

Hierarchical to:	No other components.
FCS_COP.1.1[SHA]	The TSF shall perform *cryptographic checksum generation* in accordance with the specified cryptographic algorithm *SHA-1, SHA-224 and SHA-256* and cryptographic key size *none* that meet the following: *FIPS 180-3* [33].
Application Notes:	To fend off attackers with high attack potential a security level of at least 80 Bits must 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.

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 (straight forward) and RSA-CRT* and specified cryptographic key sizes *256-4096 bits* that meet the following: *"Regulierungsbehörde für Telekommunikation und Post: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), German "Bundesanzeiger Nr. 59", p. 4695-4696, March 30th, 2005"*.
Application Notes:	The security functionality is resistant against side channel analysis and similar techniques. To fend off attackers with high attack potential a security level of at least 80 Bits must be used.
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 requirement AVA_VAN.5.

FCS_CKM.1[ECC_GF_p] Cryptographic Key Generation

Hierarchical to: No other components.

FCS_CKM.1.1[ECC_GF_p] The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECC over GF(p)* and specified cryptographic key sizes *128-544 bits* that meet the following: *ISO 15946-1-2008 [27] and "Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen"* [35].

Application Notes: The security functionality is resistant against side channel analysis and similar techniques. It is demonstrated for curves defined by NIST [36] and Brainpool [37] only. To fend off attackers with high attack potential a security level of at least 80 Bits must be used.

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 ECC key generation, if the generated ECC 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.

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 on SmartMX provides the smartcard embedded software with library calls to perform various cryptographic algoritms 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 algoritms. 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 SmartMX. 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 on SmartMX is the responsibility of the smartcard embedded software.

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:	No dependencies.

Note 10. 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.

FDP_ITT.1[COPY] Basic internal transfer protection

Basic internal transfer protection requires that user data be protected when transmitted between parts of the TOE. The TOE provides a secure copy routine which copies blocks of data in a way that protects these data against certain kinds of side channel attacks. The following Functional Requirement to the TOE can be derived from the CC component FDP_ITT.1:

Hierarchical to:	No other components.
FDP_ITT.1.1[COPY]	The TSF shall enforce the *Data Processing Policy*[8] to prevent the *disclosure*[9] of user data when it is transmitted between physically-separated parts of the TOE.
Refinement:	The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as physically separated parts of the TOE. The TSF shall provide a secure copy routine that copies blocks of data in a way that the data confidentiality is maintained in case of side channel attacks. The Data Processing Policy is defined in the PP [9], section 5.1.1, paragraph 156.

8. assignment: access control SFP(s) and/or information flow control SFP(s)
9. selection: disclosure, modification, loss of use

Dependencies:	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

FPT_ITT.1[COPY] Basic internal TSF data transfer protection

Basic internal TSF data transfer protection requires that TSF data be protected when transmitted between parts of the TOE. The TOE provides a secure copy routine which copies blocks of data in a way that protects these data against certain kinds of side channel attacks. The following Functional Requirement to the TOE can be derived from the CC component FPT_ITT.1:

Hierarchical to:	No other components.
FPT_ITT.1.1[COPY]	The TSF shall protect TSF data from *disclosure*[10] when it is transmitted between separate parts of the TOE.
Refinement:	The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as physically separated parts of the TOE. The TSF shall provide a secure copy routine that copies blocks of data in a way that the data confidentiality is maintained in case of side channel attacks.
Dependencies:	No dependencies.

Note 11. The Protection Profile [9] already includes the functional requirements FDP_ITT.1 and FPT_ITT.1 (see [9], section 6.1, paragraphs 159 and 160). These functional requirements have been iterated (with the postfix [COPY] added), since FDP_ITT.1[COPY] and FPT_ITT.1[COPY] focus on a special implementation detail (secure copy routine). Still FDP_ITT.1[COPY] refers to the same information flow control policy “Data Processing Policy” as defined in the PP [9], section 6.1, paragraph 159. FDP_ITT.1[COPY] protects user data, while FPT_ITT.1[COPY] protects TSF data (the mechanism implemented in the secure copy routine protects user data as well as TSF data).

4.2 Security Assurance Requirements

Table 10 below lists all security assurance components that are valid for this Security Target. These security assurance components are required by EAL5 or by the Protection Profile [9].

Table 10. Security Assurance Requirements EAL5+ and PP augmentations

SAR	Title	Required by
ADV_ARC.1	Security architecture description	PP / EAL5
ADV_FSP.5	Complete semi-formal functional specification with additional error information	EAL5
ADV_IMP.1	Implementation representation of the TSF	PP / EAL5
ADV_INT.2	Well-structured internals	EAL5
ADV_TDS.4	Semiformal modular design	EAL5
AGD_OPE.1	Operational user guidance	PP / EAL5

10. selection: disclosure, modification

SAR	Title	Required by
AGD_PRE.1	Preparative procedures	PP / EAL5
ALC_CMC.4	Production support, acceptance procedures and automation	PP / EAL5
ALC_CMS.5	Development tools CM coverage	EAL5
ALC_DEL.1	Delivery procedures	PP / EAL5
ALC_DVS.2	Sufficiency of security measures	PP
ALC_LCD.1	Developer defined life-cycle model	PP / EAL5
ALC_TAT.2	Compliance with implementation standards	EAL5
ASE_CCL.1	Conformance claims	PP / EAL5
ASE_ECD.1	Extended components definition	PP / EAL5
ASE_INT.1	ST introduction	PP / EAL5
ASE_OBJ.2	Security objectives	PP / EAL5
ASE_REQ.2	Derived security requirements	PP / EAL5
ASE_SPD.1	Security problem definition	PP / EAL5
ASE_TSS.1	TOE summary specification	PP / EAL5
ATE_COV.2	Analysis of coverage	PP / EAL5
ATE_DPT.3	Testing: modular design	EAL5
ATE_FUN.1	Functional testing	PP / EAL5
ATE_IND.2	Independent testing - sample	PP / EAL5
AVA_VAN.5	Advanced methodical vulnerability analysis	PP

4.2.1 Refinements of the TOE Security Assurance Requirements

The ST claims conformance to the Protection Profile “**Bundesamt für Sicherheit in der Informationstechnik (BSI):** Security IC Platform Protection Profile, Version 1.0, 15.06.2007; Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035”, and therefore it has to be conform to the refinements of the TOE security assurance requirements (see Application Note 19 of the PP).

The Hardware Security Target [10] has chosen the evaluation assurance level EAL5+. This Hardware Security Target bases on the Protection Profile [9], which requires the lower level EAL4+. This implies that the refinements made in the Protection Profile [9], section 6.2.1 Refinements of the TOE Assurance Requirements, for EAL4+ had to be refined again in order to ensure EAL5+ in the Hardware Security Target (this was necessary for ACM_CMS.5 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 [9] are valid without change for the composite TOE.

5. TOE Summary Specification

This chapter describes the “IT Security Functionality”.

5.1 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 Target [10]). The securioty functionality of the hardware platform is listed in the following table; the additional security functionality provided by the cryptographic library is described in the following sub-sections.

Table 11. IT security functionalities defined in the Hardware Security Target [10]

Name	Title
SS.RNG	Hardware Random Number Generator
SS.HW_AES	Hardware AES Co-processor
SS.HW_DES	Hardware Triple-DES Co-processor
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

Note 12. The security functionality SS.RNG implements the hardware RNG. The TOE also implements software RNG as part of security functionality F.RNG_Access; for details see section 5.1.11. 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 (F.RNG_Access).

Note 13. The security functionality F.LOG is extended by the crypto library TOE as described in section 5.1.14 (see below).

The IT security functionalities directly correspond to the TOE security functional requirements defined in section 4.1 above. The definitions of the IT security functionalities refer to the corresponding security functional requirements.

5.1.1 F.AES

The TOE uses the SmartMX AES hardware coprocessor to provide AES encryption and decryption facility using 128, 192 or 256 bit keys. The supported modes are ECB and “outer” CBC (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 ISO/IEC 9797-1 [26], Algorithm 1, or FIPS PUB 197 [34]).

F.AES is a basic cryptographic function which provides the AES algorithm as defined by the standard FIPS PUB 197 [34].

The interface to F.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 [14] and [16].

Sidechannel attack resistance for this security functionality is discussed in section 5.1.14 F.LOG.

This security functionality covers:

- FCS_COP.1[SW_AES].

5.1.2 F.DES

The TOE uses the SmartMX 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 supported modes are ECB and “outer” CBC (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 ISO/IEC 9797-1 [26], Algorithm 1, or FIPS PUB 81 [31], 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.

Note that only the Triple-DES encryption and decryption (two-key and three-key) is within the scope of the AVA_VAN.5 requirement of this evaluation (see also Note 7 in section 4.1.1).

F.DES is a modular basic cryptographic function which provides the DES algorithm as defined by the standard FIPS PUB 46-3 [30], and supports the 2-key and 3-key Triple-DES algorithm according to the ANSI X9.52 [32].

The interface to F.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 guidance [14] and [17]. 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.

Sidechannel attack resistance for this security functionality is discussed in section 5.1.14 F.LOG.

This security functionality covers:

- . FCS_COP.1[SW_DES]

5.1.3 F.RSA_encrypt

The TOE provides functions that implement the RSA algorithm for data encryption and decryption. This IT security functionality supports the EME-OAEP encoding schema, but also work without any encoding schema. All algorithms are defined in PKCS #1, v2.1 (RSAEP, RSADP, RSAES-OAEP)

This routine supports various key lengths from 256 bits to 5024 bits. To fend off attackers with high attack potential a security level of at least 80 Bits must be used.

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).

Sidechannel attack resistance for this security functionality is discussed in section 5.1.14 F.LOG.

This security functionality covers:

- . FCS_COP.1[RSA_encrypt]

5.1.4 F.RSA_sign

The TOE provides functions that implement the RSA algorithm and the RSA-CRT algorithm for signature generation and verification. This IT security functionality supports the EMSA-PSS signature schema, but also work without any signature schema. All algorithms are defined in PKCS #1, v2.1 (RSASP1, RSAVP1, RSASSA-PSS)

This routine supports various key lengths from 256 bits to 5024 bits. To fend off attackers with high attack potential a security level of at least 80 Bits must be used.

The TOE contains modular exponentiation functions, which, together with other functions in the TOE, perform the operations required for RSA signing or verifying. 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).

Sidechannel attack resistance for this security functionality is discussed in section 5.1.14 F.LOG.

This security functionality covers:

- . FCS_COP.1[RSA_sign]

5.1.5 F.RSA_public

The TOE provides functions that implement computation of an RSA public key from a private key. All algorithms are defined in PKCS #1, v2.1 (RSAEP, RSAVP1).

This routine supports various key lengths from *256 bits to 2048 bits (Straight Forward) or from 256 to 4096 bits (CRT)*. To fend off attackers with high attack potential a security level of at least 80 Bits must be used.

Sidechannel attack resistance for this security functionality is discussed in section 5.1.14 F.LOG.

This security functionality covers:

- . FCS_COP.1[RSA_public]

5.1.6 F.ECC_GF_p_ECDSA

The TOE provides functions to perform ECC Signature Generation and Signature Verification according to ISO/IEC 14888-3 [28].

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

Also the TOE provides an interface for secure point addition over GF(p).

The supported key length is 128 bits to 544 bits. To fend off attackers with high attack potential a security level of at least 80 Bits must be used.

Sidechannel attack resistance for this security functionality is discussed in section 5.1.14 F.LOG.

This security functionality covers:

- FCS_COP.1[ECC_GF_p]
- FCS_COP.1[ECC_ADD]

5.1.7 F.ECC_GF_p_DH_KeyExch

The TOE provides functions to perform Diffie-Hellman Key Exchange according to ISO 11770-3 [29] section 8.4. This interface can also be used as secure point mulriplication.

The supported key length is 128 bits to 544 bits. To fend off attackers with high attack potential a security level of at least 80 Bits must be used.

Sidechannel attack resistance for this security functionality is discussed in section 5.1.14 F.LOG.

This security functionality covers:

- . FCS_COP.1[ECC_DHKE]

5.1.8 F.RSA_KeyGen

The TOE provides functions to generate RSA key pairs as described in „Regulierungsbehörde für Telekommunikation und Post: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), German "Bundesanzeiger Nr. 59", p. 4695-4696, March 30th, 2005“.

It supports various key lengths from 256 bits to 4096 bits. To fend off attackers with high attack potential a security level of at least 80 Bits must be used.

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).

Sidechannel attack resistance for this security functionality is discussed in section 5.1.14 F.LOG.

This security functionality covers:

- . FCS_CKM.1[RSA]

5.1.9 F.ECC_GF_p_KeyGen

The TOE provides functions to perform ECC over GF(p) Key Generation according to ISO/IEC 15946-1-2008 [27] section 6.1.

It supports key length from 128 to 544 bits. To fend off attackers with high attack potential a security level of at least 80 Bits must be used.

Sidechannel attack resistance for this security functionality is discussed in section 5.1.14 F.LOG.

This security functionality covers:

- . FCS_CKM.1[ECC_GF_p]

5.1.10 F.SHA

The TOE implements functions to compute the Secure Hash Algorithms SHA-1, SHA-224 and SHA-256 according to the standard FIPS 180-3 [33]. Note that due to the AVA_VAN.5 requirement only SHA-224 and SHA-256 shall be used.

The SHA-1 can be used for applications whenever a secure hash algorithm is required to hash data, such as the input for digital signature creation.

This security functionality covers:

- . FCS_COP.1[SHA]

5.1.11 F.RNG_Access

The TOE contains both a hardware Random Number Generator (RNG) and a software RNG; for the hardware RNG (F.RNG) see the Note 12 above. F.RNG_Access consists of the implementation of the software RNG and of appropriate online tests for the hardware RNG (as required for FCS_RNG.1[DET] taken from the Protection Profile [9]):

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 SmartMX processor. The implementation of the software RNG is based on the standard ANSI X9.17 as described in **Menezes, A; van Oorschot, P. and Vanstone, S.:** *Handbook of Applied Cryptography*, CRC Press, 1996, http://www.cacr.math.uwaterloo.ca/hac/ [24].

In addition, the Crypto Library implements appropriate online tests according to the Hardware User Guidance Manual [11] for the hardware RNG, which fulfils the functionality class P2 defined by the AIS31 [6], as required by SFR FCS_RNG.1[DET]. The interface of F.RNG_Access allows to test the hardware RNG and to seed the software RNG after successful testing.

This security functionality covers:

- . FCS_RNG.1[DET]

5.1.12 F.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

5.1.13 F.COPY

The function F.COPY implements functionality to copy memory content in a manner protected against sidechannel attacks. This resistance against sidechannel attacks is described in section 5.1.14 F.LOG.

This security functionality covers:

- FDP_ITT.1[COPY]
- FPT_ITT.1[COPY]

5.1.14 F.LOG

The IT Security functionality F.LOG – Logical Protection defined in the Hardware Security Target [10] is extended in this Security Target to include software countermeasures against side channel attacks. Such attacks can be performed by externally measuring the power consumption of the SmartMX processor (Simple Power Analysis, SPA, or Differential Power Analysis, DPA) or measuring the execution time. In addition, attacks are possible that exploit unintended behaviour of the TOE in case of fault induction (Differential Fault Analysis, DFA).

The resistance against side channel attacks is required by FDP_ITT.1, FPT_ITT.1 and FDP_IFC.1 (SPA, DPA and timing attacks; see also Note 4 in section 4.1.1) as well as by FPT_FLS.1 (DFA attacks).

DES and AES

The resistance of AES, DES[11] and Triple-DES against SPA, DPA and timing protects the confidentiality of the keys used in all modes of operation (ECB, CBC, and CBC-MAC). This resistance is provided by the co-processors in the hardware part of the TOE.

The resistance of AES, DES[12] and Triple-DES against DFA is arranged by performing computations twice and verifying that the results are the same

RSA

The RSA cryptography implementations are resistant against:

- SPA and DPA attacks because of choice of modulus, exponent blinding and careful coding.
- timing attacks, by careful coding and the timing resistance of the underlying FameXE co-processor.
- DFA attacks as the private key operations are DFA resistant by verifying the result using the public key operation. The public key operations have no DFA protection, as there is nothing to attack.

RSA Public Key Computation

The RSA public key computation is resistant against:

- SPA and DPA attacks by limiting the number of executions with the same private key.
- Timing attacks, by careful coding.
- DFA attacks are not considered: At the time of writing this ST, no promising attack paths for DFA attacks against RSA public key computation were known.

ECC over GF(p)

The ECC over GF(p) implementation is resistant against:

- SPA and DPA attacks because of randomized projective coordinates and careful coding.
- Timing attacks, by careful coding and the timing resistance of the underlying FameXE co-processor.
- DFA because of verifying the results with elliptic curve equation to check they are on the curve.

11. See also Note 7 in section 4.1.1.
12. See also Note 7 in section 4.1.1.

ECC Diffie Hellman Key Exchange

The ECC Diffie Hellman Key Exchange implementation is resistant against:

- SPA and DPA attacks because of randomized projective coordinates and careful coding.
- timing attacks, by careful coding and the timing resistance of the underlying FameXE co-processor.
- DFA because of verifying the results with elliptic curve equation.

The attack resistance also includes the public key. This ensures that the function can also be used for secure point multiplication.

RSA Key generation

The RSA key generation provides two different modes. An insecure mode without countermeasures against side-channel attacks, but with high execution speed, and a secure mode with countermeasures against side-channel attacks.

The insecure mode is only protected against side channel attacks if OE.RSA-Key-Gen is fulfilled. In this case the environment has to make sure that no attacks can be performed.

In the secure mode the RSA key generation algorithm is resistant against:

- SPA attacks because of the SPA-resistance of the underlying functions, as the exponentiation function, for example, and because of careful programming. The only promising attack seems to be one on the Miller-Rabin-Primality-Test. The test frequently repeats exponentiations with similar exponents. An upper limit of the number of Miller-Rabin-tests limits those similar exponentiations and prevents such an attack.
- Timing attacks, by careful coding and the timing resistance of the underlying FameXE co-processor.
- DPA, because for every key pair generation, new random prime numbers are used. There is no interface to force the key generation to repeat the previous calculation with the same input parameters. This prevents DPA attacks.
- Perturbation attacks, by redundant checks for critical operations
- DFA attacks are not considered: At the time of writing this ST, no promising attack paths for DFA attacks against RSA key generation were known.

ECC over GF(p) Key generation

The ECC over GF(p) key generation algorithm is resistant against:

- SPA attacks because of randomized projective coordinates and careful coding
- timing attacks, by careful coding and the timing resistance of the underlying FameXE co-processor
- DPA, because there is no interface to force the key generation to repeat the previous calculation with the same input parameters. This prevents DPA attacks.
- DFA attacks are not considered: At the time of writing this ST, no promising attack paths for DFA attacks against ECC over GF(p) Key generation were known. Nevertheless, the implementation has some measurements included to detect Fault Attacks.

SHA

The TOE implements SHA-1, SHA-224 and SHA-256 calculations but these are not resistant against side-channel attacks.

Secure copy

The secure copy function is protected against SPA by randomization: the byte order in which a memory block is randomly permutated (based on F.RNG_Access). Because the randomization is different every time, the averaging of power traces is prevented, since the point in time in which a given byte is copied is different every time (with a very high probability).

DPA, DFA and timing attacks are not applicable

This security functionality covers:

- FDP_ITT.1
- FPT_ITT.1
- FDP_IFC.1
- FPT_FLS.1

6. Rationale

This chapter contains the following sections: "Security Objectives Rationale", "Security Requirements Rationale" and "Conformance Claim Rationale".

This Security Target is based on the Security Target for the hardware of the SmartMX. This rationale is given for the combination of both (composite TOE), the Crypto Library Software and the SmartMX hardware.

6.1 Security Objectives Rationale

Section 7.1 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 Protection Profile [9]. The following Table 12 reproduces the table in section 7.1 of the Protection Profile [9].

Table 12. Security Objectives versus Assumptions, Threats or Policies

Assumption, Threat or OSP	Security Objective	Note
A.Plat-Appl	OE.Plat-Appl	Phase 1
A.Resp-Appl	OE.Resp-Appl	Phase 1
P.Process-TOE	O.Identification	Phase 2 – 3, optional Phase 4
A.Process-Sec-IC	OE.Process-Sec-IC	Phase 5 – 6, optional Phase 4
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 following Table 13 provides the justification for the additional security objectives. 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 13. Additional Security Objectives versus Assumptions or Policies

Assumption/Policy	Security Objective	Note
P.Add-Components	O.HW_AES O.HW_DES3 O.MF_FW O.MEM_ACCESS O.SFR_ACCESS O.Leak-Inherent O.Phys-Probing O.Malfunction O.Phys-Manipulation O.Leak-Forced	

Assumption/Policy	Security Objective	Note
P.Add-Func	O.AES O.DES3 O.RSA O.RSA_PubKey O.RSA_KeyGen O.ECC O.ECC_DHKE O.ECC_KeyGen O.SHA O.RND O.REUSE O.COPY O.MEM_ACCESS O.Leak-Inherent O.Phys-Probing O.Malfunction O.Phys-Manipulation O.Leak-Forced	
A.Key-Function	OE.Plat-Appl OE.Resp-Appl	(Phase 1)
A.Check-Init	OE.Check-Init	(Phase 1) and (Phase 4 – 6)
A.RSA-Key-Gen	OE.RSA-Key-Gen	

P.Add-Components

Since the objectives O.HW_DES3, O.MF_FW, O.MEM_ACCESS and O.SFR_ACCESS require the TOE to implement exactly the same specific security functionality as required by P.Add-Components, the organisational security policy is covered by these 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-Components and therefore support P.Add-Components. 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.

P.Add-Func

Since the objectives O.AES, O.DES3, O.RSA, O.RSA_PubKey, O.RSA_KeyGen, O.ECC, O.ECC_DHKE, O.ECC_KeyGen, O.SHA, O.RND, O.COPY, O.REUSE and O.MEM_ACCESS 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.Key-Function

- Compared to [9] a clarification has been made for the security objective “Usage of Hardware Platform (OE.Plat-Appl)”: If required the Smartcard Embedded Software shall use the cryptographic services of the TOE and their interfaces as specified. In

addition, the Smartcard Embedded Software (i) must implement operations on keys (if any) in such a manner that they do not disclose information about confidential data and (ii) must configure the memory management in a way that different applications are sufficiently separated. If the Smartcard Embedded Software uses random numbers provided by the security functionality F.RNG these random numbers must be tested as appropriate for the intended purpose. This addition ensures that the assumption A.Key-Function is still covered by the objective OE.Plat-Appl although additional functions are being supported according to P.Add-Components.

- Compared to [9] a clarification has been made for the security objective “Treatment of User Data (OE.Resp-Appl)”: By definition cipher or plain text data and cryptographic keys are User Data. So, the Smartcard Embedded Software will protect such data if required and use keys and functions appropriately in order to ensure the strength of cryptographic operation. Quality and confidentiality must be maintained for keys that are imported and/or derived from other keys. This implies that appropriate key management has to be realised in the environment. In addition the treatment of User Data comprises the implementation of a multi-application operating system that does not disclose security relevant User Data of one application to another one. These measures make sure that the assumption A.Key-Function is still covered by the security objective OE.Resp-Appl although additional functions are being supported according to P.Add-Func.

A.Check-Init

Since OE.Check-Init requires the Smartcard Embedded Software developer to implement a function assumed in A.Check-Init, 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 for the assumptions, policy and threats defined there.

A.RSA-Key-Gen

Since OE.RSA-Key-Gen requires the insecure mode of the RSA Key Generation to be executed in a secure environment, where side-channel attacks are not possible, the assumption is covered by this objective.

6.2 Security Requirements Rationale

6.2.1 Rationale for the security functional requirements

Section 7.2 of the Protection Profile [9] 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 14. 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	FPT_PHP.3 “Resistance to physical attack”
O.Malfunction	FRU_FLT.2 “Limited fault tolerance FPT_FLS.1 “Failure with preservation of secure state”

Objective	TOE Security Functional Requirements
O.Phys-Manipulation	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 Note 14 below (for aspects concerning the software RNG)

Note 14. O.RND has been extended if compared to the PP [9] 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[DET]) have been added. The explanation following Table 16 describes 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 15. Mapping of SFRs to Security Objectives in the Hardware ST

Objectives	TOE Security Functional Requirements
O.HW_DES3	FCS_COP.1[DES]
O.HW_AES	FCS_COP.1[AES]
O.MF_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

Objectives	TOE Security Functional Requirements
O.SFR_ACCESS	FDP_ACC.1[SFR] FDP_ACF.1[SFR] FMT_MSA.3[SFR] FMT_MSA.1[SFR] FMT_SMF.1
OE.Check-Init	Not applicable

The rationales for the mappings in Table 15 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 16. Mapping of SFRs to Security Objectives in this ST

Objectives	TOE Security Functional Requirements
O.AES	FCS_COP.1[SW-AES] FDP_IFC.1 FDP_ITT.1 FPT_ITT.1 FPT_FLS.1 FRU_FLT.2
O.DES3	FCS_COP.1[SW-DES] FDP_IFC.1 FDP_ITT.1 FPT_ITT.1 FPT_FLS.1 FRU_FLT.2
O.RSA	FCS_COP.1[RSA_encrypt] FCS_COP.1[RSA_sign] FDP_IFC.1 FDP_ITT.1 FPT_ITT.1 FPT_FLS.1 FRU_FLT.2
O.RSA_PubKey	FCS_COP.1[RSA_public] FDP_IFC.1 FDP_ITT.1 FPT_ITT.1 FPT_FLS.1 FRU_FLT.2
O.RSA_KeyGen	FCS_CKM.1[RSA] FDP_IFC.1 FDP_ITT.1 FPT_ITT.1 FPT_FLS.1 FRU_FLT.2
O.ECC	FCS_COP.1[ECC_GF_p] FCS_COP.1[ECC_ADD] FDP_IFC.1 FDP_ITT.1 FPT_ITT.1

Objectives	TOE Security Functional Requirements
	FPT_FLS.1 FRU_FLT.2
O.ECC_DHKE	FCS_COP.1[ECC_DHKE] FDP_IFC.1 FDP_ITT.1 FPT_ITT.1 FPT_FLS.1 FRU_FLT.2
O.ECC_KeyGen	FCS_CKM.1[ECC_GF_p] FDP_IFC.1 FDP_ITT.1 FPT_ITT.1 FPT_FLS.1 FRU_FLT.2
O.SHA	FCS_COP.1[SHA] FDP_IFC.1 FDP_ITT.1 FPT_ITT.1 FPT_FLS.1 FRU_FLT.2
O.COPY	FDP_ITT.1[COPY] FPT_ITT.1[COPY]
O.REUSE	FDP_RIP.1 FCS_CKM.4
O.RND	FCS_RNG.1[DET] plus those for O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced: FDP_ITT.1 FPT_ITT.1 FDP_IFC.1 FPT_PHP.3 FRU_FLT.2 FPT_FLS.1
OE.Plat-Appl	Not applicable
OE.Resp-Appl	Not applicable
OE-Process-Sec-IC	Not applicable

The justification of the security objectives **O.AES, O.DES3, O.RSA, O.RSA_PubKey, O.RSA_KeyGen, O.ECC, O.ECC_DHKE, O.ECC_KeyGen and O.SHA** are all as follows:

- Each objective is directly implemented by a single SFR specifying the cryptographic service that the objective wishes to achieve (see the above table for the mapping).
- In addition, some requirements that originally were taken from the Protection Profile [9] and thus were also part of the Security Target of the hardware (chip) evaluation support the objective:
  - FRU_FLT.2 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.
  - If the TOE is used outside these specified operating conditions, FPT_FLS.1 ensures that the TSF preserve a secure state, thereby preventing attacks. According to item (ii) of FPT_FLS.1, a secure state is also entered when DFA attacks are detected.
  - FDP_ITT.1 (for the User Data) and FPT_ITT.1 (for the TSF Data) ensure that no User Data (plain text data, keys) or TSF Data are 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.
  - Finally, FDP_IFC.1 also supports this aspect (confidentiality of User Data and TSF Data) 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.COPY** is as follows:

- According to O.COPY, the secure copy routine shall avert certain kinds of side channel analysis that threaten data confidentiality by implementing countermeasures. This applies to both user data and TSF data. The requirements FDP_ITT.1[COPY] and FPT_ITT.1[COPY] exactly require this by enforcing, that the disclosure of user data (FDP_ITT.1[COPY]) or TSF data (FPT_ITT.1[COPY]) is prevented during transmission between separate parts of the TOE. Therefore these requirements are suitable to meet the objective O.COPY.

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 on SmartMX 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. (a) Ensured cryptographic quality (sufficient entropy part) of generated random numbers is met by FCS_RNG.1.1[DET] through the characteristic 'deterministic' and the random number generator meeting ANSI X9.17 (FCS_RNG.1.2[DET]). Ensured cryptographic quality (not predictable part) of generated random numbers is met by FCS_RNG.1[DET] through the characteristic 'chi-squared test of the seed generator'

and FCS_RNG.1 from the certified hardware platform.
(b) Information about the generated random numbers is not available to an attacker is met through the security functional requirements (), 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.

6.2.2 Extended requirements

This Security Target does not define any extended requirements. The PP [9] contains extended functional requirements, that are explained in the rationale of the PP (see [9], section 5).

6.2.3 Dependencies of security requirements

The dependencies of all security requirements are met.

6.2.4 Rationale for the Assurance Requirements

The selection of assurance components is generally based on EAL5 and the underlying Protection Profile [9]. The Security Target uses EAL5 and the same augmentations as the PP.

EAL5 was chosen to provide an even stronger baseline of assurance than the EAL4 in the Protection Profile. The rationale for the augmentations over and above EAL5 is the same as in the PP.

6.3 Conformance Claim Rationale

According to chapter CC Conformance and Evaluation Assurance Level this Security Target claims conformance to the Protection Profile [9].

As shown in 1.4 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 [9] and therefore the TOE type is consistent.

7. Annexes

7.1 Further Information contained in the PP

The Annex of the Protection Profile ([9], 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 7.2 of the PP is concerned with security aspects of the Smartcard Embedded Software (further information regarding A.Resp-Appl and examples of specific Functional Requirements for the Smartcard Embedded Software). Section 8.3 of the PP gives examples of Attack Scenarios.

7.2 Glossary and Vocabulary

Note: To ease understanding of the used terms the glossary of the Protection Profile [9] 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.
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 finalising the IC Embedded Software and the applications on platform transforming the TOE into the unpersonalised 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 Personaliser (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 five modes, the Boot Mode, Test Mode, Mifare Mode, System Mode and User Mode.
End-consumer	User of the Composite Product in Phase 7.
Exceptions 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, unauthorised system calls, User Mode execution of RETI instruction and .
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.
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 Soft-ware).
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.
Initialisation Data	Initialisation 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 the RAM, ROM and EEPROM. The mapping is determined by (a) the memory partition and (b) the memory segments in User Mode. Up to 64 memory segments are supported for the User Mode, whereas the memory partition is fixed. Each segment can be individually (i) positioned and sized (ii) enabled or disabled, (iii) controlled by access permissions for read, write and execute and (iv) assigns access rights for "Special Function Registers related to hardware components" for code executed in User Mode from this segment.
Memory Segment	Address spaces provided by the Memory Management Unit based on its configuration (the MMU segment table). The memory segments define which memory areas are accessible for code running in User Mode. They are located in RAM, ROM and EEPROM.

MIFARE	Contact-less smart card interface standard, complying with ISO14443A.
Mifare Mode	CPU mode of the TOE dedicated for the execution of IC Dedicated Support Software, i.e. the MIFARE Operating System. This mode is not accessible for the Smartcard Embedded Software.
MMU segment table	This structure defines the segments that the Memory Management Unit will used for code running in User Mode. The structure can be located anywhere in the available memory for System Mode code. It also contains access rights for “Special Function Registers related to hardware components” for User Mode code.
Pre-personalisation 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 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 beconsidered 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
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 FameXE co-processor for basic arithmetic functions to perform asymmetric cryptographic algorithms, the random numbers generator and chip configuration.
Security Row	Top-most 128 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 Mifare 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	Data 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 specific circuitry, in non-volatile programmable memories (for instance E2PROM) or a combination thereof.
User Mode	The User Mode has access to the memories under control of the Memory Management Unit. The access to the Special Function Registers is limited.
User Data	All data managed by the Smartcard Embedded Software in the application context. User data comprise all data in the final Smartcard IC except the TSF data.

8. Bibliography

8.1 CC + CEM

[1] **Common Criteria for Information Technology Security Evaluation** – Part 1: Introduction and general model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001

[2] **Common Criteria for Information Technology Security Evaluation** – Part 2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002

[3] **Common Criteria for Information Technology Security Evaluation** – Part 3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003

[4] **Common Criteria for Information Technology Security Evaluation** – Evaluation methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004

8.2 AIS

[5] **Bundesamt für Sicherheit in der Informationstechnik (BSI):** *AIS20: Anwendungshinweise und Interpretationen zum Schema (AIS), Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren (AIS20)*, Version 1, December 2nd, 1999

[6] **Bundesamt für Sicherheit in der Informationstechnik (BSI):** *AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren. (AIS31)*, Version 3.1, September 25th, 2001

[7] **Bundesamt für Sicherheit in der Informationstechnik (BSI)**: AIS34: Anwendungshinweise und Interpretationen zum Schema, Evaluation Methodology for CC assurance classes for EAL5+, Version 1, June 1st, 2004

[8] **Bundesamt für Sicherheit in der Informationstechnik (BSI)**: *AIS37: Anwendungshinweise und Interpretationen zum Schema: Terminologie und Vorbereitung von Smartcard-Evaluierungen*, Version 1.00, July, 29th, 2002

8.3 Hardware-related documents

[9] **Bundesamt für Sicherheit in der Informationstechnik (BSI):** Security IC Platform Protection Profile, Version 1.0, 15.06.2007; Registered and Certified by Bundesamt für Sicherheit in der Informati-onstechnik (BSI) under the reference BSI-PP-0035

[10] **NXP Semiconductors Documentation**: *Security Target Lite – P5Cx128V0A/P5Cx145V0A, MSO, BSI-DSZ-CC-0645*, Version 1.6, June 7th, 2010

[11] **Guidance, Delivery and Operation Manual NXP Secure Smartcard Controllers P5Cx128V0A/P5Cx145V0A, MSO**, Revision 1.4, January 25th, 2011 Document-ID 185114

[12] **NXP Semiconductors Data Sheet P5Cx128/P5Cx145 family;** *Secure dual interface and contact PKI smart card controller*, Revision 3.2, January 25th, 2011, Document-ID 177932

[13] **NXP Semiconductors Documentation**: *Instruction Set SmartMX-Family*, Secure Smart Card Controller, Objective Specification, Revision 1.1, July 4th, 2006, Document Number: 084111

8.4 Documents related to the crypto library

[14] **NXP Semiconductors User Guidance**: *Secured Crypto Library on the P5Cx128/P5Cx145 family*, Revision 1.2, February 3rd, 2011

[15] **NXP Semiconductors User Guidance**: *Secured Crypto Library on the SmartMX – Pseudo Random Number Generator & Chi-Squared Test Library*, Revision 5.0, August 24th, 2007

[16] **NXP Semiconductors User Guidance**: *Secured Crypto Library on the SmartMX – Secured AES Library,* Revision 1.2, August 19th, 2010

[17] **NXP Semiconductors User Guidance**: *Secured Crypto Library on the SmartMX – Secured DES Library,* Revision 3.0, August 24th, 2007

[18] **NXP Semiconductors User Guidance**: *Secured Crypto Library on the SmartMX – SHA Library*, Revision 4.1, June 12th, 2008

[19] **NXP Semiconductors User Guidance**: *Secured Crypto Library on the SmartMX – Secured RSA Library*, Revision 4.5, April 15th, 2010

[20] **NXP Semiconductors User Guidance**: *Secured Crypto Library on the SmartMX – Secured RSA Key Generation Library*, Revision 4.3, March 30th, 2010

[21] **NXP Semiconductors User Guidance**: *Secured Crypto Library on the SmartMX – Secured ECC Library*, Revision 1.4, March 30th, 2010

[22] **NXP Semiconductors User Guidance**: *Secured Crypto Library on the SmartMX – Utility Library*, Revision 1.0, August 24th, 2007

8.5 Standards and text books

[23] **Bruce Schneier**: *Applied Cryptography*, Second Edition, John Wiley & Sons, Inc., 1996

[24] **Menezes, A; van Oorschot, P. and Vanstone, S.:** *Handbook of Applied Cryptography*, CRC Press, 1996, http://www.cacr.math.uwaterloo.ca/hac/

[25] **ISO/IEC 9796-2**: *Information technology – Security techniques – Digital Signature schemes giving message recovery* – Part 2: Integer Factorization based mechanisms**,** 2002

[26] **ISO/IEC 9797-1**: *Information technology – Security techniques – Message Authentication* – Part 1: Mechanisms using a block cipher**,** 1999

[27] **ISO/IEC 15946-1**: *Information technology – Security techniques – Cryptographic techniques based on elliptic curves* – Part 1: General**,** 2003

[28] **ISO/IEC 14888-3**: *Information technology – Security techniques* – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms, 2008

[29] **ISO/IEC 11770-3**: *Information technology – Security techniques* – Key management – Part 3: Mechanisms using asymmetric techniques, 2008

[30] **FIPS PUB 46-3**, *Data Encryption Standard*, Federal Information Processing Standards Publication, October 25th, 1999, US Department of Commerce/National Institute of Standards and Technology

[31] **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

[32] **American National Standard**: *Triple data encryption algorithm modes of operation, ANSI X9.52*, November 9th, 1998

[33] **FIPS PUB 180-3**, Secure Hash Standard, Federal Information Processing Standards Publication, October 2008, US Department of Commerce/National Institute of Standards and Technology

[34] **FIPS PUB 197**, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26th, 2001, US Department of Commerce/National Institute of Standards and Technology

[35] **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. 19", p. 426, February 4th, 2010

[36] **FIPS PUB 186-3,** Digital Signature Standard (DSS). June 2009. U.S. Department of Commerce/National Institute of Standards and Technology

[37] **ECC Brainpool** Standard Curves and Curve Generation, v. 1.0, 19.10.2005

9. Legal information

9.1 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.

9.2 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.

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 medical, military, aircraft, space or life support equipment, nor in applications where failure or malfunction of a NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors accepts 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.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on a weakness or default in the customer application/use or the application/use of customer's third party customer(s) (hereinafter both referred to as "Application"). It is customer's sole responsibility to check whether the NXP Semiconductors product is suitable and fit for the Application planned. Customer has to do all necessary testing for the Application in order to avoid a default of the Application and the product. NXP Semiconductors does not accept any liability in this respect.

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 national authorities.

9.3 Licenses

ICs with DPA Countermeasures functionality

NXP ICs containing functionality implementing countermeasures to Differential Power Analysis and Simple Power Analysis are produced and sold under applicable license from Cryptography Research, Inc.

9.4 Trademarks

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

10. Contents

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

Date of release: 17 February 2011