Crypto Library V2.2 on P5CC037V0A

Security Target Lite

Rev. 1.4 — 10 May 2010 **Evaluation documentation**

Accepted **PUBLIC INFORMATION**

BSI-DSZ-CC-0612

Document information

Info	Content
Keywords	Security Target, Crypto Library, P5CC037V0A
Abstract	Security Target for the Crypto Library V2.2 on P5CC037V0A 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
1.0	08-Jul-2008	Derived from Security Target, no changes
1.1	29-Oct-2008	Added for insecure mode of RSA Key Generation: • Assumption A.RSA-Key-Gen • Security Objective OE.RSA-Key-Gen • Security Requirement RE.RSA-Key-Gen • Mapping of A.RSA-Key-Gen in Security Objective Rational (chapter 8.1) • Mapping of OE-RSA-Key-Gen in Security Requirements Rational (chapter 8.2) • Note 8 Updated RSA Key Generation part of chapter 6.1.14 F.LOG Set correct version of Crypto Library in Table 1
1.2	07-Oct-2009	• Add secure point addition for Elliptic Curves over GF(p) (new SFR FCS_COP.1[ECC_ADD]) • Add usage of ECC Diffie-Hellmann key exchange as secure point multiplication • Update reference to new version of Crypto Library binaries • Updated certification number • Updated key lengths to fulfil SOF:high • Updated reference from FIPS 180-2 to FIPS 180-3 • Update Bibliography • Updated Legal information section
1.3	27-Apr-2010	• Updated TOE name • Update Bibliography • Updated Legal Information section
1.4	10-May-2010	• Restricted DPA resistance of ECC over GF(p) Diffie-Hellman key exchange algorithm • Updated references

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 2.3
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.
SF	Security function.
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.
SOF	Strength of function.
ST	Security Target.
TOE	Target of Evaluation.
TRNG	True Random Number Generator
TSC	TSF Scope of control.
TSF	TOE Security functions.
TSFI	TSF Interface.
TSP	TOE Security Policy.
UART	Universal Asynchronous Receiver and Transmitter.

1. ST Introduction

This chapter is divided into the following sections: “ST Identification”, “ST Overview” and “Specific Issues of Smartcard Hardware and the Common Criteria”.

1.1 ST Identification

This Security Target is for the Common Criteria evaluation of the “Crypto Library V2.2 on P5CC037V0A” provided by NXP Semiconductors, Business Unit Identification.

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

The TOE is a composite TOE, consisting of:

- The hardware “NXP SmartMX P5CC037V0A Secure Smart Card Controller”, which is used as evaluated platform.
- The “Crypto Library V2.2 on P5CC037V0A”, which is built upon this platform.

This Security Target builds on the Hardware Security Target [10], which refers to the “NXP P5CC037V0A Secure Smart Card Controller” provided by NXP Semiconductors, Business Unit Identification.

1.2 ST Overview

1.2.1 Introduction

The Hardware Security Target [10] contains, in section 1.2.1 “ST Overview - Introduction”, 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 Crypto Library on SmartMX provides the security functionality listed below in addition to the functionality described in the Hardware Security Target [10] for the hardware platform:

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 5.1.1.1.
- 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 1.2.2 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 the Life Cycle Model as defined in 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 "**Bundesamt für Sicherheit in der Informationstechnik (BSI)**: *Smartcard IC Platform Protection Profile (SSVG-PP)*, Version 1.0, July 2001; registered and certified by (BSI) under the reference BSI-PP-0002-2001" and the Hardware Security Target [10]. This additional functionality is added using the policy "P.Add-Func" (see section 3.4 of this Security Target).

1.3 CC Conformance and Evaluation Assurance Level

The evaluation is based upon:

- **Common Criteria for Information Technology Security Evaluation** – Part1: Introduction and general model, Version 2.3, August 2005, CCMB-2005-08-001, [1]
- **Common Criteria for Information Technology Security Evaluation** – Part2: Security functional requirements, Version 2.3, August 2005, CCMB-2005-08-002, [2]
- **Common Criteria for Information Technology Security Evaluation** – Part3: Security assurance requirements, Version 2.3, August 2005, CCMB-2005-08-003, [3]

For the evaluation the following methodology will be used:

- **Common Methodology for Information Technology Security Evaluation** – Evaluation Methodology, Version 2.3, August 2005, CCMB-2005-08-004, [4]

The chosen level of assurance is **EAL 5 augmented**. The minimum strength level for the TOE security functional requirements is **SOF-high (Strength of function high)**.

The augmentations chosen are:

- ALC_DVS.2,
- AVA_MSU.3, and
- AVA_VLA.4.

This Security Target claims the following CC conformances:

- Part 2 extended, Part 3 conformant, EAL 5 augmented
- Conformance to the Protection Profile "**Bundesamt für Sicherheit in der Informationstechnik (BSI)**: *Smartcard IC Platform Protection Profile (SSVG-PP)*, Version 1.0, July 2001; registered and certified by (BSI) under the reference BSI-PP-0002-2001", [9] (see also section 7.1)

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 all augmentations claimed in this Security Target are covered also by the evaluation of the hardware platform (refer to the Hardware Security Target [10]).

2. TOE Description

This chapter is divided into the following sections: “TOE Definition” and “Further Definition and Explanations”. TOE Definition has the sub-sections “Hardware Description”, “Software Description”, “Interface of the TOE”, “Life Cycle and Delivery of the TOE”, “TOE Intended Usage”, “TOE User Environment” as well as “General IT features of the TOE”.

2.1 TOE Definition

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

- The hardware part consists of the NXP P5CC037V0A 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 V2.2 on P5CC037V0A” 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:

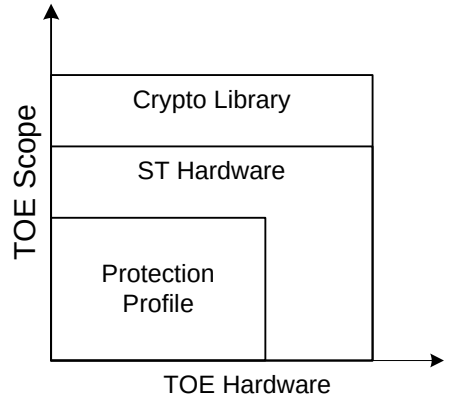


Fig 1. Scope of the Security Target

1. The Protection Profile “**Bundesamt für Sicherheit in der Informationstechnik (BSI)**: *Smartcard IC Platform Protection Profile (SSVG-PP)*, Version 1.0, July 2001; registered and certified by (BSI) under the reference BSI-PP-0002-2001” 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	2.2	25 November 2008	Electronic file
Documents	Guidance Documents [14]-[21]	See reference list	See reference list	Electronic Document

2.1.1 Hardware Description

The NXP SmartMX hardware is described in section 2.1.1 “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 2.1.2 “Software Description” of the Hardware Security Target [10].

2.1.2 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 the “Crypto Library on SmartMX“ (or parts thereof[1]) and this Crypto Library (or parts thereof) is part of the TOE.

The Crypto Library provides DES[2,3], Triple-DES (3DES), RSA, RSA key generation, RSA public key computation, ECC over GF(p), 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.

The TOE supports various key sizes for RSA up to a limit of 5024 bits. Conformance with the evaluation requirement Strength of Function: High requires a minimum key size of 1536 bits.

The TOE supports various key sizes for ECC over GF(p) up to a limit of 544 bits. Conformance with the evaluation requirement Strength of Function: High requires a minimum key size of 192 bits.

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. DES and Triple-Des can be used in ECB, CBC or CBC-MAC mode.
3. Conformance with the evaluation requirement Strength of Function: High means that Single-DES encryption or decryption operations are not in the scope of the SOF rating and should not be used by a user of the TOE for encryption of sensitive information. See also Note 7 in section 5.1.1.1.

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.

2.1.3 Documentation

The documentation for the NXP SmartMX hardware is described in section 2.1.3 “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).

2.1.4 Interface of the TOE

The interface to the NXP SmartMX hardware is described in section 2.1.4 “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.

2.1.5 Life Cycle and Delivery of the TOE

The life cycle and delivery for the NXP SmartMX hardware is described in section 2.1.5 “Life Cycle and Delivery of the TOE” 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 the Life Cycle Model as defined in 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.

2.1.6 TOE Intended Usage

Regarding to phase 7 (for a definition of the Phases refer to the Life Cycle Model as defined in 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 2.1.6 “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.

2.1.7 TOE User Environment

The user environment for the NXP SmartMX hardware is described in section 2.1.7 “TOE User Environment” of the Hardware Security Target [10]. This description is also valid for this composite TOE and is not restricted by the Crypto Library on SmartMX.

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

2.1.8 General IT features of the TOE

The general features of the NXP SmartMX hardware are described in section 2.1.8 “General IT Features of the TOE” of the Hardware Security Target [10]. These are supplemented for the TOE by the functions listed in section 1.2.1 of this Security Target.

2.2 Further Definitions and Explanations

Since the Security Target claims conformance to the PP “**Bundesamt für Sicherheit in der Informationstechnik (BSI)**: *Smartcard IC Platform Protection Profile (SSVG-PP)*, Version 1.0, July 2001; registered and certified by (BSI) under the reference BSI-PP-0002-2001” [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.

3. TOE Security Environment

This Security Target claims conformance to the **Bundesamt für Sicherheit in der Informationstechnik (BSI)**: *Smartcard IC Platform Protection Profile (SSVG-PP)*, Version 1.0, July 2001; registered and certified by (BSI) under the reference BSI-PP-0002-2001 [9]. The Assets, Assumptions, Threats and Organizational Security Policies of the Protection Profile are assumed here, together with extensions defined in sections 3.1 through 3.4 of the Hardware Security Target [10]. In the following sub-sections, only extensions to the different sections are listed. The titles of the chapters that are not extended are cited here for completeness.

3.1 Description of Assets

Since this Security Target claims conformance to the PP "**Bundesamt für Sicherheit in der Informationstechnik (BSI)**: *Smartcard IC Platform Protection Profile (SSVG-PP)*, Version 1.0, July 2001; registered and certified by (BSI) under the reference BSI-PP-0002-2001" [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 an assets in [10]. Since the data computed by the crypto library contains keys, plain text and cipher text that are considered as User Data and e.g. blinding vectors that are considered as TSF data the assets are considered as complete for this Security Target.

3.2 Assumptions

Since this Security Target claims conformance to the PP "**Bundesamt für Sicherheit in der Informationstechnik (BSI)**: *Smartcard IC Platform Protection Profile (SSVG-PP)*, Version 1.0, July 2001; registered and certified by (BSI) under the reference BSI-PP-0002-2001" [9], the assumptions defined in section 3.2 of the Protection Profile, described in section 3.2 "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-Card	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.

3.3 Threats

Since this Security Target claims conformance to the PP "**Bundesamt für Sicherheit in der Informationstechnik (BSI)**: *Smartcard IC Platform Protection Profile (SSVG-PP)*, Version 1.0, July 2001; registered and certified by (BSI) under the reference BSI-PP-0002-2001" [9], the threats defined in section 3.3 of the Protection Profile, described in section 3.3 "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. Now the TOE consists of both hardware (NXP SmartMX) and software (Crypto Library on SmartMX) and the Crypto Library in addition provides random numbers generated by a software (pseudo) random number generator. Therefore the threat T.RND now explicitly includes both deficiencies of hardware random numbers as well as deficiency of software random numbers.

3.4 Organisational Security Policies

Since this Security Target claims conformance to the PP "**Bundesamt für Sicherheit in der Informationstechnik (BSI)**: *Smartcard IC Platform Protection Profile (SSVG-PP)*, Version 1.0, July 2001; registered and certified by (BSI) under the reference BSI-PP-0002-2001" [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 components:

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
- Area based Memory Access Control
- Special Function Register Access Control
- Memory separation for different software parts

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 shall provide the following additional security functionality to the Smartcard Embedded Software:

- Triple-DES[4] 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 6.1.12 F.COPY.

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

4. See also Note 7 in section 5.1.1.1.

4. Security Objectives

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

4.1 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.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]
O.CONFIG	Protection of configuration data	HW-ST [10]

Note 3. Within the Hardware Security Target [10], the objective O.RND has been used in context with the hardware (true) random number generator (RNG). In addition to this, the TOE now 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 0, 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.DES3 The TOE includes functionality to provide encryption and decryption facilities of the Triple-DES algorithm, resistant to attack as described in. (see also Note 7 in section 5.1.1.1).

O.RSA The TOE includes functionality to provide encryption, decryption, signature creation and signature verification using the RSA algorithm, resistant to attack as described 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 described in Table 7.
O.RSA_KeyGen	The TOE includes functionality to generate RSA key pairs, resistant to attack as described 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 described 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 described in Table 7.
O.ECC_KeyGen	The TOE includes functionality to generate ECC over GF(p) key pairs, resistant to attack as described 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.

4.2 Security Objectives for the Environment

The security objectives for the 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 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-TOE	Protection during TOE Development and Production	Phase 2 up to the TOE Delivery at the end of phase 3
OE.Process-Card	Protection during Packaging, Finishing and Personalization	Begin of phase 4 up to the end of phase 6

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 Environment” of the Hardware Security Target [10].

The Hardware Security Target [10] defines, in section 4.2 “Security Objectives for the 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 one additional security objectives for the 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 environment shall ensure that side-channel attacks can not be performed.

5. IT Security Requirements

5.1 TOE Security Requirements

5.1.1 TOE Security Functional Requirements

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

5.1.1.1 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 8.6 [9] (provided by chip HW)
FCS_RND.1	Quality metric for random numbers (used here for random numbers generated by the hardware (true) random number generator; see also FCS_RND.2)	PP [9] Section 8.4, and refined in Hardware ST [10] section 5.1.1.1 “SFRs of the Protection Profile”.
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 8.5 [9] (provided by chip HW)
FMT_LIM.2	Limited availability	PP Section 8.5 [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)
FPT_SEP.1[PP]	TSF domain separation	CC Part 2 [2] (provided by chip HW)

Name	Title	Defined in
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)[5] of secret information during the application of: 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 6.1.12 F.COPY as well as the requirements FDP_ITT.1[COPY] and FPT_ITT.1[COPY] in section 5.1.1.2)[6].

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 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 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 requirement “Failure with preservation of secure state (FPT_FLS.1)” as specified below.

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 DES, 3DES, RSA and ECC over GF(p).*
Dependencies:	ADV_SPM.1 Informal TOE security policy model
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

5. see also Table 7 Algorithm Resistance Overview
6. 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 5.1.1.2), but they still refer to the same information flow control policy, i.e. FDP_IFC.1 is not iterated.

software). The software sensors detect DFA attacks in 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			
DES	Timing	SPA	DPA	DFA
3DES	Timing	SPA	DPA	DFA
RSA encryption, decryption, signature generation and verification	Timing	SPA	DPA	DFA
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 (see Note 9)	n.a.
ECC over GF(p) Key Generation	Timing	SPA	n.a.	n.a.
SHA-1, SHA-224 and SHA-256	-	-	n.a.	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 function 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

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

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 section 5.1.1.2 “Additional SFRs” 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[DES]	Cryptographic operation	CC Part 2 [2], and added to PP in the Hardware ST [10] section 5.1.1.2 “Additional SFRs regarding cryptographic functionality”.
FPT_SEP.1[CONF]	TSF Domain separation	CC Part 2 [2], and added to PP in the Hardware ST [10] section 5.1.1.3 “Additional SFRs regarding protection of configuration data”.
FDP_ACC.1[MEM]	Subset access control	CC Part 2 [2], and added to PP in the Hardware ST [10] section 5.1.1.4 “Additional SFRs regarding access control”.
FDP_ACC.1[SFR]	Subset access control	CC Part 2 [2], and added to PP in the Hardware ST [10] section 5.1.1.4 “Additional SFRs regarding access control”.
FDP_ACF.1[MEM]	Security attribute based access control	CC Part 2 [2], and added to PP in the Hardware ST [10] section 5.1.1.4 “Additional SFRs regarding access control”.
FDP_ACF.1[SFR]	Security attribute based access control	CC Part 2 [2], and added to PP in the Hardware ST [10] section 5.1.1.4 “Additional SFRs regarding access control”.
FMT_MSA.3[MEM]	Static attribute initialization	CC Part 2 [2], and added to PP in the Hardware ST [10] section 5.1.1.4 “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 5.1.1.4 “Additional SFRs regarding access control”.
FMT_MSA.1[MEM]	Management of security attributes	CC Part 2 [2], and added to PP in the Hardware ST [10] section 5.1.1.4 “Additional SFRs regarding access control”.
FMT_MSA.1[SFR]	Management of security attributes	CC Part 2 [2], and added to PP in the Hardware ST [10] section 5.1.1.4 “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 5.1.1.4 “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.

5.1.1.2 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-DES]	Cryptographic operation (TDES)	CC Part 2 [2]; specified in this ST, see below.
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.
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.
FCS_RND.2	Random number generation (used here for random numbers generated by the software (pseudo) random number generator; see also	extension of the family FCS_RND defined in the PP [9], Section 8.4; FCS_RND.2 is defined in section 9.1.1

Name	Title	Defined in
	FCS_RND.1)	
FPT_TST.2	Subset TOE security testing	extension of the family FPT_TST defined in CC Part 2; this extension has been defined in the augmentation paper to the PP [9] and will be repeated below in section 9.1.2

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-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 *Triple-DES in one of the following modes of operation: ECB, CBC or CBC-MAC* and cryptographic key sizes *double-length (112 bit) or triple-length (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 [25], Algorithm 1 (CBC-MAC mode)*.
Application Notes:	(1) The TOE also implements Single-DES, but for Single-DES no claim for SOF: HIGH can be made, therefore Single-DES is not listed here. (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 [25], 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 FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes.

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 *1536 bits to 5024 bits* that meet the following: *PKCS #1, v2.1 (RSAEP, RSADP, RSAES-OAEP)*.
Application Notes:	The TOE also supports key length from 256 to 1535 bit, but for these no claim for SOF: HIGH can be made; therefore keys with at least 1536 bit are listed here.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes.

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 *1536 bits to 5024 bits* that meet the following: *PKCS #1, v2.1 (RSASP1, RSAVP1, RSASSA-PSS)*.
Application Notes:	The TOE also supports key length from 256 to 1535 bit, but for these no claim for SOF: HIGH can be made; therefore keys with at least 1536 bit are listed here.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes.

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 *1536 bits to 2048 bits (Straight Forward) or 1536 to 4096 bits (CRT)* that meet the following: *PKCS #1, v2.1 (RSAEP, RSAVP1)*.
Application Notes:	(1) The TOE also supports key length from 256 to 1535 bit, but for these no claim for SOF: HIGH can be made; therefore keys with at least 1536 bit are listed here. (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 FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes.

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 *192 to 544 bits* that meet the following: *ISO 15946-2*.

Application Notes: The TOE also supports key length from 128 to 191 bit, but for these no claim for SOF: HIGH can be made; therefore keys with at least 192 bit are listed here.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation],
FCS_CKM.4 Cryptographic key destruction,
FMT_MSA.2 Secure security attributes.

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 *192 to 544 bits* that meet the following: *ISO 15946-1*.

Application Notes: The point addition does not have a key. The key size given is related to the length of the supported operand lengths.

The TOE also supports length from 128 to 191 bit, but for these no claim for SOF: HIGH can be made; therefore lengths with at least 192 bit are listed here.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation],
FCS_CKM.4 Cryptographic key destruction,
FMT_MSA.2 Secure security attributes.

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 *192 to 544 bits* that meet the following: *ISO 15946-3.*

Application Notes: (1) The TOE also supports key length from 128 to 191 bit, but for these no claim for SOF: HIGH can be made; therefore keys with at least 192 bit are listed here.

(2) The Diffie-Hellman Key Exchange will result in the generation of a shared secret that could subsequently be used as a cryptographic key for e.g. DES or 3DES. However, to prevent duplication in this ST, this has not been included as a separate FCS_CKM.1 SFR.

(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 FCS_CKM.1 Cryptographic key generation],

	FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes.

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-224 and SHA-256* and cryptographic key size *none* that meet the following: *FIPS 180-3* [33].
Application Notes:	The TOE also supports SHA-1, but for this no claim for SOF: HIGH can be made; therefore only SHA-225 and SHA.256 are listed here.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes.

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 *1536-4096 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 TOE also supports key length from 256 to 1535 bit, but for these no claim for SOF: HIGH can be made; therefore keys with at least 1536 bit are listed here.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes
Note:	The standard “Geeignete Algorithmen” sets up requirements for RSA key generation, if the generated RSA key pair is used in a signature application according to the German Signature Act. This standard is also accepted by the German Bundesamt für Sicherheit in der Informationstechnik (BSI) for Common Criteria evaluations that include the assurance requirements AVA_VLA.4 and AVA_SOF.1 with Strength of function: high.

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 *192-544 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 TOE also supports key length from 128 to 191 bit, but for these no claim for SOF: HIGH can be made; therefore keys with at least 192 bit are listed here.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

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_VLA.4 and AVA_SOF.1 with Strength of function: high.

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.

FCS_RND.2 Random number generation (CC part 2 extended)

The hardware part of the TOE (NXP SmartMX) provides a hardware (true) random number generator (RNG) that fulfils FCS_RND.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_RND.2 (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, as specified in FPT_TST.2 (see below).

Hierarchical to:	No other components.
FCS_RND.2.1	The TSF shall provide a mechanism to generate random numbers that meet the following: *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/ *[23].*
Application Note:	Due to specific characteristics of smart cards (e.g. the lack of real-time clocks), the random number generator does not follow this standard [23] completely, but is rather implemented based on this standard. Wherever the TOE implementation deviates from the standard [23], this has been done with the intention to enhance the quality of the random number generator even more. The random number generator implementation deviates from the standard [23] in the following details: a) High-quality random numbers from the true (hardware) random number generator are used to seed the pseudo (software) random number generator, not a timestamp as suggested in [23]. b) After each reset of the TOE, the complete internal state is re-seeded. c) After the generation of some random bytes the random number generator is re-seeded with its own output.
Dependencies:	No dependencies.

FPT_TST.2 Subset TOE security testing (CC part 2 extended)

This component addresses the self test of the hardware RNG before it is used. Before the software RNG is initialized (seeded) with random bits from the hardware RNG, an online test is performed to ensure high cryptographic quality of the hardware RNG random bits.

Hierarchical to:	No other components.
FPT_TST.2.1	The TSF shall run a suite of self tests *at the request of the authorised user*[8] to demonstrate the correct operation of *the hardware RNG (F.RNG)*[9].
Dependencies:	FPT_AMT.1
Application Note:	The authorized user is the technical user of the Crypto Library (typically this will be the Smartcard Embedded Software). The (assigned) mechanism to be tested here is the hardware RNG (F.RNG). The hardware RNG is used to seed the software RNG (F.RNG_Access), and therefore the test has to be

8. selection: during initial start-up, periodically during normal operation, at the request of the authorised user, and/or at the conditions ...
9. assignment: functions and/or mechanisms

performed in advance: Since it is absolutely necessary to guarantee the quality of the seed, a suitable online test has to be performed before the seeding, i.e. the suite of self tests is an appropriate online test. Since the Crypto Library is not invoked automatically at start-up, the operating system has to ensure that the test routine is called before seed from the hardware RNG is taken for the software RNG, i.e. before the software RNG is initialized. This is what is intended by "at the request of the authorized user".

Note:	The hardware RNG seeds the software RNG implemented as part of the Crypto Library on SmartMX, if the test succeeded (as part of security function 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.

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*[10] to prevent the *disclosure*[11] of user data when it is transmitted between physically-separated parts of the TOE.
Refinement:	The different memories of the TOE 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 protects these data's confidentiality against certain kinds of side channel attacks. The Data Processing Policy is defined in the PP [9], section 5.1.1, paragraph 156.
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

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

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[12] when it is transmitted between separate parts of the TOE.
Refinement:	The different memories of the TOE are seen as separate parts of the TOE. The TSF shall provide a secure copy routine that copies blocks of data in a way that protects these data's confidentiality against certain kinds of side channel attacks. The Data Processing Policy is defined in the PP [9], section 5.1.1, paragraph 156.
Dependencies:	No dependencies.

Note 11. The Protection Profile [9] already includes the functional requirements FDP_ITT.1 and FPT_ITT.1 (see [9], section 5.1.1, paragraphs 153 and 154). 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 both FDP_ITT.1[COPY] and FPT_ITT.1[COPY] refer to the same information flow control policy "Data Processing Policy" as defined in the PP [9], section 5.1.1, paragraph 156. 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).

5.1.1.3 SOF claim for TOE security functional requirements

The required level for the Strength of Function (SOF) of the above listed security functional requirements is "SOF-high".

5.1.2 TOE 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
ACM_AUT.1	Partial CM automation	PP/ EAL5
ACM_CAP.4	Generation support and acceptance procedures	PP/EAL5
ACM_SCP.3	Development tools CM coverage	EAL5
ADO_DEL.2	Detection of modification	PP / EAL5
ADO_IGS.1	Installation, generation, and start-up procedures	PP / EAL5
ADV_FSP.3	Semi-formal functional specification	EAL5
ADV_HLD.3	Semi-formal high-level design	EAL5
ADV_IMP.2	Implementation of the TSF	PP / EAL5

12. selection: disclosure, modification

SAR	Title	Required by
ADV_INT.1	Modularity	EAL5
ADV_LLD.1	Descriptive low-level design	PP / EAL5
ADV_RCR.2	Semiformal correspondence demonstration	PP / EAL5
ADV_SPM.3	Formal TOE Security Policy Model	EAL5
AGD_ADM.1	Administrator Guidance	PP / EAL5
AGD_USR.1	User Guidance	PP / EAL5
ALC_DVS.2	Sufficiency of security measures	PP
ALC_LCD.2	Standardised life-cycle model	EAL5
ALC_TAT.2	Compliance with implementation standards	EAL5
ATE_COV.2	Analysis of coverage	PP / EAL5
ATE_DPT.2	Testing: low-level design	EAL5
ATE_FUN.1	Functional testing	PP / EAL5
ATE_IND.2	Independent testing – sample	PP / EAL5
AVA_CCA.1	Covert Channel analysis	EAL5
AVA_MSU.3	Analysis and testing for insecure states	PP
AVA_SOF.1	Strength of TOE security function evaluation	PP / EAL5
AVA_VLA.4	Highly resistant	PP

5.1.3 Refinements of the TOE Security Assurance Requirements

The ST claims conformance to the Protection Profile "**Bundesamt für Sicherheit in der Informationstechnik (BSI)**: *Smartcard IC Platform Protection Profile (SSVG-PP)*, Version 1.0, July 2001; registered and certified by (BSI) under the reference BSI-PP-0002-2001", 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 5.1.3 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_SCP.3 and ADV_FSP.3).

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.

5.2 Security Requirements for the Environment

This chapter consists of the sections Security Requirements for the IT-Environment and Security Requirements for the Non-IT-Environment.

5.2.1 Security Requirements for the IT-Environment

The crypto library software does not address any of the Security Requirements for the IT environment stated in the Security Target for the Smart Card Controller Hardware. Thus all those requirements (FDP_ITC.1, FCS_CKM.1, FCS_CKM.4, FMT_MSA.2, FMT_SMR.1) remain valid requirements for the IT environment, which is now the CL user. The arguments given in the Hardware Security Target [10] are repeated here briefly:

- There are no Security Requirements for the IT Environment defined in the PP “Smart Card IC Platform Protection Profile” [9]. The dependencies derived from the added security functional requirements for cryptographic operation (FCS_COP.1) and for Management of security attributes (FMT_MSA.1[MEM] and FMT_MSA.1[SFR]) as well as for Static attribute initialization (FMT_MSA.3[MEM] and FMT_MSA.3[SFR]) have been defined as Security Requirements for the IT-Environment in this Security Target, since these requirements must be fulfilled by the implemented Smart Card Embedded Software.
- The dependencies of FCS_COP.1 ([FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4, and FMT_MSA.2) deal with cryptographic key management (CC family FCS_CKM) that is subject to the implemented Smart Card Embedded Software and cannot be provided by the hardware or by the crypto library.
- The dependencies of FCS_CKM.1 ([FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, and FMT_MSA.2) also deal with cryptographic key management, which is subject to the implemented Smart Card Embedded Software and cannot be provided by the hardware or by the crypto library.
- There is one exception, however: The cryptographic RSA and ECC over GF(p) keys that have been generated by the TOE can be used by the TOE, thus the dependency FCS_COP.1 is fulfilled.

  Still it shall be possible for Smartcard Embedded Software using the crypto library TOE to export keys or key parts (FCS_CKM.2). It is up to the Smart Card Embedded Software’s security policy to allow key export. For typical Smartcard Embedded Software at least the public key part of the generated key pair has to be exported; therefore FCS_CKM.2 is listed as a Security Requirement for the IT environment in Table 11 below, but this requirement can be dropped if no keys have to be exported.

  FCS_CKM.4 (cryptographic key destruction) has to be provided by the environment and is therefore listed in Table 11.
- The secure security attributes required by FMT_MSA.2 include adequate key lengths.

  The RSA key generation mechanism supports several key lengths. The Smart Card Embedded Software has to ensure that an RSA key length of 1536 bit or greater is chosen.

  The ECC over GF(p) key generation mechanism supports several key lengths. The Smart Card Embedded Software has to ensure that an ECC over GF(p) key length of 192 bit or greater is chosen.
- - The dependency of FMT_MSA.1[MEM] and FMT_MSA.1[SFR] as well as FMT_MSA.3[MEM] and FMT_MSA.3[SFR] is related to security roles (FMT_SMR.1). The security roles may be realized mode-based but the associated identification of the user must be implemented by the Smart Card Embedded Software that also must define the number and behavior of the security roles.

The security requirements for the IT environment that need to be addressed by the Smart Card Embedded Software using the crypto library with the Smart Card Controller are listed in the following Table 11.

Table 11. Security Requirements for the IT Environment

SFR	Name	Note
FDP_ITC.1	Import of user data without security attributes	Any import of user data must be realized by the Smart Card Embedded Software with the use of the related Special Function Register
FCS_CKM.1	Cryptographic key generation	The TOE contains functionality to generate RSA and ECC over GF(p) key pairs. However, the TOE provides also an implementation of the 3DES algorithms for cryptographic operation, for which no direct[13] key generation is implemented. In order to use 3DES, keys have to be generated outside the TOE[14]. Note, that “outside the TOE” means outside the crypto library, but can still be “onboard of the chip card product”, if the Embedded Software (Operating System) implement the corresponding key generation. Although the Random Number Generator can be used to derive random numbers, the generation of keys at least requires Smart Card Embedded Software to access the Random Number Generator several times to create a key.
FCS_CKM.2	Cryptographic key distribution	The TOE contains functionality to generate RSA and ECC over GF(p) key pairs (FCS_CKM.1). These keys can either be used inside the TOE or may be exported (depending on the security policy of the operating system and application, respectively). If keys shall be exported, a dependency FCS_CKM.2 arises, which has to be fulfilled by the IT environment.
FCS_CKM.4	Cryptographic key destruction	Keys can be deleted only by the Smart Card Embedded Software. This includes key pairs (or parts of key pairs) generated by the RSA and ECC over GF(p) key generation functionality.
FMT_MSA.2	Secure security attributes	The security attributes must be defined and assigned by the Smart Card Embedded Software. This includes adequate key lengths.
FMT_SMR.1	Security roles	The hardware provides different modes that shall be used by the Smart Card Embedded Software to realize the required security roles.

Note 12. The dependencies of FCS_COP.1 deal with cryptographic key management (CC family FCS_CKM) that is subject to the (operating system and) applications and cannot be provided by the crypto library.

According to the dependencies defined for FCS_COP.1, at least one of the two requirements FDP_ITC.1 and FCS_CKM.1 has to be fulfilled – either the keys used for the cryptographic algorithms have to be generated inside the TOE

13. There is an “indirect” key generation through the use of the Diffie-Hellman Key Exchange (FCS_COP.1[ECC-DHKE])

14 . Or the Diffie-Hellman Key Exchange has to be used. See the previous footnote.

(FCS_CKM.1) or they have to be loaded from the outside (FDP_ITC.1). The crypto library allows both: For RSA and ECC over GF(p) key pairs, the TOE provides key generation functionality. However, for the cryptographic algorithm Triple-DES, such functionality is not part of the TSF (except through the Diffie-Hellman Key Exchange). And even for the RSA and ECC over GF(p) it shall be possible to use key pairs that have been loaded from outside the TOE.

Since the security policy of the application determines, how this dependency will be fulfilled, both FDP_ITC.1 and FCS_CKM.1 are listed as Security Requirements for the IT-Environment. Depending on the application's security policy, these dependencies may or may not exist for a given product.

A similar situation exists for FCS_CKM.1 (RSA key pair generation and ECC over GF(p) key pair generation): At least one of the two dependent requirements FCS_COP.1 or FCS_CKM.2 has to be fulfilled.

Note 13. To be exact, the requirements [FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4 and FMT_MSA.2 have to be iterated multiple times in order to fulfill the dependencies for the various FCS_COP.1 iterations. For better readability, the iterations have not been written down explicitly.

Note 14. The operations of the Security Requirements for the IT-Environment have not been performed in this Security Target for the following reasons:

The crypto library is a general purpose library that can be used for a variety of Smart Card Embedded Software. The library itself does not impose any obligations that would lead to restrictions in the possible values for the operations.

The final values to be chosen for the operations will depend on the Smart Card Embedded Software context.

5.2.2 Security Requirements for the Non-IT-Environment

The Security Requirements for the Non-IT Environment are those detailed in section 5.2.2 "Security Requirements for the Non-IT Environment" of the Hardware Security Target [10], but with RE.RNG modified to RE.RNG2). The following table lists these requirements.

Table 12. Security Requirements for the Non-IT Environment

Requirement	Defined in
RE.Phase-1	PP [9]
RE.Process-Card	PP [9]
RE.Cipher	Hardware ST [10]
RE.RNG2	This ST Note: RE.RNG has been defined in the Hardware ST [10].
RE.Check-Init	Hardware ST [10]

The requirement RE.RNG from the Hardware ST has been addressed by the TOE: The Crypto Library implements test routines for the hardware RNG (see FPT_TST.2). The only requirement that is still left over to the environment is the requirement that these test routines have to be called appropriately. For example, the operating system has to call

the corresponding test routines before using random numbers from the hardware RNG. Therefore RE.RNG2 replaces RE.RNG. RE.RNG2 is defined as follows:

RE.RNG2	The Smart Card Embedded Software must ensure that, before using random numbers from the software RNG, the initialization routine for the software RNG is called. This routine performs an online test of the hardware RNG and uses the tested hardware RNG to seed the software RNG. The software random number generator uses an internal XRAM buffer. The Smartcard Embedded Software must ensure that this buffer is only read or written by the Crypto Library during the usage of the Crypto Library, i.e. beginning with the test of the hardware random number and ending with the last call of any routine of the Crypto Library.

Note 15. Depending on the usage of the hardware RNG, the test routines offered by the Crypto Library have to be called appropriately. The requirements for testing the random numbers provided by the random number generator are given by the AIS31 [6] and are described in the Guidance, Delivery and Operation Manual for the NXP SmartMX Secure Smart Card Controller [11]. Whenever the seed of the software RNG is deleted, invalidated or read/written by routines that are not part of the crypto library, e.g. by a reset, the operating system has to ensure that the software RNG is initialized again.

This Security Target defines one additional security requirements for the non-IT environment.

RE.RSA-Key-Gen	When executing the RSA Key Generation in the insecure mode and side-channel resistance is needed, the environment has to ensure that side-channel attacks can not be performed. This could be reached by operating the smart card in a secure environment like during personalisation.

6. TOE Summary Specification

This chapter is divided into the sections “IT Security Functions” and “Assurance Measures”.

6.1 IT Security Functions

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 6.1 “TOE Security Functions” of the Hardware Security Target [10]). The functionality of the hardware platform is listed in the following table; the new security functionality of the cryptographic library is described in the following sub-sections.

Table 13. IT security functions defined in the Hardware Security Target [10]

Name	Title
F.RNG	Hardware Random Number Generator
F.HW_DES	Hardware Triple-DES Co-processor
F.OPC	Control of Operating Conditions
F.PHY	Protection against Physical Manipulation
F.LOG	Logical Protection
F.COMP	Protection of Mode Control
F.MEM_ACC	Memory Access Control
F.SFR_ACC	Special Function Register Access Control

Note 16. The security function F.RNG implements the hardware RNG. The TOE also implements a software RNG as part of security function F.RNG_Access; for details see section 6.1.10. 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 17. The security function F.LOG is extended by the crypto library TOE as described in section 6.1.13 (see below).

The IT security functions directly correspond to the TOE security functional requirements defined in section 5.1.1 above. The definitions of the IT security functions refer to the corresponding security functional requirements.

6.1.1 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**: *Information technology – Security techniques –*

Message Authentication – Part 1: Mechanisms using a block cipher**,** 1999 [25], Algorithm 1, or **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 [31], Appendix F). Like ECB and CBC, the CBC-MAC mode of operation can also be applied to both DES or 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 SOF claim for this evaluation (see also Note 7 in section 5.1.1.1).

F.DES is a modular basic cryptographic function which provides the DES algorithm as defined by the standard **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 [30], and supports the 2-key and 3-key Triple-DES algorithm according to the **American National Standard**: *Triple data encryption algorithm modes of operation, ANSI X9.52*, November 9th, 1998 [32].

The interface to F.DES allows to perform 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 [16]. 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 function is discussed in section 6.1.13 F.LOG.

6.1.2 F.RSA_encrypt

The TOE provides functions that implement the RSA algorithm for data encryption and decryption. This IT security function 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. Note that, for the evaluated TOE, RSA keys must have a key length of at least 1536 bit.

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 function is discussed in section 6.1.13 F.LOG.

6.1.3 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 function 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. Note that, for the evaluated TOE, RSA keys must have a key length of at least 1536 bit.

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 function is discussed in section 6.1.13 F.LOG.

6.1.4 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 *1536 bits to 2048 bits (Straight Forward) or from 1536 to 4096 bits (CRT)*. Note that if the TOE uses the generated key pair later on, RSA keys must have a key length of at least 1536 bit.

Sidechannel attack resistance for this security function is discussed in section 6.1.13 F.LOG.

6.1.5 F.ECC_GF_p_ECDSA

The TOE provide functions to perform ECC Signature Generation and Signature Verification according to ISO/IEC 15946-2 section 6.

Note that hashing of the message must be done beforehand and is not provided by this security function, 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. Note, for evaluation of the TOE, ECC over GF(p) keys must have a minimum key length of 192 bits.

Sidechannel attack resistance for this security function is discussed in section 6.1.13 F.LOG.

6.1.6 F.ECC_GF_p_DH_KeyExch

The TOE provides functions to perform Diffie-Hellman Key Exchange according to ISO 15946-3 section 8.4. This interface can also be used as secure point mulriplication.

The supported key length is 128 bits to 544 bits. Note, for SOF-high, ECC over GF(p) keys must have a minimum key length of 192 bits.

Sidechannel attack resistance for this security function is discussed in section 6.1.13 F.LOG.

6.1.7 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. Note that, for the evaluated TOE, RSA keys must have a key length of at least 1536 bit. 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 function is discussed in section 6.1.13 F.LOG.

6.1.8 F.ECC_GF_p_KeyGen

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

It supports key length from 128 to 544 bits. Note, for SOF-high, ECC over GF(p) keys must have a minimum key length of 192 bits.

Sidechannel attack resistance for this security function is discussed in section 6.1.13 F.LOG.

6.1.9 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].

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.

6.1.10 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 16 above. F.RNG_Access consists of the implementation of the software RNG (FCS_RND.2) and of appropriate online tests (FPT_TST.2) for the hardware RNG:

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/ [23].

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 FPT_TST.2. The interface of F.RNG_Access allows to test the hardware RNG and to seed the software RNG after successful testing.

6.1.11 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.

6.1.12 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 6.1.13 F.LOG.

6.1.13 F.LOG

The IT Security Function 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 5.1.1.1) as well as by FPT_FLS.1 (DFA attacks).

DES

The resistance of DES[15] 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 DES[16] 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 calculating the private 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

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

15. See also Note 7 in section 5.1.1.1.
16. See also Note 7 in section 5.1.1.1.

- 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, except for DPA. This ensures that the function can also be used for secure point multiplication, if DPA like attacks on the point are not possible.

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 RE.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.
- 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. Note, for SOF-high SHA-224 and SHA-256 shall be used.

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

6.1.14 SOF claim

According to the **Common Methodology for Information Technology Security Evaluation** – Evaluation Methodology, Version 2.3, August 2005, CCMB-2005-08-004 [4] a Security Target shall identify all mechanisms, which can be assessed according to the assurance requirement AVA_SOF.1.

The following mechanisms were identified, which can be analyzed for their permutational or probabilistic properties:

- The output of the random number generators (both for the hardware RNG and for the software RNG, i.e. F.RNG and F.RNG_Access) can be analysed with probabilistic methods.
- The quality of the mechanisms contributing to the resistance against leakage attacks of F.LOG can be analysed using probabilistic or permutational methods on power consumption of the TOE.

  The implementations of the functions F.DES, F.RSA_encrypt, F.RSA_sign, F.RSA_public, F.ECC_GF_p_ECDSA, F.ECC_GF_p_KeyGen, F.ECC_GF_p_DH_KeyExch and F.RSA_KeyGen are resistant against Simple Power Analysis (SPA), Differential Power Analysis (DPA), Differential Fault Analysis (DFA) and timing attacks[17],[18]. The quality of these mechanisms against leakage attacks can be analyzed using probabilistic or permutational methods.

  The implementation of the secure copy routine is resistant (F.LOG) against Simple Power Analysis (SPA).
- The implementation of the secure copy routine (F.COPY) includes randomization as a countermeasure. The effectiveness of this countermeasure can be analysed with probabilistic methods.
- The developer does not see SHA-1, SHA-224 or SHA-256 as a cryptographic mechanism in the sense of Common Criteria.

Therefore an explicit SOF claim of “high” is made for these mechanisms.

6.2 Assurance Measures

The underlying hardware of the TOE has already been evaluated. The assurance measures applied for the TOE hardware are described in the Hardware Security Target [10]. All these assurance measures are still valid for the hardware part of this composite TOE.

In addition, the assurance measures applied for the software part of the TOE (the cryptographic library) are documented in the respective documents provided as evaluation evidence during the evaluation. The evaluation process ensures, that evidence is given for all assurance components required by EAL5+. The following table lists all applicable assurance components.

17. See F.LOG for which functions are resistant against which attacks.
18. The underlying cryptographic algorithms can also be analyzed with permutational or probabilistic methods, but this is not in the scope of Common Criteria evaluations.

Table 14. List of documents describing the measures regarding the assurance requirements

Assurance Component	Input evidence according to Common Criteria Part 3 [3]
ACM_AUT.1 ACM_CAP.4 ACM_SCP.3	Configuration Management documentation
ADO_DEL.2 ADO_IGS.1	Documentation on delivery, installation, generation and start-up
ADV_FSP.3	Functional specification (semiformal)
ADV_HLD.3	High-level design (semiformal)
ADV_IMP.2	Implementation representation
ADV_INT.1	Architectural description
ADV_LLD.1	Low level design
ADV_RCR.2	Correspondence analysis (semiformal)
ADV_SPM.3	Formal TSP model
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_DVS.2 ALC_LCD.2 ALC_TAT.2	Life cycle documentation
ATE_COV.2 ATE_DPT.2 ATE_FUN.1 ATE_IND.2	Test documentation
AVA_CCA.1 AVA_MSU.3 AVA_SOF.1 AVA_VLA.4	Vulnerability analysis

7. PP Claims

7.1 PP Reference

This Security Target claims conformance to the following Protection Profile:

Bundesamt für Sicherheit in der Informationstechnik (BSI): *Smartcard IC Platform Protection Profile (SSVG-PP)*, Version 1.0, July 2001; registered and certified by (BSI) under the reference BSI-PP-0002-2001 [9].

The short term for this Protection Profile used in this document is "**Bundesamt für Sicherheit in der Informationstechnik (BSI)**: *Smartcard IC Platform Protection Profile (SSVG-PP)*, Version 1.0, July 2001; registered and certified by (BSI) under the reference BSI-PP-0002-2001".

7.2 PP Refinements

The TOE is a composite TOE, where the underlying hardware has already been evaluated according to the PP [9]. This hardware part of the TOE remains unchanged, and thus almost all security functional requirements remain unchanged if compared to the Hardware Security Target [10].

However, the scope of four TOE Security Functional Requirements (FDP_ITT.1, FPT_ITT.1, FDP_IFC.1 and FPT_FLS.1) has been extended. These requirements asked for leakage protection of the hardware (resistance against SPA, DPA, DFA and Timing attacks). For the composite TOE, this resistance against SPA, DPA, DFA and Timing attacks is also required for the Crypto Library on SmartMX.

Therefore the following components have been refined as compared to the PP [9]:

- FDP_ITT.1, FPT_ITT.1 and FDP_IFC.1

  SPA, DPA and Timing attack resistance is now also required for the cryptographic algorithms implemented by the Crypto Library on SmartMX.

- FPT_FLS.1

  DFA attack resistance is now also required for the cryptographic algorithms implemented by the Crypto Library on SmartMX.

According to CEM [4], ASE_REQ.1-12, paragraph 415 c), components must be "refined in such manner that a TOE meeting the refined requirement also meets the unrefined requirement". This condition is fulfilled for the refinements that have been applied here.

7.3 PP Additions

The TOE is a composite TOE. Compared to the already evaluated part (SmartMX), the addition is constituted by the Crypto Library on SmartMX and its functionality. This involves the

- new Policy "P.Add-Func" (see section 3.4, Organisational Security Policies of this Security Target).

The associated additions (objectives, requirements) are derived from this new policy:

- The additional security objectives have been defined in section 4.1. As section 4.1 clearly lists them as additional, they are not repeated in this section.
- The Security Objective O.RND is extended to include also the software (pseudo) random number generator (see also Note 3).

- The additional SFRs have been defined in Table 9 SFRs defined in this Security Target. As this table clearly lists them as additional, they are not repeated in this section.
- This ST uses additional SARs: EAL5 augmented with ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4 instead of EAL4 augmented with ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4. Since ADV_IMP.2 is in EAL5 this augmentation is also covered.
- This ST has additional FCS_CKM.2 as additional Security Functional Requirements for the IT environment (see also section 5.2.1).

8. Rationale

This chapter contains the following sections: "Security Objectives Rationale", "Security Requirements Rationale", "TOE Summary Specification Rationale" and "PP Claims 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.

8.1 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 PP "**Bundesamt für Sicherheit in der Informationstechnik (BSI)**: *Smartcard IC Platform Protection Profile (SSVG-PP)*, Version 1.0, July 2001; registered and certified by (BSI) under the reference BSI-PP-0002-2001". The following Table 15 reproduces the table in section 7.1 of the PP [9].

Table 15. 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	OE.Process-TOE O.Identification	(Phase 2 – 3)
A.Process-Card	OE.Process-Card	(Phase 4 – 6)
T.Leak-Inherent	O.Leak-Inherent	
T.Phys-Probing	O.Phys-Probing	
T.Malfunction	O.Malfunction	
T.Phys-Manipulation	O.Phys-Manipulation	
T.Leak-Forced	O.Leak-Forced	
T.Abuse-Func	O.Abuse-Func	
T.RND	O.RND	

The following Table 16 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 16. Additional Security Objectives versus Assumptions or Policies

Assumption/Policy	Security Objective	Note
P.Add-Components	O.HW_DES3 O.MF_FW O.MEM_ACCESS O.SFR_ACCESS O.Leak-Inherent	

Assumption/Policy	Security Objective	Note
	O.Phys-Probing O.Malfunction O.Phys-Manipulation O.Leak-Forced	
P.Add-Func	O.DES3 O.RSA O.RSA_PubKey O.RSA_KeyGen O.ECC O.ECC_DHKA 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.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 function 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.

8.2 Security Requirements Rationale

8.2.1 Rationale for the security functional requirements

Section 7.2 of the PP “**Bundesamt für Sicherheit in der Informationstechnik (BSI)**: *Smartcard IC Platform Protection Profile (SSVG-PP)*, Version 1.0, July 2001; registered and certified by (BSI) under the reference BSI-PP-0002-2001” 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 17. Mapping of Security Requirements to Security Objectives in the PP

Objective	TOE Security Functional Requirements	Security Requirements for the environment
O.Leak-Inherent	FDP_ITT.1 “Basic internal transfer protection”	RE.Phase-1 “Design and Implementation of the

Objective	TOE Security Functional Requirements	Security Requirements for the environment
	FPT_ITT.1 “Basic internal TSF data transfer protection” FDP_IFC.1 “Subset information flow control”	Smartcard Embedded Software”
O.Phys-Probing	FPT_PHP.3 “Resistance to physical attack”	RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software”
O.Malfunction	FRU_FLT.2 “Limited fault tolerance FPT_FLS.1 “Failure with preservation of secure state” FPT_SEP.1 “TSF domain separation”	
O.Phys-Manipulation	FPT_PHP.3 “Resistance to physical attack”	RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software” (e.g. by implementing FDP_SDI.1 Stored data integrity monitoring)
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_SEP.1, FPT_PHP.3	RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software”
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, FPT_SEP.1	
O.Identification	FAU_SAS.1 “Audit storage”	
O.RND	FCS_RND.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, FPT_SEP.1 plus: see Note 18 below (for aspects	RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software” (e.g. by implementing FPT_AMT.1 “Abstract machine testing”)

Objective	TOE Security Functional Requirements	Security Requirements for the environment
	concerning the software RNG)	
OE.Plat-Appl		RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software” RE.RNG2 “Design and Implementation of the Smartcard Embedded Software”
OE.Resp-Appl		RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software”
OE.Process-TOE	FAU_SAS.1 “Audit storage”	Assurance Components: refer to below ✸
OE.Process-Card		RE.Process-Card possibly supported by RE.Phase-1

✸ Assurance Components: Delivery (ADO_DEL); Installation, generation, and start-up (ADO_IGS) (using Administrator Guidance (AGD_ADM), User guidance (AGD_USR)); CM automation (ACM_AUT); CM Capabilities (ACM_CAP); CM Scope (ACM_SCP); Development Security (ALC_DVS); Life Cycle Definition (ALC_LCD); Tools and Techniques (ALC_TAT)

Note 18. 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_RND.2, FPT_TST.2) have been added. The explanation following Table 19 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 18. Mapping of SFRs to Security Objectives in the Hardware ST

Objectives	TOE Security Functional Requirements	Security Requirements for the environment
O.HW_DES3	FCS_COP.1[DES]	RE.Phase-1 with RE.Cipher
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	RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software” (e.g. definition of separated memory segments and sufficiently graded exception handling)

Objectives	TOE Security Functional Requirements	Security Requirements for the environment
O.SFR_ACCESS	FDP_ACC.1[SFR] FDP_ACF.1[SFR] FMT_MSA.3[SFR] FMT_MSA.1[SFR] FMT_SMF.1	
O.CONFIG	FPT_SEP.1[CONF]	
OE.Plat-Appl (clarification)		RE.Phase-1 with RE.Cipher and RE.RNG
OE.Resp-Appl (clarification)		RE.Phase-1 with RE.Cipher [FDP_ITC.1 or FCS_CKM.1] FCS_CKM.2 FCS_CKM.4 FMT_MSA.2 FMT_SMR.1
OE.Check-Init		RE.Check-Init

The rationales for the mappings in Table 18 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 19. Mapping of SFRs to Security Objectives in this ST

Objectives	TOE Security Functional Requirements	Security Requirements for the environment
O.DES3	FCS_COP.1[SW-DES] FDP_IFC.1 FDP_ITT.1 FPT_ITT.1 FPT_FLS.1 FRU_FLT.2	RE.Phase-1 with RE.Cipher
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	RE.Phase-1 with RE.Cipher
O.RSA_PubKey	FCS_COP.1[RSA_public] FDP_IFC.1 FDP_ITT.1 FPT_ITT.1 FPT_FLS.1 FRU_FLT.2	RE.Phase-1 with RE.Cipher
O.RSA_KeyGen	FCS_CKM.1[RSA] FDP_IFC.1 FDP_ITT.1 FPT_ITT.1	RE.Phase-1 with RE.Cipher

Objectives	TOE Security Functional Requirements	Security Requirements for the environment
O.ECC	FCS_COP.1[ECC_GF_p] FCS_COP.1[ECC_ADD] FDP_IFC.1 FDP_ITT.1 FPT_ITT.1 FPT_FLS.1 FRU_FLT.2	RE.Phase-1 with RE.Cipher
O.ECC_DHKE	FCS_COP.1[ECC_DHKE] FDP_IFC.1 FDP_ITT.1 FPT_ITT.1 FPT_FLS.1 FRU_FLT.2	RE.Phase-1 with RE.Cipher
O.ECC_KeyGen	FCS_CKM.1[ECC_GF_p] FDP_IFC.1 FDP_ITT.1 FPT_ITT.1	RE.Phase-1 with RE.Cipher
O.SHA	FCS_COP.1[SHA] FDP_IFC.1 FDP_ITT.1 FPT_ITT.1	RE.Phase-1 with RE.Cipher
O.COPY	FDP_ITT.1[COPY] FPT_ITT.1[COPY]	
O.REUSE	FDP_RIP.1	RE.Phase-1
O.RND	FCS_RND.2 „Random number generation“ for the software RNG FPT_TST.2 „Subset TOE security testing“	RE.RNG2
OE.RSA-Key-Gen		RE.RSA-Key-Gen

The justification of the security objective **O.DES3** is as follows:

- O.DES3 requires the TOE to support Triple DES encryption and decryption. Exactly this is the requirement of FCS_COP.1[SW-DES]. Therefore FCS_COP.1[SW-DES] is suitable to meet O.DES3.
- 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 O.DES3: FRU_FLT.2 supports O.DES3 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 O.DES3 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 usage of cryptographic algorithms requires the use of appropriate keys. Otherwise they do not provide security. RE.Cipher requires that keys must be unique with a very high probability, cryptographically strong etc. If keys are imported into the TOE (usually after TOE Delivery), it must be ensured that quality and confidentiality is maintained. RE.Phase-1 requires that the developer of the Smartcard Embedded Software shall use the cryptographic function in a way that only the expected keys are used and that the Modes of the TOE are sufficiently used to ensure OE.Plat-Appl and OE.Resp-Appl. The DES implementation meets the requirement of DFA resistance by checking the correctness of the computation.

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

- The same arguments as stated above for O.DES3 are valid for O.RSA and FCS_COP.1[RSA_sign] and FCS_COP.1[RSA_encrypt], including the arguments given for side channel resistance.

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

- The same arguments as stated above for O.DES3 are valid for O.RSA_PubKey and FCS_COP.1[RSA_sign] and FCS_COP.1[RSA_encrypt], including the arguments given for side channel resistance.

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

- O.RSA_KeyGen requires the TOE to include functionality to generate RSA (and RSA CRT) key pairs. This is exactly the requirement of FCS_CKM.1. Therefore FCS_CKM.1 is suitable to meet O.RSA_KeyGen.
- 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 O.RSA_KeyGen: The resistance against side channel attacks is required by FDP_ITT.1, FPT_ITT.1 and FDP_IFC.1 (and thus these requirements are suitable to meet O.RSA_KeyGen): 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 O.RSA_KeyGen 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.
- When RSA key pairs are generated by the TOE, the keys have to be kept confidential and must not be compromised by the operating system and application. This is required by RE.Cipher. The embedded software shall protect the user data (especially keys) and the embedded software developers must follow the evaluation findings; this is required by RE.Phase-1.
- If keys are imported into the TOE (usually after TOE Delivery), it must be ensured that quality and confidentiality is maintained. RE.Phase-1 requires that the developer of the Smartcard Embedded Software shall use the cryptographic function in a way that only the expected keys are used and that the Modes of the TOE are sufficiently used to ensure OE.Plat-Appl and OE.Resp-Appl.

The justification of the security objective **O.ECC** is identical to the justification of O.DES3 (with the exception that O.ECC is related to FCS_COP.1[ECC_GF_p] and FCS_COP.1[ECC_ADD] instead of FCS_COP.1[SW_DES]).

The justification of the security objective **O.ECC_DHKA** is identical to the justification of O.DES3 (with the exception that O.ECC_DHKA is related to FCS_COP.1[ECC_DHKA] instead of FCS_COP.1[SW_DES]).

The justification of the security objective **O.ECC_KeyGen** is identical to the justification of O.RSA_KeyGen (with the exception that O.ECC is related to FCS_CKM.1[ECC_GF_p] instead of FCS_CKM.1[RSA]).

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

- O.SHA requires the TOE to implement the SHA-1, SHA-224 and SHA-256 hash algorithms. Exactly this is the requirement of FCS_COP.1[SHA]. Therefore FCS_COP.1[SHA] is suitable to meet O.SHA.
- RE.Cipher applies, if SHA-1 is used with secret input data (e.g. for key derivation), thus RE.Cipher is also mapped.

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, 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.

For the objective **O.RND** additional functional requirements have been added (compared to the “Smartcard IC Platform Protection Profile” [9]). The current TOE contains not only a hardware RNG but also a software RNG and it implements test routines for the hardware RNG. In addition to FCS_RND.1 (quality metric for the hardware RNG) the requirements FCS_RND.2 and FPT_TST.2 have been added. The explanation for these requirements is as follows:

- Since the current TOE also contains a software RNG that shall be used by the user of the Crypto Library, the random numbers taken from the software RNG also need to possess certain properties. The functional requirement FCS_RND.2 was defined and has been chosen to ensure that the implementation of the software RNG adheres to the ANSI X9.17 standard. This ensures that an implementation is used which bases upon an approved algorithm. (The evaluation scheme may imply that additional quality metrics have to be applied to ensure high cryptographic quality, e.g. the German AIS20 [5].)
- Before the software RNG can use the hardware RNG to initialize its seed, a suitable test of the hardware RNG has to be performed. Since this test is implemented within

the Crypto Library, i.e. within the TOE, the requirement FPT_TST.2 has been chosen.

- As said before, the crypto library addresses the requirement RE.RNG as defined in the Hardware Security Target by implementing test routines for the random numbers generated by the hardware RNG (FPT_TST.2). But still the user of the Crypto Library (i.e. the operating system) has to invoke the test routines before using the hardware RNG. This requirement has been defined as RE.RNG2 and is left over to the environment. Therefore RE.RNG has been replaced by RE.RNG2 in Table 17 and Table 19. See the discussion on this issue in section 5.2.2 , where the exact definition of “RE.RNG2” is given.
- Taken together, the hardware RNG provides high quality random numbers (FCS_RND.1), the software RNG is seeded with a non-defect hardware RNG (FPT_TST.2+RE.RNG2) and the software RNG is implemented according to a specified standard (FCS_RND.2). Therefore the objective O.RND is met, including both the hardware and the software aspect (refer to Note 3 on O.RND in section 4.1 as well as Note 2 on T.RND in section 0).

The justification of the security objective **OE.RSA-Key-Gen** is as follows:

OE.RSA-Key-Gen requires that the insecure mode of the RSA Key Generation has to be executed in an environment where side-channel attacks cannot be performed. The same is required by the security requirement RE.RSA-Key-Gen.

The justification of the additional security objectives and the additional requirements show that they do not contradict to the rationale already given in the Protection Profile and the HW Security Target for the assumptions, policy and threats defined there.

8.2.2 Explicitly stated TOE security functional requirements

This Security Target defines and uses the following explicitly stated IT security requirements:

- FPT_TST.2 Subset TOE security testing

  The security functional component Subset TOE security testing (FPT_TST.2) has been newly created (Common Criteria Part 2 extended). This component allows that particular parts of the security mechanisms and functions provided by the TOE can be tested after TOE Delivery. This security functional component is used instead of the functional component FPT_TST.1 from Common Criteria Part 2. For the user it is important to know which security functions or mechanisms can be tested. The functional component FPT_TST.1 does not mandate to explicitly specify the security functions being tested. In addition, FPT_TST.1 requires verifying the integrity of TSF data and stored TSF executable code, which might violate the security policy.

  FPT_TST.2 has the same dependencies than FPT_TST.1. If compared to FPT_TST.1, the new component FPT_TST.2 differs in the fact that it allows to explicitly state the function(s) and/or mechanism(s), the correct operation of which is tested. Concerning the applicability and appropriateness of assurance requirements, the evaluation assurance level chosen (EAL5+) will provide enough description of these functions and mechanisms and enough details for evaluators to decide whether self tests are being performed as required. Therefore the assurance requirements are considered as being applicable and appropriate to support the explicitly stated TOE security functional requirement FPT_TST.2 and there is no need to add any further assurance requirements.
- FCS_RND.2 Random Number Generation

The security functional component Random Number Generation (FCS_RND.2) has been newly created (Common Criteria Part 2 extended). It was chosen to define FCS_RND.2 explicitly, because Part 2 of the Common Criteria do not contain generic security functional requirements for Random Number generation. (Note, that there are security functional requirements in Part 2 of the Common Criteria, which refer to random numbers. However, they define requirements only for the authentication context, which is only one of the possible applications of random numbers.) In addition, the conformance to a standard is seen as being not exactly the same as a the fulfilling of a quality metric, therefore FCS_RND.2 has been created in addition to FCS_RND.1 already defined in the PP [9].

Like FCS_RND.1, which has been defined in the Protection Profile [9], FCS_RND.2 has no dependencies. The EAL level chosen (EAL5+) provides enough details to check the conformance to a given standard. The assurance requirements are applicable and appropriate to support the explicitly stated TOE security functional requirement FCS_RND.2, no other assurance requirements have to be specified.

In addition, the PP [9] contains more explicitly stated TOE security functional requirements, that are explained in the rationale of the PP (see [9], section 7.2.1).

8.2.3 Dependencies of security functional requirements

The dependencies listed in the Protection Profile [9] are independent from the additional dependencies listed in the table below. The dependencies of the Protection Profile are fulfilled within the Protection Profile (see [9], section 7.2.2) and at least one dependency is considered to be satisfied.

The following discussion demonstrates how the dependencies defined by Part 2 of the Common Criteria for the requirements specified in section 5.1.1.2 and 5.1.1.3 of the Hardware Security Target [10] as well as those requirements defined in this Security Target are satisfied. Together with the rationale given in the Protection Profile this mapping and the following explanatory text cover all dependencies of this Security Target.

The dependencies defined in the Common Criteria are listed in the table below:

Table 20. Dependencies of security functional requirements

Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
FCS_COP.1 with all iterations	FDP_ITC.1 or FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	Yes (by the environment / FCS_CKM.1 partly fulfilled by the TOE) See also Note 12 in section 5.2.1.
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4 FMT_MSA.2	Yes (by the environment / FCS_COP.1 can be fulfilled by the TOE) Generated keys may be used by the TOE (FCS_COP.1) or may be exported (FCS_CKM.2).
FDP_ACC.1[MEM]	FDP_ACF.1	Yes, by FDP_ACF.1[MEM]
FDP_ACC.1[SFR]	FDP_ACF.1	Yes, by FDP_ACF.1[SFR]

Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
FDP_ACF.1[MEM]	FDP_ACC.1 FMT_MSA.3	Yes, by FDP_ACC.1[MEM] Yes
FDP_ACF.1[SFR]	FDP_ACC.1 FMT_MSA.3	Yes, by FDP_ACC.1[SFR] Yes
FMT_MSA.3[MEM]	FMT_MSA.1 FMT_SMR.1	Yes, by FMT_MSA.1[MEM] See discussion below
FMT_MSA.3[SFR]	FMT_MSA.1 FMT_SMR.1	Yes, by FMT_MSA.1[SFR] See discussion below
FMT_MSA.1[MEM]	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes, by FDP_ACC.1[MEM] See discussion below Yes
FMT_MSA.1[SFR]	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes, by FDP_ACC.1[SFR] See discussion below Yes
FPT_TST.2	FPT_AMT.1	No (not applicable, see the explanation given below)
FDP_ITT.1[COPY]	FDP_ACC.1 or FDP_IFC.1	Yes, by FDP_IFC.1

The dependent requirements of FCS_COP.1 completely address the appropriate management of cryptographic keys used by the specified cryptographic function and the management of access control rights as specified for the memory access control function. All requirements concerning these management functions shall be fulfilled by the environment (Smartcard Embedded Software) according to the requirements RE.Phase-1 and RE.Cipher. This holds for all iterations of FCS_COP.1. Since the assignment within the iteration does not change the scope of the dependencies, it is not required to iterate the dependencies because an appropriate key management is required for all cryptographic operations.

With the exception of RSA and ECC over GF(p) key generation (FCS_CKM.1), the functional requirements [FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4 and FMT_MSA.2 are not included in the TOE's security functionality since the TOE only provides pure crypto-functions for encryption and decryption without additional functionality for the handling of cryptographic keys. These security functional requirements are explicitly moved to the "Security Requirements for the IT-Environment" because the Smartcard Embedded Software is seen as "IT-Environment" that must fulfil these requirements related to the needs of the realized application.

The RSA key generation can fulfil the dependent requirement FCS_CKM.1 of FCS_COP.1[RSA], and the ECC over GF(p) key generation can fulfil the dependent requirement FCS_CKM.1 of FCS_COP.1[RSA] and FCS_COP.1[ECC_GF_p], but for FCS_COP.1[SW-DES] no key generation exists, and thus FCS_CKM.1 remains a requirement for the IT environment.

However, the RSA and ECC over GF(p) key generation (FCS_CKM.1) itself introduces dependencies. The dependency FCS_COP.1 can be fulfilled by the TOE itself, but it may

still be necessary in the application context to export generated key pairs. If this is intended, then the requirement FCS_CKM.2 applies; therefore FCS_CKM.2 is listed as a requirement for the IT environment in section 5.2.1, Table 11.

The dependency FMT_SMR.1 introduced by the two components FMT_MSA.1 and FMT_MSA.3 is also addressed by the requirement RE.Phase-1 and more specific by the security functional requirements as stated in the chapter "Security Requirements for the IT-Environment". The definition and maintenance of the roles must be subject of the Smartcard Embedded Software.

For FPT_TST.2, which is based upon FPT_TST.1 from Common Criteria Part 2 [2], a dependency on FPT_AMT.1 exists. The following explanation justifies, why this dependency is not satisfied:

- According to the Annex of Common Criteria Part 2 [2], Annex J.16 TSF self test (FPT_TST), paragraph 1297, “The abstract machine upon which the TSF software is implemented is tested via dependency on FPT_AMT.” For the current TOE, the TOE consists of both hardware and software, therefore there is no underlying abstract machine on which the TOE is implemented. The TOE hardware (NXP SmartMX Secure Smart Card Controller) has been evaluated and provides several supporting security features. Therefore it can be assumed that the test routines for the hardware RNG implemented in the Crypto Library ensure that failures of the hardware RNG will be detected.

The requirements FDP_ITT.1[COPY] and FPT_ITT.1[COPY] use the same information flow control policy (see also Note 4 and Note 11): FDP_IFC.1 is not iterated, since the policy remains the same for leakage protection of both cryptographic operations as well as of the secure memory copy routine. The Data Processing Policy for FDP_IFC.1 has been defined in the PP [9] as follows:

“User Data and TSF data shall not be accessible from the TOE except when the Smartcard Embedded Software decides to communicate the User Data via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the Smartcard Embedded Software.”

The secure copy routine is expected to be used for user data (e.g. when loading keys) rather than TSF data. However, the mechanism implemented prevents leakage for any kind of data, therefore both functional requirements (FDP_ITT.1[COPY] and FPT_ITT.1[COPY]) have been chosen.

8.2.4 Rationale for the Assurance Requirements and the Strength of Function Level

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.

8.2.5 Security Requirements are Mutually Supportive and Internally Consistent

For this purpose, the security requirements may be divided into three distinct groups:

The assurance requirements (EAL5+)

4. The TOE security functional requirements in the Hardware Security Target [10]
5. The additional TOE security functional requirements in this Security Target.

In the Hardware Security Target [10] it is demonstrated that the set of assurance requirements and the TOE security functional requirements in the Hardware Security Target is internally consistent and mutually supportive.

It therefore remains to demonstrate that:

- The additional TOE security functional requirements are internally consistent
- The additional TOE security functional requirements are consistent with all other security requirements
- The additional TOE security functional requirements are mutually supportive with themselves.
- The additional TOE security functional requirements are mutually supportive with all other security requirements.

These are demonstrated in the following subsections:

8.2.5.1 The additional TOE security functional requirements are internally consistent

FCS_COP.1[SW-DES], FCS_COP.1[RSA_encrypt], FCS_COP.1[RSA_public], FCS_COP.1[RSA_sign], FCS_COP.1[ECC_GF_p], FCS_COP.1[ECC_ADD], FCS_COP.1[ECC_DHKE], FCS_COP.1[SHA], FCS_CKM.1[RSA], FCS_CKM.1[ECC_GF_p] describe a range of cryptographic functionality (encryption, decryption, signing, hashing, key exchange and key generation). These contain no inconsistencies with each other: where two requirements refer to the same algorithm, they do so consistently and use the same range of key sizes.

FDP_ITT.1[COPY] and FPT_ITT.1[COPY] deal with the moving of data while remaining protected from certain side-channel attacks. This is completely unrelated with the cryptographic functionality and therefore consistent.

FDP_RIP.1 deals with the deletion of data after the crypto library has used it. This is completely unrelated with cryptographic functionality and moving of data and therefore consistent.

FCS_RND.2 and FPT_TST.2 deal with the quality of random number generation and the testing of the generator before using these numbers. This is completely unrelated with cryptographic functionality (though the random numbers may be used for key generation), moving of data and deletion of data and therefore consistent.

Therefore the additional TOE security functional requirements are internally consistent.

8.2.5.2 The additional TOE security functional requirements are consistent with all other security requirements

The additional TOE security functional requirements are consistent with the assurance requirements: there is no conceptual overlap between these two sets, so there is no inconsistency possible.

The additional TOE security functional requirements are largely unrelated to the TOE security functional requirements in the Hardware Security Target [10], with the following exceptions:

- FCS_COP.1[SW-DES] is strongly related to FCS_COP1.[DES], but the first provides additional options and modes than the second. None of these additional options and modes is inconsistent with the options and modes already provided.
- FCS_RND.1 is strongly related to FCS_RND.2 and FPT_TST.2. The latter two provide more detail on random number generation and the testing thereof. No inconsistencies are present.

Therefore, the additional TOE security functional requirements are consistent with all other security requirements

8.2.5.3 The additional TOE security functional requirements are mutually supportive with themselves.

The requirements are mutually supportive in the following ways:

- FPT_TST.2 supports FCS_RND.2 in providing random numbers by ensuring that failure of the random number generator is detected
- FCS_RND.2 supports the various key generation requirements by generating strong random numbers
- The key generation requirements support various cryptographic requirements by being able to provide keys for their use
- FDP_ITT.1[COPY], FPT_ITT.1[COPY] and FDP_RIP.1 support al other requirements by allowing secure copy and delete-after use, thus making it harder to retrieve information on the cryptographic operations.

This list is not exhaustive, more mutual support may be found in sections 8.2.1 (the requirements mutually support each other to meet security objectives) and 8.2.3 (the dependencies are fulfilled).

Therefore, the additional TOE security functional requirements are mutually supportive with themselves.

8.2.5.4 The additional TOE security functional requirements are mutually supportive with all other security requirements.

In general, the TOE security functional requirements in the Hardware Security Target [10] provide a set of security requirements for a general smart card, which is designed to protect both itself and the software running on it from tampering and various other attacks. This supports the additional security functional requirements in this Security Target, which describe software that is designed to be integrated with Smartcard Embedded Software. More specifically,

- The SFRs do not contain FPT_RVM.1: but possible bypass is not a concern for the crypto library, as a library is intended to be invoked only when called and “bypassed” the rest of the time.
- The SFRs in the Hardware Security Target [10] contain FPT_SEP.1, which prevents tampering with other security functional requirements.
- The SFRs do not contain FMT_MOF.1, which could be used to deactivate other SFRs.
- The SFRs do not contain FAU[19] requirements to enable detection of attacks, but they do contain FPT_FLS.1 and FRU_FLT.2, which enable detection of environmental attacks.
- FCS_COP.1[SW-DES] is supported by FCS_COP1.[DES], where the hardware provides a coprocessor for DES calculation to be used by the software.
- A similar argument holds for FCS_RND.1 and FCS_RND.2 (where a hardware random number generator is provided).

[19] The SFRs do contain FAU_SAS.1 but this does not enable detection of attacks aimed at defeating other security functional requirements.

Finally, the arguments given in section 8.2.4 for the fact that the assurance components are adequate for the functionality of the TOE also show that the security functional and assurance requirements support each other.

Therefore, the additional TOE security functional requirements are mutually supportive with the other security requirements.

8.3 TOE Summary Specification Rationale

8.3.1 Rationale for IT security functions

8.3.1.1 Rationale for HW IT security functions

The mapping of IT security functions to SFR for the hardware part of the TOE is given in the Hardware Security Target [10].

The rationale for these IT security functions can also be found in the Hardware Security Target, with the exception of F.LOG.

For F.LOG, the rationale is extended for the leakage resistance aspects of the cryptographic library (see the sub-section F.LOG below).

8.3.1.2 Rationale for SW IT security functions

The mapping of IT security functions to SFR for the hardware part of the TOE is given in the following table:

Table 21. Mapping of TSFR to IT security functions for the software part of the TOE

	F.DES	F.RSA_encrypt	F.RSA_sign	F.RSA_public	F.ECC_GF_p_ECDSA	F.ECC_GF_p_DH_KeyExch	F.SHA	F.RSA_KeyGen	F.ECC_GF_p_KeyGen	F.RNG_Access	F.Object_Reuse	F.LOG	F.COPY
FCS_COP.1[SW_DES]	X												
FCS_COP.1[RSA_encrypt]		X											
FCS_COP.1[RSA_sign]			X										
FCS_COP.1[RSA_public]				X									
FCS_COP.1[ECC_GF_p]					X								
FCS_COP.1[ECC_ADD]					X								
FCS_COP.1[ECC_DHKA]						X							
FCS_COP.1[SHA]							X						
FCS_CKM.1[RSA]								X					
FCS_CKM.1[ECC_GF_p]									X				

	F.DES	F.RSA_encrypt	F.RSA_sign	F.RSA_public	F.ECC_GF_p_ECDSA	F.ECC_GF_p_DH_KeyExch	F.SHA	F.RSA_KeyGen	F.ECC_GF_p_KeyGen	F.RNG_Access	F.Object_Reuse	F.LOG	F.COPY
FCS_RND.2										X			
FPT_TST.2 FDP_RIP.1											X		
FDP_ITT.1 FPT_ITT.1 FDP_IFC.1 FPT_FLS.1												X	
FDP_ITT.1[COPY] FPT_ITT.1[COPY]												X	X

The "X" means that the IT security function realises or supports the functionality required by the respective Security Functional Requirement.

FCS_COP.1[SW-DES], FCS_COP.1[RSA_encrypt], FCS_COP.1[RSA_sign], FCS_COP.1[RSA_public], FCS_COP.1 [ECC_GF_p], FCS_COP.1 [ECC_ADD], FCS_COP.1[ECC_DHKA], FCS_COP.1[SHA], FCS_CKM.1[RSA], FCS__CKM.1[ECC_GF_p] and FDP_RIP.1

These SFRs are directly implemented by the corresponding IT security function (see Table 21). These security functions are therefore suitable to meet those SFRs.

FCS_RND.2 and FPT_TST.2

These SFRs are directly implemented by F.RNG_Access, which provide access to the software RNG (FCS_RND.2) and tests the hardware RNG which is used to seed the software RNG

FDP_ITT.1, FPT_ITT.1 and FDP_IFC.1

These SFRs are now also supported by the function F.LOG where the software part of the TOE provides additional protection against side-channel attacks over and above that provided by the hardware part of the TOE. F.LOG describes in detail how each cryptographic function is protected against side-channel attacks.

FPT_FLS.1

This SFRs is implemented by the IT security function F.LOG where protection is provided against DFA attacks. F.LOG describes in detail how each cryptographic function is protected against these DFA attacks.

FDP_ITT.1[COPY] and FPT_ITT.1[COPY]

Both of these SFRs are implemented by the IT security function F.COPY (for the copying) and F.LOG (which describes the side-channel resistance). Since neither

function differs between User data and TSF data, both SFRs are implemented in an identical manner.

8.3.2 The IT security functions work together

As can be seen from the mapping of TSFR to IT security functions, and the rationales between these two, the IT security functions are an almost 1:1 translation of each other. The additional information introduced in the IT security functions does not introduce potential security weaknesses. Therefore the IT security functions work together to satisfy the TSFRs.

8.3.3 Rationale for assurance measures

The assurance measures defined in section 6.2 are claimed to fulfil the assurance requirements of EAL5 augmented with ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.

The assurance measures are defined especially for the development and production of Smartcard IC products and observe also the refinements made in the PP.

As already explained in the Protection Profile, annex 8.1, the development and production process of a smartcard IC is complex. Regarding the great number of assurance measures, a detailed mapping of the assurance measures to the assurance requirements is beyond the scope of this Security Target. Nevertheless the suitability of the assurance measures is subject of different evaluation tasks. The documents "Quality Management Manual" and "Security Management Manual" describe the general benchmark of Philips.

8.4 PP Claims Rationale

According to chapter 7 this Security Target claims conformance to the Protection Profile “**Bundesamt für Sicherheit in der Informationstechnik (BSI)**: *Smartcard IC Platform Protection Profile (SSVG-PP)*, Version 1.0, July 2001; registered and certified by (BSI) under the reference BSI-PP-0002-2001” [9].

The sections of this document where threats, objectives and security requirements are defined, clearly state which of these items are taken from the Protection Profile and which are added in this ST. Therefore this is not repeated here. Moreover all additional stated items in this ST do not contradict with the items included from the PP (see the respective sections in this document).

The assignment performed in the PP for FPT_FLS.1 has been extended (see item (ii) in the functional requirement) as compared to its first definition in the PP [9] and its instantiation in the hardware ST [10] (which includes item (i) of the requirement only). The reason for this is, that the TOE in this ST comprises implementations of cryptographic algorithms (DES, 3DES and RSA-CRT) that might on principle be susceptible to DFA attacks. FPT_FLS.1 has been extended (item (ii) has been added) to include not only the hardware sensors but also “software sensors” that detect DFA attacks on RSA and DES computations.

The TOE consists of hardware and software. The PP [9] mainly focuses on the hardware part; the integration of the Hardware Security Target with the PP [9] has already been evaluated correctly. The software (Crypto Library) only provides additional functionality (e.g. FDP_RIP, FCS_COP).

The only cross-section between hardware and software requirements is constituted by the random number generation (F.RNG and F.RNG_Access). The software RNG builds upon the hardware RNG by drawing its seed from the hardware RNG. Before the seeding takes place, an appropriate test of the hardware RNG is performed (see

FPT_TST.1). Both the hardware RNG (FPT_RND.1) and the software RNG (FPT_RND.2) provide random numbers with certain good properties.

The operations done for the SFRs taken from the PP are also clearly indicated.

The evaluation assurance level claimed for this target (EAL5+) is identical to the requirements claimed by the Hardware ST (EAL5+), with the same augmentations and which includes the EAL4+ SARs claimed in the PP.

These considerations show that the Security Target correctly claims conformance to the **Bundesamt für Sicherheit in der Informationstechnik (BSI)**: *Smartcard IC Platform Protection Profile (SSVG-PP)*, Version 1.0, July 2001; registered and certified by (BSI) under the reference BSI-PP-0002-2001, [9].

9. Annexes

9.1 Definition of the Components FCS_RND.2 and FPT_TST.2

To define the IT security functional requirements of the TOE an additional family (FCS_RND) of the class FCS (cryptographic support) and an additional component of the family FPT_TST (TSF testing) are defined here.

The family FCS_RND describes the functional requirements for random number generation used for cryptographic purposes. The definition of this family was already begun in the PP [9] with FCS_RND.1; a new component FCS_RND.2 is added here. For ease of reading, the definition of the whole family will be repeated here.

The family FPT_TST describes the functional requirements for TSF self tests. A new component FPT_TST.2 is added to the family. The definition of the component FPT_TST.2 has already been given in the augmentation paper to the PP [9]. For ease of reading, the definition of this component is repeated here. For the definition of the family FPT_TST and of the component FPT_TST.1 see Common Criteria Part 2 [2].

9.1.1 Generation of random numbers (FCS_RND)

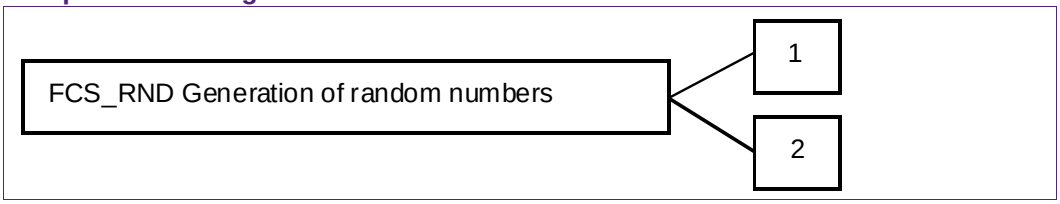
This family describes the functional requirements for random number generation used for cryptographic purposes.

Family Behaviour

This family describes the functional requirements for random number generation used for cryptographic purposes.

In order to ensure that a random number generator can be employed for different cryptographic purposes, the random number generation must assure that the generated random numbers posses certain properties. Typical properties include assurance that a given quality metric (e.g. minimum entropy) is achieved or that an implementation meets a given standard.

Component leveling



FCS_RND.1 Quality Metric for Random Numbers requires that random numbers meet a defined quality metric.

FCS_RND.2 Random Number Generation requires that random number generation is performed based on an assigned standard.

Management: FCS_RND.1, FCS_RND.2

There are no management activities foreseen.

Audit: FCS_RND.1, FCS_RND.2

There are no actions defined to be auditable.

FCS_RND.1 Quality Metric for Random Numbers

Hierarchical to: No other components

FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet *[assignment: a defined quality metric]*.
Dependencies:	No dependencies.

FCS_RND.2 Random Number Generation

Hierarchical to:	No other components
FCS_RND.2.1	The TSF shall provide a mechanism to generate random numbers that meet the following: *[assignment: list of standards]*.
Dependencies:	No dependencies.

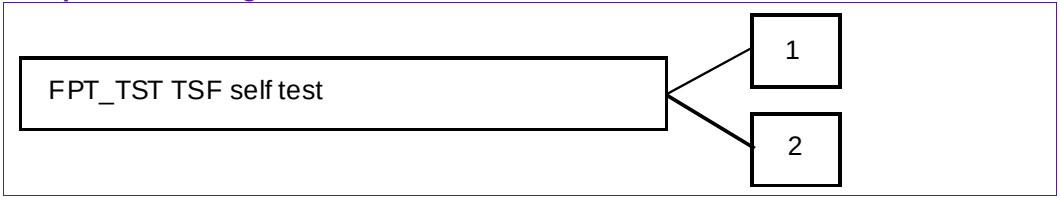
9.1.2 TSF self test (FPT_TST)

To define the IT security functional requirements of the TOE an additional component (FPT_TST.2) of the family FPT_TST (TSF self) is defined here. The family FPT_TST is taken from Common Criteria Part 2 [2]. The new component FPT_TST.2 has already been defined in the augmentation paper of the Smart Card IC Platform Protection Profile [9]. Its definition is repeated here for ease of reading.

Family behaviour

The behaviour of the family FPT_TST remains unchanged if compared to its definition within Common Criteria Part 2 [2].

Component leveling



FPT_TST.1 TSF testing, provides the ability to test the TSF's correct operation. These tests may be performed at start-up, periodically, at the request of the authorised user, or when other conditions are met. It also provides the ability to verify the integrity of TSF data and executable code.

FPT_TST.2 Subset TOE security testing, provides the ability to test the correct operation of particular security functions or mechanisms. These tests may be performed at start-up, periodically, at the request of the authorised user, or when other conditions are met. It also provides the ability to verify the integrity of TSF data and executable code.

Management: FPT_TST.1, FPT_TST.2

The management activities foreseen for FPT_TST.1 remain unchanged, i.e. as specified within Common Criteria Part 2 [2]. These management activities may also be considered for FPT_TST.2. There are no other management activities foreseen for FPT_TST.2.

Audit: FPT_TST.1, FPT_TST.2

The actions defined to be auditable for FPT_TST.1 remain unchanged, i.e. as specified within Common Criteria Part 2 [2]. The same action may also be considered for FPT_TST.2. There are no other auditable action defined for FPT_TST.2.

FPT_TST.2Subset TOE security testing

Hierarchical to:	No other components.

FPT_TST.2.1	The TSF shall run a suite of self tests *[selection: during initial start-up, periodically during normal operation, at the request of the authorised user, and/or at the conditions [assignment: conditions under which self test should occur]]* to demonstrate the correct operation of *[assignment: functions and/or mechanisms]*.
Dependencies:	FPT_AMT.1 Abstract machine testing

9.2 Further Information contained in the PP

The Annex of the Protection Profile ([9], chapter 9) provides further information. Section 8.1 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 8.2 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 gives examples of Attack Scenarios.

9.3 Glossary and Vocabulary

Note: To ease understanding of the used terms the glossary of the Protection Profile [9] is included here.

Administrator	(in the sense of the Common Criteria) The TOE may provide security functions which can or need to be administrated (i) by the Smartcard Embedded Software or (ii) using services of the TOE after delivery to Phases 4-6. Then a privileged user (in the sense of the Common Criteria, refer to definition below) becomes an administrator.
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.
Card Manufacturer	The customer of the TOE Manufacturer who receives the TOE during TOE Delivery. The Card Manufacturer includes all roles after TOE Delivery up to Phase 7 (refer to the PP [9], Figure 4 on page 17 and Section 8.1.1). The Card Manufacturer has the following roles (i) the Smartcard Product Manufacturer (Phase 5) and (ii) 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.
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.
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.
Integrated Circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions.
IC Dedicated Software	IC proprietary software embedded in a smartcard IC (also known as IC firmware) and developed by the IC Developer. Such software is required for testing purpose (IC Dedicated Test Software) but may provide additional services to facilitate usage of the hardware and/or to provide additional services (IC Dedicated Support Software).
IC Dedicated Support Software	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.
IC Dedicated Test Software	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.
Initialisation Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 3). These data are for instance used for traceability and for TOE identification (identification data).
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 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.
Smartcard	(as used in the Protection Profile [0]) Composition of the TOE, the Smartcard Embedded Software, User Data and the package (the smartcard carrier).
Smartcard Embedded Software	Software embedded in a smartcard IC and not being developed by the IC Designer. The Smartcard Embedded Software is designed in Phase 1 and embedded into the Smartcard IC in Phase 3 or in later phases of the smartcard product life-cycle. Some part of that software may actually implement a smartcard application others may provide standard services. Nevertheless, this distinction doesn’t matter here so that the Smartcard Embedded Software can be considered as being application dependent whereas the IC Dedicated Software is definitely not.
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.
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 the PP [9], Figure 4 on page 17) 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 modules.
TOE Manufacturer	The TOE Manufacturer must ensure that all requirements for the TOE and its development and production environment are fulfilled (refer to the PP [9], Figure 4 on page 17). 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 modules, 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 (for example configuration data). Note that the TOE is the Smartcard IC. Initialisation Data defined by the Integrated Circuits manufacturer to identify the TOE and to keep track of the product's production and further life-cycle phases are also considered as belonging to the TSF data.
User	(in the sense of the Common Criteria) The TOE serves as a platform for the Smartcard Embedded Software. Therefore, the "user" of the TOE (as used in the Common Criteria assurance class AGD: guidance) is the Smartcard Embedded Software. Guidance is given for the Smartcard Embedded Software Developer. On the other hand the Smartcard (with the TOE as a major element) is used in a terminal where communication is performed through the ISO interface provided by the TOE. Therefore, another "user" of the TOE is the terminal (with its software).
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.
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.

10. Bibliography

10.1 CC + CEM

[1] **Common Criteria for Information Technology Security Evaluation** – Part1: Introduction and general model, Version 2.3, August 2005, CCMB-2005-08-001

[2] **Common Criteria for Information Technology Security Evaluation** – Part2: Security functional requirements, Version 2.3, August 2005, CCMB-2005-08-002

[3] **Common Criteria for Information Technology Security Evaluation** – Part3: Security assurance requirements, Version 2.3, August 2005, CCMB-2005-08-003

[4] **Common Methodology for Information Technology Security Evaluation** – Evaluation Methodology, Version 2.3, August 2005, CCMB-2005-08-004

10.2 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

10.3 Hardware-related documents

[9] **Bundesamt für Sicherheit in der Informationstechnik (BSI)**: *Smartcard IC Platform Protection Profile (SSVG-PP)*, Version 1.0, July 2001; registered and certified by (BSI) under the reference BSI-PP-0002-2001

[10] **NXP Semiconductors Documentation:** *Security Target Lite – P5CC037V0A, BSI-DSZ-CC-0465*, Version 1.6, 9th July 2009

[11] **NXP Semiconductors Guidance, Delivery and Operation Manual for the P5xC012/02x/037/052 family of Secure Smart Card Controller**, Revision 1.5, January 23rd, 2008 Document-ID 139915

[12] **NXP Semiconductors Data Sheet P5xC012/02x/037/052 family;** *Secure contact PKI smart card controller*, Revision 3.6, April 6th, 2009, Document-ID 129036

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

10.4 Documents related to the crypto library

[14] **NXP Semiconductors User Guidance**: *Secured Crypto Library on the P5xC012/02x/037/052 Family*, Revision 1.6, May 6th, 2010

[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 DES Library,* Revision 3.0, August 24th, 2007

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

[18] **NXP Semiconductors User Guidance**: *Secured Crypto Library on the SmartMX – Secured RSA Library*, Revision 4.4, March 30th, 2010

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

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

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

10.5 Standards and text books

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

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

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

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

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

[27] **ISO/IEC 15946-2**: *Information technology – Security techniques – Cryptographic techniques based on elliptic curves* – Part 2: Digital Signatures**,** 2003

[28] **ISO/IEC 15946-3**: *Information technology – Security techniques – Cryptographic techniques based on elliptic curves* – Part 3: Key Establishment**,** 2003

[29] **ISO/IEC 15946-4**: *Information technology – Security techniques – Cryptographic techniques based on elliptic curves* – Part 4: Digital Signatures giving Message Recovery, 2004

[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] **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

11. Legal information

11.1 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.

11.2 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.

11.3 Licenses

ICs with DPA Countermeasures functionality

LICENSED DPA™ COUNTERMEASURES

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.

11.4 Trademarks

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

12. Contents

continued >>

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

Date of release: 10 May 2010