Secured Crypto Library on the P5CC036V1D

Security Target Lite

Rev. 2.2 — 8 January 2009 **Evaluation documentation**

Accepted **PUBLIC**

BSI-DSZ-CC-0584

Document information

Info	Content
Keywords	Security Target Lite, Crypto Library, P5CC036V1D
Abstract	Security Target Lite for the Secured Crypto Library on the P5CC036V1D according to the Common Criteria for Information Technology Evaluation (CC) at Level EAL4 augmented. The Crypto Library is developed and provided by NXP Semiconductors, Business Line Identification.

Revision history

Rev	Date	Description
2.2	08-Jan-2009	Changed to NXP template Updated references Changed certification number

Contact information

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

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

1. ST Introduction

This chapter is divided into the following sections: “ST Identification”, “ST Overview” and “CC Conformance and Evaluation Assurance Level”.

1.1 ST Identification

This Security Target is for the Common Criteria evaluation of the “NXP SmartMX P5CC036V1D Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software”, in short “Secured Crypto Library on the P5CC036V1D” or “Crypto Library on SmartMX” provided by NXP Semiconductors, Business Line Identification.

The TOE is a composite TOE, consisting of the hardware “NXP SmartMX P5CC036V1D Secure Smart Card Controller”, which is used as evaluated platform, and the “Secured Crypto Library on the P5CC036V1D”, which is built upon this platform.

The Security Target NXP Semiconductors Documentation: Security Target – Evaluation of the NXP P5CC036V1D Secure Smart Card Controller, Version 1.2, January 8th, 2009 [11] refers to the “NXP P5CC036V1D Secure Smart Card Controller” provided by NXP Semiconductors, Business Line Identification for a Common Criteria evaluation of the processor hardware. This is henceforward referred to as the “Hardware Security Target [11]”.

1.2 ST Overview

1.2.1 Introduction

The Hardware Security Target [11] contains in section 1.2.1 “ST Overview - Introduction” an introduction about the SmartMX hardware TOE that is considered in the evaluation. The P5CC036V1D covers IC Dedicated Software stored in the ROM provided with the SmartMX hardware platform.

The IC Dedicated Support Software “Secured Crypto Library on the P5CC036V1D“ 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 must be linked to the Smartcard Embedded Software. The NXP SmartMX smart card processor P5CC036V1D provides the computing platform and the cryptographic support by means of co-processors for the Secured Crypto Library on the P5CC036V1D. The used parts of the Secured Crypto Library on the P5CC036V1D are linked to the Smartcard Embedded Software during the development process and implemented with the Smartcard Embedded Software in the User ROM.

The security functionality listed below is provided by the Secured Crypto Library on the P5CC036V1D in addition to the functionality described in the Hardware Security Target [11] for the hardware platform:

- 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**.

- The **RSA** algorithm and the **RSA-CRT**[1]) algorithm can be used for encryption and decryption as well as for signature generation and signature verification[2].
- The **SHA-1** algorithm can be used for different purposes such as computing hash values in the course of digital signature creation or key derivation.
- The **RSA key generation** can be used to generate RSA key pairs in RSA “straight forward” or RSA-CRT format.
- The DES[3], Triple-DES and RSA-CRT implementations are **resistant to Side Channel Attacks**, including Simple Power Analysis (SPA), Differential Power Analysis (DPA), Differential Fault Analysis (DFA) and timing attacks.
- The RSA implementation is resistant to Side Channel Attacks, including Simple Power Analysis (SPA), Differential Power Analysis (DPA) and timing attacks.
- The RSA key generation is resistant against Simple Power Analysis (SPA) and timing attacks.
- The SHA-1 algorithm is resistant against Simple Power Analysis (SPA) and timing attacks under certain preconditions.
- Details of the algorithm resistance can be found in Table 7 in section 5.1.1.1.
- 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.
- The TOE includes internal security measures for **residual information protection**.
- The TOE provides a **secure copy routine**.

Note that the functions provided by the hardware platform are not restricted by the Crypto Library on SmartMX.

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 [11]. The delivery process or the hardware platform is independent from the Crypto Library on SmartMX.

The cryptographic library is delivered in Phase 1 (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 cryptographic 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 Line Identification; the integration of the crypto library into a 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

1 RSA using the Chinese Remainder Theorem

2 Note that the cryptographic library does not provide any padding in the RSA functionality.

3 See also Note 7 in section 5.1.1.1.

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 [11]. This additional functionality is added using the policy "*P.Add-Func*" (see section 3.4, Organisational Security Policies 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 2.1, August 1999, CCIMB-99-031, [1]
- **Common Criteria for Information Technology Security Evaluation** – Part2: Security functional requirements, Version 2.1, August 1999, CCIMB-99-032, [2]
- **Common Criteria for Information Technology Security Evaluation** – Part3: Security assurance requirements, Version 2.1, August 1999, CCIMB-99-033, [3]
- and the final interpretations as referenced by AIS32 [7].

For the evaluation the following methodology will be used:

- **Common Methodology for Information Technology Security Evaluation** CEM-99/045 Part 2: Evaluation Methodology, Version1.0, August 1999, [4]

The chosen level of assurance is **EAL 4 augmented**. The minimum strength level for the TOE security functions is **SOF-high (Strength of functions high)**.

The **augmentations** chosen are:

- ADV_IMP.2,
- 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 4 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 [11]).

2. TOE Description

This chapter is divided into the following sections: “TOE Definition” and “Further Definitions and Explanations”. TOE Definition has the sub-sections “Hardware Description”, “Software Description”, “Documentation”, “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 P5CC036V1D 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. There is dedicated documentation regarding the hardware. The additional IC Dedicated Support Software “Secured Crypto Library on the P5CC036V1D” consists of a software library and associated documentation. The Secured Crypto Library on the P5CC036V1D is an additional part that provides cryptographic functions that can be operated on the hardware platform as described in this Security Target.

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

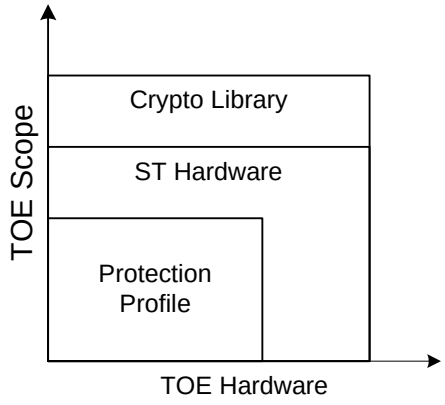


Figure 1: Scope of the Security Target

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 to the TOE hardware and the associated functionality.
2. The Hardware Security Target [11] defines the functionality of the platform provided by the P5CC036V1D Smart Card Controller. It comprises the specific hardware features of this platform.
3. The Secured Crypto Library on the P5CC036V1D 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 P5CC036V1D 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 [11] and therefore this latter document will be cited where ever appropriate. However the assets, assumptions, threats, objectives and security functional requirements are tracked in this Security Target.

The following table lists the TOE components.

Type	Name	Re-lease	Date	Form of delivery
Hardware	NXP P5CC036V1D Secure Smart Card Controller	V1D	T503D.gds2_200 40915	wafer (dice include reference T503D)
Software	Test ROM Software (the *IC Dedicated Test Software*)	1.4	August 16th, 2004	Test ROM on the chip *(tmfos.lst, V1.4)*
Software	Boot ROM Software (boot.asm, part of the *IC Dedicated Support Software*)	1.7	March 9th, 2004	Test ROM on the chip *(tmfos.lst, V1.4)*
Document	Philips Semiconductors Data Sheet: SmartMX - P5CC036 Secure Smart Card Controller, Revision 3.3, June 27th, 2005, Document-ID 081733	3.3	June 27th, 2005	electronic document
Document	Philips Semiconductors Documentation: Instruction Set SmartMX-Family, Secure Smart Card Controller, Objective Specification, Revision 1.1, July 4th, 2006, Document Number: 084111	1.1	July 4th, 2006	electronic document
Document	NXP Semiconductors Guidance, Delivery and Operation Manual: Evaluation of NXP P5CC036V1D - Secure Smart Card Controller, Revision 1.2, January 8th, 2009	1.2	January 8th, 2009	electronic document
Software	Secured Crypto Library on the P5CC036V1D Pseudo Random Number Generator	2.0	n/a	binary library file(s) plus the required header file(s), on CD or electronically
Software	Secured Crypto Library on the P5CC036V1D Secured DES Library	1.0	n/a	binary library file(s) plus the required header file(s), on CD or electronically
Software	Secured Crypto Library on the P5CC036V1D Secured RSA Library	2.0	n/a	binary library file(s) plus the required header file(s), on CD or electronically
Software	Secured Crypto Library on the P5CC036V1D Secured RSA Key Generation Library	2.0	n/a	binary library file(s) plus the required header file(s), on CD or electronically

Type	Name	Re-lease	Date	Form of delivery
Software	Secured Crypto Library on the P5CC036V1D SHA-1 Library	2.0	n/a	binary library file(s) plus the required header file(s), on CD or electronically
Document	NXP Semiconductors User Guidance: Secured Crypto Library on the P5CC036V1D, User Guidance, Revision 2.2, January 8th, 2009	2.2	January 8th, 2009	printed on paper, or electronically with the crypto library
Document	Philips Semiconductors User Guidance: Crypto Library on SmartMX – Pseudo Random Number Generator & Chi-Squared Test Library, User Guidance, Revision 3.0, November 23rd, 2005	3.0	November 23rd, 2005	printed on paper, or electronically with the crypto library
Document	Philips Semiconductors User Guidance: *Crypto Library on SmartMX – Secured DES Library,* User Guidance, Revision 2.0, November 23rd, 2005	2.0	November 23rd, 2005	printed on paper, or electronically with the crypto library
Document	Philips Semiconductors User Guidance: Crypto Library on *SmartMX – SHA-1 Library, User Guidance, Revision 3.0, November 23rd,* 2005	3.0	November 23rd, 2005	printed on paper, or electronically with the crypto library
Document	Philips Semiconductors User Guidance: Crypto Library on SmartMX – Secured RSA Library, User Guidance, Revision 3.0, November 23rd, 2005	3.0	November 23rd, 2005	printed on paper, or electronically with the crypto library
Document	Philips Semiconductors User Guidance: Crypto Library on SmartMX – Secured RSA Key Generation Library, User Guidance, Revision 3.0, November 23rd, 2005	3.0	November 23rd, 2005	printed on paper, or electronically with the crypto library
Document	Philips Semiconductors Software Delivery Description: Crypto *Library on SmartMX, Secured Random Number Library,* CC EAL4+ on P5CC036V1D, Delivery Module Contents, Revision 1.0, November 23rd, 2005, Document-ID 117410	1.0	November 23rd, 2005	electronic document

Type	Name	Re-lease	Date	Form of delivery
Document	Philips Semiconductors Software Delivery Description: Crypto *Library on SmartMX, Secured DES Library,* CC EAL4+ on P5CC036V1D, Delivery Module Contents, Revision 1.0, November 23rd, 2005, Document-ID 117110	1.0	November 23rd, 2005	electronic document
Document	Philips Semiconductors Software Delivery Description: Crypto *Library on SmartMX, SHA-1 Library,* CC EAL4+ on P5CC036V1D, Delivery Module Contents, Revision 1.0, November 23rd, 2005, Document-ID 117510	1.0	November 23rd, 2005	electronic document
Document	Philips Semiconductors Software Delivery Description: Crypto *Library on SmartMX, Secured RSA Library,* CC EAL4+ on P5CC036V1D, Delivery Module Contents, Revision 1.0, November 23rd, 2005, Document-ID 117210	1.0	November 23rd, 2005	electronic document
Document	Philips Semiconductors Software Delivery Description: Crypto *Library on SmartMX, Secured RSA Key Generation Library,* CC EAL4+ on P5CC036V1D, Delivery Module Contents, Revision 1.0, November 23rd, 2005, Document-ID 117310	1.0	November 23rd, 2005	electronic document

Table 1: Components of the TOE

2.1.1 Hardware Description

The NXP SmartMX hardware is described in section 2.1.1 “Hardware Description” of the Hardware Security Target [11]. The IC Dedicated 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 [11]. The Smartcard Embedded Software that is stored in the User-ROM that is not part of the TOE.

2.1.2 Software Description

The additional IC Dedicated Support Software “Secured Crypto Library on the P5CC036V1D “ is part of the TOE. It provides cryptographic support for the NXP P5CC036V1D smart card processor. The IC Dedicated Support Software as part of the TOE provides an interface between the smart card hardware (P5CC036V1D) and a smart card operating system or smart card application for the usage of the cryptographic functions provided by the TOE. It uses the specific functionality of the hardware to provide these cryptographic services.

The considered configuration of the Secured Crypto Library on the P5CC036V1D assumes that the crypto library is executed in System Mode. In addition the following Compiler Options are required:

- Memory Model: Large
- Code ROM size: huge

The Embedded Software developer has to be aware, that no restrictions regarding the access to the memory and to Special Function Registers are available in the System Mode.

For performance reasons, specific checks on the input data have to be performed by the Smartcard Embedded Software before the crypto library is called. Details are described in the User Guidance [16], [17], [18], [19], [20], [21].

The crypto library provides DES[4], Triple-DES (3DES), RSA, RSA-CRT, RSA key generation and SHA-1 algorithms. Both DES and Triple-DES can be used in one of the following modes of operation: ECB, CBC or CBC-MAC. 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. The DES[5], Triple-DES, SHA-1, RSA, RSA-CRT and RSA key generation cryptographic functions are resistant to side channel attacks as described in Table 7: Algorithm Resistance Overview.

These crypto functions are supplied as a library rather than as a monolithic program, and hence a user of the library may include those functions he requires – 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 [16].

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.

The TOE supports various key sizes for RSA up to a limit of 2048 bits. Conformance with the evaluation requirement Strength of Function: High requires a minimum key size of 1536 bits.

2.1.3 Documentation

The documentation for the NXP SmartMX hardware is described in section 2.1.3 “Documentation” of the Hardware Security Target [11].

The cryptographic library has associated user guidance documentation (see Table 1). This contains:

- the specification of the functions provided by the 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 as environment).

[4] Note, that Single-DES with a key length of 56 bits is not considered to be resistant against attacks with a high attack potential, therefore Single-DES must not be used. See also Note 7 in section 5.1.1.1.

[5] See also Note 7 in section 5.1.1.1.

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 [11]. 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 the TOE” of the Hardware Security Target [11].

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.

2.1.6 TOE Intended Usage

Regarding to phase 7, 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 does not avoid a threat.

For details on the usage of the hardware platform refer to section 2.1.6 “TOE Intended Usage” in the Hardware Security Target [11].

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 P5CC036V1D hardware is described in section 2.1.7 “TOE User Environment” of the Hardware Security Target [11]. 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 P5CC036V1D hardware.

2.1.8 General IT features of the TOE

The general features of the NXP P5CC036V1D hardware are described in section 2.1.8 “General IT Features of the TOE” of the Hardware Security Target [11]. These are supplemented for the TOE by the functions listed in *P.Add-Func* in section 3.4 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 [11]. 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 [11]. 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 [11], and shown in Table 2, are valid for this Security Target.

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 [11]
A.Key-Function	Usage of Key-dependent Functions	HW-ST [11]

Table 2: Assumptions defined in the PP [9] and the Hardware Security Target [11]

This Security Target defines one additional assumption:

A.Preconditions: Operational preconditions

(1) In case that resistance of the SHA-1 implementation against side channel attacks as described in Table 7 is required, then the Smartcard Embedded Software developer shall ensure that the necessary operational preconditions are met.

(2) For the RSA-CRT there exist two algorithms. Only one of them provides built-in resistance against DFA attacks. When using the second algorithm, it is assumed that the user of the Secured Crypto Library on the P5CC036V1D first analyses and decides whether DFA attacks are applicable in the specific field of application, and that he implements effective DFA countermeasures on his own, if necessary.

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 [11], and shown in Table 3, are valid for this Security Target.

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]

Table 3: Threats defined in the Protection Profile

Note 2. Within the Hardware Security Target [11], 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 P5CC036V1D) and software (Secured Crypto Library on the P5CC036V1D) 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 deficiency 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 P5CC036V1D, 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[6] encryption and decryption,
- RSA algorithm and RSA-CRT algorithm,
- RSA key generation,
- SHA-1 Hash Algorithm,
- 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: Algorithm Resistance Overview and in section 6.1.8 F.COPY.

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

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 [11].

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]

[6] See also Note 7 in section 5.1.1.1.

Name	Title	Defined in
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 [11]
O.MF_FW	MIFARE Firewall	HW-ST [11]
O.MEM_ACCESS	Area based Memory Access Control	HW-ST [11]
O.SFR_ACCESS	Special Function Register Access Control	HW-ST [11]

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

Note 3. Within the Hardware Security Target [11], the objective O.RND has been used in context with the hardware (true) random number generator (RNG). In addition to this, the TOE (Secured Crypto Library on the P5CC036V1D) 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 3.3, which extends T.RND in a similar way.

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

O.DES3 — The TOE includes functionality to provide encryption and decryption facilities of the Triple-DES algorithm, resistant to attack as described in Table 7: Algorithm Resistance Overview (see also Note 7 in section 5.1.1.1). This uses the hardware DES engine specified in the security objective O.HW_DES3 defined in the hardware Security Target.

O.RSA — The TOE includes functionality to provide public key facilities using the RSA algorithm and RSA-CRT algorithm, resistant to attack as described in Table 7: Algorithm Resistance Overview.

O.RSA_KeyGen — The TOE includes functionality to generate RSA and RSA CRT key pairs, resistant to attack as described in Table 7: Algorithm Resistance Overview.

O.SHA-1 — The TOE includes functionality to provide electronic hashing facilities using the SHA-1 algorithm, resistant to attack as described in Table 7: Algorithm Resistance Overview.

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 [11] are also valid in the ST for the Crypto Library (the “IC Dedicated Support Software”).

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

Table 5: Security Objectives for the environment

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 [11].

The Hardware Security Target [11] 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 objective for the environment:

OE.Preconditions Operational preconditions.

The environment shall ensure the following two operational preconditions:

1. In case that resistance of the SHA-1 implementation against side channel attacks as described in Table 7 is required, then the Smartcard Embedded Software developer shall ensure that the necessary operational preconditions are met.
2. The user of the Secured Crypto Library on the P5CC036V1D is responsible to analyse and decide whether DFA attacks are applicable in the specific field of application.

   If resistance against DFA Attacks is required for the RSA-CRT algorithm, two solutions are possible:

   a. The first DFA-CRT algorithm (called “RSA-CRT algorithm 1” in Table 7: Algorithm Resistance Overview) provides built-in resistance against DFA Attacks, but this algorithm requires the public exponent as input parameter.

   b. If the public exponent is not available as input parameter, then the second DFA-CRT algorithm (called “RSA-CRT algorithm 2 in Table 7: Algorithm Resistance Overview) shall be used, but this algorithm does not provide built-in resistance against DFA Attacks. In this case the user of the Secured Crypto Library on the P5CC036V1D has to implement effective DFA countermeasures on his own.

5. IT Security Requirements

5.1 TOE Security Requirements

This section consists of the subsections “TOE Security Functional Requirements”, “TOE Security Assurance Requirements” and “Refinements of the TOE Security Assurance 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 (P5CC036V1D) 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:

Name	Title	Defined in
FRU_FLT.2	Limited fault tolerance	CC Part 2 [2] (provided by chip HW)
FPT_FLS.1	Failure with preservation of secure state	CC Part 2 [2] (provided by chip HW)
FPT_SEP.1	TSF domain separation	CC Part 2 [2] (provided by chip HW)
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)
FAU_SAS.1	Audit storage	PP Section 8.6 [9] (provided by chip HW)
FPT_PHP.3	Resistance to physical attack	CC Part 2 [2] (provided by chip HW)
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)
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)
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)
FCS_RND.1	Quality metric for random numbers (used here for random numbers generated by the hardware (true) random	PP [9] Section 8.4, and refined in Hardware ST [11] section 5.1.1.1 “SFRs of the Protection Profile”.

Name	Title	Defined in
	number generator; see also FCS_RND.2)	

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

These requirements have already been stated in the hardware ST [11] 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)[7] of secret information during the application of the crypto algorithms DES, 3DES, SHA-1, RSA and RSA-CRT as well as RSA key generation. Compared to the Hardware Security Target [11], 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 6.1.8 F.COPY as well as the requirements FDP_ITT.1[COPY] and FPT_ITT.1[COPY] in section 5.1.1.2).[8]

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 [11] to include not only the hardware sensors but also “software sensors” that detect DFA attacks on DES, 3DES and RSA-CRT computations. Therefore the requirement is repeated here together with the extended refinement. FPT_FLS.1 now includes also DFA protection for DES, 3DES and RSA-CRT. 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 and RSA-CRT.***

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 software). The software sensors detect DFA attacks in DES, 3DES and RSA-CRT computations and lead to a secure state (no computation results are

[7] see also Table 7: Algorithm Resistance Overview

[8] 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.

output) in case such an attack occurs. The OS is responsible to ensure a secure state, since an exception is thrown if a DFA has been detected.

The properties of the cryptographic algorithms in respect to their **resistance**[9] **against Side Channel Analysis** (FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_FLS.1) can be summarized as follows:

Algorithm	Resistant against the following attacks			
DES and 3DES	Timing	SPA	DPA	DFA
RSA-CRT algorithm 1	Timing	SPA	DPA	DFA
RSA-CRT algorithm 2	Timing	SPA	DPA	n.a.**
RSA	Timing	SPA	DPA	n.a.
RSA Key Generation	Timing	SPA	n.a.	n.a.
SHA-1	Timing*	SPA*	n.a.	n.a.

Table 7: Algorithm Resistance Overview

The abbreviation “n.a.” in Table 7 shall be understood as “not available”, 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.

*: The resistance of SHA-1 is only guaranteed if the TOE is operated under the necessary operational preconditions as specified in the user guidance [16] and [19].

**: For the RSA-CRT, there exist two implementations. Only one of them implements DFA countermeasures. When using the second algorithm without built-in DFA protection, the user of the Secured Crypto Library on the P5CC036V1D first has to analyze and decide whether DFA attacks are applicable in the specific field of application, and has to implement effective DFA countermeasures on his own, if necessary (see also OE.Preconditions).

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 can also be 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).

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 [11] and shown in the following table.

Name	Title	Defined in
FCS_COP.1[DES]	Cryptographic operation	CC Part 2 [2], and added to PP in the Hardware ST [11] section 5.1.1.2 “Additional SFRs”.

[9] SPA = Simple Power Analysis, DPA = Differential Power Analysis, DFA = Differential Fault Analysis

Name	Title	Defined in
FDP_ACC.1[MEM]	Subset access control	CC Part 2 [2], and added to PP in the Hardware ST [11] section 5.1.1.2 “Additional SFRs”.
FDP_ACC.1[SFR]	Subset access control	CC Part 2 [2], and added to PP in the Hardware ST [11] section 5.1.1.2 “Additional SFRs”.
FDP_ACF.1[MEM]	Security attribute based access control	CC Part 2 [2], and added to PP in the Hardware ST [11] section 5.1.1.2 “Additional SFRs”.
FDP_ACF.1[SFR]	Security attribute based access control	CC Part 2 [2], and added to PP in the Hardware ST [11] section 5.1.1.2 “Additional SFRs”.
FMT_MSA.3[MEM]	Static attribute initialization	CC Part 2 [2], and added to PP in the Hardware ST [11] section 5.1.1.2 “Additional SFRs”.
FMT_MSA.3[SFR]	Static attribute initialization	CC Part 2 [2], and added to PP in the Hardware ST [11] section 5.1.1.2 “Additional SFRs”.
FMT_MSA.1[MEM]	Management of security attributes	CC Part 2 [2], and added to PP in the Hardware ST [11] section 5.1.1.2 “Additional SFRs”.
FMT_MSA.1[SFR]	Management of security attributes	CC Part 2 [2], and added to PP in the Hardware ST [11] section 5.1.1.2 “Additional SFRs”.
FMT_SMF.1	Specification of management functions	CC Part 2 [2][10], and added to PP in the Hardware ST [11] section 5.1.1.2 “Additional SFRs”.

Table 8: SFRs defined in the Hardware Security Target

Like the requirements already listed in Table 6, the requirements listed in Table 8 have already been stated in the Hardware Security Target [11] and are fulfilled by the chip hardware, too.

5.1.1.2 Additional SFRs

These SFRs (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.

Name	Title	Defined in
FCS_COP.1[SW-DES]	Cryptographic operation (TDES)	CC Part 2; specified in this ST, see below.
FCS_COP.1[RSA]	Cryptographic operation (RSA)	CC Part 2; specified in this ST, see below.

[10] This is seen as equivalent to CC Part 2 [2] according to AIS32 [7] and Final Interpretation 065.

Name	Title	Defined in
FCS_COP.1[SHA-1]	Cryptographic operation (SHA-1)	CC Part 2; specified in this ST, see below.
FCS_CKM.1	Cryptographic key generation (RSA key generation)	CC Part 2; specified in this ST, see below.
FDP_RIP.1	Subset residual information protection	CC Part 2; specified in this ST, see below.
FDP_ITT.1[COPY]	Basic internal (user data) transfer protection	CC Part 2; specified in this ST, see below.
FPT_ITT.1[COPY]	Basic internal TSF data transfer protection	CC Part 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 FCS_RND.1)	extension of the family FCS_RND defined in the PP [9], Section 8.4; FCS_RND.2 is defined in section 9.1.1
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

Table 9: SFRs defined in this Security Target

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: ***standards ANSI X9.52-1998 [33] (ECB and CBC mode) and FIPS PUB 81 [32] (ECB and CBC mode) and ISO 9797-1 [30], Algorithm 1 (CBC-MAC mode)***.

Application Notes: 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.

The CBC mode is to be understood as “outer” CBC mode, i.e. CBC mode as defined in [32] and [33] applied to the block

cipher algorithm (either DES or Triple-DES). The CBC-MAC mode of operation as defined in ISO 9797-1 [30], Algorithm 1, and also described in Appendix F of [32] 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] **Cryptographic operation**

Hierarchical to: No other components.

FCS_COP.1.1[RSA] The TSF shall perform ***encryption and decryption*** in accordance with the specified cryptographic algorithm ***RSA and RSA-CRT*** and cryptographic key sizes ***1536 bits to 2048 bits*** that meet the following: ***as described in Schneier [27] page 468, or Menezes, van Oorshot and Vanstone [28] section 8.2, and also mentioned in the standard ISO/IEC 9796 [29] Annex A, section A.4.***

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-1] **Cryptographic operation**

Hierarchical to: No other components.

FCS_COP.1.1[SHA-1] The TSF shall perform ***cryptographic checksum generation*** in accordance with the specified cryptographic algorithm ***SHA-1*** and cryptographic key size ***none*** that meet the following: ***standard FIPS 180-1 [34]***.

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 RSA public key pairs in RSA “straight forward” and RSA CRT format. 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 Functional Requirement to the TOE can be derived from this CC component:

FCS_CKM.1 Cryptographic Key Generation

Hierarchical to: No other components.

FCS_CKM.1.1 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 ***1536-2048 bits*** that meet the following ***standard:*** ***"****Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung, Übersicht über*

geeignete Algorithmen vom 17. Dezember 2007, published at 05 February 2008 in Bundesanzeiger Nr 19, page 376***" [35]***.

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 8. The standard [35] 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.

FDP_RIP.1 Subset Residual Information Protection

Hierarchical to: No other components.

This family addresses the need to ensure that deleted information is no longer accessible, and that newly created objects do not contain information that should not be accessible. 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[11] used by the Crypto Library as specified in the user guidance documentation***.

Dependencies: No dependencies.

Note 9. 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 ***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/ ***[28]***.

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 [28] completely, but is rather implemented based on this standard. Wherever the TOE implementation

[11] in this context “objects” are variables

deviates from the standard [28], 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 [28] 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 [28].
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.2Subset 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***[12] to demonstrate the correct operation of ***the hardware RNG (F.RNG)***[13].

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 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 (see RE.RNG2 in section 5.2.2). This is what is intended by “at the request of the authorized user”. In addition to the online test mentioned above, the Crypto Library may implement other test(s). The use of these tests depends on the intended application. For example, if the hardware RNG is to be used for re-seeding[14], a more simple test may be sufficient to ensure correct operation of the RNG.

Note 10. 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).

[12] selection: during initial start-up, periodically during normal operation, at the request of the authorised user, and/or at the conditions ...

[13] assignment: functions and/or mechanisms

[14] “re-seeding” here means adding additional entropy taken from the hardware RNG to the software RNG; this can be performed by adding entropy to the software RNG’s internal state, by adding entropy to the random output bits, or any combination

Note 11. 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 P5CC036V1D Secure Smart Card Controller (SmartMX) 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***[15] to prevent the ***disclosure***[16] 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 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***[17] 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.

[15] assignment: access control SFP(s) and/or information flow control SFP(s)

[16] selection: disclosure, modification, loss of use

[17] selection: disclosure, modification

Note 12. 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

Since the assurance level is augmented with AVA_VLA.4 the required level for the Strength of Function (SOF) of the above listed security functional requirements level 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[18]. These security assurance components are required by EAL4 (see section 1.3) or by the Protection Profile.

SAR	Title	Required by
ACM_AUT.1	Partial CM automation	PP[19] / EAL4
ACM_CAP.4	Generation support and acceptance procedures	PP / EAL4
ACM_SCP.2	Problem tracking CM coverage	PP / EAL4
ADO_DEL.2	Detection of modification	PP / EAL4
ADO_IGS.1	Installation, generation, and start-up procedures	PP / EAL4
ADV_FSP.2	Fully defined external interfaces	PP / EAL4
ADV_HLD.2	Security-enforcing high-level design	PP / EAL4
ADV_IMP.2	Implementation of the TSF	PP[20]
ADV_LLD.1	Descriptive low-level design	PP / EAL4
ADV_RCR.1	Informal correspondence demonstration	PP / EAL4
ADV_SPM.1	Informal TOE Security Policy Model	PP / EAL4
AGD_ADM.1	Administrator Guidance	PP / EAL4
AGD_USR.1	User Guidance	PP / EAL4
ALC_DVS.2	Sufficiency of security measures	PP[21]
ALC_LCD.1	Developer-defined life-cycle model	PP / EAL4
ALC_TAT.1	Well-defined development tools	PP / EAL4
ATE_COV.2	Analysis of coverage	PP / EAL4

[18] These requirements correspond to those detailed in section 5.1.2 "TOE Security Assurance Requirements" of the Hardware Security Target [11], except for the fact, that the Hardware Security Target uses Level EAL5+ instead of EAL4+.

[19] The Protection Profile [9] requires the evaluation assurance level EAL4.

[20] EAL4 requires ADV_IMP.1, the PP [9] has augmented this requirement to ADV_IMP.2.

[21] EAL4 requires ALC_DVS.1, the PP [9] has augmented this requirement to ALC_DVS.2.

SAR	Title	Required by
ATE_DPT.1	Testing: high-level design	PP / EAL4
ATE_FUN.1	Functional testing	PP / EAL4
ATE_IND.2	Independent testing – sample	PP / EAL4
AVA_MSU.3	Analysis and testing for insecure states	PP[22]
AVA_SOF.1	Strength of TOE security function evaluation	PP / EAL4
AVA_VLA.4	Highly resistant	PP[23]

Table 10: Security Assurance Requirements EAL4+ and PP augmentations

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 [11] 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 the evaluation of the Crypto Library on SmartMX has chosen EAL4+, i.e. the same evaluation assurance level as in the PP, no changes are necessary here.

Therefore all refinements made in the PP [9] are valid without change for the crypto library 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 [11] 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

[22] EAL4 requires AVA_MSU.2, the PP [9] has augmented this requirement to AVA_MSU.3.

[23] EAL4 requires AVA_VLA.2, the PP [9] has augmented this requirement to AVA_VLA.4.

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 applications 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 applications and cannot be provided by the hardware or by the crypto library.
  - There is one exception, however: The cryptographic RSA and RSA-CRT 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 products using the crypto library TOE to export keys or key parts (FCS_CKM.2). It is up to the application's security policy to allow key export. For typical applications 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 application has to ensure that an RSA key length in the range of 1536 to 2048 bit 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.

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

SFR	Name	Note
FCS_CKM.1	Cryptographic key generation	The TOE contains functionality to generate RSA and RSA CRT key pairs. However, the TOE provides also an implementation of the 3DES algorithm for cryptographic operation (FCS_COP.1[SW-DES]), for which no key generation is implemented. In order to use 3DES, keys have to be generated outside the TOE. 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 RSA CRT 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 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.

Table 11: Security Requirements for the IT Environment

Note 13. 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 (FCS_CKM.1) or they have to be loaded from the outside (FDP_ITC.1). The crypto library allows both: For RSA and RSA CRT key pairs, the TOE provides key generation functionality. However, for the cryptographic algorithm Triple-DES, such functionality is not part of the TSF. And even for the RSA it shall be possible to use RSA or RSA CRT 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): At least one of the two dependent requirements FCS_COP.1 or FCS_CKM.2 has to be fulfilled.

Note 14. To be exact, the requirements [FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4 and FMT_MSA.2 have to be iterated two to three times in order to fulfill the dependencies for FCS_COP.1[SW-DES] and FCS_COP.1[RSA] as well as FCS_COP.1[SHA-1] (three iterations in case that SHA-1 is used for key derivation, else two iterations). For better readability, the iterations have not been written down explicitly.

Note 15. 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 applications. 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 application 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 [11], but with RE.RNG modified to RE.RNG2, and one new requirement added (RE.Precondictions). The following table lists these requirements.

Requirement	Defined in
RE.Phase-1	PP [9]
RE.Process-Card	PP [9]
RE.Cipher	Hardware ST [11]
RE.RNG2	This ST (see below) Note: RE.RNG has been defined in the Hardware ST [11].
RE.Check-Init	Hardware ST [11]

Table 12: Security Requirements for the Non-IT Environment

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 developers of Smart Card Embedded Software must appropriately call the test routines for the hardware RNG, which are implemented inside the Crypto Library, before using random numbers generated by the hardware RNG. The operating system especially has to make sure 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 16. 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 P5CC036V1D Secure Smart Card Controller (SmartMX) [13]. 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 requirement for the non-IT environment:

RE.Preconditions Operational preconditions.

The environment shall ensure that the following two operational preconditions (for SHA-1 and RSA-CRT) are met:

1. In case that resistance of the SHA-1 implementation against side channel attacks as described in Table 7 is required, then the Smartcard Embedded Software developer (i.e. crypto library user / operating system) shall ensure that the necessary operational preconditions are met. These preconditions are met, if
   - the TOE is operated in voltage class A (5 V) or B (3,0 V) **and**
   - the CPU is operated with activated CSEC mode.

   The Smartcard Embedded Software shall enforce that these preconditions are met, if a secure SHA-1 is needed. This can be achieved for example by performing the following actions before a sensitive SHA-1 operation is started:
   - Checking the voltage class, and resetting the chip if voltage class C is detected, and
   - checking the CSEC mode status, and activating the CSEC mode if necessary.
2. The user of the Secured Crypto Library on the P5CC036V1D is responsible to analyse and decide whether DFA attacks are applicable in the specific field of application.

   If resistance against DFA Attacks is required for the RSA-CRT algorithm, two solutions are possible:

   a. The first DFA-CRT algorithm (called “RSA-CRT algorithm 1” in Table 7: Algorithm Resistance Overview) provides built-in resistance against DFA Attacks, but this algorithm requires the public exponent as input parameter.

   b. If the public exponent is not available as input parameter, then the second DFA-CRT algorithm (called “RSA-CRT algorithm 2 in Table 7: Algorithm Resistance Overview) shall be used, but this algorithm does not provide built-in resistance against DFA Attacks. In this case the user of the Secured Crypto Library on the P5CC036V1D has to implement effective DFA countermeasures on his own.

Note 17. (1) For the SHA-1, all other security functions are still provided even if the DCDC converter is not active. Therefore all other security functions (including the correct SHA-1 implementation, but except for the SPA and timing resistance of the SHA-1 implementation) are still guaranteed, even if the requirements listed under no. (1) of RE.Preconditions are not fulfilled. The certified status of the TOE will not get lost when the TOE is operated in voltage class C or if the CSEC mode is not activated; instead only the side channel resistance of the SHA-1 implementation will be lost in this case.

It can be checked if the CSEC mode is active by inspecting the SECMOD SFR. Note, the CSEC mode is not available if the CPU is operated in "free running" mode.

(2) For the second RSA-CRT algorithm, the resistance against other kinds of Side Channel Attacks is still provided, if the second algorithm without built-in DFA protection is used. This second algorithm (called “RSA-CRT algorithm 2” in Table 7) still implements countermeasures and provides resistance against SPA and DPA attacks. However, without additional measures for DFA protection, the private key used during the RSA-CRT calculation may be at risk.

6. TOE Summary Specification

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

6.1 TOE 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 [11]). 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.

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

Table 13: TSFs defined in the Hardware Security Target [11]

Note 18. 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 6.1.5. 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 19. The security function F.LOG is extended by the crypto library TOE as described in section 6.1.7 (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. This functionality is required by the security functional component FCS_COP.1[SW-DES] taken from the Common Criteria Part 2 [2]. 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 [30], 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* [32], 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 [31], 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 [33]. Note that, for the evaluated TOE, it is permitted to use only the Triple-DES for encryption or decryption.

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 [16] and [18]. 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.

SPA/DPA, timing and DFA attack resistance for F.DES is discussed in section 6.1.7 F.LOG.

6.1.2 F.RSA

The TOE provides functions that implement the **RSA** algorithm and the **RSA-CRT** algorithm as described in Schneier [27] page 468 or Menezes, van Oorshot and Vanstone [28] section 8.2, and also mentioned in the standard ISO/IEC 9796 [29] Annex

A, section A.4. This functionality is required by the security functional component FCS_COP.1[RSA] taken from the Common Criteria Part 2 [2]. This routine supports various key lengths from 256 bits to 2048 bits. Note that, for the evaluated TOE, RSA keys must have a key length in the range 1536 to 2048 bits.

The TOE contains modular exponentiation functions, which, together with other functions in the TOE, perform the operations required for RSA encryption or decryption. Two different RSA algorithms are supported by the TOE, namely the “Simple Straight Forward Method” (called RSA “straight forward”) and RSA using the “Chinese Remainder Theorem” (RSA CRT).

SPA/DPA, timing and DFA attack resistance for F.RSA is discussed in section 6.1.7 F.LOG.

6.1.3 F.RSA_KeyGen

The TSF **F.RSA_KeyGen - RSA Key Generation** provides functionality to generate RSA public key pairs as described in Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung, Übersicht über geeignete Algorithmen vom 17. Dezember 2007, published at 05 February 2008 in Bundesanzeiger Nr 19, page 376 [35]. This functionality is required by the security functional component FCS_CKM.1 taken from the Common Criteria Part 2. It supports various key lengths from 256 bits to 2048 bits. Note that, for the evaluated TOE, RSA keys must have a key length in the range 1536 to 2048 bits. Two different output formats for the key parameters are supported by the TOE, namely the “Simple Straight Forward Method” (RSA “straight forward”) and RSA using the “Chinese Remainder Theorem” (RSA CRT).

SPA/DPA, timing and DFA attack resistance for F.RSA_KeyGen is discussed in section 6.1.7 F.LOG.

6.1.4 F.SHA-1

The TOE implements functions to compute the Secure Hash Algorithm **SHA-1** according to the standard FIPS 180-1 [34]. This functionality is required by the security functional component FCS_COP.1[SHA-1] taken from the Common Criteria Part 2 [2]. The SHA-1 algorithm generates an output of length 160 bits.

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. If the IT environment ensures the necessary preconditions, the implementation of SHA-1 is also resistant against Side Channel Attacks as described in section 6.1.7 F.LOG.

6.1.5 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 18 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/ [28], as specified in the SFR FCS_RND.2.

In addition, the Crypto Library implements appropriate online tests according to the Hardware User Guidance Manual [13] 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.

6.1.6 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.

Note, that the secure copy routine (see F.COPY below) does not clear the source data, i.e. F.Object_Reuse does not apply there.

6.1.7 F.LOG

The TSF **F.LOG – Logical Protection** defined in the Hardware Security Target [11] 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 below Table 6 in section 5.1.1.1) as well as by FPT_FLS.1 (DFA attacks).

- The DES[24], Triple-DES and RSA-CRT implementations are resistant to Side Channel Attacks, including Simple Power Analysis (SPA), Differential Power Analysis (DPA), timing attacks and Differential Fault Analysis (DFA).

  For RSA-CRT there exist two algorithms. Only one of them provides built-in resistance against DFA Attacks. The other algorithm (called “RSA-CRT algorithm 2” in Table 7) does not provide countermeasures against DFA Attacks, but still provides all other countermeasures against Side Channel Attacks. When using that second algorithm, the user of the Secured Crypto Library on the P5CC036V1D first has to analyze and decide whether DFA attacks are applicable in the specific field of application, and has to implement effective DFA countermeasures on his own, if necessary (see also RE.Preconditions).
- The RSA “straight forward” implementation is resistant to Side Channel Attacks, including Simple Power Analysis (SPA), Differential Power Analysis (DPA) and timing attacks.
- The resistance of DES and Triple-DES against side channel attacks protects the confidentiality of the keys used in all modes of operation (ECB, CBC, and CBC-MAC).
- The SHA-1 implementation and the RSA key generation algorithm are resistant against Simple Power Analysis (SPA) and timing attacks.

An overview of the TOE’s resistance against side channel attacks is given in Table 7: Algorithm Resistance Overview in section 5.1.1.1.

[24] See also Note 7 in section 5.1.1.1.

Note, that the Side Channel Resistance for the secure copy functionality as required by FDP_ITT.1[COPY] and FPT_ITT.1[COPY] is implemented in function F.COPY, see section 6.1.8 below).

Note 20. The TOE implements a secure SHA-1 calculation, but neither a keyed hash function like an HMAC nor any predefined key derivation schemes. Therefore side channel analysis of the SHA-1 implementation can only focus on SPA and timing attacks, based on correlations to the SHA-1 input data blocks. The resistance of the SHA-1 implementation (F.LOG) constitutes a necessary, but not a sufficient condition for side channel resistant implementations of keyed hash functions or key derivation schemes. Depending on the application, additional analysis may become necessary.

The resistance of SHA-1 against Side Channel Attacks can be guaranteed only if certain operational preconditions are met. If this resistance is needed, the IT environment (crypto library user, i.e. operating system) has to ensure that the necessary operational preconditions are met (see also RE.Preconditions above).

6.1.8 F.COPY

The TSF **F.COPY – Secure Copy Routine** implements functionality to copy memory content using a routine that includes countermeasures against side channel attacks. This function can be used for copying sensitive data (e.g. loading of key data). The secure copy functionality includes randomization which effectively counters attacks based on Simple Power Analysis (SPA). This resistance against SPA attacks is part of F.COPY.

Note, that this routine copies the data and does not delete the source, i.e. F.Object_Reuse does not apply here.

6.1.9 SOF claim

According to the ***Common Methodology for Information Technology Security Evaluation*** CEM-99/045 Part 2: Evaluation Methodology, Version1.0, August 1999 [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 algorithms F.DES and F.RSA are resistant (F.LOG) against Simple Power Analysis (SPA), Differential Power Analysis (DPA), Differential Fault Analysis (DFA) and timing attacks. The quality of these mechanisms against leakage attacks can be analyzed using probabilistic or permutational methods.
  - The implementation of the RSA key generation F.RSA_KeyGen is resistant (F.LOG) against Simple Power Analysis (SPA) and timing attacks. The quality of these mechanisms against leakage attacks can be analyzed using probabilistic or permutational methods.

- The implementation of the RSA key generation F.RSA_KeyGen contains a primality test. The error probability of this test 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 as a cryptographic mechanism in the sense of Common Criteria.

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

Note 21. The cryptographic algorithms of F.HW_DES, F.DES, F.RSA as well as F.RSA_KeyGen can also be analyzed with permutational or probabilistic methods, but this is not in the scope of Common Criteria evaluations.

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 [11]. 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 EAL4+ as defined in section 1.3. The following table lists all assurance components applicable.

Assurance Component	Input evidence according to Common Criteria Part 3 [3]
ACM_AUT.1 ACM_CAP.4 ACM_SCP.2	Configuration Management documentation
ADO_DEL.2 ADO_IGS.1	Documentation on delivery, installation, generation and start-up
ADV_FSP.2	functional specification
ADV_HLD.2	high-level design (semiformal)
ADV_IMP.2	implementation representation
ADV_LLD.1	low level design
ADV_RCR.1	correspondence analysis
ADV_SPM.1	informal TSP model
AGD_ADM.1	administrator guidance
AGD_USR.1	user guidance

Assurance Component	Input evidence according to Common Criteria Part 3 [3]
ALC_DVS.2 ALC_LCD.1 ALC_TAT.1	life cycle documentation
ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2	test documentation
AVA_MSU.3 AVA_SOF.1 AVA_VLA.4	vulnerability analysis

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

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 [11].

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 P5CC036V1D), 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, TSFR) are derived from this new policy.

The Security Objective O.RND is extended to include also the software (pseudo) random number generator (see also Note 3).

The following Security Objectives (see also section 4.1) are additionally included in this current Security Target:

- O.DES3
- O.RSA
- O.RSA_KeyGen
- O.SHA-1
- O.REUSE
- O.COPY

The following IT Security Requirements (see also chapter 5) are additionally included in this current Security Target:

- TOE Security Functional Requirements (see also section 5.1.1):
  - FCS_COP.1[SW DES]
  - FCS_COP.1[RSA]
  - FCS_COP.1[SHA-1]
  - FCS_CKM.1
  - FDP_RIP.1
  - FCS_RND.2
  - FPT_TST.2
- Security Functional Requirements for the IT environment (see also section 5.2.1):
  - FCS_CKM.2 (as a dependency of the new RSA key generation)

This ST does not add any new TOE Security Assurance Requirements (see also section 5.1.2). The assurance requirements are those defined in the PP [9] (EAL4 augmented by ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4, see also section 1.3).

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].

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	

Table 15: Security Objectives versus Assumptions, Threats or Policies

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.

Assumption/Policy	Security Objective	Note
P.Add-Components	O.HW_DES3 O.MF_FW O.MEM_ACCESS O.SFR_ACCESS O.Leak-Inherent O.Phys-Probing O.Malfunction O.Phys-Manipulation O.Leak-Forced	
P.Add-Func	O.DES3 O.RSA O.SHA-1 O.RSA_KeyGen O.RND O.REUSE	

Assumption/Policy	Security Objective	Note
	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.Preconditions	OE.Preconditions	

Table 16: Additional Security Objectives versus Assumptions or Policies

The justification related to the policy “Additional Specific Security Components (**P.Add-Components**)” is as follows:

The justification related to the security objectives O.HW_DES3, O.MF_FW, O.MEM_ACCESS and O.SFR_ACCESS is as follows: Since these objectives requires the TOE to implement exactly the same specific security functionality as required by P.Add-Components, the organisational security policy is covered by the objectives.

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

The requirements for a multi-application platform necessitate the separation of users. Therefore it is volitional that most of the security functions cannot be influenced or used in the User Mode.

The justification related to the policy “Additional Specific Security Functionality (**P.Add-Func**)” is as follows:

The justification related to the security objectives O.DES3, O.RSA, O.SHA-1, O.RSA_KeyGen, O.RND, O.COPY, O.REUSE and O.MEM_ACCESS is as follows: Since the objectives 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 objectives listed above.

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 also support P.Add-Func. These security objectives are also valid for the additional specific security functionality since they must avert the related threats also for the components added related to the policy.

The justification related to the assumption “Usage of Key-dependent Functions (**A.Key-Function**)” is as follows:

- 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.

The justification related to the assumption "Check of initialisation data by the Smartcard Embedded Software (**A.Check-Init**)" is as follows:

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 objective.

The justification related to the assumption "Operational preconditions (**A.Preconditions**)" is as follows:

Since OE.Preconditions requires the Smartcard Embedded Software developer to ensure that the necessary preconditions as stated in the assumption A.Preconditions are met, the assumption is covered by the objective. This applies to (1) the operational preconditions for SHA-1 as well as to (2) the preconditions for RSA-CRT.

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

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.

Objective	TOE Security Functional Requirements	Security Requirements for the environment
O.Leak-Inherent	- FDP_ITT.1 “Basic internal transfer protection” - FPT_ITT.1 “Basic internal TSF data transfer protection” - FDP_IFC.1 “Subset information flow control”	RE.Phase-1 “Design and Implementation of the 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”	

Objective	TOE Security Functional Requirements	Security Requirements for the environment
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 22 below (for aspects concerning the software RNG)	RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software” (e.g. by implementing FPT_AMT.1 “Abstract machine testing”)
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

Table 17: Mapping of Security Requirements to Security Objectives in the PP

✸ 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 22. 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 18 describes this in more detail.

The Security Target additionally defines the SFRs for the TOE that are listed in Table 18. In addition Security Requirements for the Environment are defined. The following table, which bases upon the Hardware Security Target [11], gives an overview, how the requirements are combined to meet the security objectives.

Objectives	TOE Security Functional Requirements	Security Requirements for the environment
O.RND	FCS_RND.2 „Random number generation“ for the software RNG FPT_TST.2 „Subset TOE security testing“	RE.RNG2
O.HW_DES3	FCS_COP.1[DES]	RE.Phase-1 with RE.Cipher
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] FDP_IFC.1 FDP_ITT.1 FPT_ITT.1 FPT_FLS.1 FRU_FLT.2	RE.Phase-1 with RE.Cipher
O.SHA-1	FCS_COP.1[SHA-1] FDP_IFC.1 FDP_ITT.1 FPT_ITT.1	RE.Phase-1 with RE.Cipher
O.RSA_KeyGen	FCS_CKM.1 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.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)
O.SFR_ACCESS	FDP_ACC.1[SFR] FDP_ACF.1[SFR] FMT_MSA.3[SFR] FMT_MSA.1[SFR] FMT_SMF.1	
OE.Plat-Appl (clarification)		RE.Phase-1 with RE.Cipher and RE.RNG

Objectives	TOE Security Functional Requirements	Security Requirements for the environment
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
OE.Preconditions		RE.Preconditions

Table 18: Mapping of Security Requirements to Security Objectives in this ST

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 18. 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 3.3).

The justification related to the security objective “Triple DES Functionality” (**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 to use 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 related to the security objectives "RSA algorithm (**O.RSA**)" is as follows:

- The same arguments as stated above for O.DES3 are valid for O.RSA and FCS_COP.1[RSA], including the arguments given for side channel resistance. Note that as of today no promising DFA attack scenarios are know for "straight forward" RSA, so that explicit DFA countermeasures are only included for the RSA-CRT implementation; this is indicated by "n.a." in Table 7.

  For the RSA-CRT, there exist two implementations, called "RSA-CRT algorithm 1" and "RSA-CRT algorithm 2" in Table 7. Only "RSA-CRT algorithm 1" provides built-in resistance against DFA Attacks. The other algorithm does not provide countermeasures against DFA Attacks, but still provides all other countermeasures against Side Channel Attacks. When using that second algorithm, the user of the Secured Crypto Library on the P5CC036V1D first has to analyze and decide whether DFA attacks are applicable in the specific field of application, and has to implement effective DFA countermeasures on his own, if necessary. Therefore here the security functionality is split over the TOE and the environment. This fact is correctly formulated in the objective for the environment OE.Preconditions and the derived requirement for the environment, RE.Preconditions.

The justification related to the security objective "SHA-1 hash algorithm (**O.SHA-1**)" is as follows:

- O.SHA-1 requires the TOE to implement the SHA-1 hash algorithm. Exactly this is the requirement of FCS_COP.1[SHA-1]. Therefore FCS_COP.1[SHA-1] is suitable to meet O.SHA-1.
- FDP_IFC.1, FDP_ITT.1 and FPT_ITT.1 are mapped to O.SHA-1 because of the intended resistance of SHA-1 against SPA and timing attacks. SHA-1 does not include DFA countermeasures for side channel resistance, therefore FPT_FLS.1 and FRU_FLT.2 (which together require DFA resistance) are not mapped to O.SHA-1.
- 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 related to the security objective “RSA key generation (**O.RSA_KeyGen**)” is as follows:

- O.RSA_KeyGen requires the TOE to include functionality to generate RSA (and RSA CRT) key pairs (resistant to attack as described in Table 7). 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. Note, that O.RSA_KeyGen does not claim do be resistant against DFA attacks (no such attack scenarios are known at the moment; this is indicated by “n.a.” in Table 7), therefore FRU_FLT.2 and FPT_FLS.1 are not mapped.
- 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 related to the security objective “Secure Memory Copy (**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 related to the security objective “Protection of residual information (**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.

The justifications for the following hardware-related security objectives have already been given in the Hardware Security Target [11] or even in the Protection Profile [9] and are still valid. For ease of reading those parts of the rationale taken from the Hardware Security Target [11] (O.HW_DES3, O.MEM_ACCESS and O.SFR_ACCESS as well as security objectives for the environment) will be repeated here (at least partly). The rather long rationale within the PP, however, is not repeated here; please refer to [9].

The justification related to the security objective “Triple DES Functionality“(**O.HW-DES3**) is as follows:

- O.HW_DES3 requires the TOE to support Triple DES encryption and decryption. Exactly this is the requirement of FCS_COP.1. Therefore FCS_COP.1 is suitable to meet O.HW_DES3.

The justification related to the security objective “Area based Memory Access Control (**O.MEM_ACCESS**)” is as follows:

- The security functional requirement “Subset access control (FDP_ACC.1[MEM])” together with the related Security Function Policy (SFP) “Memory Access Control Policy” exactly require to implement an area based memory access control as demanded by O.MEM_ACCESS. Therefore, FDP_ACC.1 with its SFP (defined by FDP_ACF.1[MEM]) is suitable to meet the security objective. Details about the contribution of FMT_MSA.3[MEM], FMT_MSA.1[MEM], FMT_MSA.1[SFR] and FMT_SMF.1 can be found in section 8.2.1 of the Hardware Security Target [11] rationale.

The justification related to the security objective “Special Function Register Access Control” (**O.SFR_ACCESS**) is as follows:

- The security functional requirement “Subset access control (FDP_ACC.1[SFR])” with the related Security Function Policy (SFP) “Access Control Policy” requires to implement access control for Special Function Register as demanded by O.SFR_ACCESS. Therefore, FDP_ACC.1[SFR] with its SFP (defined by FDP_ACF.1[SFR]) is suitable to meet the security objective. Details about the contribution of FMT_MSA.3[SFR], FMT_MSA.1[SFR] and FMT_SMF.1 can be found in section 8.2.1 of the Hardware Security Target [11] rationale.

The crypto library has been developed taking the objectives **OE.Plat-Appl** and **OE.Resp-Appl** into account. The issue of the treatment of cryptographic keys has already been addressed above. However, since the crypto library is only one part of the Smartcard Embedded Software, the requirements OE.Plat-Appl and OE.Resp-Appl also need to be satisfied by any Smartcard Embedded Software that uses the crypto library.

The justification related to the clarification of the security objectives “Usage of Hardware Platform (**OE.Plat-Appl**)” and “Treatment of User Data (**OE.Resp-Appl**)” is as follows:

- The usage of cryptographic algorithms requires to use 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.Cipher addresses the usage of keys generated inside the Smartcard IC as well as keys downloaded into the Smartcard IC. The requirement for the usage of appropriate cryptographic keys for the cryptographic functions is suitable to meet OE.Plat-Appl and OE.Resp-Appl.
- The Crypto Library has added implementations of the cryptographic functions 3DES, RSA and SHA-1 (FCS_COP.1[SW-DES], FCS_COP.1[RSA] and FCS_COP.1[SHA-1]) as well as RSA key generation (FCS_CKM.1). From FCS_COP.1 and FCS_CKM.1 dependencies arise: Generation or import (loading) of keys to be used for the cryptographic operations has to be ensured, as well as destruction of such keys after use. Likewise, the generated RSA key pairs have to be exported (typically at least the public key part has to be exported). Note that no dependencies arise from FCS_COP.1[SHA-1], if SHA-1 does not calculate on keys. If, however, SHA-1 is used for key derivation, the Smartcard Embedded Software has to ensure .
  - The dependencies that arise from FCS_COP.1[SW-DES] and FCS_COP.1[RSA] (and possibly also from FCS_COP.1[SHA-1]) are: [**FDP_ITC.1** or **FCS_CKM.1**], **FCS_CKM.4**, and **FMT_MSA.2**. To be exact, all these dependencies would have to be iterated two or three time (for FCS_COP.1[SW-DES] and FCS_COP.1[RSA] and FCS_COP.1[SHA-1], respectively). These iterations have not been written down explicitly in section 5.2.1; instead Note 14 has been added to section 5.2.1.
  - The dependencies that arise from FCS_CKM.1 (RSA key pair generation) are: [**FCS_CKM.2** or **FCS_COP.1**], **FCS_CKM.4**, and **FMT_MSA.2**.
- All these requirements ([FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2 and [FCS_CKM.2 or FCS_COP.1]) have to be fulfilled by the IT security environment and can be traced back to the objective for the environment **OE.Resp-Appl** (see also the Clarification of “Treatment of User Data (OE.Resp-Appl)” in the Hardware Security Target [11]).

  Since the Crypto Library implements functionality to generate RSA key pairs, the dependency from FCS_COP.1[RSA] to FCS_CKM.1 is fulfilled by the TOE itself. However, if an application intends to load RSA key pairs from the outside, then the dependency remains. – For other cryptographic algorithms for which the TOE does not implement a key generation method, the dependency also remains and leads to a security functional requirement for the IT environment. See also the discussion in Note 13.
- **FMT_SMR.1** requires the definition and maintenance of the roles that act on behalf of the functions provided by the hardware. This role model must be the subject of the Smartcard Embedded Software. (The hardware provides different modes of operation that shall be used by the Smartcard Embedded Software to realise the required security roles.) Therefore FMT_SMR.1 can be traced back to OE.Resp-Appl.
- The developer of the Smartcard Embedded Software must ensure that the additional functions are used as specified and that the User Data processed by these functions are protected as defined for the application context. Using a multi-application operating system may add additional requirements for the separation of different

applications by a memory management scheme based upon security mechanisms of the TOE. These issues are addressed by the requirement RE.Phase-1.

- Using a multi-application operating system may add additional requirements for the separation of different applications by a memory management scheme based upon security mechanisms of the TOE. These issues are addressed by the requirement **RE.Phase-1**. The Smartcard Embedded Software must implement additional measures regarding RE.Phase-1 defined in the PP [9] (refer to the third point of the enumeration under RE.Phase-1 "findings of the TOE evaluation reports relevant for the Smartcard Embedded Software"). These measures are addressed in the **NXP Semiconductors Guidance, Delivery and Operation Manual:** *Evaluation of NXP P5CC036V1D - Secure Smart Card Controller, Revision 1.2,* January 8th, 2009.
- In addition RE.Phase-1 requires beside the specified usage of all security functions the treatment of User Data that means security relevant user data of one application cannot be disclosed to another application when a multi-application operating system is implemented as part of the Smartcard Embedded Software. Therefore the developer of the Smartcard Embedded Software, shall design mainly the operating system in a way that user data cannot be disclosed to an unauthorized subject.
- The justification of the additional security objective and the additional requirements (both Security Functional Requirements and Security Requirements for the Environment) show that they do not contradict to the rationale already given in the Protection Profile for the assumptions, policy and threats defined there.

The justification related to the security objective "Check of initialisation data by the Smartcard Embedded Software" (**OE.Check-Init**) is as follows:

- RE.Check-Init requires at least a check of the FabKey data that is part of the pre-personalization data to prevent the use of Smartcard ICs that are not correctly tested and pre-personalised by the TOE Manufacturer. The FabKey comprises secret information that is exchanged between the Card Manufacturer and the TOE Manufacturer. F.COMP supports the storage of the FabKey data at the end of the test phase in the Test Mode. Only the Smartcard Embedded Software is able to check this data in the Application Mode. Therefore RE.Check-Init is suitable to meet OE.Check-Init.

The justification related to the security objective “Operational Preconditions (**OE.Preconditions**)” is as follows:

- OE.Preconditions requires the Smartcard Embedded Software developer to ensure that the necessary operational preconditions are met in order to avert side channel attacks (1) against the SHA-1 implementation and (2) against one of the RSA-CRT implementations. This is exactly is the requirement of RE.Preconditions, and RE.Preconditions specifies these preconditions by explicitly stating that
  a. an enforcement of voltage class A or B and activated CSEC mode establishes the necessary preconditions for SHA-1, and
  b. the applicability of DFA attacks has to be analysed and decided upon for RSA-CRT. If DFA attacks are applicable, then either the first DFA-CRT algorithm (called “RSA-CRT algorithm 1” in Table 7) shall be used or if using the second DFA-CRT algorithm (called “RSA-CRT algorithm 2” in Table 7) additional effective DFA countermeasures have to be implemented by the user of the crypto library.

Therefore RE.Preconditions is suitable to meet OE.Preconditions.

The justification of the additional security objectives and the additional requirements (both Security Functional Requirements and Security Requirements for the Environment) show that they do not contradict to the rationale already given in the Protection Profile 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 (EAL4+) 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 (EAL4+) 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 form 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 [11] 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:

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 13 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]
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

Table 19: Dependencies of security functional requirements

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 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], 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 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 12): 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 based on the underlying Protection Profile [9]. The Security Target uses the same augmentations as the PP.

The rationale for the augmentations is the same as in the PP.

As stated in the Protection Profile, section 7.2.3, it has to be assumed that attackers with high attack potential try to attack smart cards used for digital signature applications or payment systems. Therefore specifically AVA_VLA.4 was chosen by the PP in order to assure that even these attackers cannot successfully attack the TOE. For the same reason the Strength of Function level "high" is required.

8.2.5 Security Requirements are Mutually Supportive and Internally Consistent

The discussion of security functional requirements and assurance components in the preceding sections has shown that mutual support and consistency are given for both groups of requirements. The arguments given 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 and that there are no inconsistencies between these groups.

The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the cryptographic algorithms and the memory access/separation control function as well as the access control to Special Function Register implemented according to the security functional requirement FCS_COP.1 with its iterations and FDP_ACC.1[MEM], FDP_ACC.1[SFR] with reference to the Access Control Policies defined in FDP_ACF.1[MEM] and FDP_ACF.1[SFR]. Therefore, these security functional requirements support the secure implementation and operation of FCS_COP.1 and of FDP_ACC.1 with FDP_ACF.1 as well as the dependent security functional requirements.

A smartcard platform requires Smartcard Embedded Software to build a secure product. Thereby the Smartcard Embedded Software must support the security functions of the crypto library and implement a sufficient management of the security functions implemented. The realisation of the Security Functional Requirements within the TOE provide a good balance between flexible configuration and restrictions to ensure a secure behaviour of the TOE.

8.3 TOE Summary Specification Rationale

8.3.1 Rationale for TOE security functions

The following table reproduces the mapping of TSF to SFR for the hardware part of the TOE given in the Hardware Security Target [11]. After this an additional table with a

mapping for the new TSF of the crypto library is given. The mapping is described in detail only in the full version of the Security Target

	F.RNG	F.HW_DEA	F.OPC	F.PHY	F.LOG	F.COMP	F.MEM_ACC	F.SFR_ACC
FAU_SAS.1				X		X		
FCS_RND.1	X			X				
FDP_IFC.1				X	X			
FDP_ITT.1				X	X			
FMT_LIM.1				X		X		
FMT_LIM.2				X		X		
FPT_FLS.1			X	X				
FPT_ITT.1				X	X			
FPT_PHP.3				X				
FPT_SEP.1			X	X		X		
FRU_FLT.2			X	X				
FCS_COP.1[DES]		X		X				
FDP_ACC.1[MEM]				X			X	
FDP_ACC.1[SFR]				X				X
FDP_ACF.1[MEM]				X			X	
FDP_ACF.1[SFR]				X				X
FMT_MSA.1[MEM]				X			X	
FMT_MSA.1[SFR]				X				X
FMT_MSA.3[MEM]				X			X	
FMT_MSA.3[SFR]				X				X
FMT_SMF.1				X			X	X

Table 20: Mapping of TSFR to TSF for the hardware part of the TOE

	F.RNG_Access	F.DES	F.RSA	F.SHA-1	F.RSA_KeyGen	F.Object_Reuse	F.LOG	F.COPY
FCS_COP.1[SW-DES]		X						
FCS_COP.1[RSA]			X					
FCS_COP.1[SHA-1]				X				
FCS_CKM.1					X			
FCS_RND.2	X							
FPT_TST.2	X							

	F.RNG_Access	F.DES	F.RSA	F.SHA-1	F.RSA_KeyGen	F.Object_Reuse	F.LOG	F.COPY
FDP_RIP.1						X		
FDP_ITT.1, FPT_ITT.1 and FDP_IFC.1							X	
FPT_FLS.1							X	
FDP_ITT.1[COPY], FPT_ITT.1[COPY]								X

Table 21: Mapping of TSFR to TSF for the crypto library part of the TOE

The "X" means that the TOE Security Function realises or supports the functionality required by the respective Security Functional Requirement.

There are additional security features that can contribute to the security of the TOE when they are sufficiently controlled by the Smartcard Embedded Software. For example, the CRC-component of the underlying hardware can be used to verify the integrity of memory areas defined by the Smartcard Embedded Software.

8.3.2 Rationale for assurance measures

The assurance measures defined in section 6.2 are considered to fulfil the assurance requirements of the CC [3] level EAL4. Since the Protection Profile also defines assurance measures that are suitable to fulfil the requirements of EAL4, all input deliverables as listed in section 6.2 shall be sufficient to fulfil the assurance requirements of the PP. 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 NXP.

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 to 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 [11] (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 current 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 (EAL4+) is identical to the requirements claimed by the PP (EAL4+), with the same augmentations.

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)

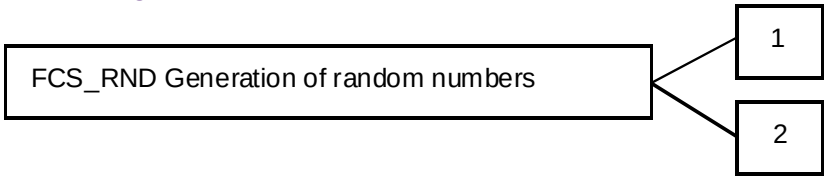
This family describes the functional requirements for random number generation used for cryptographic purposes.

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 levelling



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.

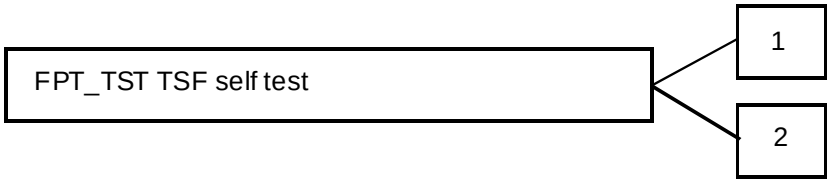
9.1.2 TSF self test (FPT_TST)

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 levelling



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.2	Subset 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 [9]) 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.

9.4 List of Abbreviations

CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
CC	Common Criteria Version 2.2 or Version 2.1. Note that the Version 2.2 is technically identical with Version 2.1 (ISO 15408) of the Common Criteria with all final interpretations until Dec. 31st, 2003, applied.
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[25]
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.

9.5 Bibliography

9.5.1 CC + CEM

[1] **Common Criteria for Information Technology Security Evaluation** – Part1: Introduction and general model, Version 2.1, August 1999, CCIMB-99-031

[2] **Common Criteria for Information Technology Security Evaluation** – Part2: Security functional requirements, Version 2.1, August 1999, CCIMB-99-032

[3] **Common Criteria for Information Technology Security Evaluation** – Part3: Security assurance requirements, Version 2.1, August 1999, CCIMB-99-033

[4] **Common Methodology for Information Technology Security Evaluation** CEM-99/045 Part 2: Evaluation Methodology, Version1.0, August 1999

9.5.2 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):** *AIS32: Anwendungshinweise und Interpretationen zum Schema, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema,* Version 1, July 2nd, 2001

[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

9.5.3 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

[25] This security target does not use SFR as abbreviation of Special Function Register in the explanatory text to avoid confusion. However, the abbreviation is used in objective or security function identifiers and to distinct iterations.

[10] **Atmel, Hitachi Europe, Infineon Technologies, Philips Semiconductors, T-Systems ISS GmbH:** *Smartcard Integrated Circuit Platform Augmentations,* Version 1.00, March 8th, 2002

[11] **NXP Semiconductors Documentation: Security Target –** *Evaluation of the* NXP P5CC036V1D Secure *Smart Card Controller, Version 1.2, January* 8th, 2009

[12] **NXP Semiconductors Documentation: Security Target Lite** – *Evaluation of* the NXP P5CC036V1D *Secure Smart Card Controller, Version 1.2,* January 8th, 2009

[13] **NXP Semiconductors Guidance, Delivery and Operation Manual:** *Evaluation of NXP P5CC036V1D - Secure Smart Card Controller, Revision 1.2,* January 8th, 2009

[14] **Philips Semiconductors Data Sheet:** *SmartMX - P5CC036 Secure Smart Card Controller,* Revision 3.3, June 27th, 2005, Document-ID 081733

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

9.5.4 Documents related to the crypto library

[16] **NXP Semiconductors User Guidance: Secured Crypto Library** *on the P5CC036V1D, User Guidance, Revision 2.2, January 8th, 2009*

[17] **Philips Semiconductors User Guidance: Crypto Library on** *SmartMX – Pseudo Random Number Generator & Chi-Squared Test Library,* User Guidance, Revision 3.0, November 23rd, 2005

[18] **Philips Semiconductors User Guidance:** *Crypto Library on SmartMX – Secured DES Library,* User Guidance, Revision 2.0, November 23rd, 2005

[19] **Philips Semiconductors User Guidance:** Crypto Library on *SmartMX – SHA-1 Library, User Guidance, Revision 3.0, November 23rd,* 2005

[20] **Philips Semiconductors User Guidance: Crypto Library on** *SmartMX – Secured RSA Library, User Guidance, Revision 3.0, November* 23rd, 2005

[21] **Philips Semiconductors User Guidance: Crypto Library on** *SmartMX – Secured RSA Key Generation Library, User Guidance, Revision* 3.0, November 23rd, 2005

[22] **Philips Semiconductors Software Delivery Description:** *Crypto Library on SmartMX, Secured Random Number Library,* CC EAL4+ on P5CC036V1D, Delivery Module Contents, Revision 1.0, November 23rd, 2005, Document-ID 117410

[23] **Philips Semiconductors Software Delivery Description:** *Crypto Library on SmartMX, Secured DES Library,* CC EAL4+ on P5CC036V1D, Delivery Module Contents, Revision 1.0, November 23rd, 2005, Document-ID 117110

[24] **Philips Semiconductors Software Delivery Description:** *Crypto Library on SmartMX, SHA-1 Library,* CC EAL4+ on P5CC036V1D, Delivery Module Contents, Revision 1.0, November 23rd, 2005, Document-ID 117510

[25] **Philips Semiconductors Software Delivery Description:** *Crypto Library on SmartMX, Secured RSA Library,* CC EAL4+ on P5CC036V1D, Delivery Module Contents, Revision 1.0, November 23rd, 2005, Document-ID 117210

[26] **Philips Semiconductors Software Delivery Description:** *Crypto Library on SmartMX, Secured RSA Key Generation Library,* CC EAL4+ on P5CC036V1D, Delivery Module Contents, Revision 1.0, November 23rd, 2005, Document-ID 117310

9.5.5 Standards and text books

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

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

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

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

[31] **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

[32] **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

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

[34] **FIPS PUB 180-1,** Secure Hash Standard, Federal Information Processing Standards Publication, April 17th, 1995, US Department of Commerce/National Institute of Standards and Technology

[35] *Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung, Übersicht über geeignete Algorithmen vom 17. Dezember 2007*, published at 05 February 2008 in Bundesanzeiger Nr 19, page 376

10. Legal information

10.1 Definitions

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

10.2 Disclaimers

General — 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.

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 for 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.

10.3 Trademarks

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

11. Contents

continued >>

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

Date of release: 8 January 2009