Firmware Libraries V1.1 on P40C012/040/072 VD

Security Target Lite

Rev. 1.1 – 09 January 2015 **Evaluation documentation**

Final **Public**

NSCIB-CC-13-37968

Document Information

Info	Content
Keywords	CC, Security Target Lite, SmartMX2 P40 FW Libraries V1.1
Abstract	Security Target Lite of the Firmware Libraries V1.1 on P40C012/040/072 VD, which is developed and provided by NXP Semiconductors, Business Unit Identification according to the Common Criteria for Information Technology Security Evaluation Version 3.1 at EAL5 augmented

Rev	Date	Description
0.9	11-December-2014	Initial Version
1.0	19-December-2014	Updated RNG User Manual reference.
1.1	09-January-2015	Additional statement on TOE scope added to section 1.3.1.

1 ST Introduction

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

1.1 ST Reference

Firmware Libraries V1.1 on P40C012/040/072 VD Security Target, 1.1, NXP Semiconductors, 09 January 2015.

1.2 TOE Reference

This Security Target refers to the Firmware Libraries V1.1 on P40C012/040/072 VD (TOE) provided by NXP Semiconductors, Business Unit Identification for Common Criteria evaluation.
The TOE is a composite TOE, consisting of:

- The hardware “NXP Secure Smart Card Controller P40C012/040/072 VD”, which is used as evaluated platform, and all its Major Configurations (see [12] for details)
- The ”SmartMX2 P40 FW Libraries V1.1”, which is built upon this platform.

This Security Target builds on the Hardware Security Target [12], which refers to the ”NXP Secure Smart Card Controller P40C012/040/072 VD” provided by NXP Semiconductors, Business Unit Identification.

1.3 TOE Overview

1.3.1 Introduction

The Hardware Security Target [12] contains, in section “ST Overview”, an introduction about the P40C012/040/072 hardware TOE that is considered in the evaluation. The Hardware Security Target includes IC Dedicated Software stored in the ROM provided with the P40C012/040/072 hardware platform. The “SmartMX2 P40 FW Libraries V1.1” is a set of firmware libraries, which provides cryptographic functions and memory functions that can be used by the Smartcard embedded Software. The firmware libraries consist of several binary packages that are intended to be linked to the Smartcard Embedded Software. The Smartcard Embedded Software developer links the binary packages that he needs to his Smartcard Embedded Software and the whole is subsequently implemented in the User ROM. The NXP Secure Smart Card Controller P40C012/040/072 VD provides the computing platform and cryptographic support by means of co-processors for the SmartMX2 P40 FW Libraries V1.1. The SmartMX2 P40 FW Libraries V1.1 provides the security functionality described below in addition to the functionality described in the Hardware Security Target [12] for the hardware platform.
The SmartMX2 P40 FW Libraries V1.1 consists of of three parts, the Crypto Library, the HAL-Library and the Comm-Library.
The Crypto Library provides AES, DES, Triple-DES (3DES), RSA, , SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 algorithms. Most algorithms are resistant against attacks as described in the JIL attack methods for

smartcard and similar devices [8]. In addition, the Crypto Library implements a software (pseudo) random number generator which is initialized (seeded) by the hardware random number generator of the P40C012/040/072. Finally, the TOE provides a secure copy routine, a secure memory compare routine and includes internal security measures for residual information protection.
The HAL-Library provides memory functions to operate on RAM and NV memory, functions to compute CRCs and Config and Patch functionality.
The Comm-Library provides an interface to the T=0 and T=1 protocols of ISO/IEC 7816-3.
This Security Target defines a set of security requirements for the Crypto Library. There are no specific security requirements for the HAL and Comm-Library. For more details on the security requirements for the TOE please refer to Section 6 of this Security Target.

1.4 TOE Description

1.4.1 Physical Scope of TOE

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

- The hardware part consists of the NXP Secure Smart Card Controller P40C012/040/072 VD with IC Dedicated Software stored in the Test-ROM that is not accessible in the System Mode or the User Mode after Phase 3 (please see Section 1.4.4 for more details on the life cycle of the TOE). The hardware part of the TOE includes dedicated guidance documentation.

- The software part consists of the IC Dedicated Support Software ”SmartMX2 P40 FW Libraries V1.1” which consists of a software library and associated documentation. The SmartMX2 P40 FW Libraries V1.1 is an additional part that provides cryptographic functions that can be operated on the hardware platform as described in this Security Target.

The hardware part of the TOE is not described in detail in this document. Details are included in the Hardware Security Target [12] and therefore this latter document will be cited wherever appropriate. However the assets, assumptions, threats, objectives and security functional requirements are tracked in this Security Target.
The TOE components consist of all the TOE components listed in Table 1.1 of the Hardware Security Target [12] plus all TOE components listed in the Table 1.1 and Table 1.2, resp. 1.3, resp. 1.4 below:

Type	Name	Release	Date	Form of Delivery
Library File	libCryptoLibSymCiphers.a	1.0	11.09.2014	Electronic file
Library File	libCryptoLibSha.a	1.0	11.09.2014	Electronic file
Library File	libCryptoLibRng.a	1.0	11.09.2014	Electronic file
Library File	libCryptoLibRsa.a	1.0	11.09.2014	Electronic file
Library File	libCryptoLibUtils.a	1.0	11.09.2014	Electronic file
Header File	phCryptoLibSymCiphers.h	1.0	11.09.2014	Electronic file
Header File	phCryptoLibSha.h	1.0	11.09.2014	Electronic file
Header File	phCryptoLibRng.h	1.0	11.09.2014	Electronic file
Header File	phCryptoLibRsa.h	1.0	11.09.2014	Electronic file
Header File	phCryptoLibRsa_OAEP.h	1.0	11.09.2014	Electronic file
Header File	phCryptoLibRsa_PSS.h	1.0	11.09.2014	Electronic file
Header File	phCryptoLibUtils_Arith.h	1.0	11.09.2014	Electronic file
Header File	phCryptoLibUtils_MemMgmt.h	1.0	11.09.2014	Electronic file
Document	User guidance manual Firmware Libraries V1.1 on P40C012/040/072 VD, Preparative procedures and operational user guidance [15]	1.4	19.12.2014	Electronic Document
Document	User Guidance: Symmetric Crypto Library [19]	1.4	16.10.2014	Electronic Document
Document	User Guidance: SHA Library [18]	1.4	16.10.2014	Electronic Document
Document	User Guidance: RNG Library [16]	1.5	19.12.2014	Electronic Document
Document	User Guidance: RSA Library [17]	1.4	16.10.2014	Electronic Document
Document	User Guidance: Utils Library [20]	1.4	16.10.2014	Electronic Document

Tab. 1.1: Components of the TOE (CryptoLib)

Type	Name	Release	Date	Form of Delivery
DAT File	SystemMode.dat	1.1	18.11.2014	Electronic file
Library File	libHALLibComm.a	1.1	18.11.2014	Electronic file
BCF File	HAL.bcf	1.1	18.11.2014	Electronic file
CFG File	SystemMode_FirewallValues.cfg	1.1	18.11.2014	Electronic file
Header File	phhalComm.h	1.1	18.11.2014	Electronic file
Header File	phhalConf.h	1.1	18.11.2014	Electronic file
Header File	phhalCrc.h	1.1	18.11.2014	Electronic file
Header File	phhalMem.h	1.1	18.11.2014	Electronic file
Header File	phhalMem_AT.h	1.1	18.11.2014	Electronic file
Header File	phhalMem_NV.h	1.1	18.11.2014	Electronic file
Header File	phhalPatch.h	1.1	18.11.2014	Electronic file
Header File	phP4xAppl.h	1.1	18.11.2014	Electronic file
Document	User guidance manual Firmware Libraries V1.1 on P40C012/040/072 VD, Preparative procedures and operational user guidance [15]	1.4	19.12.2014	Electronic Document
Document	Product data sheet addendum: SmartMX2 P40 family P40Cxxx HAL Interface Specification [13]	2.4	21.11.2014	Electronic Document

Tab. 1.2: Components of the TOE (HAL-Lib and Comm-Lib) - UserMode Customer

Type	Name	Release	Date	Form of Delivery
Library File	libHalCL.a	1.1	18.11.2014	Electronic file
Library File	libHalMem.a	1.1	18.11.2014	Electronic file
Library File	libHALLibComm.a	1.1	18.11.2014	Electronic file
Header File	phhalComm.h	1.1	18.11.2014	Electronic file
Header File	phhalCrc.h	1.1	18.11.2014	Electronic file
Header File	phhalMem.h	1.1	18.11.2014	Electronic file
Header File	phhalMem_AT.h	1.1	18.11.2014	Electronic file
Header File	phhalMem_NV.h	1.1	18.11.2014	Electronic file
Header File	phhalInit_CryptoLibSetup.h	1.1	18.11.2014	Electronic file
Header File	phhalInit_ATSetup.h	1.1	18.11.2014	Electronic file
Document	User guidance manual Firmware Libraries V1.1 on P40C012/040/072 VD, Preparative procedures and operational user guidance [15]	1.4	19.12.2014	Electronic Document
Document	Product data sheet addendum: SmartMX2 P40 family P40Cxxx HAL Interface Specification [13]	2.4	21.11.2014	Electronic Document

Tab. 1.3: Components of the TOE (HAL-Lib and Comm-Lib) - SystemMode Customer

Type	Name	Release	Date	Form of Delivery
Library File	libHalCL.a	1.1	18.11.2014	Electronic file
Library File	libHALLibComm.a	1.1	18.11.2014	Electronic file
Header File	phhalComm.h	1.1	18.11.2014	Electronic file
Header File	phhalCrc.h	1.1	18.11.2014	Electronic file
Header File	phhalMem.h	1.1	18.11.2014	Electronic file
Header File	phhalMem_AT_Minimal.h	1.1	18.11.2014	Electronic file
Header File	phhalMem_NV.h	1.1	18.11.2014	Electronic file
Header File	phhalInit_CryptoLibSetup.h	1.1	18.11.2014	Electronic file
Document	User guidance manual Firmware Libraries V1.1 on P40C012/040/072 VD, Preparative procedures and operational user guidance [15]	1.4	19.12.2014	Electronic Document
Document	Product data sheet addendum: SmartMX2 P40 family P40Cxxx HAL Interface Specification [13]	2.4	21.11.2014	Electronic Document

Tab. 1.4: Components of the TOE (HAL-Lib and Comm-Lib) - SystemMode Customer without libHalMem.a

Remark 1. For more information on the configuration options of the TOE the user is referred to [15].

1.4.2 Logical Scope of TOE

1.4.2.1 Hardware Description

The NXP SmartMX2 P40 hardware is described in section “Hardware Description” of the Hardware Security Target [12]. The IC Dedicated Test Software and IC Dedicated Support Software stored in the Test-ROM and delivered with the hardware platform is described in section “Software Description” of the Hardware Security Target [12].

1.4.2.2 Software Description

The IC Dedicated Test Software and IC Dedicated Support Software stored in the Test-ROM and delivered with the hardware platform is described in section “Software Description” of the Hardware Security Target [12].
A Smartcard embedded Software developer may create Smartcard embedded Software to execute on the P40C012/040/072 hardware. This software is stored in the User ROM of the P40C012/040/072 hardware and is not part of the TOE, with one exception: the Smartcard embedded Software may contain the ”SmartMX2 P40 FW Libraries V1.1” (or parts thereof and this SmartMX2 P40 FW Libraries V1.1 (or parts thereof) is part of the TOE.

1.4.2.2.1 Crypto-Library

1.4.2.2.1.1 AES

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

1.4.2.2.1.2 DES/3DES

- The DES and 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,CMAC

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

1.4.2.2.1.3 RSA

- The RSA algorithm can be used for encryption and decryption as well as for signature generation, signature verification, message encoding and signature encoding.
- The RSA public key computation can be used to compute the public key that belongs to a given private CRT key. The TOE supports various key sizes for RSA up to a limit of 2048 bits. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

1.4.2.2.1.4 SHA

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

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

1.4.2.2.1.5 Resistance of cryptographic algorithms against attacks

The cryptographic algorithms are resistant against attacks as described in JIL, Attack Methods for Smartcards and Similar Devices [8], which include Side Channel Attacks, Pertubation attacks, Differential Fault Analysis (DFA) and timing attacks, except for SHA, which is only resistant against Side Channel Attacks and timing attacks.

1.4.2.2.1.6 Random number generation

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

1.4.2.2.1.7 Other security functionality

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

1.4.2.2.2 HAL-Library

1.4.2.2.2.1 Configuration

The Configuration block of the HAL-Library allows to configure and retrieve generic parameters of the system, not covered in any specific module.

1.4.2.2.2.2 Communication

The Communication library is designed to abstract the interface for ISO/IEC 7816-3 communication from an application point of view. It implements both T=0 and T=1 protocol as described in the ISO/IEC 7816-3 specification and provides an API which hides the details in the specific protocol. For receptions, it transforms the received bytes from the UART into an APDU that is suitable for usage. For transmissions, it transforms an APDU from the application into bytes to sent over the UART.

1.4.2.2.2.3 Memory

The Memory component of the HAL-Library is responsible for implementing HW independent memory copy, set and compare functions. It takes care of the underlying type of destination memory (EEPROM, RAM) and calls the respective functions accordingly. The module can also handle overlapping buffers correctly. In addition, the Memory component takes care of the integrity of Non Volatile Memory (NVM) write operations even in case of unexpected power loss. This feature is called Anti-Tearing and it provides a mechanism such that all nonvolatile write operations are ensured to be atomic and the integrity of the data is maintained.

1.4.2.2.2.4 CRC

The CRC component of the HAL-Library is an external accessible block for calculating cyclic redundancy checks (CRC). It implements functions that support the calculation of several different CRC types which are listed below:

- CRC-8 (ITU-T)
- CRC-16 (CRC-CCITT)
- CRC-32 (IEEE 802.3)

1.4.2.2.2.5 Patch

To correct issues in an late OS development state or even when the product is released a patch mechanism is provided.

1.4.2.3 Documentation

The documentation for the NXP Secure Smart Card Controller P40C012/040/072 VD is listed in section “Documentation” of the Hardware Security Target [12].
The documentation of the SmartMX2 P40 FW Libraries V1.1 consists of the following documents:
For the crypto library, the user manuals contain:

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

For the HAL library and Comm library, there exists the

- SmartMX2 P40 family P40C12/040/072 HAL Interface Specification [13]

The user guidance document [15] contains:

- guidelines on the secure usage of the SmartMX2 P40 FW Libraries V1.1, including the requirements on the environment (the Smartcard Embedded Software calling the SmartMX2 P40 FW Libraries V1.1 is considered to be part of the environment).

1.4.3 Interface of the TOE

The interface to the NXP Secure Smart Card Controller P40C012/040/072 VD hardware is described in section “Interface of the TOE” of the Hardware Security Target [12]. The use of this interface is not restricted by the use of the SmartMX2 P40 FW Libraries V1.1.
The interface to the TOE additionally consists of software function calls, as detailed in the “User Manual” and “Interface Specification” documents the SmartMX2 P40 FW Libraries V1.1. The developer of the Smartcard Embedded Software will link the required functionality of the SmartMX2 P40 FW Libraries V1.1 into the Smartcard Embedded Software as required for his application.

1.4.4 Life Cycle

The life cycle of the hardware platform as part of the TOE is described in section “TOE Intended Usage” of the Hardware Security Target [12]. The delivery process or the hardware platform is independent from the SmartMX2 P40 FW Libraries V1.1.
The life-cycle phases are according to the Security IC Platform Protection Profile [14], section 1.2.4:

- Phase 1: IC Embedded Software Development

- Phase 2: IC Development
- Phase 3: IC Manufacturing
- Phase 4: IC Packaging
- Phase 5: Composite Product Integration
- Phase 6: Personalisation
- Phase 7: Operational Usage

The SmartMX2 P40 FW Libraries V1.1 is delivered as part of Phase 1 above to the Smartcard Embedded Software developer. The SmartMX2 P40 FW Libraries V1.1 may be delivered by e-mail or by delivering physical media such as compact disks by mail or courier. To protect the SmartMX2 P40 FW Libraries V1.1 during the delivery process, the SmartMX2 P40 FW Libraries V1.1 is encrypted and digitally signed. The Smartcard Embedded Software may comprise in this case an operating system and/or other smart card software (applications). The Smartcard Embedded Software developer then integrates the SmartMX2 P40 FW Libraries V1.1 in the Smartcard Embedded Software. The subsequent use of the SmartMX2 P40 FW Libraries V1.1 by Smartcard Embedded Software Developers is out of the control of the developer NXP Semiconductors, Business Line Identification; the integration of the SmartMX2 P40 FW Libraries V1.1 into Smartcard Embedded Software is not part of this evaluation.

1.4.5 Security during Development and Production

The development process of the SmartMX2 P40 FW Libraries V1.1 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 SmartMX2 P40 FW Libraries V1.1. The security measures installed within NXP, including a secure delivery process, ensure the integrity and quality of the delivered SmartMX2 P40 FW Libraries V1.1 binary files.

1.4.6 Specific Issues of Smartcard Hardware and the Common Criteria

Regarding the Application Note 4 of the Protection Profile [14] the TOE provides additional functionality which is not covered in the Protection profile [14] and the Hardware Security Target [12]. This additional functionality is added using the policy P.Add-Func (see section 3.3 of this Security Target).

1.4.7 TOE Intended Usage

The TOE user environment is the environment from TOE Delivery to phase 7. At the phases up to 6, the TOE user environment must be a controlled environment. Regarding to phase 7, the TOE 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 1.4.6 “TOE Intended Usage” in the Hardware Security Target [12].
The SmartMX2 P40 FW Libraries V1.1 is intended to support the development of the Smartcard Embedded Software since the cryptographic functions provided by the SmartMX2 P40 FW Libraries V1.1 include countermeasures against the threats described in this Security Target. The used modules of the SmartMX2 P40 FW Libraries V1.1 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.

Remark 2. The phases from TOE Delivery to phase 7 of the smart card life cycle are not part of the TOE construction process in the sense of this Security Target. Information about those phases is just included to describe how the TOE is used after its construction. Nevertheless the security features of the TOE cannot be disabled in these phases.

1.4.8 TOE User Environment

The user environment for the SmartMX2 P40 FW Libraries V1.1 is the Smartcard Embedded Software, developed by customers of NXP, to run on the NXP Secure Smart Card Controller P40C012/040/072 VD hardware.

1.4.9 General IT features of the TOE

The general features of the NXP Secure Smart Card Controller P40C012/040/072 VD hardware are described in section ”TOE overview” of the Hardware Security Target [12]. These are supplemented for the TOE by the functions listed in section 1.3.1 of this Security Target.

2 Conformance Claims

This Security Target claims to be conformant to the Common Criteria version 3.1:

- Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model - Version 3.1 CCMB-2012-09-001, Revision 4, September 2012, [2]
- Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components, Version 3.1 CCMB-2012-09-002, Revision 4, September 2012, [3]
- Common Criteria for Information Technology Security Evaluation, Part 3 – Security Assurance Components, Version 3.1 CCMB-2012-09-003, Revision 4, September 2012, [4]

For the evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2 – Evaluation Methodology, Version 3.1 CCMB-2012-09-004, Revision 4, September 2012, [5]

This Security Target claims to be conformant to CC Part 2 extended and to be CC Part 3 conformant. The extended Security Functional Requirements are defined in chapter 6.

2.1 Package Claim

This Security Target claims conformance to the assurance package **EAL5 augmented** augmented. The augmentations to EAL5 are ALC_DVS.2 and AVA_VAN.5. In addition, the Security Target is augmented using the component ASE_TSS.2, which is chosen to include architectural information on the security functionality of the TOE.

2.2 PP Claim

This Security Target claims conformance to the Protection Profile “Security IC Platform Protection Profile”, [14]. Since the Security Target claims conformance to the PP “Security IC Platform Protection Profile”, the concepts are used in the same sense. For the definition of terms refer to the Protection Profile [14]. This chapter does not need any supplement in the Security Target.
Regarding the Application Note 4 of [14] the TOE provides additional functionality which is not covered in the “Security IC Platform Protection Profile”. This additional functionality is added using the policy P.Add-Func (see section 3.3 of this Security Target).

2.3 Conformance Claim Rationale

According to section 2.2 this Security Target claims conformance to the Protection Profile “Security IC Platform Protection Profile, registered and certified by Bundesamt fuer Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035, Rev 1.0, 15 June 2007”[14].

The composed TOE type defined in section 1.4 of this Security Target is a smart card controller with IC dedicated software. This is consistent with the TOE definition for a Security IC in section 1.2.2 of [14].
The sections within this document where security problem definitions, 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 the content of the Protection Profile is not repeated in this Security Target. Moreover, all additionally stated items in this Security Target do not contradict the items included from the PP (see the respective sections in this document). The operations done for the SFRs taken from the PP are also clearly indicated.
The evaluation assurance level claimed for this TOE is shown in section 6.2 to include respectively exceed the requirements claimed by the PP.
These considerations show that the Security Target correctly claims conformance to the “Security IC Platform Protection Profile”, [14].

3 Security Problem Definition

This Security Target claims conformance to the "Security IC Platform Protection Profile", [14]. The Assets, Threats, Assumptions, and Organizational Security Policies are taken from the Protection Profile. In the following only the extensions of the different sections are detailed. The elements of the Security Problem Definition that are not extended in the Security Target. They are cited here for completeness.

This chapter is divided into the following sections: "Description of Assets", "Threats", "Organizational Security Policies", and "Assumptions".

3.1 Description of Assets

Since this Security Target claims conformance to the PP "Security IC Platform Protection Profile", [14], the assets defined in section 3.1 of the Protection Profile apply to this Security Target.
User Data and TSF data are mentioned as assets in [12]. 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.
More details about conditions and restrictions for resistance against attacks are given in the user documentation of the SmartMX2 P40 FW Libraries V1.1 [15].

3.2 Threats

Since this Security Target claims conformance to the PP "Security IC Platform Protection Profile", [14], the threats defined in section 3.2 of the Protection Profile are valid for this Security Target. The following table lists the threats defined by the PP:

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

Tab. 3.1: Threats defined in the Security IC Protection Profile

Remark 3. Within the Hardware Security Target [12], the threat T.RND has been used in a context where the hardware (true) random number generator is threatened. The TOE consists of both hardware (NXP Secure Smart Card Controller P40C012/040/072 VD) and software (SmartMX2 P40 FW Libraries V1.1). The Crypto Library

provides random numbers generated by a software (pseudo) random number generator. Therefore the threat T.RND explicitly includes both deficiencies of hardware random numbers as well as deficiency of software random numbers.

In compliance with Application Note 5 in the PP [14] the TOE provides additional functionality to protect against threats that appear when the TOE is used for multiple applications.
The TOE provides the Security IC Embedded Software running in System Mode with control of access to memories and hardware components by different applications running in User Mode. In this context, User Data of different applications is stored to such memory and processed by such hardware components. The Security IC Embedded Software controls all these User Data. Any access to User Data assigned to one application by another application contradicts separation between different applications and is considered as a threat.
The TOE shall avert threat T.Unauthorised-Access as specified below.

T.Unauthorised-Acce ss **Unauthorized Memory or Hardware Access**

Adverse action: An attacker may try to read, modify or execute code or data stored in restricted memory areas. And or an attacker may try to access or operate hardware resources that are restricted by executing code that accidentally or deliberately accesses these restricted hardware resources.
Any code executed or data used in Boot Mode, System Mode or User Mode may accidentally or deliberately access code or User Data of other applications. Any code executed or data used in Boot Mode, System Mode or User Mode may accidentally or deliberately access hardware resources that are restricted to other applications.

Threat agent: Attacker having high attack potential and access to the TOE.

Asset: Code executed by and data belonging to the IC Dedicated Support Software running in Super System Mode as well as code executed by and data belonging to the Security IC Embedded Software.

Restrictions of access to memories and hardware resources, which are available to the Security IC Embedded Software, must be defined and implemented by the security policy of the Security IC Embedded Software based on the specific application context.
The threats defined in the Hardware Security Target are summarized in Table 3.2.

Name	Title
T.Unauthorised-Access	Unauthorized Memory or Hardware Access

Tab. 3.2: Additional Threats defined in the HW-ST

3.3 Organizational Security Policies

Since this Security Target claims conformance to the PP “Security IC Platform Protection Profile”, [14], the policy P.Process-TOE: “Protection during TOE Development and Production” of the Protection Profile is applied here also.

Name	Title
P.Process-TOE	Protection during TOE Development and Production

Tab. 3.3: Policies defined in the Security IC Protection Profile

The hardware security target defines additional security policies.
The Crypto Library part of the TOE uses the symmetric crypto coprocessor hardware to provide DES security functionality and AES security functionality as listed below in P.Add-Func: Additional Specific Security Functionality.
In addition to the security functionality provided by the hardware mentioned above and defined in the Security Target of the NXP Secure Smart Card Controller P40C012/040/072 VD. 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

P.Add-Func **Additional Specific Security Functionality**

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

- AES encryption and decryption
- DES and Triple-DES encryption and decryption
- RSA encryption, decryption, signature generation, signature verification, message encoding and signature encoding.
- RSA public key computation
- SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 Hash Algorithms,
- access to the RNG (implementation of a software RNG),
- secure copy routine,
- secure compare routine;

In addition, the TOE shall

- provide protection of residual information.

Name	Title
P.Add-Func	Additional Specific Security Functionality

Tab. 3.4: Additional Security Policies defined in this ST

Regarding the Application Note 6 of “Security IC Platform Protection Profile”, [14] there are no other additional policies defined in this Security Target.

3.4 Assumptions

Since this Security Target claims conformance to the PP “Security IC Platform Protection Profile”[14], the assumptions defined in section 3.4 of the Protection Profile are valid for this Security Target. The following table lists the assumptions of the Protection Profile.

Name	Title
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation
A.Plat-Appl	Usage of Hardware Platform
A.Resp-Appl	Treatment of User Data

Tab. 3.5: Assumptions defined in the Security IC Protection Profile

The following additional assumptions are added in this Security Target from the P40C012/040/072 Hardware Security Target [12] and are valid for this Security Target.

Name	Title
A.Check-Init	Check of initialization data by the Security IC Embedded Software
A.Key-Function	Usage of Key-dependent Functions

Tab. 3.6: Assumptions defined in the Hardware Security Target [12]

4 Security Objectives

4.1 Security Objectives for the TOE

The TOE shall provide the following security objectives, taken from the Protection Profile “Security IC Platform Protection Profile”, [14]:

Name	Title
O.Leak-Inherent	Protection against Inherent Information Leakage
O.Phys-Probing	Protection against Physical Probing
O.Malfunction	Protection against Malfunctions
O.Phys-Manipulation	Protection against Physical Manipulation
O.Leak-Forced	Protection against Forced Information Leakage
O.Abuse-Func	Protection against Abuse of Functionality
O.Identification	TOE Identification
O.RND	Random Numbers

Tab. 4.1: Security Objectives of the TOE (PP)

Remark 4. Within the Hardware Security Target [12], the objective O.RND has been used in context with the hardware (true) random number generator (RNG). In addition to this, the TOE also provides a software (pseudo) RNG. Therefore the objective O.RND is extended to comprise also the quality of random numbers generated by the software (pseudo) RNG. See also Remark 3 in section 3.2, which extends T.RND in a similar way.

Additionally, the TOE shall provide the following security objectives, taken from the Hardware Security Target [12]:

Name	Title
O.HW_DES3	Triple DES Encryption
O.HW_AES	AES Encryption
O.INTEGRITY_CHK	Integrity Control of Transferred Data
O.CUST_RECONFIG	Post Delivery Configuration
O.NVM_INTEGRITY	Integrity Support of data stored to NVM
O.MEM_ACCESS	Area based Memory Access Control
O.SFR_ACCESS	Special Function Register Access Control
O.Self-Test	Self Test
O.Reset	Reset function

Tab. 4.2: Security Objectives of the TOE (HW-ST)

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

O.AES **Advanced Encryption Standard**

	The TOE shall provide the cryptographic functionality to calculate AES encryption and decryption over one up to several blocks in the following modes of operation: ECB, CBC, CBC-MAC and CMAC.
O.DES	**Data Encryption Standard** The TOE shall provide the cryptographic functionality to calculate Triple DES encryption and decryption over one up to several blocks in the following modes of operation: ECB, CBC, CBC-MAC and CMAC.
O.RSA	**RSA** The TOE includes functionality to provide encryption, decryption, signature creation, signature verification, message encoding and signature encoding using the RSA algorithm.
O.RSA_PubExp	**RSA Public Exponent Computation** The TOE includes functionality to to compute an RSA public key from an RSA private CRT key.
O.SHA	**Secure Hash Algorithm** The TOE includes functionality to provide electronic hashing facilities using the SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 algorithms.
O.Copy	**Secure Copy** The TOE includes functionality to copy data from memories/Special Function Registers to memories/Special Function Registers.
O.Compare	**Secure Compare** The TOE includes functionality to compare data from memories/Special Function Registers to data from memories/Special Function Registers.
O.REUSE	**Reuse of Memory** The TOE includes measures to ensure that the memory resources being used by the TOE for the CryptoLib cannot be disclosed to subsequent users of the same memory resource.

Remark 5. All introduced security objectives claiming cryptographic functionality and the security objectives for copy and compare are protected against attacks as described in the JIL, Attack Methods for Smartcards and Similar Devices [8], which include Side Channel Attacks, Perturbation attacks, Differential Fault Analysis (DFA) and timing attack. The following exceptions apply:

(a) RSA Public Key computation does not contain protective measures against DPA.

(c) SHA-1 SHA-224, SHA-256, SHA-384 and SHA-512 do not contain protective measures against DPA and DFA This does not mean that the algorithm is insecure; rather at the time of this security target no promising attacks were found. To fend off attackers with high attack potential an adequate security level must be used (references can be found in national and international documents and standards). In particular this means that SHA-1, Single-DES, and short key lengths for RSA shall not be used.

4.2 Security Objectives for the Security IC Embedded Software Development Environment

In addition to the security objectives for the operational environment as required by CC Part 1 [2] the Protection Profile [14] defines security objectives for the Security IC Embedded Software development environment which are listed below. Additional refinements in the Hardware Security Target [12] are also valid in the ST for the Crypto Library (the “Security IC Embedded Software”).

Name	Title
OE.Plat-Appl	Usage of Hardware Platform
OE.Resp-Appl	Treatment of User Data

Tab. 4.3: Security Objectives of the DVE (PP)

The crypto library TOE assumes that the Security IC Embedded Software abides by the provisions detailed in **Clarification related to ”Usage of Hardware Platform (OE.Plat-Appl)”** and **Clarification related to ”Treatment of User Data (OE.Resp-Appl)”** contained within Section “Security Objectives for the Security IC Embedded Software Development Environment” of the Hardware Security Target [12].
The following additional security objective for the Security IC Embedded Software introduced in the Hardware Security Target [12] is also valid in the ST for the crypto library:
OE.Check-Init: Check of initialization data by the Security IC Embedded Software

4.3 Security Objectives for the Operational Environment

The security objective for the Security Objectives for the Operational environment, listed in Table 4.4. Additional refinements in the Hardware Security Target [12] are also valid in the ST for the Crypto Library.

Name	Title
OE.Process-Sec-IC	Protection during composite product manufacturing

Tab. 4.4: Security Objectives of the OPE (PP)

Name	Title
OE.Check-Init	Check of initialization data by the Security IC Embedded Software

Tab. 4.5: Security Objectives of the OPE (HW-ST)

4.4 Security Objectives Rationale

Section 4.4 of the Protection Profile provides a rationale how the assumptions, threats, and organizational security policies are addressed by the objectives that are specified in the PP “Security IC Platform Protection Profile”, [14]. Table 4.6 reproduces the table in section 4.4 of [14].

Security Problem Definition	Security Objective	Notes
T.Leak-Inherent	O.Leak-Inherent	
T.Phys-Probing	O.Phys-Probing	
T.Malfunction	O.Malfunction O.Self-Test O.INTEGRITY_CHK	
T.Phys-Manipulation	O.Phys-Manipulation O.Self-Test	
T.Leak-Forced	O.Leak-Forced	
T.Abuse-Func	O.Abuse-Func	
T.RND	O.RND	
P.Process-TOE	O.Identification	Phases 2–3
A.Process-Sec-IC	OE.Process-Sec-IC	Phases 4–6
A.Plat-Appl	OE.Plat-Appl	Phase 1
A.Resp-Appl	OE.Resp-Appl	Phase 1

Tab. 4.6: Security Objectives vs. Security Problem Definition (PP0035)

Table 4.7 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 organizational security policy.

Security Problem Definition	Security Objective	Notes
T.Unauthorised-Access	O.MEM_ACCESS O.SFR_ACCESS	
P.Add-Components	O.HW_DES3 O.HW_AES O.Self-Test O.Reset O.CUST_RECONFIG O.NVM_INTEGRITY	
A.Check-Init	OE.Check-Init	Phases 1 and 4–6
A.Key-Function	OE.Plat-Appl OE.Resp-Appl	Phase 1 Phase 1

Tab. 4.7: Additional Security Objectives vs. Security Problem Definition (HW-ST)

Justification related to T.Unauthorised-Access:

Objective	Rationale
O.MEM_ACCESS	TOE must enforce memory partitioning with address mapping and control of access to memories in System Mode and User Mode. Access rights in User Mode must be explicitly granted by Security IC Embedded Software running in System Mode. Thus, security violations caused by accidental or deliberate access to restricted data, code and shared hardware resources can be prevented.
O.SFR_ACCESS	The TOE must enforce control of access to Special Function Registers in System Mode and User Mode. Access rights in User Mode must be explicitly granted by code running in System Mode. Thus, security violations caused by accidental or deliberate access to restricted data, code and shared hardware resources can be prevented.

Justification related to P.Add-Components:

Objective	Rationale
O.HW_DES3	This objective covers the security policy because it requires the TOE to partly implement the functionality as required by the security policy.
O.HW_AES	This objective covers the security policy because it requires the TOE to partly implement the functionality as required by the security policy.
O.Self-Test	This objective covers the security policy because it requires the TOE to partly implement the functionality as required by the security policy.
O.Reset	This objective covers the security policy because it requires the TOE to partly implement the functionality as required by the security policy.
O.CUST_RECONFIG	This objective covers the security policy because it requires the TOE to partly implement the functionality as required by the security policy.
O.NVM_INTEGRITY	This objective covers the security policy because it requires the TOE to partly implement the functionality as required by the security policy.

Justification related to A.Check-Init:

Objective	Rationale
OE.Check-Init	This objective requires the Security IC Embedded Software developer to implement a function as stated in this assumption.

Justification related to A.Key-Function:

Objective	Rationale
OE.Plat-Appl	The definition of this objective of the PP [14] is further clarified in this Security Target: If required the Security IC Embedded Software shall use the cryptographic services of the TOE and its interface as specified. In addition, the Security IC 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 Security IC Embedded Software uses random numbers provided by the security service SS.RNG these random numbers must be tested as appropriate for the intended purpose. This addition ensures that A.Key-Function is still covered this objective although additional functions are being supported according to P.Add-Components.
OE.Resp-Appl	The definition of this objective of the PP [14] is further clarified in this Security Target: By definition cipher or plain text data and cryptographic keys are User Data. So, the Security IC 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 implemented 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 this objective although additional functions are being supported according to P.Add-Components.

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.

Security Problem Definition	Security Objective	Notes
P.Add-Func	O.AES	

Security Problem Definition	Security Objective	Notes
	O.DES O.RSA O.SHA O.Copy O.Compare O.REUSE O.RSA_PubExp O.RND	

Tab. 4.12: Additional Security Objectives vs. Security Problem Definition (CL-ST)

Justification related to P.Add-Func:

Objective	Rationale
O.AES	This objective covers the security policy because it requires the TOE to partly implement the functionality as required by the security policy.
O.DES	This objective covers the security policy because it requires the TOE to partly implement the functionality as required by the security policy.
O.RSA	This objective covers the security policy because it requires the TOE to partly implement the functionality as required by the security policy.
O.SHA	This objective covers the security policy because it requires the TOE to partly implement the functionality as required by the security policy.
O.Copy	This objective covers the security policy because it requires the TOE to partly implement the functionality as required by the security policy.
O.Compare	This objective covers the security policy because it requires the TOE to partly implement the functionality as required by the security policy.
O.REUSE	This objective covers the security policy because it requires the TOE to partly implement the functionality as required by the security policy.
O.RSA_PubExp	This objective covers the security policy because it requires the TOE to partly implement the functionality as required by the security policy.
O.RND	This objective covers the security policy because it requires the TOE to partly implement the functionality as required by the security policy.

Additionally, the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced define how to implement the specific security functionality required by P.Add-Func and therefore support P.Add-Func. These security objectives are also valid for the additional specific security functionality since they must also avert the related threats for the components added to the organisational security policy.

5 Extended Components Definitions

The IT security functional requirements of the TOE an additional family (FDP_SOP) of the Class FDP (user data protection) is defined here. This family describes the functional requirements for basic operations on data in the TOE.

Note that the PP “Security IC Platform Protection Profile”, [14] defines extended security functional requirements in Chapter 5, which are included in this Security Target.

As defined in CC Part 2, FDP class addresses user data protection. Secure basic operations (FDP_SOP) address protection of user data when it is processed by Copy or Compare function, respectively. Therefore, it is judged that FDP class is suitable for FDP_SOP family. The reason for adding an extra family to FDP class is that existing families do not address protection of user data against all relevant attacks. In particular, FDP_IFC and FDP_ITT[HW] (as well as FPT_ITT) are associated with protection against side-channel attacks.

5.1 Secure basic operations (FDP_SOP)

Family Behaviour

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

Component levelling

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

Management: FDP_SOP.1

There are no management activities foreseen.

Audit: FDP_SOP.1

There are no actions defined to be auditable.

FDP_SOP.1 Secure basic operations

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_SOP.1.1

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

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

6 Security Requirements

This chapter defines the security requirements that shall be met by the TOE. These security requirements are composed of the security functional requirements and the security assurance requirements that the TOE must meet in order to achieve its security objectives. This chapter is divided into sections ”Security Functional Requirements”, ”Security Assurance Requirements” and ”Security Requirements Rationale”.

CC allows several operations to be performed on security requirements (on the component level); refinement, selection, assignment, and iteration are defined in section 8.1 of CC Part 1 [2]. These operations are used in the PP [14] and in this Security Target, respectively.

The refinement operation is used to add details to requirements, and thus, further intensifies a requirement. Refinements of security requirements are denoted in such a way that added words are in bold text and changed words are crossed out.

The selection operation is used to select one or more options provided by the PP [14] or CC in stating a requirement. Selections having been made are denoted as italic text. The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made are denoted as italic text.

The iteration operation is used when a component is repeated with varying operations. It is denoted by showing brackets ”[iteration indicator]” and the iteration indicator within the brackets.

For the sake of a better readability, the iteration operation may also be applied to some single components (being not repeated) in order to indicate belonging of such SFRs to same functional cluster. In such a case, the iteration operation is applied to only one single component.

Whenever an element in the PP [14] contains an operation that is left uncompleted, the Security Target has to complete that operation.

6.1 Security Functional Requirements

To support a better understanding of the combination Protection Profile and Security of the hardware platform NXP Secure Smart Card Controller P40C012/040/072 VD vs. this Security Target (SmartMX2 P40 FW Libraries V1.1), the TOE SFRs are presented in the following sections.

6.1.1 SFRs of the Protection Profile

Table 6.1 shows all SFRs which are specified in the Protection Profile “Security IC Platform Protection Profile”, [14]. Some of the SFRs are CC Part 2 extended and defined in the Protection Profile. This is shown in the third column of the table.

Name	Title
FAU_SAS.1[HW]	Audit Storage
FCS_RNG.1[HW]	Random Number Generation (Class PTG.2)
FDP_ITT.1[HW]	Basic Internal Transfer Protection

Name	Title
FDP_IFC.1	Subset Information Flow Control
FMT_LIM.1[HW]	Limited Capabilities
FMT_LIM.2[HW]	Limited Availability
FPT_FLS.1	Failure with Preservation of Secure State
FPT_ITT.1[HW]	Basic Internal TSF Data Transfer Protection
FPT_PHP.3	Resistance to Physical Attack
FRU_FLT.2	Limited Fault Tolerance

Tab. 6.1: Security Functional Requirements defined in the Security IC Protection Profile

Remark 6. These requirements have already been stated in the hardware ST [12] and are fulfilled by the chip hardware, if not indicated otherwise in Table 6.1.

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

FCS_RNG.1[DET] **Random Number Generation (Deterministic)**

Hierarchical-To: No other components.

Dependencies: No dependencies

FCS_RNG.1.1[DET] The TSF shall provide a *deterministic* random number generator that implements:

(DRG.3.1) *If initialized with a random seed using a PTRNG of class PTG.2 (as defined in [1]) as random source, the internal state of the RNG shall have at least 230 bits (TDES) resp. 254 bits (AES) of entropy.*

(DRG.3.2) *The RNG provides forward secrecy (as defined in [1]).*

(DRG.3.3) *The RNG provides backward secrecy even if the current internal state is known (as defined in [1]).*

FCS_RNG.1.2[DET] The TSF shall provide random numbers that meet:

(DRG.3.4) *The RNG, initialized with a random seed using a PTRNG of class PTG.2 (as defined in [1]) as random source, generates output for which in AES mode* 2^{48} *and in 3DES mode* 2^{35} *strings of bit length 128 are mutually different with probability at least* $1 - 2^{-24}$ *in AES mode and* $1 - 2^{-17}$ *in 3DES mode.*

(DRG.3.5) *Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A (as defined in [1]).*

Note: The CryptoLib ROM Software provides the Security IC Embedded Software with seperate functionality to initialise the deterministic random number generator (which includes the chi-square test) and to generate pseudo-random data. It is the responsibility of the user to initialise the DRNG before generating random data. If it is tried to request pseudo-random numbers without having seeded the DRNG a security reset is triggered.

Note: Only if the chi-square test succeeds the hardware random number generator seeds the deterministic random number generator implemented as part of the CryptoLib ROM Software.

6.1.2 SFRs of the Hardware Security Target

The SFRs from Table 6.1 are supplemented by additional SFRs, defined in the Common Criteria, as described in sections “Additional SFRs regarding cryptographic functionality” and “Additional SFRs regarding access control” of the Hardware Security Target [12] and shown in Table 6.2.

Name	Title
FCS_COP.1[HW_DES]	Cryptographic Operation (DES)
FCS_COP.1[HW_AES]	Cryptographic Operation (AES)
FDP_ACC.1[MEM]	Subset Access Control (Memories)
FDP_ACC.1[SFR]	Subset Access Control (Special Function Registers)
FDP_ACF.1[MEM]	Security Attribute Based Access Control (Memories)
FDP_ACF.1[SFR]	Security Attribute Based Access Control (Special Function Registers)
FDP_SDI.2[HW]	Stored Data Integrity Monitoring and Action
FMT_MSA.1[MEM]	Management of Security Attributes (Memories)
FMT_MSA.1[SFR]	Management of Security Attributes (Special Function Registers)
FMT_MSA.3[MEM]	Static Attribute Initialization (Memories)
FMT_MSA.3[SFR]	Static Attribute Initialization (Special Function Registers)
FMT_SMF.1[HW]	Specification of Management Functions (Hardware)
FMT_SMF.1[SW]	Specification of Management Functions (Software)
FPT_TST.1	TSF Testing

Tab. 6.2: Security Functional Requirements defined in the Hardware Security Target

Like the requirements already listed in Table 6.1, the requirements listed in Table 6.2 have already been stated in the Hardware Security Target [12] and are fulfilled by the chip hardware.

6.1.3 SFRs added by the Crypto Library

The SFRs in Table 6.1 and Table 6.2 are further supplemented by the additional SFRs described in the following subsections of this Security Target, as listed in Table 6.3. The SFRs described in Table 6.3 are new for the crypto library. The composite TOE, consisting of chip hardware and crypto library software, fulfills all requirements from Table 6.1, Table 6.2 and Table 6.3.

Name	Title
FCS_RNG.1[DET]	Random Number Generation (Deterministic)
FCS_COP.1[SW_DES]	Cryptographic Operation (DES & TDES)

Name	Title
FCS_COP.1[SW_AES]	Cryptographic Operation (AES)
FCS_COP.1[RSA]	Cryptographic Operation (RSA encryption, decryption, signature and verification)
FCS_COP.1[RSA_Pad]	Cryptographic Operation (RSA message and signature encoding)
FCS_COP.1[RSA_PubExp]	Cryptographic Operation (RSA public key computation)
FCS_COP.1[SHA]	Cryptographic Operation (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)
FCS_CKM.4	Cryptographic key destruction
FDP_RIP.1[SW]	Subset Residual Information Protection
FDP_SOP.1[Compare]	Secure Basic Operations (Compare)
FDP_SOP.1[Copy]	Secure Basic Operations (Copy)

Tab. 6.3: SFRs defined in this Security Target

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

FCS_COP.1[SW_AES] **Cryptographic Operation (AES)**

Hierarchical-To: No other components.

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

FCS_COP.1.1[SW_AES] The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *AES in one of the following modes of operation: ECB, CBC, CBC-MAC or CMAC* and cryptographic key sizes *128, 192 and 256 bit* that meet the following *standards*:

- *FIPS Publication 197, Advanced Encryption Standard (AES)*
- *NIST Special Publication 800-38A Recommendation for Block Cipher Modes of Operation*
- *NIST Special Publication 800-38C Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality – CBCMAC*
- *NIST Special Publication 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*

Application Note: The security functionality is resistant against side channel analysis and other attacks described in [8].

FCS_COP.1[SW_DES] **Cryptographic Operation (DES & TDES)**

Hierarchical-To	No other components.
Dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1.1[SW_DES]	The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *DES and Triple-DES in one of the following modes of operation: ECB, CBC, CBC-MAC or CMAC* and cryptographic key sizes *1-key DES (56 bit), 2-key TDES (112 bit) or 3-key (168 bit)* that meet the following *standards*: • *FIPS Publication 46-3 (DES and TDES)* • *NIST Special Publication 800-38A Recommendation for Block Cipher Modes of Operation* • *NIST Special Publication 800-38C Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality – CBCMAC* • *NIST Special Publication 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*
Application Note:	The security functionality is resistant against side channel analysis and other attacks described in [8]. To fend off attackers with high attack potential an adequate security level must be used (references can be found in national and international documents and standards). In particular this means that Single-DES shall not be used.
FCS_COP.1[RSA]	**Cryptographic Operation (RSA encryption, decryption, signature and verification)**
Hierarchical-To	No other components.
Dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1.1[RSA]	The TSF shall perform *encryption, decryption, signature and verification* in accordance with the specified cryptographic algorithm *RSA* and cryptographic key sizes *512 bits to 2048 bits* that meet the following *standards*: *PKCS #1, v2.1: RSAEP, RSADP, RSASP1, RSAVP1*.
Application Note:	The security functionality is resistant against side channel analysis and other attacks described in [8]. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).
FCS_COP.1[RSA_Pad]	**Cryptographic Operation (RSA message and signature encoding)**
Hierarchical-To	No other components.
Dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.

FCS_COP.1.1[RSA_Pad]	The TSF shall perform *message and signature encoding methods* in accordance with the specified cryptographic algorithm *EME-OAEP and EMSA-PSS* and cryptographic key sizes *512 bits to 2048 bits*that meet the following *standards*: *PKCS #1, v2.1: EME-OAEP and EMSA-PSS*.
Application Note:	The security functionality is resistant against side channel analysis and other attacks described in [8]. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

FCS_COP.1[RSA_PubExp]	**Cryptographic Operation (RSA public key computation)**
Hierarchical-To	No other components.
Dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1.1[RSA_PubExp]	The TSF shall perform *public key computation* in accordance with the specified cryptographic algorithm *RSA* and cryptographic key sizes *512 bits to 2048 bits* that meet the following *standards*: *PKCS #1, v2.1: RSAEP, RSADP, RSASP1, RSAVP1*.
Application Note:	The security functionality is resistant against side channel analysis and other attacks described in [8]. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards). The computation will result in the generation of a public RSA key from the private key (in CRT format). As this key is implied by the private key, this is not true key generation, and, to prevent duplication in this ST, this has not been included as a separate FCS_CKM.1 SFR.

FCS_COP.1[SHA]	**Cryptographic Operation (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)**
Hierarchical-To	No other components.
Dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1.1[SHA]	The TSF shall perform cryptographic checksum generation in accordance with the specified cryptographic algorithm *SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512*and cryptographic key size *none* that meet the following *standard: FIPS 180-3*.
Application Note:	• *The security functionality is resistant against side channel analysis and other attacks described in [8]. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards). In particular this means that SHA-1 shall not be used.* • *The length of the data to hash has to be a multiple of one byte. Arbitrary bit lengths are not supported.*

FDP_RIP.1[SW]	**Subset Residual Information Protection**
Hierarchical-To	No other components.
Dependencies	No dependencies
FDP_RIP.1.1[SW]	The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from the following objects: *all objects (variables)* used by the *Crypto Library* as specified in the user guidance documentation.
FCS_CKM.4	**Cryptographic key destruction**
Hierarchical-To	No other components.
Dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic Key Generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwrite* that meets the following *standards: ISO11568*.
Note:	The *SmartMX2 P40 FW Libraries V1.1* provides the embedded software with functionality for key destruction for FCS_COP.1[SW_AES] and FCS_COP.1[SW_DES]. Clearing of keys that are provided by the smartcard embedded software to the *SmartMX2 P40 FW Libraries V1.1* is the responsibility of the smartcard embedded software.

6.1.4 Extended TOE security functional requirements

The SFRs in Table 6.1, Table 6.2, and Table 6.3 are further supplemented by two iterations of an extended SFR introduced in the following subsections of this Security Target.
The FDP_SOP (secure basic operations) is introduced as a new component within a new family FDP_SOP consisting only of that new component.

FDP_SOP.1[Copy]	**Secure Basic Operations (Copy)**
Hierarchical-To	No other components.
Dependencies	No dependencies
FDP_SOP.1.1[Copy]	The TSF shall provide a *Copy* function on data from *source ROM, RAM and EEPROM* to destination *RAM*.
Application Note:	The security functionality is resistant against side channel analysis and other attacks described in [8].
FDP_SOP.1[Compare]	**Secure Basic Operations (Compare)**
Hierarchical-To	No other components.
Dependencies	No dependencies
FDP_SOP.1.1[Compare]	The TSF shall provide a *Compare* function on data residing in *source ROM, RAM and EEPROM*.

Application Note: The security functionality is resistant against side channel analysis and other attacks described in [8].

6.2 Security Assurance Requirements

Table 6.4 below lists all security assurance components that are valid for this Security Target. With one exception these security assurance components are required by EAL5 (see section 2.2) or by the Protection Profile.
The exception is the component ASE_TSS.2 which is chosen as an augmentation in this ST to give architectural information on the security functionality of the TOE.
Considering Application Note 21 of [14] the column ”Required by” shows the differences in the requirements of security assurance components between the PP [14] and the Security Target. The entry ”EAL5 / PP” denotes, that an SAR is required by both EAL5 and the requirement of the PP [14], ”EAL5” means that this requirement is due to EAL5 and beyond the requirement of the PP [14], and ”PP” identifies this component as a requirement of the PP which is beyond EAL5. The augmentation ASE_TSS.2 chosen in this Security Target is denoted by ”ST”. The refinements of the PP [14], that must be adapted for EAL5, are described in section 6.2.1.

Name	Title
ADV_ARC.1	Security architecture description
ADV_FSP.5	Complete semi-formal functional specification with additional error information
ADV_IMP.1	Implementation representation of the TSF
ADV_INT.2	Well-structured internals
ADV_TDS.4	Semiformal modular design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.4	Production support, acceptance procedures and automation
ALC_CMS.5	Development tools CM coverage
ALC_DEL.1	Delivery procedures
ALC_DVS.2	Sufficiency of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.2	Compliance with implementation standards
ASE_INT.1	ST introduction
ASE_CCL.1	Conformance claims
ASE_SPD.1	Security problem definition
ASE_OBJ.2	Security objectives
ASE_ECD.1	Extended components definition
ASE_REQ.2	Derived security requirements
ASE_TSS.2	TOE summary specification with architectural design summary

Name	Title
ATE_COV.2	Analysis of coverage
ATE_DPT.3	Testing: modular design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing - sample
AVA_VAN.5	Advanced methodical vulnerability analysis

Tab. 6.4: Security Assurance Requirements

6.2.1 Refinements of the TOE Security Assurance Requirements

The Security Target claims conformance to the PP [14] and therefore it has to be conform to the refinements of the TOE security assurance requirements (see Application Note 22 in [14]). Because the refinements in the PP [14] are defined for the security assurance components of EAL4, some refinements have to be applied to assurance components of the higher level EAL5 stated in the Security Target.

The Hardware Security Target [12] has chosen the evaluation assurance level EAL5. This Hardware Security Target bases on the Protection Profile [14], which requires the lower level EAL4+. This implies that the refinements made in the Protection Profile [14], section 6.2.1 “Refinements of the TOE Assurance Requirements”, for EAL4+ had to be refined again in order to ensure EAL5 in the Hardware Security Target (this was necessary for ALC_CMS.5 and ADV_FSP.5).
Since these refinements explain and interpret the CC for hardware, these refinements do not affect the additional software in this composite TOE. Therefore all refinements made in the PP [14] are valid without change for the composite TOE.

6.3 Security Requirements Rationale

6.3.1 Rationale for the Security Functional Requirements

Section 6.3.1 in [14] provides a rationale for the mapping between security functional requirements and security objectives defined n the PP [14]. The mapping is reproduced in the following table.

SO	SFR
O.Leak-Inherent	FDP_ITT.1[HW] FPT_ITT.1[HW] FDP_IFC.1
O.Phys-Probing	FPT_PHP.3
O.Malfunction	FRU_FLT.2 FPT_FLS.1
O.Phys-Manipulation	FPT_PHP.3

SO	SFR
O.Leak-Forced	FRU_FLT.2 FPT_FLS.1 FPT_PHP.3 FDP_ITT.1[HW] FPT_ITT.1[HW] FDP_IFC.1
O.Abuse-Func	FRU_FLT.2 FPT_FLS.1 FMT_LIM.1[HW] FMT_LIM.2[HW] FPT_PHP.3 FDP_ITT.1[HW] FPT_ITT.1[HW] FDP_IFC.1
O.Identification	FAU_SAS.1[HW]
O.RND	FCS_RNG.1[DET] FRU_FLT.2 FPT_FLS.1 FDP_ITT.1[HW] FPT_ITT.1[HW] FDP_IFC.1 FCS_RNG.1[HW]

Tab. 6.5: Security Functional Requirements vs. Security Objectives (PP0035)

Remark 7. O.RND has been extended if compared to the PP [14] to include also a software RNG (see also Remark 4). The rationale given in the PP only covers the part of O.RND dealing with the hardware RNG. For O.RND additional functionality (software RNG) and additional requirements FCS_RNG.1[DET] have been added. The explanation following Table 6.6 describes this in more detail.

The Hardware Security Target [12] lists a number of security objectives and SFRs that are additional to the Security Objectives and SFRs in the Protection Profile. These are listed in the following table.

SO	SFR
O.HW_DES3	FCS_COP.1[HW_DES]
O.HW_AES	FCS_COP.1[HW_AES]
O.INTEGRITY_CHK	FDP_ITT.1[HW] FPT_ITT.1[HW]
O.CUST_RECONFIG	FMT_SMF.1[HW]
O.NVM_INTEGRITY	FDP_SDI.2[HW]

SO	SFR
O.MEM_ACCESS	FDP_ACC.1[MEM] FDP_ACF.1[MEM] FMT_MSA.3[MEM] FMT_MSA.1[MEM] FMT_SMF.1[HW]
O.SFR_ACCESS	FDP_ACC.1[SFR] FDP_ACF.1[SFR] FMT_MSA.3[SFR] FMT_MSA.1[SFR] FMT_SMF.1[HW]
O.Self-Test	FPT_TST.1
O.Reset	FMT_SMF.1[SW]

Tab. 6.6: Security Functional Requirements vs. Security Objectives (HW-ST)

The rationales for the mappings in Table 6.6 may be found in the Hardware ST [12].
Finally, this ST lists a number of security objectives and SFRs additional to both the PP and the Hardware ST. These are listed in the following table.

SO	SFR
O.AES	FCS_COP.1[SW_AES] FCS_COP.1[HW_AES]
O.DES	FCS_COP.1[SW_DES] FCS_COP.1[HW_DES]
O.RSA	FCS_COP.1[RSA] FCS_COP.1[RSA_Pad]
O.RSA_PubExp	FCS_COP.1[RSA_PubExp]
O.SHA	FCS_COP.1[SHA]
O.Copy	FDP_SOP.1[Copy]
O.Compare	FDP_SOP.1[Compare]
O.REUSE	FDP_RIP.1[SW] FCS_CKM.4

Tab. 6.7: Security Functional Requirements vs. Security Objectives in this ST

The rationale for all items defined in this Security Target is given below.
Justification related to O.AES:

SFR	Rationale
FCS_COP.1[SW_AES]	This SFR requires the TOE to support AES encryption and decryption as demanded by the objective. FCS_COP.1[SW_AES] requires the modes of operation on top of FCS_COP.1[HW_AES].
FCS_COP.1[HW_AES]	This objective requires the TOE to support AES encryption and decryption. FCS_COP.1[HW_AES] requires the AES according to the standard.

Justification related to O.DES:

SFR	Rationale
FCS_COP.1[SW_DES]	This SFR requires the TOE to support Triple-DES encryption and decryption as demanded by the objective. FCS_COP.1[SW_DES] requires the modes of operation on top of FCS_COP.1[HW_DES].
FCS_COP.1[HW_DES]	This objective requires the TOE to support Tripe-DES encryption and decryption. FCS_COP.1[HW_DES] requires the Triple-DES according to the standard.

Justification related to O.RSA:

SFR	Rationale
FCS_COP.1[RSA]	This SFR requires the TOE to support RSA en- cryption, decryption, signature and verification according to the standard as demanded by the objective.
FCS_COP.1[RSA_Pad]	This SFR requires the TOE to support RSA-OAEP message encoding and decoding and RSA-PSS padding and padding verification according to the standard.

Justification related to O.RSA_PubExp:

SFR	Rationale
FCS_COP.1[RSA_PubExp]	This SFR requires the TOE to support the compuation of a public exponent from an RSA private CRT key as demanded by the objective.

Justification related to O.SHA:

SFR	Rationale
FCS_COP.1[SHA]	This SFR requires the TOE to support secure hash function computation of the SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 hash functions according to the standard as demanded by the objective.

Justification related to O.RND:

SFR	Rationale
FCS_RNG.1[DET]	This SFR requires the TOE to generate random numbers with ensured cryptographic quality (i.e. not predictable and with sufficient entropy) such that information about the generated random numbers is not available to an attacker as demanded by the objective. • *Ensured cryptographic quality (sufficient entropy part) of generated random numbers is met by FCS_RNG.1.1[DET] through the characteristic* deterministic *and the random number generator meeting NIST SP 800-90 (FCS_RNG.1.1[DET]). Ensured cryptographic quality (not predictable part) of generated random numbers is met by FCS_RNG.1[DET] through the characteristic* chi-squared test of the seed generator *and FCS_RNG.1[HW] from the certified hardware platform.* • *Information about the generated random numbers is not available to an attacker is met through ADV_ARC.1, which prevent physical manipulation and malfunction of the TOE and support this objective because they prevent attackers from manipulating or otherwise affecting the random number generator.*
FRU_FLT.2	See PP0035.
FPT_FLS.1	See PP0035.
FDP_ITT.1[HW]	See PP0035.
FPT_ITT.1[HW]	See PP0035.
FDP_IFC.1	See PP0035.
FCS_RNG.1[HW]	See PP0035.

Justification related to O.Copy:

SFR	Rationale
FDP_SOP.1[Copy]	This SFR requires the TOE to support secure copy which is exactly addressed by FDP_SOP.1[Copy] as demanded by the objective.

Justification related to O.Compare:

SFR	Rationale
FDP_SOP.1[Compare]	This SFR requires the TOE to support secure compare which is exactly addressed by FDP_SOP.1[Compare] as demanded by the objective.

Justification related to O.REUSE:

SFR	Rationale
FDP_RIP.1[SW]	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 code segments run in System Mode and is met by the SFR FDP_RIP.1[SW], which requires the CryptoLib to make unavailable all memory contents that has been used by it.
FCS_CKM.4	FCS_CKM.4 contributes in addition to FDP_RIP.1[SW].

- Each objective is directly implemented by a single SFR specifying the (cryptographic) service that the objective wishes to achieve (see the above table for the mapping).
- The requirements and architectural measures that originally were taken from the Protection Profile [14] and thus were also part of the Security Target of the hardware (chip) evaluation support the objective:
  - ADV_ARC.1 (and underlying platform SFRs) supports the objective by ensuring that the TOE works correctly (i.e., all of the TOE's capabilities are ensured) within the specified operating conditions and maintains a secure state when the TOE is outside the specified operating conditions. A secure state is also entered when perturbation or DFA attacks are detected.
  - ADV_ARC.1 (and underlying platform SFRs) ensures that no User Data (plain text data, keys) or TSF Data is disclosed when they are transmitted between different functional units of the TOE (i.e., the different memories, the CPU, cryptographic co-processors), thereby supporting the objective in keeping confidential data secret.
- ADV_ARC.1 (and underlying platform SFRs) by ensuring that User Data and TSF Data are not accessible from the TOE except when the Smartcard Embedded Software decides to communicate them via an external interface.

6.3.2 Extended Requirements

This Security Target does define extended requirements, because there are no existing SFRs available that cover the claimed functionality. The PP [14] contains extended functional requirements, which are explained in the rationale of the PP (see [14], section 5).

6.3.3 Dependencies of Security Functional Requirements

The dependencies listed in the PP [14] are independent of the additional dependencies listed in the table below. The dependencies of the PP [14] are fulfilled within the PP [14] 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 sections 6.1 and 6.2 are satisfied.
The dependencies defined in the Common Criteria are listed in the table below:

SFR	Dependencies	Fulfilled by Security Requirements in the ST
FCS_RNG.1[DET]	No dependencies	
FCS_COP.1[SW_DES]	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction.	See discussion below.
FCS_COP.1[SW_AES]	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction.	See discussion below.
FCS_COP.1[RSA]	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.	

SFR	Dependencies	Fulfilled by Security Requirements in the ST
FCS_COP.1[RSA_Pad]	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.	
FCS_COP.1[RSA_PubExp]	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.	
FCS_COP.1[SHA]	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.	
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic Key Generation]	
FDP_RIP.1[SW]	No dependencies	
FDP_SOP.1[Compare]	No dependencies	
FDP_SOP.1[Copy]	No dependencies	

Tab. 6.17: Dependencies of Security Functional Requirements

The functional requirements [FDP_ITC.1, or FDP_ITC.2 or FCS_CKM.1] are not included in this Security Target since the TOE only provides a pure engine for encryption and decryption without additional features for the creation of cryptographic keys. In the case of the symmetric crypto module the TOE provides functionality for key destruction. Therefore the Security IC Embedded Software must fulfill these requirements related to the needs of the realised application.

6.3.4 Rationale for the Assurance Requirements

The selection of assurance components is based on the underlying PP [14]. The Security Target uses the same augmentations as the PP, but chooses a higher assurance level. The level EAL5 is chosen in order to meet assurance expectations of digital signature applications and electronic payment systems. Additionally, the requirement of the PP [14] to choose at least EAL4 is fulfilled.

The rationale for the augmentations is the same as in the PP. The assurance level EAL5 is an elaborated predefined level of the CC, part 3 [4]. The assurance components in an EAL level are chosen in a way that they build a mutually supportive and complete set of components. The requirements chosen for augmentation do not add any dependencies, which are not already fulfilled for the corresponding requirements contained in EAL 5. Therefore, these components add additional assurance to EAL 5, but the mutual support of the requirements is still guaranteed.

As stated in the section 6.3.3 of [14], 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_VAN.5 was chosen by the PP [14] in order to assure that even these attackers cannot successfully attack the TOE.

7 TOE Summary Specification

7.1 IT Security Functionality

The evaluation of this cryptographic library is performed as a composite evaluation, where the TOE comprises both the underlying hardware and the embedded software (cryptographic library). The TOE of this composite evaluation therefore extends the security functionality already available in the chip platform (see section “Portions of the TOE Security Functionality” of the Hardware Security Target [12]). The security functionality of the hardware platform is listed in the following two tables; the additional security functionality provided by the cryptographic library is described in the following sub-sections.

Name	Title
SS.RNG	Random Number Generation

Tab. 7.1: Security Services defined in the scope of the Protection Profile

Name	Title
SS.HW_DES3	Triple-DES Operations
SS.HW_AES	AES Operations
SS.SELF_TEST	Self Test
SS.RESET	Reset Functionality
SS.RECONFIG	Post Delivery Configuration

Tab. 7.2: Security Services defined in the HW Security Target

Remark 8. The security functionality SS.RNG implements the hardware RNG. The TOE also implements a software RNG as part of security functionality SS.SW_RNG.

SS.RNG **Random Number Generation**

The Random Number Generator continously produces random numbers with a length of one byte. The TOE implements SS.RNG by means of a physical hardware random number generator working stable within the valid ranges of operating conditions, which are guaranteed by SF.OPC.

refining SMs: SM.Sw_Rng.HQC

The physical random number generator partially fulfills AIS31 class PTG.2 [1]. The behaviour of the Random Number Generator is independent of the Security IC Embedded Software. The entropy of the random numbers as claimed by the security functional requirement are ensured by the requirements of AIS31. Therefore SS.RNG obviously meets FCS_RNG.1[HW]. Note that statistical tests are requested from the Security IC Embedded Software (refer to [15]). This means that the Random Number Generator together with the according online test features to guarantee its correct operation and quality of randomness provided by the Security IC Embedded

Software is suitable for generation of signature key pairs, generation of session keys for symmetric encryption mechanisms, random padding bits, zero-knowledge proofs and the generation of seeds for DRNGs.

SS.HW_DES3 **Triple-DES Operations**

SS.HW_DES3 provides DES encryption and decryption based on 112 bit and 168 bit keys.

The TOE provides the Single DES according to the Data Encryption Standard (DES). SS.HW_DES3 is a modular basic cryptographic function, which provides the TDEA algorithm as defined by FIPS PUB 46 [7] by means of a hardware coprocessor which provides Single-DES. The document [15] provides guidance how to use the hardware coprocessor such that (a) the 3-key Triple-DEA algorithm according to keying option 1 and (b) the 2-key Triple DEA algorithm according to keying option 1 and 2 in FIPS PUB 46-3 [7] can be implemented by the Security IC Embedded Software. Also the key management for the 2-key (112 bit) Triple DES algorithm shall be provided by the Security IC Embedded Software. For encryption the Security IC Embedded Software provides 8 bytes of the plain text and SS.HW_DES3 calculates 8 bytes cipher text. The calculation output is read by the Security IC Embedded Software. For decryption the Security IC Embedded Software provides 8 bytes of cipher text and SS.HW_DES3 calculates 8 bytes plain text. The calculation output is read by the Security IC Embedded Software.

SS.HW_AES **AES Operations**

SS.HW_AES provides AES encryption and decryption based on 128 bit keys.

The TOE provides the Advanced Encryption Standard (AES) algorithm according to the Advanced Encryption Standard as defined by FIPS PUB 197 [6]. SS.HW_AES is a modular basic cryptographic function, which provides the AES algorithm by means of a hardware coprocessor and supports the AES algorithm with key length of 128, 192 and 256 bit. The key management for the AES algorithm shall be provided by the Security IC Embedded Software. For encryption the Security IC Embedded Software provides 16 bytes of the plain text and SS.HW_AES calculates 16 bytes cipher text. The calculation output is read by the Security IC Embedded Software. For decryption the Security IC Embedded Software provides 16 bytes of cipher text and SS.HW_AES calculates 16 bytes plain text. The calculation output is read by the Security IC Embedded Software.

SS.SELF_TEST **Self Test**

SS.SELF_TEST provides a function to check whether the TOE has been manipulated physically. This includes an active shielding check, sensor check, verifying the signature of code and performing a consistency check of Special Function Registers with statis configuration.

SS.RESET **Reset Functionality**

SS.RESET provides the Security IC Embedded Software with a function to reset the device. This enables the Security IC Embedded Software preserving a secure state in case it detects abnormal operations or attacks. The reset functionality provides an ordinary System Reset (i.e. ”Power-On Reset”) and a security relevant reset (Security Reset) which can be executed only a

limited time before the device is disabled permanently. The IC can also be terminated with one call, where the error counter is set to its end state.

SS.RECONFIG **Post Delivery Configuration**

SS.RECONFIG realizes the Post Delivery Configuration. These can be used by the customer to set the accessible size of the EEPROM, enable or disable the PKCC co-processor, the AES co-processor, the DES co-processor, the number of keys in the EEPROM key store and the number of Anti-Tearing pages. The configuration values of the Post Delivery Configuration are stored in a special area in the NXP_ConfigData_Seg.

Note that if the PKCC coprocessor, the AES coprocessor and the DES coprocessor are disabled, both will no longer be available to the Security IC Embedded Software and attempting to use it will raise an exception. This means the availability of SS.HW_AES and SS.HW_DES3 is configurable. The customer can change the values of the Post Delivery Configuration through invoking the Post Delivery Configuration functionality in Boot Software (see SF.MEM_ACC) . This functionality is invoked by using the chip health mode via the ISO/IEC 7816 interface and applying the required Post Delivery Configuration commands.
The customer can change these values as many times as he wishes. However, once he calls the Boot Software using the chip health mode via the ISO/IEC 7816 interface with a certain parameter set to a specific value, the options are locked permanently, and can no longer be changed. The options must be locked before the TOE is delivered to the customer before phase 7 of the life cycle.
Tables 7.3 (for PP) and 7.4 list the Security Features defined for the TOE in the HW-ST.

Name	Title
SF.OPC	Control of Operating Conditions
SF.PHY	Protection against Physical Manipulation
SF.LOG	Logical Protection
SF.COMP	Protection of Mode Control

Tab. 7.3: Security Features defined in the scope of the Protection Profile

Name	Title
SF.MEM_ACC	Memory Access Control
SF.SFR_ACC	Special Function Register Access Control

Tab. 7.4: Security Features defined in the HW-ST

7.1.1 Security Services

SS.SW_RNG **Deterministic Random Number Generator**

The CryptoLib 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 provided via SS.RNG. Then implementation of the software RNG is based on the standard NIST-SP-800-90 CTR-DBRG.

SS.SW_DES **Triple DES**

SS.SW_DES supports four modes of operation on top of SS.HW_DES3:

- *ECB according to [9]*
- *CBC according to [9]*
- *CBC-MAC according to [10]*
- *CMAC according to [11]*

A keystore concept is used for secure handling of DES, 2K3DES and 3K3DES keys.

SS.SW_AES **AES**

SS.SW_AES supports four modes of operation on top of SS.HW_AES:

- *ECB according to [9]*
- *CBC according to [9]*
- *CBC-MAC according to [10]*
- *CMAC according to [11]*

A keystore concept is used for secure handling of AES keys.

SS.RSA **RSA**

SS.RSA provides functions that implement the RSA algorithm for data encryption, decryption, signature and verification. All algorithms are defined in PKCS#1, v2.2 (RSAEP, RSADP, RSAP1, RSAVP1) [22].

This routine supports various key lengths from 512 bits to 2048 bits. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

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

SS.RSAPad **RSAPad**

SS.RSAPad provides functions that implement the RSA algorithm and the RSA-CRT algorithm for message and signature encoding. This IT security functionality supports the EME-OAEP and EMSA-PSS signature scheme. All algorithms are defined in PKCS#1, v2.2 (EME-OAEP, EMSA-PSS) [22].

This routine supports various key lengths from 512 bits to 2048 bits. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

SS.RSAPubExp **RSA_PublicExp**

SS.RSAPubExp provides functions that implement computation of an RSA public key from a private CRT key. This routine supports various key lengths from 512 bits to 2048 bits (CRT). To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

SS.SHA **SHA**

SS.SHA provides functions to compute the Secure Hash Algorithms SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 according to the standard FIPS 180-3 [21].

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

SS.COPY **Secure Copy**

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

SS.COMPARE **Secure Compare**

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

7.1.2 Security Features

SF.Object_Reuse **Object Reuse**

The TOE provides internal security measures which clear memory areas used by the CryptoLib after usage.

7.2 Security architectural information

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

SF.COMP

The protection of mode control is completely covered by the underlying hardware platform [12].

SF.LOG

The logical protection relates to the SFRs FDP_ITT.1[HW], FPT_ITT.1[HW] and FDP_IFC.1. The underlying hardware platform contains a number of hardware countermeasures, and for details is referred to the Security Target of the hardware platform [12]. For DES and AES; the resistance against SPA, DPA and timing attacks is provided by the co-processors in the hardware part of the TOE and partly by software countermeasures in the crypto lib. The TOE adds a number of countermeasures to protect RSA calculations and RSA key generation, like modulus and exponent blinding. Furthermore, timing attacks are prevented using careful coding.Timing attacks are prevented using careful coding and timing resistance of the underlying co-processor. For the key generation algorithms, there is no interface available to force the key generation to repeat the previous calculation with the same parameters. For the secure compare and secure copy function measures randomizing the program flow are implemented.

SF.OPC

The control of operation conditions relates to the security requirements FRU_FLT.2 and FPT_FLS.1. The underlying hardware platform contains a number of hardware countermeasures. For the details is referred to the Security Target of the hardware platform [12]. The TOE implements a number of software sensors that detect DFA attacks on AES, DES, RSA . Also software sensors are implemented to detect perturbation attacks in the secure copy and the secure compare functions.

SF.PHY

Protection against physical manipulation and probing is completely covered by the underlying hardware platform [12].

7.3 TOE Summary Specification Rationale

7.3.1 Mapping of Security Functional Requirements and TOE Security Functionality

The following table provides a mapping of portions of the TSF to SFR. The mapping is described in detail in the text following the table.

TSF	SFR	Title
SS.RNG	FCS_RNG.1[HW]	Random Number Generation (Class PTG.2)
SF.OPC	FRU_FLT.2	Limited Fault Tolerance
	FPT_FLS.1	Failure with Preservation of Secure State
SF.PHY	FPT_PHP.3	Resistance to Physical Attack
	FDP_ITT.1[HW]	Basic Internal Transfer Protection
	FPT_ITT.1[HW]	Basic Internal TSF Data Transfer Protection
	FMT_SMF.1[HW]	Specification of Management Functions (Hardware)
	FDP_SDI.2[HW]	Stored Data Integrity Monitoring and Action
SF.LOG	FDP_ITT.1[HW]	Basic Internal Transfer Protection
	FPT_ITT.1[HW]	Basic Internal TSF Data Transfer Protection
	FDP_IFC.1	Subset Information Flow Control
SF.COMP	FMT_LIM.1[HW]	Limited Capabilities
	FMT_LIM.2[HW]	Limited Availability
	FAU_SAS.1[HW]	Audit Storage

Tab. 7.5: TOE Security Functionality vs. Security Functional Requirements (PP0035)

TSF	SFR	Title
SS.HW_DES3	FCS_COP.1[HW_DES]	Cryptographic Operation (DES)
SS.HW_AES	FCS_COP.1[HW_AES]	Cryptographic Operation (AES)
SS.SELF_TEST	FPT_TST.1	TSF Testing
SS.RESET	FMT_SMF.1[SW]	Specification of Management Functions (Software)
SS.RECONFIG	FMT_SMF.1[HW]	Specification of Management Functions (Hardware)
SF.MEM_ACC	FMT_LIM.2[HW]	Limited Availability
	FDP_ACC.1[MEM]	Subset Access Control (Memories)
	FDP_ACF.1[MEM]	Security Attribute Based Access Control (Memories)
	FMT_MSA.3[MEM]	Static Attribute Initialization (Memories)
	FMT_MSA.1[MEM]	Management of Security Attributes (Memories)
	FMT_SMF.1[HW]	Specification of Management Functions (Hardware)
SF.SFR_ACC	FMT_LIM.2[HW]	Limited Availability
	FDP_ACC.1[SFR]	Subset Access Control (Special Function Registers)

TSF	SFR	Title
	FDP_ACF.1[SFR]	Security Attribute Based Access Control (Special Function Registers)
	FMT_MSA.3[SFR]	Static Attribute Initialization (Special Function Registers)
	FMT_MSA.1[SFR]	Management of Security Attributes (Special Function Registers)
	FMT_SMF.1[HW]	Specification of Management Functions (Hardware)

Tab. 7.6: TOE Security Functionality vs. Security Functional Requirements (HW-ST)

As already stated in the definition of the portions of the TOE security functionality there are additional security mechanisms, which can contribute to security functionality when they are appropriately controlled by the Security IC Embedded Software. E.g. the PKCC can be used to implement leakage-resistant asymmetric cryptographic algorithms.

TSF	SFR	Title
SS.SW_DES	FCS_COP.1[SW_DES]	Cryptographic Operation (DES & TDES)
SS.SW_AES	FCS_COP.1[SW_AES]	Cryptographic Operation (AES)
SS.RSA	FCS_COP.1[RSA]	Cryptographic Operation (RSA encryption, decryption, signature and verification)
SS.RSAPad	FCS_COP.1[RSA_Pad]	Cryptographic Operation (RSA message and signature encoding)
SS.RSAPubExp	FCS_COP.1[RSA_PubExp]	Cryptographic Operation (RSA public key computation)
SS.SHA	FCS_COP.1[SHA]	Cryptographic Operation (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)
SS.COPY	FDP_SOP.1[Copy]	Secure Basic Operations (Copy)
SS.COMPARE	FDP_SOP.1[Compare]	Secure Basic Operations (Compare)
SS.SW_RNG	FCS_RNG.1[DET]	Random Number Generation (Deterministic)
SF.Object_Reuse	FDP_RIP.1[SW]	Subset Residual Information Protection
	FCS_CKM.4	Cryptographic key destruction

Tab. 7.7: TOE Security Functionality vs. Security Functional Requirements (ST)

8 Bibliography

[1] Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Bundesamt für Sicherheit in der Informationstechnik. Version 2.0, September 18, 2011.

[2] Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model - Version 3.1 CCMB-2012-09-001, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components, Version 3.1 CCMB-2012-09-002, Revision 4, September 2012.

[4] Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components, Version 3.1 CCMB-2012-09-003, Revision 4, September 2012.

[5] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2 - Evaluation Methodology, Version 3.1 CCMB-2012-09-004, Revision 4, September 2012.

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

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

[8] JIL: Attack Methods for Smartcards and Similar Devices.

[9] NIST Special Publication 800-38A Recommendation for BlockCipher Modes of Operation. http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf.

[10] NIST Special Publication 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf.

[11] NIST Special Publication 800-38C Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality - CBCMAC. http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C.pdf.

[12] NXP Secure Smart Card Controller P40C012/040/072 VD, Security Target Lite, NXP Semiconductors, Revision 1.1, 2014-09-25.

[13] Product data sheet addendum SmartMX2 P40 family P40Cxxx, HAL interface specification, NXP Semiconductors, Document number 267424, 2014-11-21.

[14] Security IC Platform Protection Profile, registered and certified by Bundesamt fuer Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035, Rev 1.0, 15 June 2007.

[15] User guidance manual Firmware Libraries on P40C012/040/072, Preparative procedures and operational user guidance, NXP Semiconductors, Document number 301814, 2014-12-19.

[16] User manual Crypto Library on SmartMX2 P40 family P40Cxxx RNG Library, NXP Semiconductors, Document number 266315, 2014-12-19.

[17] User manual Crypto Library on SmartMX2 P40 family P40Cxxx RSA Library, NXP Semiconductors, Document number 266614, 2014-10-16.

[18] User manual Crypto Library on SmartMX2 P40 family P40Cxxx SHA Library, NXP Semiconductors, Document number 266414, 2014-10-16.

[19] User manual Crypto Library on SmartMX2 P40 family P40Cxxx Symmetric Crypto Library, NXP Semiconductors, Document number 266514, 2014-10-16.

[20] User manual Crypto Library on SmartMX2 P40 family P40Cxxx Utils Library, NXP Semiconductors, Document number 266714, 2014-10-16.

[21] Federal Information Processing Standard (FIPS) 180-4: Secure Hash Standard (SHS)., 2012.

[22] J. Jonsson and B. Kaliski. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2, 2012.

9 Contents

10 Legal information

10.1 Definitions

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

10.2 Disclaimers

Limited warranty and liability – Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information.

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

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

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

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

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

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

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

Evaluation products – This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer.

In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages.

Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

10.3 Licenses

ICs with DPA Countermeasures functionality

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

10.4 Patents

Notice is herewith given that the subject device uses one or more of the following patents and that each of these patents may have corresponding patents in other jurisdictions.
<Patent ID> – owned by <Company name>

10.5 Trademarks

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

MIFARE – is a trademark of NXP B.V.

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

Date of release: 09 January 2015

Document identifier: NSCIB-CC-13-37968