

# Firmware Libraries V2.0 and V2.0.x on P40C008/012/024/040/072 VD/VE

Security Target

Rev. 0.8 – 02. March 2016

Evaluation documentation

SECURED, STRICTLY CONFIDENTIAL

NSCIB-CC-15-65156

## Document Information

| Info            | Content                                                                                                                                                                                                                                                                                                |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Keywords</b> | CC, Security Target, SmartMX2 P40 FW Libraries V2.0/V2.0.x                                                                                                                                                                                                                                             |
| <b>Abstract</b> | Security Target of the Firmware Libraries V2.0 and V2.0.x on P40C008/012/024/040/072 VD/VE, which is developed and provided by NXP Semiconductors, Business Unit Security & Connectivity according to the Common Criteria for Information Technology Security Evaluation Version 3.1 at EAL5 augmented |



| Rev | Date             | Description                                                                                                                                |
|-----|------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| 0.1 | 12-February-2015 | Initial version of the document.                                                                                                           |
| 0.2 | 11-May-2015      | Including review comments of evaluator + rework to PP0084 + removal of Sw_Comm + addition of EEPROM sizes '008' and '024' for HW platform. |
| 0.3 | 15-Jun-2015      | Added refinement regarding use of PP0084 in Section <a href="#">2</a>                                                                      |
| 0.4 | 21-Aug-2015      | Addressed additional comments from evaluator. Updated tables.                                                                              |
| 0.5 | 02-Oct-2015      | Corrected UM-Rng reference.                                                                                                                |
| 0.6 | 11-Nov-2015      | Corrected UserManuals and UGM reference.                                                                                                   |
| 0.7 | 16-Nov-2015      | Updated HAL-Lib, FWLibsV2.0-UGM and HW-ST and HW-UGM reference.                                                                            |
| 0.8 | 02-Mar-2016      | Included HAL-Lib v1.2.1 (FWLibs v2.0.1), updated FWLibsV2.X-UGM reference.                                                                 |

# 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 V2.0 and V2.0.x on P40C008/012/024/040/072 VD/VE Security Target, 0.8, NXP Semiconductors, 02. March 2016.

## 1.2 TOE Reference

This Security Target refers to the Firmware Libraries V2.0 and V2.0.x on P40C008/012/024/040/072 VD/VE (TOE) provided by NXP Semiconductors, Business Unit Security & Connectivity for Common Criteria evaluation. The TOE is a composite TOE, consisting of:

- The hardware “NXP Secure Smart Card Controller P40C008/012/024/040/072 VD/VE”, which is used as evaluated platform, and all its Major Configurations (see [\[13\]](#) for details)
- The “SmartMX2 P40 FW Libraries V2.0/V2.0.x”, which is built upon this platform.

This Security Target builds on the Hardware Security Target [\[13\]](#), which refers to the “NXP Secure Smart Card Controller P40C008/012/024/040/072 VD/VE” provided by NXP Semiconductors, Business Unit Security & Connectivity.

The SmartMX2 P40 FW Libraries V2.0/V2.0.x covers both SmartMX2 P40 FW Libraries V2.0 and SmartMX2 P40 FW Libraries V2.0.1. In case of a composite evaluation the chosen minor version of the FW Libraries should be mentioned explicitly.

## 1.3 TOE Overview

### 1.3.1 Introduction

The Hardware Security Target [\[13\]](#) contains, in section “ST Overview”, an introduction about the P40C008/012/024/040/072 hardware TOE that is considered in the evaluation. The Hardware Security Target includes IC Dedicated Software stored in the ROM provided with the P40C008/012/024/040/072 hardware platform. The “SmartMX2 P40 FW Libraries V2.0/V2.0.x” 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

P40C008/012/024/040/072 VD/VE provides the computing platform and cryptographic support by means of co-processors for the SmartMX2 P40 FW Libraries V2.0/V2.0.x. The SmartMX2 P40 FW Libraries V2.0/V2.0.x provides the security functionality described below in addition to the functionality described in the Hardware Security Target [13] for the hardware platform.

The SmartMX2 P40 FW Libraries V2.0/V2.0.x consists of two parts, the Crypto Library and the the Hardware Abstraction Layer (HAL)-Library. The Crypto Library provides AES, DES, Triple-DES (3DES), RSA, RSA key generation, ECDSA (ECC over GF(p)) signature generation and verification, ECDSA (ECC over GF(p)) key generation, ECDH (ECC Diffie-Hellmann) key-exchange, full point addition (ECC over GF(p)), 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 [9]. In addition, the Crypto Library implements a software (pseudo) random number generator which is initialized (seeded) by the hardware random number generator of the P40C008/012/024/040/072. 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 Configuration and Patch functionality.

This Security Target defines a set of security requirements for the Crypto Library. There are no specific security requirements for the HAL-Library.

For more details on the security requirements for the TOE please refer to Section 6 of this Security Target.

### 1.3.2 Difference to previous version of the product

An earlier version of this product, the “SmartMX2 P40 FW Libraries V1.1” contained a communication library alongside the HAL library as part of the SmartMX2 P40 FW Libraries V1.1. We want to state explicitly that the TOE in this security target SmartMX2 P40 FW Libraries V2.0/V2.0.x does not include a communication library.

## 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 P40C008/012/024/040/072 VD/VE 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 V2.0/V2.0.x” which consists of a software library and associated documentation. The SmartMX2 P40 FW Libraries V2.0/V2.0.x 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 [13] 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 [13] plus all TOE components listed in the Table 1.1 and Table 1.2, resp. 1.3, resp. 1.4, resp. 1.5, resp. 1.6, resp. 1.7 below:

| Type         | Name                                                                                                                                  | Release | Date       | Form of Delivery    |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------|---------|------------|---------------------|
| Library File | libCryptoLibSymCiphers.a                                                                                                              | 2.0     | 17.09.2015 | Electronic file     |
| Library File | libCryptoLibSha.a                                                                                                                     | 2.0     | 17.09.2015 | Electronic file     |
| Library File | libCryptoLibRng.a                                                                                                                     | 2.0     | 17.09.2015 | Electronic file     |
| Library File | libCryptoLibRsa.a                                                                                                                     | 2.0     | 17.09.2015 | Electronic file     |
| Library File | libCryptoLibUtils.a                                                                                                                   | 2.0     | 17.09.2015 | Electronic file     |
| Library File | libCryptoLibUtils_ImportExport.a                                                                                                      | 2.0     | 17.09.2015 | Electronic file     |
| Library File | libCryptoLibRsaKg.a                                                                                                                   | 2.0     | 17.09.2015 | Electronic file     |
| Library File | libCryptoLibEccGfp.a                                                                                                                  | 2.0     | 17.09.2015 | Electronic file     |
| Header File  | phCryptoLibSymCiphers.h                                                                                                               | 2.0     | 17.09.2015 | Electronic file     |
| Header File  | phCryptoLibSha.h                                                                                                                      | 2.0     | 17.09.2015 | Electronic file     |
| Header File  | phCryptoLibRng.h                                                                                                                      | 2.0     | 17.09.2015 | Electronic file     |
| Header File  | phCryptoLibRsa.h                                                                                                                      | 2.0     | 17.09.2015 | Electronic file     |
| Header File  | phCryptoLibRsa_OAEP.h                                                                                                                 | 2.0     | 17.09.2015 | Electronic file     |
| Header File  | phCryptoLibRsa_PSS.h                                                                                                                  | 2.0     | 17.09.2015 | Electronic file     |
| Header File  | phCryptoLibUtils_Arith.h                                                                                                              | 2.0     | 17.09.2015 | Electronic file     |
| Header File  | phCryptoLibUtils_MemMgmt.h                                                                                                            | 2.0     | 17.09.2015 | Electronic file     |
| Header File  | phCryptoLibRsaKg.h                                                                                                                    | 2.0     | 17.09.2015 | Electronic file     |
| Header File  | phCryptoLibEccGfp.h                                                                                                                   | 2.0     | 17.09.2015 | Electronic file     |
| Document     | User guidance manual Firmware Libraries V2.x on P40C008/012/024/040/072 VE, Preparative procedures and operational user guidance [16] | 0.7     | 16.02.2016 | Electronic Document |
| Document     | User Guidance: Symmetric Crypto Library [22]                                                                                          | 1.6     | 11.11.2015 | Electronic Document |
| Document     | User Guidance: SHA Library [21]                                                                                                       | 1.6     | 11.11.2015 | Electronic Document |
| Document     | User Guidance: RNG Library [18]                                                                                                       | 1.9     | 11.11.2015 | Electronic Document |
| Document     | User Guidance: RSA Library [20]                                                                                                       | 1.6     | 11.11.2015 | Electronic Document |
| Document     | User Guidance: Utils Library [23]                                                                                                     | 1.6     | 11.11.2015 | Electronic Document |
| Document     | User Guidance: RSA Key Generation Library [19]                                                                                        | 0.3     | 11.11.2015 | Electronic Document |
| Document     | User Guidance: ECC over GF(p) Library [17]                                                                                            | 0.3     | 11.11.2015 | Electronic Document |

**Tab. 1.1:** Components of the TOE (CryptoLib)

| Type        | Name                                                                                                                                  | Release | Date       | Form of Delivery    |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------|---------|------------|---------------------|
| DAT File    | SystemMode.dat                                                                                                                        | 1.2     | 27.04.2015 | Electronic file     |
| BCF File    | HAL.bcf                                                                                                                               | 1.2     | 27.04.2015 | Electronic file     |
| CFG File    | SystemMode_FirewallValues.cfg                                                                                                         | 1.2     | 27.04.2015 | Electronic file     |
| Header File | phhalConf.h                                                                                                                           | 1.2     | 27.04.2015 | Electronic file     |
| Header File | phhalCrc.h                                                                                                                            | 1.2     | 27.04.2015 | Electronic file     |
| Header File | phhalMem.h                                                                                                                            | 1.2     | 27.04.2015 | Electronic file     |
| Header File | phhalMem_AT.h                                                                                                                         | 1.2     | 27.04.2015 | Electronic file     |
| Header File | phhalMem_NV.h                                                                                                                         | 1.2     | 27.04.2015 | Electronic file     |
| Header File | phhalPatch.h                                                                                                                          | 1.2     | 27.04.2015 | Electronic file     |
| Header File | phP4xAppl.h                                                                                                                           | 1.2     | 27.04.2015 | Electronic file     |
| Document    | User guidance manual Firmware Libraries V2.x on P40C008/012/024/040/072 VE, Preparative procedures and operational user guidance [16] | 0.7     | 16.02.2016 | Electronic Document |
| Document    | Product data sheet addendum: SmartMX2 P40 family P40Cxxx HAL Interface Specification [14]                                             | 3.2     | 16.11.2015 | Electronic Document |

Tab. 1.2: Components of the TOE (HAL-Lib v1.2) - UserMode Customer

| Type         | Name                                                                                                                                  | Release | Date       | Form of Delivery    |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------|---------|------------|---------------------|
| Library File | libHalCL.a                                                                                                                            | 1.2     | 27.04.2015 | Electronic file     |
| Library File | libHalMem.a                                                                                                                           | 1.2     | 27.04.2015 | Electronic file     |
| Header File  | phhalCrc.h                                                                                                                            | 1.2     | 27.04.2015 | Electronic file     |
| Header File  | phhalMem.h                                                                                                                            | 1.2     | 27.04.2015 | Electronic file     |
| Header File  | phhalMem_AT.h                                                                                                                         | 1.2     | 27.04.2015 | Electronic file     |
| Header File  | phhalMem_NV.h                                                                                                                         | 1.2     | 27.04.2015 | Electronic file     |
| Header File  | phhalInit_CryptoLibSetup.h                                                                                                            | 1.2     | 27.04.2015 | Electronic file     |
| Header File  | phhalInit_ATSetup.h                                                                                                                   | 1.2     | 27.04.2015 | Electronic file     |
| Document     | User guidance manual Firmware Libraries V2.x on P40C008/012/024/040/072 VE, Preparative procedures and operational user guidance [16] | 0.7     | 16.02.2016 | Electronic Document |
| Document     | Product data sheet addendum: SmartMX2 P40 family P40Cxxx HAL Interface Specification [14]                                             | 3.2     | 16.11.2015 | Electronic Document |

Tab. 1.3: Components of the TOE (HAL-Lib v1.2) - SystemMode Customer

| Type         | Name                                                                                                                                  | Release | Date       | Form of Delivery    |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------|---------|------------|---------------------|
| Library File | libHalCL.a                                                                                                                            | 1.2     | 27.04.2015 | Electronic file     |
| Header File  | phhalCrc.h                                                                                                                            | 1.2     | 27.04.2015 | Electronic file     |
| Header File  | phhalMem.h                                                                                                                            | 1.2     | 27.04.2015 | Electronic file     |
| Header File  | phhalMem_AT_Minimal.h                                                                                                                 | 1.2     | 27.04.2015 | Electronic file     |
| Header File  | phhalMem_NV.h                                                                                                                         | 1.2     | 27.04.2015 | Electronic file     |
| Header File  | phhalInit_CryptoLibSetup.h                                                                                                            | 1.2     | 27.04.2015 | Electronic file     |
| Document     | User guidance manual Firmware Libraries V2.x on P40C008/012/024/040/072 VE, Preparative procedures and operational user guidance [16] | 0.7     | 16.02.2016 | Electronic Document |
| Document     | Product data sheet addendum: SmartMX2 P40 family P40Cxxx HAL Interface Specification [14]                                             | 3.2     | 16.11.2015 | Electronic Document |

**Tab. 1.4:** Components of the TOE (HAL-Lib v1.2) - SystemMode Customer without libHalMem.a

| Type        | Name                                                                                                                                  | Release | Date       | Form of Delivery    |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------|---------|------------|---------------------|
| DAT File    | SystemMode.dat                                                                                                                        | 1.2.1   | 25.01.2016 | Electronic file     |
| BCF File    | HAL.bcf                                                                                                                               | 1.2.1   | 25.01.2016 | Electronic file     |
| CFG File    | SystemMode_FirewallValues.cfg                                                                                                         | 1.2.1   | 25.01.2016 | Electronic file     |
| Header File | phhalConf.h                                                                                                                           | 1.2.1   | 25.01.2016 | Electronic file     |
| Header File | phhalCrc.h                                                                                                                            | 1.2.1   | 25.01.2016 | Electronic file     |
| Header File | phhalMem.h                                                                                                                            | 1.2.1   | 25.01.2016 | Electronic file     |
| Header File | phhalMem_AT.h                                                                                                                         | 1.2.1   | 25.01.2016 | Electronic file     |
| Header File | phhalMem_NV.h                                                                                                                         | 1.2.1   | 25.01.2016 | Electronic file     |
| Header File | phhalPatch.h                                                                                                                          | 1.2.1   | 25.01.2016 | Electronic file     |
| Header File | phP4xAppl.h                                                                                                                           | 1.2.1   | 25.01.2016 | Electronic file     |
| Document    | User guidance manual Firmware Libraries V2.x on P40C008/012/024/040/072 VE, Preparative procedures and operational user guidance [16] | 0.7     | 16.02.2016 | Electronic Document |
| Document    | Product data sheet addendum: SmartMX2 P40 family P40Cxxx HAL Interface Specification [14]                                             | 3.2     | 16.11.2015 | Electronic Document |

**Tab. 1.5:** Components of the TOE (HAL-Lib v1.2.1) - UserMode Customer

| Type         | Name                                                                                                                                  | Release | Date       | Form of Delivery    |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------|---------|------------|---------------------|
| Library File | libHalCL.a                                                                                                                            | 1.2.1   | 25.01.2016 | Electronic file     |
| Library File | libHalMem.a                                                                                                                           | 1.2.1   | 25.01.2016 | Electronic file     |
| Header File  | phhalCrc.h                                                                                                                            | 1.2.1   | 25.01.2016 | Electronic file     |
| Header File  | phhalMem.h                                                                                                                            | 1.2.1   | 25.01.2016 | Electronic file     |
| Header File  | phhalMem_AT.h                                                                                                                         | 1.2.1   | 25.01.2016 | Electronic file     |
| Header File  | phhalMem_NV.h                                                                                                                         | 1.2.1   | 25.01.2016 | Electronic file     |
| Header File  | phhalInit_CryptoLibSetup.h                                                                                                            | 1.2.1   | 25.01.2016 | Electronic file     |
| Header File  | phhalInit_ATSetup.h                                                                                                                   | 1.2.1   | 25.01.2016 | Electronic file     |
| Document     | User guidance manual Firmware Libraries V2.x on P40C008/012/024/040/072 VE, Preparative procedures and operational user guidance [16] | 0.7     | 16.02.2016 | Electronic Document |
| Document     | Product data sheet addendum: SmartMX2 P40 family P40Cxxx HAL Interface Specification [14]                                             | 3.2     | 16.11.2015 | Electronic Document |

Tab. 1.6: Components of the TOE (HAL-Lib v1.2.1) - SystemMode Customer

| Type         | Name                                                                                                                                  | Release | Date       | Form of Delivery    |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------|---------|------------|---------------------|
| Library File | libHalCL.a                                                                                                                            | 1.2.1   | 25.01.2016 | Electronic file     |
| Header File  | phhalCrc.h                                                                                                                            | 1.2.1   | 25.01.2016 | Electronic file     |
| Header File  | phhalMem.h                                                                                                                            | 1.2.1   | 25.01.2016 | Electronic file     |
| Header File  | phhalMem_AT_Minimal.h                                                                                                                 | 1.2.1   | 25.01.2016 | Electronic file     |
| Header File  | phhalMem_NV.h                                                                                                                         | 1.2.1   | 25.01.2016 | Electronic file     |
| Header File  | phhalInit_CryptoLibSetup.h                                                                                                            | 1.2.1   | 25.01.2016 | Electronic file     |
| Document     | User guidance manual Firmware Libraries V2.x on P40C008/012/024/040/072 VE, Preparative procedures and operational user guidance [16] | 0.7     | 16.02.2016 | Electronic Document |
| Document     | Product data sheet addendum: SmartMX2 P40 family P40Cxxx HAL Interface Specification [14]                                             | 3.2     | 16.11.2015 | Electronic Document |

Tab. 1.7: Components of the TOE (HAL-Lib v1.2.1) - SystemMode Customer without libHalMem.a

*Remark 1.* For more information on the configuration options of the TOE the user is referred to [16].

## 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 [13]. 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 [13].

### 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 [13].

A Smartcard embedded Software developer may create Smartcard embedded Software to execute on the P40C008/012/024/040/072 hardware. This software is stored in the User ROM of the P40C008/012/024/040/072 hardware and is not part of the TOE, with one exception: the Smartcard embedded Software may contain the “SmartMX2 P40 FW Libraries V2.0/V2.0.x” (or parts thereof and this SmartMX2 P40 FW Libraries V2.0/V2.0.x (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 key generation can be used to generate RSA key pairs.
- The RSA public key computation can be used to compute the public key that belongs to a given private CRT key. The TOE supports various key sizes for RSA up to a limit of 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 ECDSA (ECC over GF(p))**

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

The TOE supports various key sizes for ECC over GF(p) up to a limit of 384 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).

**1.4.2.2.1.5 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).

**1.4.2.2.1.6 Resistance of cryptographic algorithms against attacks**

The cryptographic algorithms are resistant against attacks as described in JIL, Attack Methods for Smartcards and Similar Devices [9], which include Side Channel Attacks, Perturbation attacks, Differential Fault Analysis (DFA) and timing attacks, except for SHA, which is only resistant against Side Channel Attacks and timing attacks.

**1.4.2.2.1.7 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.

**1.4.2.2.1.8 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 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.

##### **1.4.2.2.2.3 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)

##### **1.4.2.2.2.4 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 P40C008/012/024/040/072 VD/VE is listed in section “Documentation” of the Hardware Security Target [13].

The documentation of the SmartMX2 P40 FW Libraries V2.0/V2.0.x 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 there exists the

- SmartMX2 P40 family P40C008/012/024/040/072 HAL Interface Specification [14]

The user guidance document [16] contains:

- guidelines on the secure usage of the SmartMX2 P40 FW Libraries V2.0/V2.0.x, including the requirements on the environment (the Smartcard Embedded Software calling the SmartMX2 P40 FW Libraries V2.0/V2.0.x is considered to be part of the environment).

### 1.4.3 Interface of the TOE

The interface to the NXP Secure Smart Card Controller P40C008/012/024/040/072 VD/VE hardware is described in section “Interface of the TOE” of the Hardware Security Target [13]. The use of this interface is not restricted by the use of the SmartMX2 P40 FW Libraries V2.0/V2.0.x.

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 V2.0/V2.0.x. The developer of the Smartcard Embedded Software will link the required functionality of the SmartMX2 P40 FW Libraries V2.0/V2.0.x 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 [13]. The delivery process or the hardware platform is independent from the SmartMX2 P40 FW Libraries V2.0/V2.0.x.

The life-cycle phases are according to the Security IC Platform Protection Profile with Augmentation Packages [15], 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 V2.0/V2.0.x is delivered as part of Phase 1 above to the Smartcard Embedded Software developer. The SmartMX2 P40 FW Libraries V2.0/V2.0.x 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 V2.0/V2.0.x during the delivery process, the SmartMX2 P40 FW Libraries V2.0/V2.0.x 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 V2.0/V2.0.x in the Smartcard Embedded Software. The subsequent use of the SmartMX2 P40 FW Libraries V2.0/V2.0.x by Smartcard Embedded Software Developers is out of the control of the developer NXP Semiconductors, Business Unit Security & Connectivity; the integration of the SmartMX2 P40 FW Libraries V2.0/V2.0.x 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 V2.0/V2.0.x 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 V2.0/V2.0.x. The security measures installed within NXP, including a secure delivery process, ensure the integrity and quality of the delivered SmartMX2 P40 FW Libraries V2.0/V2.0.x binary files.

#### **1.4.6 Specific Issues of Smartcard Hardware and the Common Criteria**

Regarding the Application Note 4 of the Protection Profile [15] the TOE provides additional functionality which is not covered in the Protection profile [15] and the Hardware Security Target [13]. 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 [13].

The SmartMX2 P40 FW Libraries V2.0/V2.0.x is intended to support the development of the Smartcard Embedded Software since the cryptographic functions provided by the SmartMX2 P40 FW Libraries V2.0/V2.0.x include countermeasures against the threats described in this Security Target. The used modules of the SmartMX2 P40 FW Libraries V2.0/V2.0.x 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 V2.0/V2.0.x is the Smartcard Embedded Software, developed by customers of NXP, to run on the NXP Secure Smart Card Controller P40C008/012/024/040/072 VD/VE hardware.

### **1.4.9 General IT features of the TOE**

The general features of the NXP Secure Smart Card Controller P40C008/012/024/040/072 VD/VE hardware are described in section "TOE overview" of the Hardware Security Target [13]. 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 with Augmentation Packages](#), [15].

Since the Security Target claims conformance to the PP Security IC Platform Protection Profile with Augmentation Packages, the concepts are used in the same sense. For the definition of terms refer to the Protection Profile [15]. This chapter does not need any supplement in the Security Target.

The Protection Profile (PP) "Security IC Platform Protection Profile with Augmentation Packages" [15] defines "Augmentation Packages". This Security Target does not use any of the packages defined in the PP [15].

Regarding the Application Note 4 of [15] the TOE provides additional functionality which is not covered in the Security IC Platform Protection Profile with Augmentation Packages. 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 with Augmentation Packages](#), [15]

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 [15].

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 with Augmentation Packages](#), [15].

### 3 Security Problem Definition

This Security Target claims conformance to the “Security IC Platform Protection Profile”, [15]. 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”, [15], 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 [13]. 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 V2.0/V2.0.x [16].

#### 3.2 Threats

Since this Security Target claims conformance to the PP “Security IC Platform Protection Profile”, [15], 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 [13], 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 P40C008/012/024/040/072 VD/VE) and software (SmartMX2 P40 FW Libraries V2.0/V2.0.x). 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 [15] 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 Unauthorized Memory or Hardware Access**  
**ss**

Adverse action: An attacker may try to read, modify or execute code or data stored in restricted memory areas.  
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                                  |
|---------------------------------------|----------------------------------------|
| <a href="#">T.Unauthorised-Access</a> | 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”, [15], the policy [P.Process-TOE](#): “Identification during TOE Development and Production” of the Protection Profile is applied here

also.

| Name          | Title                                                |
|---------------|------------------------------------------------------|
| P.Process-TOE | Identification 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 P40C008/012/024/040/072 VD/VE. 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
- RSA key generation
- ECDSA (ECC over GF(p)) signature generation and verification,
- ECC over GF(p) key generation,
- ECDH (ECC Diffie-Hellman) key exchange,
- ECC over GF(p) point addition,
- ECC over GF(p) curve parameter verification,
- 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”, [15] 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”[15], 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.Resp-Appl      | Treatment of user data of the Composite TOE                |

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

The following additional assumptions are added in this Security Target from the P40C008/012/024/040/072 Hardware Security Target [13] 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 [13]

## 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”, [15]:

| 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 [13], 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 [13]:

| 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 shall provide the cryptographic functionality to perform encryption, decryption, signature creation, signature verification, message encoding and signature encoding using the RSA algorithm.

**O.RSA\_PubExp****RSA Public Exponent Computation**

The TOE shall provide the cryptographic functionality to compute an RSA public key from an RSA private CRT key.

**O.RSA\_KeyGen****RSA Key Generation**

The TOE shall provide the cryptographic functionality to generate RSA key pairs .

**O.ECDSA****ECDSA**

The TOE shall provide the cryptographic functionality to perform signature creation and signature verification using the ECC over  $GF(p)$  algorithm.

**O.ECC\_DHKE****EC Diffie-Hellman Key Exchange**

The TOE shall provide the cryptographic functionality to perform Diffie-Hellman key exchange based on ECC over  $GF(p)$  algorithm.

**O.ECC\_KeyGen****ECC Key Generation**

The TOE shall provide the cryptographic functionality to generate ECC over  $GF(p)$  key pairs .

**O.ECC\_Additional****ECC Point Addition and Domain Parameter Verification**

The TOE shall provide the cryptographic functionality to perform a point addition based on ECC over  $GF(p)$  and domain parameter verification for ECC over  $GF(p)$ .

**O.SHA****Secure Hash Algorithm**

The TOE shall provide the cryptographic functionality to perform electronic hashing using the SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 algorithms.

**O.Copy****Secure Copy**

The TOE shall provide the functionality to copy data from memories/Special Function Registers to memories/Special Function Registers.

**O.Compare****Secure Compare**

The TOE shall provide the functionality to compare data from memories/Special Function Registers to data from memories/Special Function Registers.

**O.REUSE****Reuse of Memory**

The TOE shall provide the 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 [9], which include Side Channel Attacks, Perturbation attacks, Differential Fault Analysis (DFA) and timing attack. The following exceptions apply:

- (a) RSA Public Key computation and RSA Key generation does not contain protective measures against DPA.
- (b) ECDSA (ECC over GF(p)) Key Generation 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 and ECC 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 [15] defines security objectives for the Security IC Embedded Software development environment which are listed below. Additional refinements in the Hardware Security Target [13] are also valid in the ST for the Crypto Library (the “Security IC Embedded Software”).

| Name         | Title                  |
|--------------|------------------------|
| 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 “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 [13].

The following additional security objective for the Security IC Embedded Software introduced in the Hardware Security Target [13] 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 [13] 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”, [15]. Table 4.6 reproduces the table in section 4.4 of [15].

| Security Problem Definition | Security Objective                              | Notes      |
|-----------------------------|-------------------------------------------------|------------|
| T.Leak-Inherent             | O.Leak-Inherent                                 |            |
| T.Phys-Probing              | O.Phys-Probing                                  |            |
| T.Malfunction               | O.Malfunction<br>O.Self-Test<br>O.INTEGRITY_CHK |            |
| T.Phys-Manipulation         | O.Phys-Manipulation<br>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.Resp-Appl                 | OE.Resp-Appl                                    | Phase 1    |

| Security Problem Definition | Security Objective | Notes |
|-----------------------------|--------------------|-------|
|-----------------------------|--------------------|-------|

Tab. 4.6: Security Objectives vs. Security Problem Definition (PP0084)

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<br>O.SFR_ACCESS                                                          |                  |
| P.Add-Components            | O.HW_DES3<br>O.HW_AES<br>O.Self-Test<br>O.Reset<br>O.CUST_RECONFIG<br>O.NVM_INTEGRITY |                  |
| A.Check-Init                | OE.Check-Init                                                                         | Phases 1 and 4–6 |
| A.Key-Function              | OE.Resp-Appl                                                                          | 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.Resp-Appl | The definition of this objective of the PP [15] 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 by this objective. |

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<br>O.DES<br>O.RSA<br>O.RSA_KeyGen<br>O.ECDSA<br>O.ECC_DHKE<br>O.ECC_KeyGen<br>O.ECC_Additional<br>O.SHA<br>O.Copy<br>O.Compare<br>O.REUSE<br>O.RSA_PubExp<br>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.RSA_KeyGen     | This objective covers the security policy because it requires the TOE to partly implement the functionality as required by the security policy. |
| O.ECDSA          | This objective covers the security policy because it requires the TOE to partly implement the functionality as required by the security policy. |
| O.ECC_DHKE       | This objective covers the security policy because it requires the TOE to partly implement the functionality as required by the security policy. |
| O.ECC_KeyGen     | This objective covers the security policy because it requires the TOE to partly implement the functionality as required by the security policy. |
| O.ECC_Additional | 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. |

| Objective             | Rationale                                                                                                                                       |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">O.RND</a> | 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”, [15] 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 [15] 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 [15] 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 [15] 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 P40C008/012/024/040/072 VD/VE vs. this Security Target (SmartMX2 P40 FW Libraries V2.0/V2.0.x), 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", [15]. 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             |
| FDP_SDC.1[HW] | Stored data confidentiality                 |
| FDP_SDI.2[HW] | Stored data integrity monitoring and action |
| 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 [13] 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 separate 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 [13] 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) |
| 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 [13] 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) |

| Name                      | Title                                                                                         |
|---------------------------|-----------------------------------------------------------------------------------------------|
| FCS_COP.1[SW_DES]         | Cryptographic Operation (DES & TDES)                                                          |
| 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[ECDSA]          | ECDSA Cryptographic Operation (ECC over GF(p) signature generation and verification)          |
| FCS_COP.1[ECC_DHKE]       | ECDH Cryptographic Operation (ECC over GF(p) Diffie-Hellman key exchange)                     |
| FCS_COP.1[ECC_Additional] | ECC Cryptographic Operation (ECC over GF(p) point addition and domain parameter verification) |
| FCS_COP.1[SHA]            | Cryptographic Operation (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)                           |
| FCS_CKM.1[RSA]            | Cryptographic key generation (RSA key generation)                                             |
| FCS_CKM.1[ECC]            | Cryptographic key generation (ECC key generation)                                             |
| 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 [9].

## **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 [9]. 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 [9]. 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 [9]. 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 [9]. 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[ECDSA] ECDSA Cryptographic Operation (ECC over GF(p) signature generation 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[ECDSE]** The TSF shall perform *signature generation and verification* in accordance with the specified cryptographic algorithm *ECDSE / ECC over GF(p)* and cryptographic key sizes *128 to 384 bits* that meet the following *standards: ISO/IEC 15946-2*.

**Application Note:** The security functionality is resistant against side channel analysis and other attacks described in [9]. 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[ECC\_DHE]** **ECDH Cryptographic Operation (ECC over GF(p) Diffie-Hellman key exchange)**

**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[ECC\_DHE]** The TSF shall perform *Diffie-Hellman Key Exchange* in accordance with the specified cryptographic algorithm *ECC over GF(p)* and cryptographic key sizes *128 to 384 bits* that meet the following *standards: ISO/IEC 15946-3*.

**Application Note:**

- The security functionality is resistant against side channel analysis and other attacks described in [9]. 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 security functionality does not provide the complete key exchange procedure, but only the point multiplication which is used for the multiplication of the private key with the communication partner's public key. Therefore this function can be used as part of a Diffie-Hellman key exchange as well as pure point multiplication.

**FCS\_COP.1[ECC\_Additional]** **ECC Cryptographic Operation (ECC over GF(p) point addition and domain parameter 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[ECC\_Additional]** The TSF shall perform a *full point addition* in accordance with the specified cryptographic algorithm *ECC over GF(p)* and cryptographic key sizes *128 to 384 bits* that meet the following *standard: ISO/IEC 15946-1*.  
The TSF shall perform a *basic ECC over GF(p) domain parameter check* in accordance with the specified cryptographic algorithm *ECC over GF(p)* and cryptographic key sizes *128 to 384 bits* that meet the following *standard: ISO/IEC 15946-1..*

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Application Note:</b> | The security functionality is resistant against side channel analysis and other attacks described in [9]. 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).                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>FCS_COP.1[SHA]</b>    | <b>Cryptographic Operation (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 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 <i>SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512</i> and cryptographic key size <i>none</i> that meet the following <i>standard: FIPS 180-3</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Application Note:</b> | <ul style="list-style-type: none"> <li>The security functionality is resistant against side channel analysis and other attacks described in [9]. 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.</li> <li>The length of the data to hash has to be a multiple of one byte. Arbitrary bit lengths are not supported.</li> </ul>                                                                                                                                                                                                                                                |
| <b>FCS_CKM.1[RSA]</b>    | <b>Cryptographic key generation (RSA key generation)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Hierarchical-To          | No other components.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Dependencies             | [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| FCS_CKM.1.1[RSA]         | The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm <i>RSA</i> and specified cryptographic key sizes <i>512-2048 bits</i> that meet the following <i>standards: PKCS #1, v2.2</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Application Note:</b> | The security functionality is resistant against side channel analysis and other attacks described in [9]. 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).                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Note:</b>             | The implementation of RSA key generation is aligned with the "Bundesnetzagentur fuer Elektrizitaet, Gas, Telekommunikation, Post und Eisenbahnen: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Uebersicht ueber geeignete Algorithmen)", German "Bundesanzeiger (www.bundesanzeiger.de) BAnz AT 30.01.2015 B3". This standard sets up requirements for RSA key generation, if the generated RSA key pair is used in a signature application according to the German Signature Act. This standard is also accepted by the German Bundesamt fuer Sicherheit in der Informationstechnik (BSI) for Common Criteria evaluations that include the assurance requirements AVA_VAN.5 with high attack potential. |

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>FCS_CKM.1[ECC]</b>    | <b>Cryptographic key generation (ECC key generation)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Hierarchical-To          | No other components.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Dependencies             | [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]<br>FCS_CKM.4 Cryptographic key destruction                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| FCS_CKM.1.1[ECC]         | The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm <i>ECDSA (ECC over GF(p))</i> and specified cryptographic key sizes <i>128 to 384 bits</i> that meet the following <i>standards: ISO/IEC 15946-1</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Application Note:</b> | The security functionality is resistant against side channel analysis and other attacks described in [9]. 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).                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Note:</b>             | The implementation of ECC key generation is aligned with the "Bundesnetzagentur fuer Elektrizitaet, Gas, Telekommunikation, Post und Eisenbahnen: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Uebersicht ueber geeignete Algorithmen)", German "Bundesanzeiger (www.bundesanzeiger.de) BAnz AT 30.01.2015 B3". This standard sets up requirements for ECC key generation, if the generated ECC key pair is used in a signature application according to the German Signature Act. This standard is also accepted by the German Bundesamt fuer Sicherheit in der Informationstechnik (BSI) for Common Criteria evaluations that include the assurance requirements AVA_VAN.5 with high attack potential. |
| <b>FDP_RIP.1[SW]</b>     | <b>Subset Residual Information Protection</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 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: <i>all objects (variables)</i> used by the <i>Crypto Library</i> as specified in the user guidance documentation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>FCS_CKM.4</b>         | <b>Cryptographic key destruction</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 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 <i>overwrite</i> that meets the following <i>standards: ISO11568</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Note:</b>             | The <i>SmartMX2 P40 FW Libraries V2.0/V2.0.x</i> provides the embedded software with functionality for key destruction for <a href="#">FCS_COP.1[SW_AES]</a> and <a href="#">FCS_COP.1[SW_DES]</a> and <a href="#">FCS_CKM.1[RSA]</a> .<br>Clearing of keys that are provided by the smartcard embedded software to the <i>SmartMX2 P40 FW Libraries V2.0/V2.0.x</i> 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 [9].

#### 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 *ROM*, *RAM* and *EEPROM*.

**Application Note:** The security functionality is resistant against side channel analysis and other attacks described in [9].

## 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 [15] the column "Required by" shows the differences in the requirements of security assurance components between the PP [15] and the Security Target. The entry "EAL5 / PP" denotes, that an SAR is required by both EAL5 and the requirement of the PP [15], "EAL5" means that this requirement is due to EAL5 and beyond the requirement of the PP [15], 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 [15], 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 |

| Name      | Title                                                          |
|-----------|----------------------------------------------------------------|
| 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 automa-<br>tion  |
| 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<br>summary |
| 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 [15] and therefore it has to be conform to the refinements of the TOE security assurance requirements (see Application Note 22 in [15]). Because the refinements in the PP [15] 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 [13] has chosen the evaluation assurance level EAL5. This Hardware Security Target bases on the Protection Profile [15], which requires the lower level EAL4+. This implies that the refinements made in the Protection Profile [15], 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 [15] 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 [15] provides a rationale for the mapping between security functional requirements and security objectives defined in the PP [15]. The mapping is reproduced in the following table.

| SO                  | SFR                                                                                                                  |
|---------------------|----------------------------------------------------------------------------------------------------------------------|
| O.Leak-Inherent     | FDP_IFC.1<br>FDP_ITT.1[HW]<br>FPT_ITT.1[HW]                                                                          |
| O.Phys-Probing      | FDP_SDC.1[HW]<br>FPT_PHP.3                                                                                           |
| O.Malfunction       | FPT_FLS.1<br>FRU_FLT.2                                                                                               |
| O.Phys-Manipulation | FDP_SDI.2[HW]<br>FPT_PHP.3                                                                                           |
| O.Leak-Forced       | FDP_IFC.1<br>FDP_ITT.1[HW]<br>FPT_FLS.1<br>FPT_ITT.1[HW]<br>FPT_PHP.3<br>FRU_FLT.2                                   |
| O.Abuse-Func        | FDP_IFC.1<br>FDP_ITT.1[HW]<br>FMT_LIM.1[HW]<br>FMT_LIM.2[HW]<br>FPT_FLS.1<br>FPT_ITT.1[HW]<br>FPT_PHP.3<br>FRU_FLT.2 |
| O.Identification    | FAU_SAS.1[HW]                                                                                                        |
| O.RND               | FCS_RNG.1[DET]<br>FCS_RNG.1[HW]<br>FDP_IFC.1<br>FDP_ITT.1[HW]                                                        |

| SO | SFR                                                  |
|----|------------------------------------------------------|
|    | FPT_FLS.1<br>FPT_ITT.1[HW]<br>FPT_PHP.3<br>FRU_FLT.2 |

**Tab. 6.5:** Security Functional Requirements vs. Security Objectives (PP0084)

*Remark 7.* [O.RND](#) has been extended if compared to the PP [15] 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 [13] 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                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">O.HW_DES3</a>       | <a href="#">FCS_COP.1[HW_DES]</a>                                                                                                                                     |
| <a href="#">O.HW_AES</a>        | <a href="#">FCS_COP.1[HW_AES]</a>                                                                                                                                     |
| <a href="#">O.INTEGRITY_CHK</a> | <a href="#">FDP_ITT.1[HW]</a><br><a href="#">FPT_ITT.1[HW]</a>                                                                                                        |
| <a href="#">O.CUST_RECONFIG</a> | <a href="#">FMT_SMF.1[HW]</a>                                                                                                                                         |
| <a href="#">O.NVM_INTEGRITY</a> | <a href="#">FDP_SDI.2[HW]</a>                                                                                                                                         |
| <a href="#">O.MEM_ACCESS</a>    | <a href="#">FDP_ACC.1[MEM]</a><br><a href="#">FDP_ACF.1[MEM]</a><br><a href="#">FMT_MSA.1[MEM]</a><br><a href="#">FMT_MSA.3[MEM]</a><br><a href="#">FMT_SMF.1[HW]</a> |
| <a href="#">O.SFR_ACCESS</a>    | <a href="#">FDP_ACC.1[SFR]</a><br><a href="#">FDP_ACF.1[SFR]</a><br><a href="#">FMT_MSA.1[SFR]</a><br><a href="#">FMT_MSA.3[SFR]</a><br><a href="#">FMT_SMF.1[HW]</a> |
| <a href="#">O.Self-Test</a>     | <a href="#">FPT_TST.1</a>                                                                                                                                             |
| <a href="#">O.Reset</a>         | <a href="#">FMT_SMF.1[SW]</a>                                                                                                                                         |

**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 [13].

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[HW_AES]<br>FCS_COP.1[SW_AES] |
| O.DES            | FCS_COP.1[HW_DES]<br>FCS_COP.1[SW_DES] |
| O.RSA            | FCS_COP.1[RSA]<br>FCS_COP.1[RSA_Pad]   |
| O.RSA_PubExp     | FCS_COP.1[RSA_PubExp]                  |
| O.RSA_KeyGen     | FCS_CKM.1[RSA]                         |
| O.ECDSA          | FCS_COP.1[ECDSA]                       |
| O.ECC_DHKE       | FCS_COP.1[ECC_DHKE]                    |
| O.ECC_KeyGen     | FCS_CKM.1[ECC]                         |
| O.ECC_Additional | FCS_COP.1[ECC_Additional]              |
| O.SHA            | FCS_COP.1[SHA]                         |
| O.Copy           | FDP_SOP.1[Copy]                        |
| O.Compare        | FDP_SOP.1[Compare]                     |
| O.REUSE          | FCS_CKM.4<br>FDP_RIP.1[SW]             |

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]. |

| SFR                               | Rationale                                                                                                                                                            |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">FCS_COP.1[HW_DES]</a> | This objective requires the TOE to support Tripe-DES encryption and decryption. <a href="#">FCS_COP.1[HW_DES]</a> requires the Triple-DES according to the standard. |

**Justification related to [O.RSA](#):**

| SFR                                | Rationale                                                                                                                                           |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">FCS_COP.1[RSA]</a>     | This SFR requires the TOE to support RSA encryption, decryption, signature and verification according to the standard as demanded by the objective. |
| <a href="#">FCS_COP.1[RSA_Pad]</a> | 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                                                                                                                           |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">FCS_COP.1[RSA_PubExp]</a> | This SFR requires the TOE to support the computation of a public exponent from an RSA private CRT key as demanded by the objective. |

**Justification related to [O.RSA\\_KeyGen](#):**

| SFR                            | Rationale                                                                                                       |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <a href="#">FCS_CKM.1[RSA]</a> | This SFR requires the TOE to support RSA key generation according to the standard as demanded by the objective. |

**Justification related to [O.ECDSA](#):**

| SFR                              | Rationale                                                                                                                     |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">FCS_COP.1[ECDSA]</a> | This SFR requires the TOE to support ECDSA signature and verification according to the standard as demanded by the objective. |

**Justification related to [O.ECC\\_DHKE](#):**

| SFR                                 | Rationale                                                                                                       |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <a href="#">FCS_COP.1[ECC_DHKE]</a> | This SFR requires the TOE to support ECDH key agreement according to the standard as demanded by the objective. |

Justification related to [O.ECC\\_Additional](#):

| SFR                                       | Rationale                                                                                                                  |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <a href="#">FCS_COP.1[ECC_Additional]</a> | This SFR requires the TOE to support elliptic curve point addition according to the standard as demanded by the objective. |

Justification related to [O.ECC\\_KeyGen](#):

| SFR                            | Rationale                                                                                                       |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <a href="#">FCS_CKM.1[ECC]</a> | This SFR requires the TOE to support RSA key generation according to the standard as demanded by the objective. |

Justification related to [O.SHA](#):

| SFR                            | Rationale                                                                                                                                                                                        |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">FCS_COP.1[SHA]</a> | 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">FCS_RNG.1[DET]</a> | <p>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.</p> <ul style="list-style-type: none"><li>• <i>Ensured cryptographic quality (sufficient entropy part) of generated random numbers is met by <a href="#">FCS_RNG.1.1[DET]</a> through the characteristic deterministic and the random number generator meeting NIST SP 800-90 (<a href="#">FCS_RNG.1.1[DET]</a>). Ensured cryptographic quality (not predictable part) of generated random numbers is met by <a href="#">FCS_RNG.1[DET]</a> through the characteristic chi-squared test of the seed generator and <a href="#">FCS_RNG.1[HW]</a> from the certified hardware platform.</i></li><li>• <i>Information about the generated random numbers is not available to an attacker is met through <a href="#">ADV_ARC.1</a>, 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.</i></li></ul> |
| <a href="#">FCS_RNG.1[HW]</a>  | See PP0084.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <a href="#">FDP_ITT.1[HW]</a>  | See PP0084.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <a href="#">FDP_IFC.1</a>      | See PP0084.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <a href="#">FPT_FLS.1</a>      | See PP0084.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <a href="#">FPT_ITT.1[HW]</a>  | See PP0084.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <a href="#">FPT_PHP.3</a>      | See PP0084.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <a href="#">FRU_FLT.2</a>      | See PP0084.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

**Justification related to [O.Copy](#):**

| SFR                             | Rationale                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">FDP_SOP.1[Copy]</a> | This SFR requires the TOE to support secure copy which is exactly addressed by <a href="#">FDP_SOP.1[Copy]</a> as demanded by the objective. |

**Justification related to O.Compare:**

| SFR                                | Rationale                                                                                                                                          |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">FDP_SOP.1[Compare]</a> | This SFR requires the TOE to support secure compare which is exactly addressed by <a href="#">FDP_SOP.1[Compare]</a> as demanded by the objective. |

**Justification related to O.REUSE:**

| SFR                           | Rationale                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">FDP_RIP.1[SW]</a> | <a href="#">O.REUSE</a> 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 <a href="#">System Mode</a> and is met by the SFR <a href="#">FDP_RIP.1[SW]</a> , which requires the CryptoLib to make unavailable all memory contents that has been used by it. |
| <a href="#">FCS_CKM.4</a>     | <a href="#">FCS_CKM.4</a> contributes in addition to <a href="#">FDP_RIP.1[SW]</a> .                                                                                                                                                                                                                                                                                 |

- 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 [15] 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 [15] contains extended functional requirements, which are explained in the rationale of the PP (see [15], section 5).

### 6.3.3 Dependencies of Security Functional Requirements

The dependencies listed in the PP [15] are independent of the additional dependencies listed in the table below. The dependencies of the PP [15] are fulfilled within the PP [15] 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       |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
| <a href="#">FCS_RNG.1[DET]</a>     | No dependencies                                                                                                                                                                                                |                                                    |
| <a href="#">FCS_COP.1[SW_DES]</a>  | [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]<br>FCS_CKM.4 Cryptographic key destruction.  | See note below.                                    |
| <a href="#">FCS_COP.1[SW_AES]</a>  | [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]<br>FCS_CKM.4 Cryptographic key destruction.  | See note below.                                    |
| <a href="#">FCS_COP.1[RSA]</a>     | [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],<br>FCS_CKM.4 Cryptographic key destruction. | See <a href="#">FCS_CKM.1[RSA]</a> and note below. |
| <a href="#">FCS_COP.1[RSA_Pad]</a> | [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],<br>FCS_CKM.4 Cryptographic key destruction. | See <a href="#">FCS_CKM.1[RSA]</a> and note below. |

| SFR                                       | Dependencies                                                                                                                                                                                                | Fulfilled by Security Requirements in the ST       |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
| <a href="#">FCS_COP.1[RSA_PubExp]</a>     | [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 <a href="#">FCS_CKM.1[RSA]</a> and note below. |
| <a href="#">FCS_COP.1[ECDSA]</a>          | [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 <a href="#">FCS_CKM.1[ECC]</a> and note below. |
| <a href="#">FCS_COP.1[ECC_DHKE]</a>       | [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 <a href="#">FCS_CKM.1[ECC]</a> and note below. |
| <a href="#">FCS_COP.1[ECC_Additional]</a> | [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 <a href="#">FCS_CKM.1[ECC]</a> and note below. |
| <a href="#">FCS_COP.1[SHA]</a>            | [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 note below.                                    |
| <a href="#">FCS_CKM.1[RSA]</a>            | [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction                                                                                    | See note below.                                    |

| SFR                                | Dependencies                                                                                                                                                      | Fulfilled by Security Requirements in the ST |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| <a href="#">FCS_CKM.1[ECC]</a>     | [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction                                          | See note below.                              |
| <a href="#">FCS_CKM.4</a>          | [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] | See note below.                              |
| <a href="#">FDP_RIP.1[SW]</a>      | No dependencies                                                                                                                                                   |                                              |
| <a href="#">FDP_SOP.1[Compare]</a> | No dependencies                                                                                                                                                   |                                              |
| <a href="#">FDP_SOP.1[Copy]</a>    | No dependencies                                                                                                                                                   |                                              |

Tab. 6.22: Dependencies of Security Functional Requirements

**Note:**

The functional requirements [FDP\_ITC.1, or FDP\_ITC.2 or FCS\_CKM.1] are not included in this Security Target for [FCS\\_COP.1\[SW\\_AES\]](#), [FCS\\_COP.1\[SW\\_DES\]](#) and [FCS\\_COP.1\[SHA\]](#) since with respect to AES, DES, SHA the TOE only provides a pure engine for encryption and decryption (and hash computation) without additional features for the creation of cryptographic keys. In the case of the AES, DES and RSA the TOE provides functionality for key destruction (cf. [FCS\\_CKM.4](#)).

For ECC the [Security IC Embedded Software](#) must fulfill the requirements for key destruction 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 [15]. 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 [15] 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 [15], 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 [15] 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 [13]). 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 continuously 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 [16]). 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 [16] 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 static 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 (that is, "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 [10]*
- *CBC according to [10]*
- *CBC-MAC according to [11]*
- *CMAC according to [12]*

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 [10]*
- *CBC according to [10]*
- *CBC-MAC according to [11]*
- *CMAC according to [12]*

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) [28].

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) [28].

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.RSA\_KeyGen****RSA\_KeyGen**

[SS.RSA\\_KeyGen](#) provides functions to generate RSA key pairs as described in [28] and [29].

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).

Two different output formats for the key parameters are supported by the TOE, namely the *Simple Straight Forward Method* (called *RSA straight forward* and *RSA* using the *Chinese Remainder Theorem* (RSA CRT)).

**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 [27].

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.ECDSA****ECDSA**

[SS.ECDSA](#) provides functions that implement the ECDSA algorithm for signature and verification. All algorithms are defined in ISO/IEC 15946-2 [24].

Note that hashing of the message must be done beforehand and is not provided by this security functionality, but could be provided by [SS.SHA](#).

This routine supports various key lengths from 128 bits to 384 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.ECC\_DHKE**      **ECC\_DHKE**

[SS.ECC\\_DHKE](#) provides functions that perform the elliptic curve Diffie-Hellman Key Exchange as defined in ISO/IEC 15946-3 [25].

This routine supports various key lengths from 128 bits to 384 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.ECC\_Additional**      **ECC\_Additional**

[SS.ECC\\_Additional](#) provides functions that perform a full elliptic curve point addition as defined in ISO/IEC 15946-1 [26] as well as a basic curve parameter check for EC domain parameters.

This routine supports various key lengths from 128 bits to 384 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.ECC\_KeyGen**      **ECC\_KeyGen**

[SS.ECC\\_KeyGen](#) provides functions that perform ECC over GF(p) key generation as defined in ISO/IEC 15946-1 [26].

This routine supports various key lengths from 128 bits to 384 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.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 [\[13\]](#).

### 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 [\[13\]](#).

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.

For all ECC related calculations, randomized projective coordinates are used. Timing attacks are prevented using careful coding

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 [\[13\]](#). The TOE implements a number of software sensors that detect DFA attacks on AES, DES, RSA and ECC. Also software sensors are implemented to detect perturbation attacks in the secure copy and the secure compare functions.

### SF.PHY

Protection against physical manipulation and probing is completely covered by the underlying hardware platform [\[13\]](#).

## 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  | FPT_FLS.1     | Failure with Preservation of Secure State        |
|         | FRU_FLT.2     | Limited Fault Tolerance                          |
| SF.PHY  | FDP_ITT.1[HW] | Basic Internal Transfer Protection               |
|         | FDP_SDI.2[HW] | Stored data integrity monitoring and action      |
|         | FPT_ITT.1[HW] | Basic Internal TSF Data Transfer Protection      |
|         | FPT_PHP.3     | Resistance to Physical Attack                    |
|         | FMT_SMF.1[HW] | Specification of Management Functions (Hardware) |
| SF.LOG  | FDP_ITT.1[HW] | Basic Internal Transfer Protection               |
|         | FDP_IFC.1     | Subset Information Flow Control                  |
|         | FDP_SDC.1[HW] | Stored data confidentiality                      |
|         | FPT_ITT.1[HW] | Basic Internal TSF Data Transfer Protection      |
| SF.COMP | FAU_SAS.1[HW] | Audit Storage                                    |
|         | FMT_LIM.1[HW] | Limited Capabilities                             |
|         | FMT_LIM.2[HW] | Limited Availability                             |

Tab. 7.5: TOE Security Functionality vs. Security Functional Requirements (PP0084)

| 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.RSA_KeyGen     | FCS_CKM.1[RSA]            | Cryptographic key generation (RSA key generation)                                             |
| 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.ECDSA          | FCS_COP.1[ECDSA]          | ECDSA Cryptographic Operation (ECC over GF(p) signature generation and verification)          |
| SS.ECC_DHKE       | FCS_COP.1[ECC_DHKE]       | ECDH Cryptographic Operation (ECC over GF(p) Diffie-Hellman key exchange)                     |
| SS.ECC_Additional | FCS_COP.1[ECC_Additional] | ECC Cryptographic Operation (ECC over GF(p) point addition and domain parameter verification) |
| SS.ECC_KeyGen     | FCS_CKM.1[ECC]            | Cryptographic key generation (ECC key generation)                                             |
| 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)                                                                |

| TSF             | SFR                | Title                                    |
|-----------------|--------------------|------------------------------------------|
| 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)

### 7.3.2 Rationale for the portions of the TOE security functionality

#### SS.SW\_RNG: Deterministic Random Number Generator

The Crypto Library implements appropriate online tests according to the Hardware User Guidance Manual for the hardware RNG (cf. [8]), which fulfills the functionality class PTG.2 defined by AIS20/31 [1], as required by FCS\_RNG.1[DET].

#### SS.SW\_AES: AES

SS.SW\_AES provides AES en-/decryption with key sizes 128, 192 and 256 bit in ECB and CBC mode, as well as MAC-calculation in CBC-MAC and CMAC mode. SS.SW\_AES builds upon SS.HW\_AES following the Hardware User Guidance Manual [8]. Additionally, SS.SW\_AES implements countermeasures against leakage, and therefore supports FDP\_ITT.1[HW], FPT\_ITT.1[HW] and FDP\_IFC.1. SS.SW\_AES covers FCS\_COP.1[SW\_AES].

#### SS.SW\_DES: Triple DES

SS.SW\_DES provides DES en-/decryption with key sizes 56 (Single-DES), 112 (Two-Key TripleDES) and 168 bit (Three-Key TripleDES) in ECB and CBC mode, as well as MAC-calculation in CBC-MAC and CMAC mode. SS.SW\_DES builds upon SS.HW\_DES3 following the Hardware User Guidance Manual [8]. Additionally, SS.SW\_DES implements countermeasures against leakage, and therefore supports FDP\_ITT.1[HW], FPT\_ITT.1[HW] and FDP\_IFC.1. SS.SW\_DES covers FCS\_COP.1[SW\_DES].

#### SS.RSA: RSA

SS.RSA provides RSA public key and private key operations with key sizes from 512 up to 2048 bits. SS.RSA implements countermeasures against leakage, and therefore supports FDP\_ITT.1[HW], FPT\_ITT.1[HW] and FDP\_IFC.1. SS.RSA covers FCS\_COP.1[RSA].

#### SS.RSAPad: RSAPad

SS.RSAPad provides RSA message encoding and decoding for en-/decryption and signature/verification. SS.RSAPad implements countermeasures against leakage, and therefore supports FDP\_ITT.1[HW], FPT\_ITT.1[HW] and FDP\_IFC.1. SS.RSAPad covers FCS\_COP.1[RSA\_Pad].

#### SS.RSAPubExp: RSA\_PublicExp

[SS.RSAPubExp](#) provides the computation of an RSA public key from and RSA private CRT key. [SS.RSAPubExp](#) covers [FCS\\_COP.1\[RSA\\_PubExp\]](#).

#### **SS.RSA\_KeyGen: RSA\_KeyGen**

[SS.RSA\\_KeyGen](#) provides the generation of an RSA key pair. [SS.RSA\\_KeyGen](#) implements countermeasures against leakage, and therefore supports [FDP\\_ITT.1\[HW\]](#), [FPT\\_ITT.1\[HW\]](#) and [FDP\\_IFC.1](#). [SS.RSA\\_KeyGen](#) covers [FCS\\_CKM.1\[RSA\]](#).

#### **SS.SHA: SHA**

[SS.SHA](#) provides the computation of secure hash functions SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512. [SS.SHA](#) covers [FCS\\_COP.1\[SHA\]](#).

#### **SS.ECDSA: ECDSA**

[SS.ECDSA](#) provides ECDSA signature and verification operations with key sizes from 128 up to 384 bits. [SS.ECDSA](#) implements countermeasures against leakage, and therefore supports [FDP\\_ITT.1\[HW\]](#), [FPT\\_ITT.1\[HW\]](#) and [FDP\\_IFC.1](#). [SS.ECDSA](#) covers [FCS\\_COP.1\[ECDSA\]](#).

#### **SS.ECC\_DHKE: ECC\_DHKE**

[SS.ECC\\_DHKE](#) provides ECC Diffie-Hellman key exchange with key sizes from 128 up to 384 bits. [SS.ECC\\_DHKE](#) implements countermeasures against leakage, and therefore supports [FDP\\_ITT.1\[HW\]](#), [FPT\\_ITT.1\[HW\]](#) and [FDP\\_IFC.1](#). [SS.ECC\\_DHKE](#) covers [FCS\\_COP.1\[ECC\\_DHKE\]](#).

#### **SS.ECC\_Additional: ECC\_Additional**

[SS.ECC\\_Additional](#) provides ECC secure point addition with key sizes from 128 up to 384 bits. [SS.ECC\\_Additional](#) implements countermeasures against leakage, and therefore supports [FDP\\_ITT.1\[HW\]](#), [FPT\\_ITT.1\[HW\]](#) and [FDP\\_IFC.1](#). [SS.ECC\\_Additional](#) covers [FCS\\_COP.1\[ECC\\_Additional\]](#).

#### **SS.ECC\_KeyGen: ECC\_KeyGen**

[SS.ECC\\_KeyGen](#) provides the generation of an RSA key pair. [SS.ECC\\_KeyGen](#) implements countermeasures against leakage, and therefore supports [FDP\\_ITT.1\[HW\]](#), [FPT\\_ITT.1\[HW\]](#) and [FDP\\_IFC.1](#). [SS.ECC\\_KeyGen](#) covers [FCS\\_CKM.1\[ECC\]](#).

#### **SS.COPY: Secure Copy**

Since [SS.COPY](#) provides secure copy and moving of data between memories and within memories it contributes to meeting [FDP\\_ITT.1\[HW\]](#) and [FPT\\_ITT.1\[HW\]](#). [SS.COPY](#) covers [FDP\\_SOP.1\[Copy\]](#).

#### **SS.COMPARE: Secure Compare**

Since [SS.COMPARE](#) provides secure compare functionality to compare different blocks of memory content in a manner protected against attacks, it contributes to meeting [FDP\\_ITT.1\[HW\]](#) and [FPT\\_ITT.1\[HW\]](#). [SS.COMPARE](#) covers [FDP\\_SOP.1\[Compare\]](#).

**SF.Object\_Reuse: Object Reuse**

The TOE provides internal security measures which clear memory areas used by the Crypto Library after usage. This functionality is required by the security functional component [FDP\\_RIP.1\[SW\]](#) taken from the Common Criteria Part 2. These measures ensure that a subsequent process may not gain access to cryptographic assets stored temporarily in memory used by the TOE. [SF.Object\\_Reuse](#) covers [FDP\\_RIP.1\[SW\]](#) and [FCS\\_CKM.4](#).

## 8 Glossary

| Abbreviation | Definition                                                                                                                                                                           |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CRC          | Cyclic Redundancy Check                                                                                                                                                              |
| CBC          | Cipher Block Chaining (a block cipher mode of operation)                                                                                                                             |
| CBC-MAC      | Cipher Block Chaining Message Authentication Code                                                                                                                                    |
| CC           | Common Criteria Version 3.1                                                                                                                                                          |
| CPU          | Central Processing Unit                                                                                                                                                              |
| DEA          | Data Encryption Algorithm                                                                                                                                                            |
| DES          | Data Encryption Standard                                                                                                                                                             |
| DRNG         | Deterministic Random Number Generator                                                                                                                                                |
| EAL          | Evaluation Assurance Level                                                                                                                                                           |
| ECB          | Electronic Code Book (a block cipher mode of operation)                                                                                                                              |
| IC           | Integrated circuit                                                                                                                                                                   |
| IT           | Information Technology                                                                                                                                                               |
| MMU          | Memory Management Unit                                                                                                                                                               |
| n/a          | not applicable                                                                                                                                                                       |
| NDA          | Non Disclosure Agreement                                                                                                                                                             |
| PKC          | Public Key Cryptography                                                                                                                                                              |
| ECC          | Elliptic Curve Cryptography                                                                                                                                                          |
| ECDSA        | Elliptic Curve Digital Signature Algorithm                                                                                                                                           |
| ECDH         | Elliptic Curve Diffie-Hellman (key exchange)                                                                                                                                         |
| PP           | Protection Profile                                                                                                                                                                   |
| SAR          | Security Assurance Requirement                                                                                                                                                       |
| SFR          | as abbreviation of the CC term: Security Functional Requirement, as abbreviation of the technical term of the SmartMX2-P40-family: Special Function Register                         |
| ST           | Security Target.                                                                                                                                                                     |
| TOE          | Target of Evaluation.                                                                                                                                                                |
| TRNG         | True Random Number Generator                                                                                                                                                         |
| TSF          | Part of the TOE that realises the security functionality                                                                                                                             |
| TSFI         | TSF Interface, a means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF |
| UART         | Universal Asynchronous Receiver and Transmitter                                                                                                                                      |
| RAM          | Random Access Memory                                                                                                                                                                 |
| ROM          | Read-Only Memory                                                                                                                                                                     |
| NV           | Non-Volatile                                                                                                                                                                         |
| DVE          | Development Environment                                                                                                                                                              |
| OPE          | Operational Environment                                                                                                                                                              |
| P40Cxxx      | used as placeholder for P40C008/012/024/040/072                                                                                                                                      |

| Abbreviation | Definition |
|--------------|------------|
|--------------|------------|

**Tab. 8.1:** Glossary

## 9 Bibliography

- [1] Bundesamt für Sicherheit in der Informationstechnik. A proposal for: Functionality classes and evaluation methodology for true (physical) random number generators, 09 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] Guidance and Operation Manual NXP Secure Smart Card Controller P40C008/012/024/040/072, Information on Guidance and Operation, NXP Semiconductors, Document number 269432, 2015-05-07.
- [9] JIL: Attack Methods for Smartcards and Similar Devices, Version 1.5, February 2009.
- [10] NIST Special Publication 800-38A Recommendation for BlockCipher Modes of Operation. <http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf>.
- [11] 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](http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf).
- [12] 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>.
- [13] NXP Secure Smart Card Controller P40C008/012/024/040/072 VD/VE, Security Target, NXP Semiconductors, Revision 2.0, 2015-07-07.
- [14] Product data sheet addendum SmartMX2 P40 family P40Cxxx, HAL interface specification, NXP Semiconductors, Document number 267432, 2015-11-16.

- [15] Security IC Platform Protection Profile with Augmentation Packages, registered and certified by Bundesamt fuer Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014, Rev 1.0, 13 January 2014.
- [16] User guidance manual Firmware Libraries V2.X on P40C008/012/024/040/072, Preparative procedures and operational user guidance, NXP Semiconductors, Document number 340307, 2016-02-16.
- [17] User manual Crypto Library on SmartMX2 P40 family P40Cxxx ECC over GF(p) Library, NXP Semiconductors, Document number 276003, 2015-11-11.
- [18] User manual Crypto Library on SmartMX2 P40 family P40Cxxx RNG Library, NXP Semiconductors, Document number 266319, 2015-11-11.
- [19] User manual Crypto Library on SmartMX2 P40 family P40Cxxx Rsa Key Generation Library, NXP Semiconductors, Document number 276103, 2015-11-11.
- [20] User manual Crypto Library on SmartMX2 P40 family P40Cxxx RSA Library, NXP Semiconductors, Document number 266616, 2015-11-11.
- [21] User manual Crypto Library on SmartMX2 P40 family P40Cxxx SHA Library, NXP Semiconductors, Document number 266416, 2015-11-11.
- [22] User manual Crypto Library on SmartMX2 P40 family P40Cxxx Symmetric Crypto Library, NXP Semiconductors, Document number 266516, 2015-11-11.
- [23] User manual Crypto Library on SmartMX2 P40 family P40Cxxx Utils Library, NXP Semiconductors, Document number 266716, 2015-11-11.
- [24] ISO/IEC 15946-2:2002: Information technology, Security techniques, Cryptographic techniques based on elliptic curves, Part 2: Digital signatures, 2002.
- [25] ISO/IEC 15946-3:2002: Information technology, Security techniques, Cryptographic techniques based on elliptic curves, Part 3: Key establishment, 2002.
- [26] ISO/IEC 15946-1:2008: Information technology, Security techniques, Cryptographic techniques based on elliptic curves, Part 1: General. ISO/IEC 15946-1:2008, 2008.
- [27] Federal Information Processing Standard (FIPS) 180-4: Secure Hash Standard (SHS)., 2012.
- [28] J. Jonsson and B. Kaliski. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2, 2012.
- [29] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION. Digital Signature Standard (DSS). <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>, 07 2013.

## 10 Contents

|                                                                                                 |           |                                                                                            |           |
|-------------------------------------------------------------------------------------------------|-----------|--------------------------------------------------------------------------------------------|-----------|
| <b>1 ST Introduction</b>                                                                        | <b>2</b>  | <b>5 Extended Components Definitions</b>                                                   | <b>29</b> |
| 1.1 ST Reference . . . . .                                                                      | 2         | 5.1 Secure basic operations (FDP_SOP) . . . . .                                            | 29        |
| 1.2 TOE Reference . . . . .                                                                     | 2         | <b>6 Security Requirements</b>                                                             | <b>30</b> |
| 1.3 TOE Overview . . . . .                                                                      | 2         | 6.1 Security Functional Requirements . . . . .                                             | 30        |
| 1.3.1 Introduction . . . . .                                                                    | 2         | 6.1.1 SFRs of the Protection Profile . . . . .                                             | 30        |
| 1.3.2 Difference to previous version of the product . . . . .                                   | 3         | 6.1.2 SFRs of the Hardware Security Target . . . . .                                       | 32        |
| 1.4 TOE Description . . . . .                                                                   | 3         | 6.1.3 SFRs added by the Crypto Library . . . . .                                           | 32        |
| 1.4.1 Physical Scope of TOE . . . . .                                                           | 3         | 6.1.4 Extended TOE security functional requirements . . . . .                              | 39        |
| 1.4.2 Logical Scope of TOE . . . . .                                                            | 7         | 6.2 Security Assurance Requirements . . . . .                                              | 39        |
| 1.4.3 Interface of the TOE . . . . .                                                            | 11        | 6.2.1 Refinements of the TOE Security Assurance Requirements . . . . .                     | 40        |
| 1.4.4 Life Cycle . . . . .                                                                      | 11        | 6.3 Security Requirements Rationale . . . . .                                              | 41        |
| 1.4.5 Security during Development and Production . . . . .                                      | 12        | 6.3.1 Rationale for the Security Functional Requirements . . . . .                         | 41        |
| 1.4.6 Specific Issues of Smartcard Hardware and the Common Criteria . . . . .                   | 12        | 6.3.2 Extended Requirements . . . . .                                                      | 47        |
| 1.4.7 TOE Intended Usage . . . . .                                                              | 12        | 6.3.3 Dependencies of Security Functional Requirements . . . . .                           | 48        |
| 1.4.8 TOE User Environment . . . . .                                                            | 13        | 6.3.4 Rationale for the Assurance Requirements . . . . .                                   | 50        |
| 1.4.9 General IT features of the TOE . . . . .                                                  | 13        | <b>7 TOE Summary Specification</b>                                                         | <b>52</b> |
| <b>2 Conformance Claims</b>                                                                     | <b>14</b> | 7.1 IT Security Functionality . . . . .                                                    | 52        |
| 2.1 Package Claim . . . . .                                                                     | 14        | 7.1.1 Security Services . . . . .                                                          | 54        |
| 2.2 PP Claim . . . . .                                                                          | 14        | 7.1.2 Security Features . . . . .                                                          | 57        |
| 2.3 Conformance Claim Rationale . . . . .                                                       | 15        | 7.2 Security architectural information . . . . .                                           | 58        |
| <b>3 Security Problem Definition</b>                                                            | <b>16</b> | 7.3 TOE Summary Specification Rationale . . . . .                                          | 58        |
| 3.1 Description of Assets . . . . .                                                             | 16        | 7.3.1 Mapping of Security Functional Requirements and TOE Security Functionality . . . . . | 58        |
| 3.2 Threats . . . . .                                                                           | 16        | 7.3.2 Rationale for the portions of the TOE security functionality . . . . .               | 61        |
| 3.3 Organizational Security Policies . . . . .                                                  | 17        | <b>8 Glossary</b>                                                                          | <b>64</b> |
| 3.4 Assumptions . . . . .                                                                       | 19        | <b>9 Bibliography</b>                                                                      | <b>68</b> |
| <b>4 Security Objectives</b>                                                                    | <b>20</b> | <b>10 Contents</b>                                                                         | <b>68</b> |
| 4.1 Security Objectives for the TOE . . . . .                                                   | 20        |                                                                                            |           |
| 4.2 Security Objectives for the Security IC Embedded Software Development Environment . . . . . | 22        |                                                                                            |           |
| 4.3 Security Objectives for the Operational Environment . . . . .                               | 23        |                                                                                            |           |
| 4.4 Security Objectives Rationale . . . . .                                                     | 23        |                                                                                            |           |

Please pay attention to the important notices concerning this document and the product(s) described herein, have been included in the section 'Legal information'.