SECURITY TARGET LITE

For the BCM_SPS02

Version 1.2

2016-11-28

Developed By

Broadcom Corporation

16340 West Bernardo Drive

San Diego California 92127

Certified by

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Table 1. Revision history

Revision Number	Date	Description
1.0	02/14/2016	Initial version
1.1	05/24/2016	Added FW Maintenance Updates
1.2	11/28/2016	Added FW Maintenance Update

Table of Contents

1 ST Introduction

This Security Target Lite (ST lite) defines the security objectives and requirements for the BCM_SPS02.

1.1 ST Reference

Title:	Security Target Lite for the BCM_SPS02
Version Number:	1.2
Date:	2016-11-28
Provided by:	Broadcom Corporation 16340 West Bernardo Drive San Diego, California 92127
Certified by:	Bundesamt für Sicherheit in der Informationstechnik (BSI)

The Security Target is based on the Protection Profile PP-0084 “Security IC Platform Protection Profile with Augmentation Packages” [PP] as publicly available for download at https://www.bsi.bund.de and certified under BSI-CC-PP-0084-2014. The Protection Profile and the Security Target are built in compliance with Common Criteria v3.1.

The certification body of this process is the German BSI, whereas the abbreviation stands for Federal Office for Information Security, in German language Bundesamt für Sicherheit in der Informationstechnik.

Note: The Embedded Security IC Software is not part of the TOE and is not covered by this Security Target.

1.2 TOE Reference

The TOE name is ”BCM_SPS02 Secure Processing System with Firmware version 002.030”.

1.3 TOE Overview

The TOE comprises the Broadcom BCM_SPS02 with specific IC dedicated software.

The BCM_SPS02 is intended to protect critical User Data, TSF Data (including the Security IC Embedded Software executing on the TOE) and provide a platform to load application software which provides functions to support financial transactions with embedded devices. The BCM_SPS02 is designed to be very flexible and to be able to support several different devices. These can include devices which use direct transaction media (point of sale terminals) or those which use Near Field Communication (NFC) such as cellular telephones.

The TOE is the physical representation of a die isolated hard macro that can be instantiated in an ASIC design (for an example refer to Figure 1). The BCM_SPS02 is self-sufficient at the boundary of the hard macro.

The BCM_SPS02 utilizes a variety of interfaces to communicate using ISO 7816 APDU commands to the external systems outside the TOE. The BCM_SPS02 includes a local SPI FLASH interface for storage of static information outside the TOE in external NVM. Confidentiality and integrity of any data stored outside of the SPS is in the responsibility of the Embedded Software developer.

An example implementation of an ASIC using the BCM_SPS02 is shown in Figure 1. The Peripheral Processing System (PPS) is used to implement further functionality for the system (e.g. keyboard input, USB interfaces, etc.).

The PPS is not part of this evaluation.

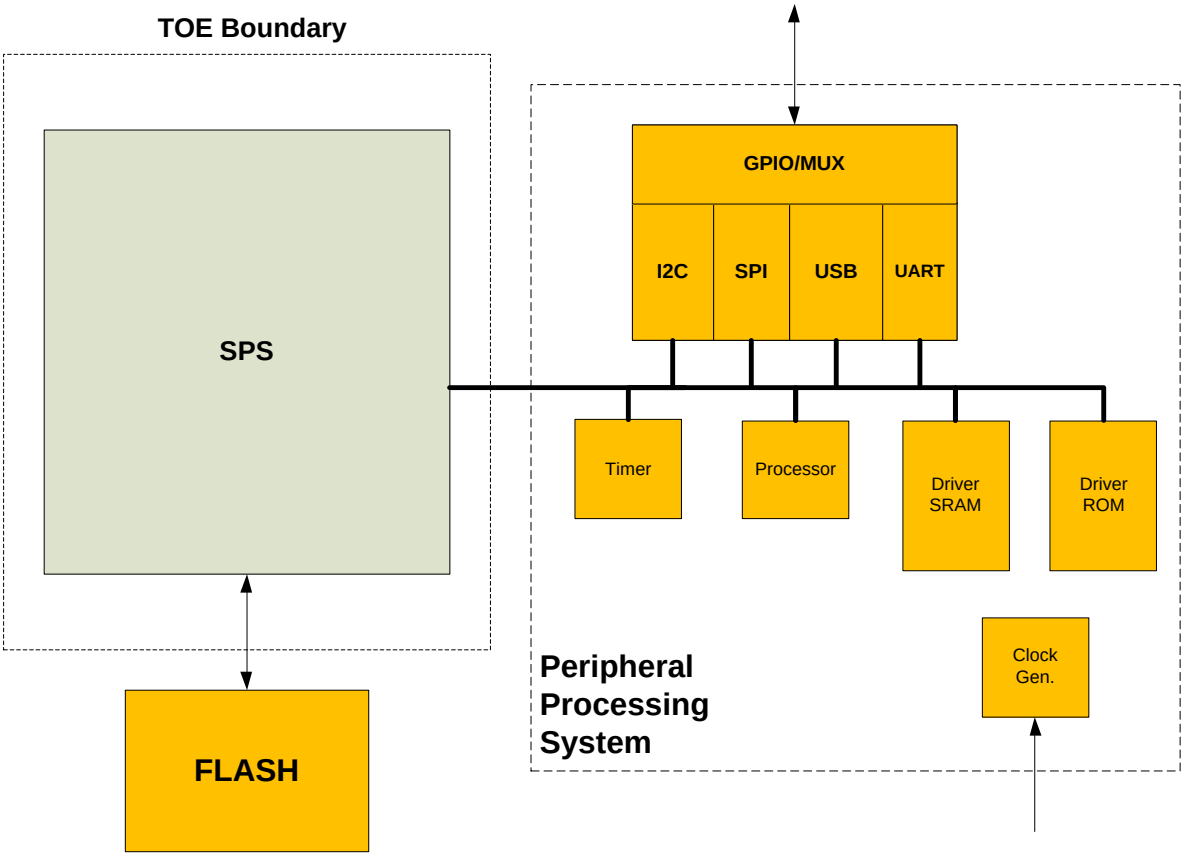


Figure 1. Example system block diagram.

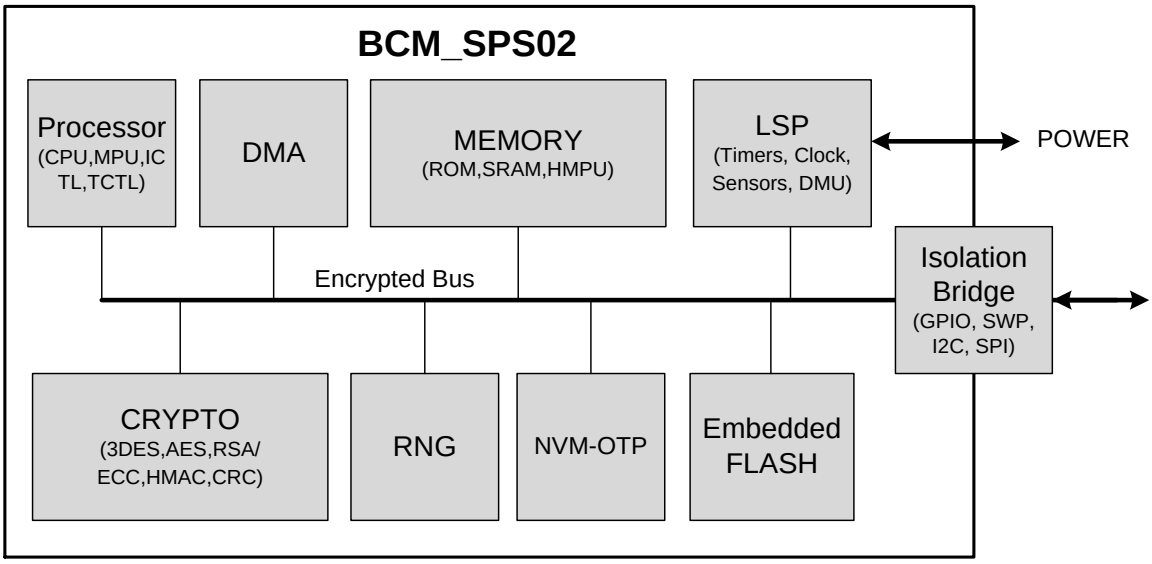


Figure 2. Simplified BCM_SPS02 Block Diagram.

Table 2 describes the acronyms used in Figure 1 and Figure 2.

Acronym	Meaning
SPS	Secure Processing System
GPIO	General purpose I/O
I2C	Inter-IC Communications
SPI	Serial Peripheral Interface
USB	Universal Serial Bus
UART	Universal Asynchronous Receiver Transmitter
ICTL	Interrupt Controller
TCTL	Tamper Controller
DMA	Direct Memory Access
HMPU	Hardware Memory Protection Unit
DMA	Direct Memory Access Engine
SWP	Single Wire protocol
RNG	Random Number Generator
NVM-OTP	One Time Programmable Memory

Acronym	Meaning
AES	Advanced Encryption Standard (Accelerator)
HMAC	Hash-based Message Authentication Code (Accelerator)
CRC	Cyclic Redundancy Check (Accelerator)
3DES	Triple Data Encryption Standard (Accelerator)
RSA	Rivest, Shamir und Adleman
ECC	Elliptic Curve Cryptography

Table 2. Block diagram legend

1.4 TOE Description

1.4.1 Physical scope of the TOE

The TOE consists of the IC hardware (SPS) with specific IC dedicated software (Secure Firmware and Secure Bootloader). The TOE configuration is summarized in the table below and described in detail in chapter 1.4.2:

Item Type	Item	Version	Date	Form of Delivery
Hardware	BCM_SPS02, Secure Processing System	-	-	Hard macro instantiated within packaged product
Firmware	BCM_SPS02 Secure Firmware	002.030	-	Flash
Bootloader	BCM_SPS02 Secure Bootloader	002.030	-	Flash
Document	Datasheet 20211	V1.0	March 22, 2015	Electronic media, Portable Data Format (PDF)
Document	BCM_SPS02 User's Guide	v2.14	-	Electronic media, html files
Document	BCM20211 – Update of FW and Secure OS	V1.5	01/08/2016	Electronic media, PDF file
Document	ARM Architecture v6M Reference Manual, ARMDDI0419C(ID092410)	Rev C	September 2010	Electronic media, Portable Data Format (PDF)
Document	BCM_SPS02 Errata	V1.0	04/26/2016	Electronic media, Portable Data Format (PDF)

Table 3. TOE Configurations

Note: The Embedded Security IC Software is not part of the TOE and is not covered by this Security Target.

1.4.2 Logical scope of the TOE

1.4.2.1 TOE hardware description

The BCM_SPS02 (SPS) consists of several subsystems which are described below.

1.4.2.1.1 Secure Processor

The SPS is controlled by a secure processor core. The processor core executes the low-level boot code, the cryptographic libraries and the Security IC Embedded Software. The secure processor has cached memory to enhance performance.

The processor includes a memory protection unit (MPU) that provides partitioning of resources between different software tasks.

1.4.2.1.2 DMA

The SPS includes an isolated DMA controller to accelerate data transfers. The DMA controller can act as a bus master that is partitioned in hardware for the encrypted bus matrix.

1.4.2.1.3 Bus Matrix

To provide enhanced protection of the TOE, all address and data busses accesses are encrypted.

1.4.2.1.4 Memory

The SPS includes 64 Kbytes of integrated data static RAM (dSRAM) and all data in SRAM is stored in an encrypted form. The dSRAM is used for dynamic data that is not maintained between power or reset cycles.

The SPS contains 48 Kbytes of internal Read Only Memory (ROM) which holds the initial boot firmware and test firmware (ICDT mode only). All data in the ROM is encrypted.

The SPS contains 2 Mbyte of internal FLASH memory. All data in the internal FLASH is encrypted.

The SPS includes a Hardware Memory Protection Unit (HMPU) to provide hardware partitioning between masters and privilege modes within memory segments.

1.4.2.1.5 RNG

The SPS supports a True Random Number (TRNG). The True Random Number generator which is part of the TOE fulfills the requirements from the functionality class PTG.2 of the AIS31.

1.4.2.1.6 LSP

The low speed peripheral (LSP) block contains timers, security sensors and clock generation controls. The SPS supports detection of tampering with a series of analog and digital sensors. These include detection of voltage range violation, glitch detection, temperature, and other parameters. The Low Speed Peripheral (LSP) contains a dedicated watchdog timer to prevent lockups. The LSP also provides general-purpose timers.

1.4.2.1.7 CRYPTO

The SPS hardware supports accelerators for AES, HMAC, CRC and Triple-DES (TDES) cryptographic operations. The secure boot firmware supports a cryptographic library (refer to section 1.4.2.2) which provides support for additional symmetric cryptographic operations such as SHA-384.

The SPS implements key generation and asymmetric cryptographic acceleration using a dedicated Public Key Accelerator (PKA) module. The secure boot firmware supports the cryptographic library (refer to section 1.4.2.2) which provides support for additional operations including Elliptic Curve (EC) cryptography and Rivest-Shamir-Adleman (RSA) using this module.

1.4.2.1.8 Isolation Bridge (Interfaces)

To ensure the confidentiality and integrity of the TOE and associated User Data, the only interface for TOE communication is through a dedicated Isolation Bridge. The Isolation Bridge contains a variety of physical transport interfaces that can be multiplexed to provide either SPI or I2C in simultaneously with SWP. There is also a discrete set of General Purpose I/O pins controlled by the SPS. The isolation bridge provides complete decoupling from the SPS.

1.4.2.2 BCM_SPS02 Secure Firmware

The TOE includes IC Dedicated Support Software in internal FLASH to support five primary functionalities:

1. Initializing the TOE and transfer control to the Embedded Software after the boot process is complete.
2. Providing read, write and erase capabilities for the internal FLASH.
3. Providing a set of drivers for hardware interfaces and internal hardware blocks related to DMA operation, HMPU configuration and Random Number Generation. The HAL drivers provide an abstracted interface for the embedded software.

4. Providing a set of drivers for hardware interfaces and internal hardware blocks related to Timer, GPIO, transport (SPI/I2C), Watch Dog and SWP/NFC usage. The HAL drivers provide an abstracted interface for the embedded software.
5. Providing control and access to the SPS cryptographic accelerator hardware blocks and some additional cryptographic functionality.
   The scope of certification includes RSA signature generation and verification, RSA key generation, ECDH Key Exchange, ECDSA signature generation and verification, EC Key pair generation, AES and DES in various operation modes, Secure Hash Computation and CRC computation.
   For ECC the certification covers the standard NIST [NIST] and Brainpool [brainpool] Elliptic Curves with key lengths of 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 Bits, due to national AIS32 regulations by the BSI. Numerous other curve types, being also secure in terms of side channel attacks on this TOE, exist, which the user optionally can add in the composition certification process.

1.4.2.3 BCM_SPS02 Secure Bootloader

The TOE includes IC Dedicated Support Software in internal FLASH to support update functionalities:

1. Protection of the TOE user data against misuse of the Loader,
2. Trusted channel between Security IC and the authorized role to change the user data by means of the Loader,
3. Checking the integrity and the authenticity of the data provided by the authorized user to the Loader,
4. Access control on Loader usage.

1.4.2.4 TOE Guidance description

The guidance documentation for the TOE is comprised of five main documents described below:

- BCM_SPS02 Datasheet – The data sheet contains high level description of the pin out and electrical data such as power consumption of the TOE.
- BCM_SPS02 Security Guidelines – This includes information on how to utilize the device in a secure manner and also discusses use cases and configurations to avoid that might reduce the device's security strength.
- BCM20211 – Update of FW and Secure OS - This manual introduces the reader to secure usage of the TOE's Flash Loader.

- ARM Architecture v6M Reference Manual – This includes the ARM core related information such as ARM instruction set and programming model.

The exact versions of the guidance documents are listed in Table 3.

1.4.2.5 TOE Interface description

- The physical interface of the TOE to the external environment is the entire surface of the IC.
- The electrical and the data-oriented interface of the TOE to the external environment is constituted by the Isolation Bridge (discussed in section 1.4.2.1.8). This is the primary method of communicating with the TOE. The TOE will accept and respond to ISO-7816 APDU commands from the Isolation Bridge. The Isolation Bridge also includes 32 general purpose IO (GPIO) signals.
- The interface of the TOE to the IC Embedded Software is constituted by the Hardware Abstraction Layer (HAL) and by special registers used for hardware configuration and control.
- The interface of the TOE to the test routines is formed by the Secure Boot Firmware executed automatically after power on reset.
- The interfaces to the RSA, ECC and SHA services are defined by the cryptographic library interface.
- Execution of the Secure Flash Loader can be initiated by either setting well-defined GPIO pins during reset, or via writing a dedicated value (token) at a well-defined address in Flash.

1.4.2.6 TOE Life Cycle

The design and manufacturing life cycle for the TOE is shown in Figure 3 (as derived from section 1.2.3 of [PP]). The TOE can be delivered either at the end of phase 3 or at the end of phase 4. In other words, the device containing the BCM_SPS02 can be delivered either as wafers (die) or sawn wafers (dice), or packaged device. Therefore all requirements, assumptions and constraints listed in this Security Target are applicable as specified by [PP] and this Security Target. In any case the extended test features are removed.

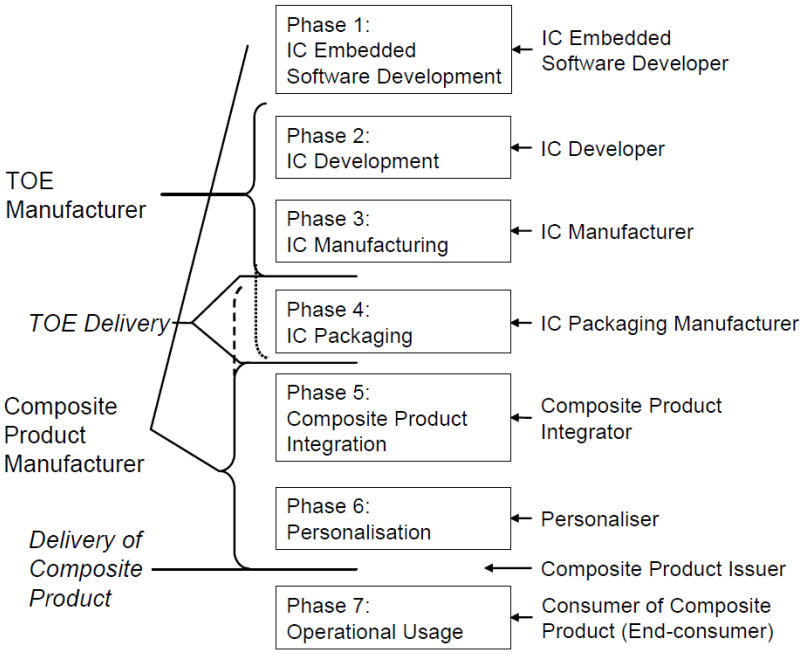


Figure 3. Security IC Life cycle

Loading of the Embedded Software Developer can either be done by the IC Developer or by the IC Embedded Software Developer. In case it is done by the IC developer, it is securely transferred to and handled by the IC developer. Pre-personalization data is also sent via a secure route to the IC Developer in a similar manner. Secure receipt and handling of these data by the IC Developer is included within the scope of this Security Target.

To enable the IC Embedded Software to be written, the IC Developer may ship Development tools (such as Field Programmable Gate Array (FPGA) development boards and emulators) and IC samples to developers. These released under Non-Disclosure Agreement(s) to ensure that their distribution is controlled and limited, protecting the confidentiality and integrity of the TOE in all phases of the life cycle but other than outside of this certification.

2 Conformance Claims

2.1 CC Conformance Claim

This ST claims to be conformant to the Common Criteria version 3.1

Furthermore it claims to be CC Part 2 extended and CC part 3 conformant. The extended Security Functional Requirements are defined in chapter 5.

This ST has been built with the Common Criteria for Information Technology Security Evaluation; Version 3.1

which comprises

[CC_1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 4 (Final) Sept 2012

[CC_2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 4 (Final), Sept 2012

[CC_3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 3.1, Revision 4 (Final), Sept 2012

The

[CEM] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 4 (Final), Sept 2012

has been taken into account.

2.2 Protection Profile Conformance Claim and Package Claim

This Security Target claims **strict conformance** to [PP]. [PP] is registered and certified by the Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0084, Version 1.0, dated 2014-01-13.

This Security Target claims EAL5 augmented with AVA_VAN.5 and ALC_DVS.2 (refer to Section 6.3 for more detail).

This Security Target further claims strict conformance to the following packages of [PP].

- Package “TDES”; [PP, 7.4.1],
- Package “AES”; [PP, 7.4.2],
- Package “Hash Functions”; [PP, 7.4.3], and
- Package “Loader dedicated for usage by authorized users only”; [PP, 7.3.2].

2.3 Conformance Rationale

2.3.1 CC Conformance Rationale

This ST implements all the requirements of [CC_1], [CC_2], and [CC_3] by inclusion (as shown in the relevant sections). Therefore no further rationale is required.

2.3.2 PP Conformance Rationale

This ST, for the TOE type described in Section 1.2, implements all the requirements specified in [PP] (as shown in the relevant sections). Although several additional requirements are included within this Security Target, strict conformance is still given as by [CC_1, D.2]. Adding additional requirements yields adding additional policies and assumptions. Again, strict conformance to [PP] is still given as by [PP, 3.3 / 3.4], especially the Application notes given in these chapters.

2.3.3 Package Claims Rationale

This ST implements all requirements of EAL5 augmented with AVA_VAN.5 and ALC_DVS.2.

[PP] requires the assurance level of EAL4 augmented with AVA_VAN.5 and ALC_DVS.2. Regarding the Application Note 22 of [PP] the changes needed to meet EAL5 (augmented) are described in the relevant sections of this Security Target.

3 Security Problem Definition

3.1 Description of Assets

The high level security concerns as described in [PP] are listed below:

SC1 Integrity of user data of the Composite TOE

SC2 Confidentiality of user data of the Composite TOE being stored in the TOE's protected memory areas

SC3 Correct operation of the security services provided by the TOE for the Security IC Embedded Software

SC4 Deficiency of random numbers

The assets (related to standard functionality) to be protected are listed below.

- The user data of the Composite TOE.
- The Security IC Embedded Software, stored and in operation.
- The security services provided by the TOE for the Security IC Embedded Software.
- Logical design data, physical design data, IC Dedicated Software, and configuration data.
- Initialization Data and Pre-personalization Data, specific development aids, test and characterization related data, material for software development support, and photomasks.
- Specific development aids.
- Test and characterization related data.
- Material for software development support.
- Photomasks and products in any form.

3.2 Threats

3.2.1 Standard Threats

The following threats are specified in [PP] and apply for the TOE. Note that several threats are only a means to attack the TOE and its assets and are not a success for the attacker in themselves.

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

Table 4. Standard threats from [PP]

Further details about the threats can be found in [PP. 3.2].

3.2.2 Additional threats

The following table summarized the additional threats that will be described in more detail in the subsequent sections.

Abbreviation	Threat
T.Mem-Access	Memory Access Violation

Table 5. Additional threats

3.2.2.1 T.Mem-Access

The TOE shall avert the threat “Memory Access Violation” as specified below.

T. Mem-Access	Memory Access Violation Parts of the Security IC Embedded Software may cause security violations by accidentally or deliberately accessing restricted data (which may include code). Any restrictions are defined by the security policy of the specific application context and must be implemented by the Security IC Embedded Software.

3.3 Organizational Security Policies

3.3.1 Standard Organizational Security Polices

The following Organizational Security Polices are mandated by [PP] and apply for the TOE.

Abbreviation	Policy
P.Process-TOE	Identification during TOE Development and Production

Table 6. Standard policy from [PP]

Further details about the Organizational Security Polices can be found in [PP. 3.3].

3.3.2 Additional Organizational Security Polices

Due to augmentations in the [PP], additional policies are defined in this chapter.

Abbreviation	Threat
P.Crypto-Service	Cryptographic services of the TOE
P.Ctlr_Loader	Controlled usage to Loader Functionality

Table 7. Additional Organizational Security Polices

3.3.2.1 P.Crypto-Service-Functions

The TOE shall apply the policy "Additional Specific Security Functionality" as specified below.

P.Crypto-Service Cryptographic services of the TOE

The TOE provides secure hardware based cryptographic services for the IC Embedded Software.

Note: The following cryptographic services are provided by the TOE:

- Triple Data Encryption Standard (TDES)
- Advanced Encryption Standard (AES)
- Rivest-Shamir-Adleman (RSA)
- Elliptic Curve Cryptography (EC)
- Secure Hash Algorithm (SHA)
- Hash-based Message Authentication Code (HMAC)

In addition, the TOE provides a CRC module that is hardened such that confidential data can be processed. However, as CRC computations are not regarded cryptographic services, the CRC computation is not further modeled as such.

3.3.2.2 P.Ctlr_Loader-Service-Functions

The TOE shall apply the policy “Additional Specific Security Functionality” as specified below.

P.Ctlr_Loader	Controlled usage to Loader Functionality Authorized user controls the usage of the Loader functionality in order to protect stored and loaded user data from disclosure and manipulation.

3.4 Assumptions

3.4.1 PP Assumptions

Abbreviation	Assumption
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation
A.Resp-Appl	Treatment of user data of the Composite TOE

Table 8. Assumptions from [PP]

Further details about the Assumptions can be found in [PP. 3.4].

4 Security Objectives

4.1 Security Objectives for the TOE

This section provides a brief overview about the security goals related to the assets as per [PP]:

SG1 Maintain the integrity of User Data and of the Security IC Embedded Software.

SG2 Maintain the confidentiality of User Data and of the Security IC Embedded Software.

SG3 Maintain the correct operation of the security services provided by the TOE for the Security IC Embedded Software.

SG4 Provision of random numbers.

In addition to the security goals as per [PP] the TOE has the following security goal:

SG5 AES, Triple-DES, RSA, ECDSA, ECDH, SHA and HMAC security services provided by the TOE for the Security IC Embedded Software.

SG6 Flash Loader services provided by the TOE for the Security IC Embedded Software that maintains integrity and confidentiality of loaded data.

4.1.1 Standard Security Objectives for the TOE

The security objectives of the TOE defined and described in [PP, 4.1] apply for the TOE. They are summarized in the following table, for details refer to [PP, 4.1].

Abbreviation	Assumption
O.Phys-Manipulation	Protection against Physical Manipulation
O.Phys-Probing	Protection against Physical Probing
O.Malfunction	Protection against Malfunction
O.Leak-Inherent	Protection against Inherent Information Leakage
O.Leak-Forced	Protection against Forced Information Leakage
O.Abuse-Func	Protection against Abuse of Functionality

Abbreviation	Assumption
O.Identification	TOE Identification
O.RND	Random Numbers

Table 9. Standard Security Objectives as per [PP]

4.1.2 Augmented Security Objectives for the TOE – package TDES, AES, Hash of [PP]

This TOE further claims conformance to the following packages of [PP].

- Package “TDES”; [PP, 7.4.1],
- Package “AES”; [PP, 7.4.2],
- Package “Hash Functions”; [PP, 7.4.3],
- Package “Loader dedicated for usage by authorized users only”; [PP, 7.3.2].

Therefore, the following augmented Security Objectives are applicable for the TOE as defined and described in [PP, 7.4]:

Abbreviation	Assumption
O.TDES	Cryptographic service Triple-DES
O.AES	Cryptographic service AES
O.SHA	Cryptographic service Hash function
O.Ctrl_Auth_Loader	Access control and authenticity for the Loader

Table 10. Augmented Security Objectives – packages TDES, AES, Hash and Loader 2 of [PP]

4.1.3 Further Augmented Security Objectives for the TOE

The TOE shall offer additional facilities to protect embedded software from corrupted, erroneous, or malicious software. These same facilities may protect from some results of attempts at physical manipulation. The corresponding Security Objective O.Mem-Access is described below.

In addition, the TOE shall provide O.RSA, O.ECC and O.HMAC as specified below.

Abbreviation	Assumption
O.Mem-Access	Area based Memory Access Control
O.RSA	Cryptographic service RSA

Abbreviation	Assumption
O.ECC	Cryptographic service ECC
O.HMAC	Cryptographic service HMAC

Table 11. Augmented Security Objectives

4.1.3.1 O.Mem-Access

The TOE shall provide “Area based Memory Access Control” as specified below.

O.Mem-Access Area based Memory Access Control

The TOE shall provide the Security IC Embedded Software with the capability to define restricted access memory areas. The TOE must then enforce the partitioning of such memory areas so that access of software to memory areas is controlled as required, for example, in a multi-application environment.

4.1.3.2 O.RSA

The TOE shall provide “Cryptographic service RSA (O.RSA)” as specified below.

O.RSA Cryptographic service RSA

The TOE provides secure hardware based cryptographic services for the RSA for encryption, decryption, signature generation, signature verification and RSA key generation.

4.1.3.3 O.ECC

The TOE shall provide “Cryptographic service ECC (O.ECC)” as specified below.

O.ECC Cryptographic service ECC

The TOE provides secure hardware based cryptographic services for the ECC for signature generation, signature verification, key exchange and key generation.

4.1.3.4 O.HMAC

The TOE shall provide “Cryptographic service HMAC (O.HMAC)” as specified below.

O.HMAC	Cryptographic service HMAC The TOE provides secure hardware based cryptographic services for the HMAC generation and verification.

4.2 Security Objectives for the Security IC Embedded Software

According to [PP], the development of the Security IC Embedded Software is outside the development and manufacturing of the TOE. This section therefore summarizes the security objective for the Security IC Embedded Software as defined and described in [PP, 4.2].

Abbreviation	Assumption
OE.Resp-Appl	Treatment of user data of the Composite TOE

Table 12. Security Objectives for the Security IC Embedded Software

4.3 Security Objectives for the Operational Environment

According to [PP], the development of the Security IC Embedded Software is outside the development and manufacturing of the TOE. This section therefore summarizes the security objective for the Security IC Embedded Software as defined and described in [PP, 4.2]. In addition, the security objective for the authorized user of the Flash Loader is defined here as per [PP, §364].

Abbreviation	Assumption
OE.Process-Sec-IC	Protection during composite product manufacturing
OE.Loader_Usage	Secure communication and usage of the Loader

Table 13. Security Objectives for the operational environment

4.4 Security Objectives Rationale

Table 14 below gives an overview, how the assumptions, threat, and organizational security policies are addressed by the objectives. The text following after the table justifies this in detail.

Assumption, Threat or Organizational Security Policy	Security Objective	Notes
A.Resp-Appl	OE.Resp-Appl	
P.Process-TOE	O.Identification	Phase 2 – 3 optional Phase 4
A.Process-Sec-IC	OE.Process-Sec-IC	Phase 5 – 6 optional Phase 4

Assumption, Threat or Organizational Security Policy	Security Objective	Notes
T.Leak-Inherent	O.Leak-Inherent	
T.Phys-Probing	O.Phys-Probing	
T.Malfunction	O.Malfunction	
T.Phys-Manipulation	O.Phys-Manipulation	
T.Leak-Forced	O.Leak-Forced	
T.Abuse-Func	O.Abuse-Func	
T.RND	O.RND	
T.Mem-Access	O.Mem-Access	
P.Crypto-Service	O.TDES O.AES O.SHA O.RSA O.ECC O.HMAC	
P.Ctlr_Loader	O.Ctrl_Auth_Loader OE.Loader_Usage	

Table 14. Security Objectives versus Assumptions, Threats or Policies

The rationale for A.Resp-Appl, P.Process-TOE, A.Process-Sec-IC, T.Leak-Inherent, T.Phys-Probing, T.Malfunction, T.Phys-Manipulation, T.Leak-Forced, T.Abuse-Func and T.RND is already given in [PP, 4.4] and applies for the TOE unchanged.

The justification related to the threat “Memory Access Violation (T.Mem-Access)” is as follows:

According to O.Mem-Access the TOE must enforce the partitioning of memory areas so that access of software to memory areas is controlled. Any restrictions are to be defined by the Security IC Embedded Software. Therefore, security violations caused by accidental or deliberate access to restricted data (which may include code) can be prevented (refer to T.Mem-Access). The threat T.Mem-Access is therefore removed and the objective is met.

The rationale related to the organizational security policy P.Crypto-Service is as follows:

Since P.Crypto-Service requires that the TOE provides secure hardware based cryptographic services for the IC Embedded Software the Security Objectives O.TDES, O.AES, O.SHA, O.RSA, O.ECC, O.HMAC. For O.TDES the rationale is given in [PP, §378], for O.AES in [PP, §386] and for O.Hash the rationale is given

in [PP, §394]. Similar to aforementioned rationales, O.RSA, O.ECC and O.HMAC directly enforce the organizational security policy P.Crypto-Service.

The rationale related to the organizational security policy P.Ctrl_Loader-Service is as follows:

The organizational security policy “Controlled usage to Loader Functionality (P.Ctlr_Loader) is directly implemented by the security objective for the TOE “Access control and authenticity for the Loader (O.Ctrl_Auth_Loader)” and the security objective for the TOE environment “Secure communication and usage of the Loader (OE.Loader_Usage)” as per [PP, §364].

5 Extended Components Definition

There are four extended components defined and described for the TOE in [PP, 5]:

- the family **FCS_RNG** at the class FCS Cryptographic Support
- the family **FMT_LIM** at the class FMT Security Management
- the family **FAU_SAS** at the class FAU Security Audit
- the family **FDP_SDC.1** of the Class FDP User data protection

This Security Target additional defines a new component to extend the Common Criteria Part 2, namely

- the family FPT_TST.2 of the Class FPT Protection of the TSF

The following sections provide further information on the SFRs extended in this Security Target.

5.1 Definition of Security Functional Requirement FPT_TST.2

The family FPT_TST (TSF self-test) of the Class FPT (Protection of the TSF) defines the requirements for the self-testing of the TSF with respect to some expected correct operation. This family is defined in Common Criteria for Information Technology Security Evaluation Part 2.

The security is strongly dependent on the correct operation of the security functions. Therefore, the TOE shall support that particular security functions or mechanisms are tested in the operational phase (Phase 7). The test can be initiated by the Security IC Embedded Software and/or by the TOE.

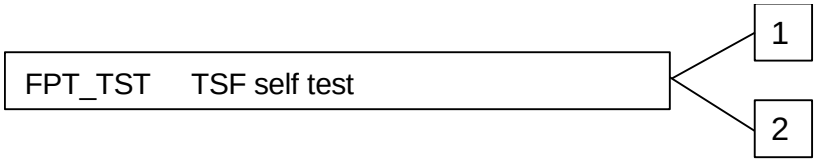
Part 2 of the Common Criteria provides the security functional component “TSF testing (FPT_TST.1)”. The component FPT_TST.1 provides the ability to test the TSF’s correct operation.

For the user it is important to know which security functions or mechanisms can be tested. The functional component FPT_TST.1 does not mandate to explicitly specify the security functions being tested. In addition, FPT_TST.1 requires to verify the integrity of the TSF data and stored TSF executable code which might violate the security policy. Therefore the security functional component **“Subset TOE security testing (FPT_TST.2)”** has been created. This component allows that particular paths of the security mechanisms and functions provided by the TOE are tested.

The functional component “Subset TOE testing (FPT_TST.2)” is specified as follows (Common Criteria Part 2 extended).

Family Behavior The Family Behavior is defined in Common Criteria Part 2.

Component levelling



FPT_TST.1: The component FPT_TST.1 is defined in Common Criteria Part 2

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

Management: FPT_TST.2

There are no management activities foreseen.

Audit: FPT_TST.2

There are no auditable events foreseen.

FPT_TST.2 Subset TOE testing

Hierarchical to: No other components

FPT_TST.2.1 The TSF shall run a suite of tests [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, and/or at the

	conditions [assignment: conditions under which self test should occur]] to demonstrate the correct operation of [assignment: functions and/or mechanisms]
Dependencies	No dependencies

6 Security Requirements

For this section [PP, 6] applies completely.

6.1 Security Functional Requirements for the TOE

The security functional requirements (SFR) for the TOE are defined and described in [PP, 6] and in the following description. Following table provides an overview of the functional security requirements of the TOE, defined in the in [PP, 6.1]. In the last column it is marked if the requirement is refined. The refinements are then also valid for this ST.

Security Functional Requirement	Defined via package	Refined in [PP]
FRU_FLT.2 "Limited fault tolerance"	No	Yes
FPT_FLS.1 "Failure with preservation of secure state"	No	Yes
FMT_LIM.1 "Limited capabilities"	No	No
FMT_LIM.2 "Limited availability"	No	No
FAU_SAS.1 "Audit storage"	No	No
FDP_SDC.1 "Stored data confidentiality"	No	Yes
FDP_SDI.2 "Stored data integrity monitoring and action"	No	Yes
FPT_PHP.3 "Resistance to physical attack"	No	Yes
FDP_ITT.1 "Basic internal transfer protection"	No	Yes
FPT_ITT.1 "Basic internal TSF data transfer protection	No	Yes
FDP_IFC.1 "Subset information flow control"	No	No
FCS_RNG.1 "Random number generation"	No	Yes
FCS_COP.1/TDES "Cryptographic Operation - TDES"	Yes, package "TDES"	Yes
FCS_COP.1/AES "Cryptographic Operation - AES"	Yes, package "AES"	Yes
FCS_COP.1/SHA "Cryptographic Operation - SHA"	Yes, package "Hash functions"	Yes
FCS_CKM.4/TDES "Cryptographic key destruction – TDES"	Yes, package "TDES"	No
FCS_CKM.4/AES "Cryptographic key destruction – AES"	Yes, package "AES"	No
FTP_ITC.1 "Inter-TSF trusted channel"	Yes, package "Loader dedicated for usage by authorized users only"	Yes

Security Functional Requirement	Defined via package	Refined in [PP]
FTP_ITC.1 "Inter-TSF trusted channel"	Yes, package "Loader dedicated for usage by authorized users only"	Yes
FDP_UCT.1 "Basic data exchange confidentiality"	Yes, package "Loader dedicated for usage by authorized users only"	Yes
FDP_UIT.1 "Data exchange integrity"	Yes, package "Loader dedicated for usage by authorized users only"	Yes
FDP_ACC.1/Loader "Subset access control - Loader"	Yes, package "Loader dedicated for usage by authorized users only"	Yes
FDP_ACF.1/Loader "Security attribute based access control - Loader"	Yes, package "Loader dedicated for usage by authorized users only"	Yes

Table 15. Security functional requirements defined in [PP]

Following table provides an overview about the augmented security functional requirements, which are added additional to the TOE and defined in this ST. All requirements are taken from [CC_2], with the exception of the requirement FPT_TST.2 which is defined in this ST completely. FCS_COP.1 has six iterations for cryptographic services and FCS_CKM.1 has three iterations for cryptographic iterations.

Security Functional Requirement
FPT_TST.2 "Subset TOE testing"
FCS_COP.1/RSA "Cryptographic Operation - RSA"
FCS_COP.1/ECDH "Cryptographic Operation - ECDH"
FCS_COP.1/ECDSA "Cryptographic Operation - ECDSA"

Security Functional Requirement
FCS_COP.1/HMAC "Cryptographic Operation - HMAC"
FCS_CKM.1/RSA "Cryptographic key generation - RSA"
FCS_CKM.1/ECC "Cryptographic key generation - ECC"
FDP_ACC.1 "Subset access control"
FDP_ACF.1 "Security attribute based access control"
FMT_MSA.1 "Management of security attributes"
FMT_MSA.3 "Static attribute initialization"
FMT_SMF.1 "Specification of Management functions"
FCS_COP.1/ AES_decrypt_Loader "Cryptographic Operation AES CBC decryption and CMAC verification"
FCS_COP.1/ECDSA_verify_Loader "Cryptographic Operation ECDSA signature verification"
FCS_CKM.4/AES_keyDest_Loader "Cryptographic key destruction – AES decryption key"

Table 16. Security functional requirements defined in [ST]

All assignments and selections of the security functional requirements of the TOE are done in [PP] and in the following description.

FRU_FLT.2, FPT_FLS.1, FMT_LIM.1, FMT_LIM.2, FDP_ITT.1, FPT_ITT.1, FDP_IFC.1 and FPT_PHP.3 are completely defined in [PP] and are not repeated here.

Regarding FPT_FLS.1 and Application Note 14 of [PP] the secure state of the TOE is defined as a full reset. Furthermore, in context of Application Note 15 of [PP] the Common Criteria suggests that the TOE generates audit data for such events. As the Secure State is defined as a full reset, no audit data is provided such as a file that is written to the NVM. However, the TOE is equipped with sticky registers which content is not reset every power cycle and hence can persist reset events over a short period of time.

Regarding FPT_PHP.3 and Application Note 19 the automatic response of the TOE is defined as a full reset. Therefore, the security functional requirements are enforced as the TOE stops operation or does not operate at all if a physical manipulation or physical probing attack is detected.

6.1.1 Security Functional Requirements from [PP]

In this section the following Security Functional Requirements defined in [PP] are completed: FAU_SAS.1, FDP_SDC.1, FDP_SDI.2, FCS_RNG.1, FCS_COP.1/TDES, FCS_COP.1/AES, FCS_COP.1/SHA,

FCS_CKM.4/TDES, FCS_CKM.4/AES, FTP_ITC.1, FTP_ITC.1, FDP_UCT.1, FDP_UIT.1, FDP_ACC.1/Loader, FDP_ACF.1/Loader.

The operations made in [PP] fully apply for the TOE, and are not highlighted explicitly. Only the operations made within this Security Target are highlighted in *italics*.

6.1.1.1 FAU_SAS.1

The TOE shall meet the requirement "Audit storage" as defined in [PP, §163] and as specified below.

FAU_SAS.1	Audit storage
Hierarchical to	No other components
FAU_SAS.1.1	The TSF shall provide *the test process before TOE Delivery* with the capability to store *the Initialization Data, Pre-Personalization Data* in *FLASH*[1].
Dependencies	No dependencies.
Refinement	None

6.1.1.2 FDP_SDC.1

The TOE shall meet the requirement "Stored data confidentiality" as defined in [PP, §168] and as specified below.

FDP_SDC.1	Stored data confidentiality
Hierarchical to	No other components
FDP_SDC.1.1	The TSF shall ensure the confidentiality of the information of the user data while it is stored in the *Flash memory*[2].

[1] [selection: the Initialisation Data, Pre-personalisation Data, [assignment: other data]]
[2] [assignment: memory area].

Dependencies	No dependencies.
Refinement	None

6.1.1.3 FDP_SDI.2

The TOE shall meet the requirement "Stored data integrity monitoring and action" as defined in [PP, §169] and as specified below.

FDP_SDI.2	Stored data integrity monitoring and action
Hierarchical to	FDP_SDI.1 Stored data integrity monitoring
FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for *single- and multi-bit errors*[3] on all objects, based on the following attributes: *Error Detection Code*[4].
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall - *correct single-bit errors automatically when reading from Flash* - *trigger tamper alert in case of multi-bit errors when reading from Flash* - *trigger tamper alert in case of multi-bit errors when reading from ROM or RAM.*[5]
Dependencies	No dependencies.
Refinement	None

[3] [assignment: integrity errors]
[4] [assignment: user data attributes]
[5] [assignment: action to be taken]

6.1.1.4 FCS_RNG.1

The TOE shall meet the requirement "Random number generation" as defined in [PP, §178] and as specified below. As the TOE is certified in the German scheme, the operations as performed in [PP, §400] apply.

FCS_RNG.1/PTG.2	Random number generation – PTG.2
Hierarchical to	No other components.
FCS_RNG.1.1/PTG.2	The TSF shall provide a physical random number generator that implements: (PTG.2.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output. (PTG.2.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG *prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source*[6]. (PTG.2.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected. (PTG.2.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.

[6] [selection: prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source, generates the internal random numbers with a post-processing algorithm of class DRG.2 as long as its internal state entropy guarantees the claimed output entropy]

	(PTG.2.5) The online test procedure checks the quality of the raw random number sequence. It is triggered *at regular intervals*[7]. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.
FCS_RNG.1.2/PTG.2	The TSF shall provide *numbers in 32-bit binary format*[8] that meet (PTG.2.6) Test procedure A[9] does not distinguish the internal random numbers from output sequences of an ideal RNG. (PTG.2.7) The average Shannon entropy per internal random bit exceeds 0.997.
Dependencies	No dependencies.
Refinement	None

Application Note: The evaluation of the random number generator shall follow [AIS31] and [KS2011].

6.1.1.5 FCS_COP.1/TDES

The TOE shall meet the requirement "Cryptographic operation – TDES" as defined in [PP, §379] and as specified below.

FCS_COP.1/TDES	Cryptographic operation – TDES
Hierarchical to	No other components.
FCS_COP.1.1	The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm TDES in *ECB mode, CBC mode, CBC-MAC Mode, Retail MAC Mode and Full Triple DES MAC Mode with ISO 9797-1_M1, ISO 9797-1_M2*

[7] [selection: externally, at regular intervals, continuously, applied upon specified internal events]
[8] [selection: bits, octets of bits, numbers [assignment: format of the numbers]]
[9] [assignment: additional standard test suites]. Assignment is empty as per Application Note 44.

	or no padding scheme[10] and cryptographic key sizes *112 bit and 168 bit*[11] that meet the following [SP800-67], [SP800-38A], [GP].
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
Refinement	FCS_COP.1/TDES has been refined within this Security Target. [PP] provides a template for TDES in ECB and CBC mode. The TOE further supports CBC-MAC Mode, Retail MAC Mode and Full Triple DES MAC Mode with ISO 9797-1_M1, ISO 9797-1_M2 or no padding scheme and has thus been refined. Further, the list of standards supported is refined by adding [ISO 9796-1], [ISO 9796-2] and [GP].

Application Note: Note FIPS 46-3 was withdrawn in 2005. The Triple Data Encryption Algorithm with 112 bit and 168 bit keys is still an NIST approved cryptographic algorithm as defined in [SP800-67]. Single-DES functionality is implicitly supported by the TOE as TDES is backward compatible by design. However, the scope of evaluation is restricted to two and three key TDES only.

To provide more information to the reader, the following list provides more detailed references regarding the specification of supported modes of operations:

- *ECB: NIST Special Publication 800-38A Section 6.1*
- *CBC: NIST Special Publication 800-38A Section 6.2*
- *CBC-MAC: ISO 9797-1 – MAC algorithm 1, Section 7.2*
- *Retail MAC: ISO 9797-1 MAC algorithm 3, Section 7.4*
- *Full Triple DES MAC: Global Platform Card Specification 2.2.1, page 174*

[10] [selection: ECB mode, CBC mode]
[11] [selection: 112 bit, 168 bit]

The following list provides more detailed references regarding the specification of supported padding schemes:

- *ISO 9797-1_M1: ISO 9797-1 – Padding Method 1, Section 6.3.2*
- *ISO 9797-1_M2: ISO 9797-1 –Padding Method 2, Section 6.3.3*

6.1.1.6 FCS_CKM.4/TDES

The TOE shall meet the requirement "Cryptographic key destruction" as defined in [PP, §380] and as specified below.

FCS_CKM.4/TDES	Cryptographic key destruction
Hierarchical to	No other components.
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method key zeroization [12] that meets the following: *None*[13].
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]
Refinement	None.

Application Note: According to Application Note 41 of [PP] the key zeroization initiated by special signal is considered a valid key destruction method. For the TOE, key zeroization is performed when resetting the DES engine.

6.1.1.7 FCS_COP.1/AES

The TOE shall meet the requirement "Cryptographic operation – AES" as defined in [PP, §385] and as specified below.

[12] [assignment: cryptographic key destruction method]
[13] [assignment: list of standards]

FCS_COP.1/AES	Cryptographic operation – AES
Hierarchical to	No other components.
FCS_COP.1.1	The TSF shall perform decryption and encryption in accordance with a specified cryptographic algorithm AES in *ECB mode, CBC mode, Counter (CTR) mode, OFB mode, AES MAC mode and CMAC mode with ISO 9797-1_M1, ISO 9797-1_M2 or no padding scheme*[14] and cryptographic key sizes *128 bit, 192 bit and 256 bit*[15] that meet the following: [PUB197], [SP800-38A], [SP800-38B], [ISO 9796-1], [ISO 9796-2].
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
Refinement	FCS_COP.1/AES has been refined within this Security Target. [PP] provides a template for AES in ECB and CBC mode. The TOE further supports OFB mode, Counter mode, AES MAC mode and CMAC mode with ISO 9797-1_M1, ISO 9797-1_M2 or no padding scheme and has thus been refined by adding [SP800-38B], [ISO 9796-1], [ISO 9796-2].

To provide more information to the reader, the following list provides more detailed references regarding the specification of supported modes of operations:

- *ECB: NIST Special Publication 800-38A Section 6.1*
- *CBC: NIST Special Publication 800-38A Section 6.2*
- *CTR: NIST Special Publication 800-38A Section 6.5*
- *AES MAC: ISO 9797-1 – MAC algorithm 1, Section 7.2*

[14] [selection: ECB mode, CBC mode]
[15] [selection: 128 bit, 192 bit, 256 bit]

- *CMAC: NIST Special Publication 800-38B*
- *OFB: NIST Special Publication 800-38A Section 6.4*

The following list provides more detailed references regarding the specification of supported padding schemes:

- *ISO 9797-1_M1: ISO 9797-1 – Padding Method 1, Section 6.3.2*
- *ISO 9797-1_M2: ISO 9797-1 –Padding Method 2, Section 6.3.3*

6.1.1.8 FCS_CKM.4/AES

The TOE shall meet the requirement "Cryptographic key destruction" as defined in [PP, §388] and as specified below.

FCS_CKM.4/AES	Cryptographic key destruction
Hierarchical to	No other components.
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method key zeroization[16] that meets the following: *None*[17].
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]
Refinement	None.

Application Note: According to Application Note 42 of [PP] the key zeroization initiated by special signal is considered a valid key destruction method. For the TOE, key zeroization is performed when resetting the AES engine and overwriting the key caches.

[16] [assignment: cryptographic key destruction method]
[17] [assignment: list of standards]

6.1.1.9 FCS_COP.1/SHA

The TOE shall meet the requirement "Cryptographic operation – SHA" as defined in [PP, §395] and as specified below.

FCS_COP.1/SHA	Cryptographic operation – SHA
Hierarchical to	No other components.
FCS_COP.1.1	The TSF shall perform hashing in accordance with a specified cryptographic algorithm *SHA-1, SHA-224, SHA-256, SHA-384, SHA-512*[18] and cryptographic key sizes none that meet the following [FIPS 180-4].
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
Refinement	None.

Application Note: The TOE also provides means for keyed hash operations, see FCS_COP.1/HMAC.

Note: The SHA-384 and SHA-512 implementations are not designed to withstand side-channel attacks such as DPA or similar. Therefore, side-channel analysis for these primitives is not in scope of the evaluation.

6.1.1.10 FTP_ITC.1

The TOE shall meet the requirement "Inter-TSF trusted channel" as defined in [PP, §365] and as specified below.

FTP_ITC.1	Inter-TSF trusted channel

[18] [selection: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512]

Hierarchical to	No other components.
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and *the IC vendor and the Security IC Embedded Software developer*[19] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for deploying Loader *when indicated by the user via* - *Applying well-defined signals on GPIO pads during start-up, or* - *Writing the update token to a dedicated address in embedded flash.*[20].
Dependencies	No dependencies.
Refinement	None.

6.1.1.11 FDP_UCT.1

The TOE shall meet the requirement “Basic data exchange confidentiality” as defined in [PP, §367] and as specified below.

FDP_UCT.1	Basic data exchange confidentiality
Hierarchical to	No other components.
FDP_UCT.1.1	The TSF shall enforce the Loader SFP to receive user data in a manner protected from unauthorised disclosure.

[19] [assignment: users authorized for using the Loader]
[20] [assignment: rules]

Dependencies	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
Refinement	None.

Above SFR is taken over from [PP, §367] without any change. We here list it for completeness as the following Security Function Policy (SFP) “Loader Security Functional Policy” remains to be defined by the author of the Security Target. Therefore, the Loader SFP is defined as follows:

The TOE supports secure download and update of the following

1) IC Dedicated Support Software,
2) Security IC Embedded Software, and
3) The Flash bootloader itself.

When updating either one of aforementioned images the TOE validates the integrity of the update image by means of ECDSA signatures. In detail, the following rules are applied:

1. When updating the IC Dedicated Support Software, the package
   a. must be ECDSA signed by the IC vendor, and
   b. must not come without an update of the Security IC Embedded Software (which is itself signed by the Security IC Embedded Software developer).
2. When updating the Security IC Embedded Software, the package
   a. must be ECDSA signed by the Security IC Embedded Software developer, and
   b. must not come without an update of the IC Dedicated Support Software (which is itself signed by the IC vendor).
3. When updating the Flash bootloader itself, the package
   a. must be ECDSA signed by the IC vendor, and
   b. must be ECDSA signed by the Security IC Embedded Software developer.
   c. In addition, each update of the Flash bootloader must be followed by an update of the IC Dedicated Support Software and an update of the Security IC Embedded Software.

The scheme therefore enforces that the IC vendor cannot update the Loader, the IC Dedicated Support Software or the Security IC Embedded Software without a valid countersignature of the Security IC Embedded Software developer.

Furthermore, the TOE assumes that any data received is encrypted in AES-CMC mode. Therefore the TOE auto-decrypts the data and by that provides means to maintain the confidentiality of all, the IC Dedicated Support Software, the Security IC Embedded Software and the Flash bootloader itself. A complex key management system is supported by the TOE that enforces that

1. the IC Dedicated Support Software and the Flash bootloader itself are encrypted using keys only known to the IC vendor, and
2. the Security IC Embedded Software is encrypted using keys only known to the Security IC Embedded Software developer.

The subjects related to the Loader Security Functionality Policy are:

- IC vendor and
- Security IC Embedded Software developer.

The objects related to the Loader Security Functional Policy are:

- User data in Flash memory.

The operations on the objects are:

- Read data from the memory,
- Write data into the memory and
- Execute data in the memory.

There are no security attributes related to the Loader SFP.

6.1.1.12 FDP_UIT.1

The TOE shall meet the requirement “Data exchange integrity” as defined in [PP, §368] and as specified below.

FDP_UIT.1	Data exchange integrity

Hierarchical to	No other components.
FDP_UIT.1.1	The TSF shall enforce the Loader SFP to receive user data in a manner protected from modification, deletion, insertion errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion has occurred.
Dependencies	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
Refinement	None.

Above SFR is taken over from [PP, §368] without any change. We here list it for completeness as the Security Function Policy (SFP) "Loader Security Functional Policy" remains to be defined by the author of the Security Target. Therefore, the Loader SFP was defined in section 6.1.1.11.

6.1.1.13 FDP_ACC.1/Loader

The TOE shall meet the requirement "Subset access control - Loader" as defined in [PP, §369] and as specified below.

FDP_ACC.1/Loader	Subset access control - Loader
Hierarchical to	No other components.
FDP_ACC.1.1/Loader	The TSF shall enforce the Loader SFP on (1) the subjects *IC vendor and Security IC Embedded Software developer*[21], (2) the objects user data in *Flash memory*[22], (3) the operation deployment of Loader.

[21] [assignment: authorized roles for using Loader]
[22] [assignment: memory areas]

Dependencies	FDP_ACF.1 Security attribute based access control.
Refinement	None.

6.1.1.14 FDP_ACF.1/Loader

The TOE shall meet the requirement "Security attribute based access control - Loader" as defined in [PP, §370] and as specified below.

FDP_ACF.1	Security attribute based access control - Loader
Hierarchical to	No other components.
FDP_ACF.1.1/Loader	The TSF shall enforce the Loader SFP to objects based on the following: (1) the subjects *IC vendor and Security IC Embedded Software developer*[23] with security attributes *None*[24]. (2) the objects user data in *Flash memory*[25] with security attributes *None.*[26].
FDP_ACF.1.2/Loader	FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: 1. *When updating the IC Dedicated Support Software, the package* a. *must be ECDSA signed by the IC vendor, and* b. *must not come without an update of the Security IC Embedded Software (which is itself signed by the Security IC Embedded Software developer).* 2. *When updating the Security IC Embedded Software, the package* a. *must be ECDSA signed by the Security IC Embedded Software developer, and*

[23] [assignment: authorized roles for using Loader]
[24] [assignment: SFP-relevant security attributes, or named groups of SFP-relevant security attributes]
[25] [assignment: memory areas]
[26] [assignment: SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

b. *must not come without an update of the IC Dedicated Support Software (which is itself signed by the IC vendor).*

3. *When updating the Flash bootloader itself, the package*
   a. *must be ECDSA signed by the IC vendor, and*
   b. *must be ECDSA signed by the Security IC Embedded Software developer*.[27]

FDP_ACF.1.3/Loader	FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *None*[28].
FDP_ACF.1.4/Loader	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *None*[29].
Dependencies	FMT_MSA.3 Static attribute initialization
Refinement	None.

6.1.2 Security Functional Requirements from [ST]

In this section the following Security Functional Requirements defined and are completed: FPT_TST.2, FCS_COP.1/RSA, FCS_COP.1/ECDH, FCS_COP.1/ECDSA, FCS_COP.1/HMAC, FCS_CKM.1/RSA, FCS_CKM.1/ECC, FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FCS_COP.1/AES_decrypt_Loader, FCS_COP.1/ECDSA_verify_Loader, and FCS_CKM.4/AES_keyDest_Loader.

All operations made within this Security Target are highlighted in *italics*.

6.1.2.1 FPT_TST.2

The TOE shall meet the requirement “Subset TOE testing (FPT_TST.2)” as defined in Section 5 of this Security Target and as specified below.

[27] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[28] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[29] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

FPT_TST.2	Subset TOE testing
Hierarchical to	No other components.
FPT_TST.2.1	The TSF shall run a suite of self tests *at the request of the authorized user* to demonstrate the correct operation of *the following mechanisms:* • *AES and TDES encryption engine in ECB mode (known answer test)* • *PKA (Asymmetric engine) (known answer test)*
Dependencies	No dependencies.
Refinement	None.

6.1.2.2 FDP_ACC.1

The TOE shall meet the requirement "Subset access control (FDP_ACC.1)" as defined in Common Criteria Part 2 and as specified below.

FDP_ACC.1	Subset access control
Hierarchical to	No other components.
FDP_ACC.1.1	The TSF shall enforce the *Memory Access Control Policy*[30] on *all subjects (software), all objects (data including code stored in memories) and all the operations defined in the Memory Access Control Policy*[31].
Dependencies	FDP_ACF.1 Security attribute based access control
Refinement	None.

[30] [assignment: access control SFP]
[31] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

The following Security Function Policy (SFP) “Memory Access Control Policy” is defined for this requirement:

The TOE shall control *read, write and execute accesses* of *software residing in memory areas (i.e. address ranges)* on *data including code stored in memory areas.*

The subjects regarding the Memory Access Control Policy are:

- The Security IC Embedded Software
- The IC support software (Secure Firmware and Secure Bootloader) stored in internal Flash.

The objects related to the Memory Access Control Policy are:

- Data including code stored in memories,
- Memories (internal Flash).

The operations related to the memories are:

- Read data from the memory
- Write data into the memory and
- Execute data in the memory.

Finally the security attributes related to the Memory Access Control Policy are:

- Attributes used to enforce the *SFP (permission control information)*

The first bus master is the secure processor core. Here, the memory model provides two distinct, independent levels separated from each other. These levels are referred to as the privileged level and the user level. In the user level up to eight regions can be defined with different access rights. The access rights are controlled by the MPU related to the following rules:

- the privilege level has access to the user level
- the user level have no access to the privilege level
- the user level have no access to other user levels in the case that no overlapping exist
- overlapping user levels, have access to other user levels with ascending region priority
- access permissions (read only, read and write, read only & execute never, read & write & execute never)

The DMA acts as a second bus master. The DMA controller is programmed by the secure processor core. MPU permissions and restrictions do not apply to the DMA controller.

The HMPU is used to restrict the access writes of the DMA controller. It uses two programmable windows to restrict DMA access to specific memory regions. DMA controller memory access is always limited to those sub windows and is further restricted by the following permission settings which can be set for each window individually:

- Read only
- Write only
- Read and Write

The DMA controller cannot access data outside the defined windows and the secure processor core cannot execute data from DMA windows while enabled.

6.1.2.3 FDP_ACF.1

The TOE shall meet the requirement "Security Attribute based access control (FDP_ACF.1)" as defined in Common Criteria Part 2 and as specified below

FDP_ACF.1	Security Attribute based access control
Hierarchical to	No other components.
FDP_ACF.1.1	The TSF shall enforce the *Memory Access Control Policy (refer to FDP_ACC.1)*[32] to objects based on *the memory area where the software is executed from and/or the memory area where the access is performed to and/or the operation to be performed*[33].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *evaluate the corresponding permission control information before, during or after the*

[32] [assignment: access control SFP]
[33] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

	access so that accesses to be denied cannot be utilized by the subject attempting to perform the operation[34]*.*
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none*[35]*.*
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none*[36]*.*
Dependencies	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
Refinement	None.

6.1.2.4 FMT_MSA.3

The TOE shall meet the requirement "Static attribute initialization (FMT_MSA.3)" as defined in Common Criteria Part 2 and as specified below.

FMT_MSA.3	Static attribute initialization
Hierarchical to	No other components.
FMT_MSA.3.1	The TSF shall enforce the *Memory Access Control Policy (refer to FDP_ACC.1)*[37] to provide *restrictive*[38] default values for security attributes that are used to enforce the SFP.

[34] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[35] [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]
[36] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
[37] [assignment: access control SFP, information flow control SFP]
[38] [selection, choose one of: restrictive, permissive, [assignment: other property]]

FMT_MSA.3.2	The TSF shall allow *any subject (provided that the Memory Access Control Policy is enforced and the necessary access is therefore allowed)*[39] to specify alternative initial values when an object or information is created.
Dependencies	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Refinement	None.

6.1.2.5 FMT_MSA.1

The TOE shall meet the requirement "Management of security attributes (FMT_MSA.1)" as defined in Common Criteria Part 2 and as specified below.

FMT_MSA.1	Management of security attributes
Hierarchical to	No other components.
FMT_MSA.1.1	The TSF shall enforce the *Memory Access Control Policy (refer to FDP_ACC.1)*[40] to restrict the ability to *change_default, modify or delete*[41] the security attributes *permission control information*[42] to *Privilege level*[43].
Dependencies	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

[39] [assignment: the authorized identified roles]
[40] [assignment: access control SFP(s), information flow control SFP(s)]
[41] [selection: change_default, query, modify, delete, [assignment: other operations]]
[42] [assignment: list of security attributes]
[43] [assignment: the authorized identified roles]

Refinement	None.

6.1.2.6 FMT_SMF.1

The TOE shall meet the requirement "Specification of management functions (FMT_SMF.1)" as defined in Common Criteria Part 2 and as specified below.

FMT_SMF.1	Specification of management functions
Hierarchical to	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: *access the configuration registers of the MPU and HMPU*[44].
Dependencies	No dependencies.
Refinement	None.

6.1.2.7 FCS_COP.1/RSA

The TOE shall meet the requirement "Cryptographic operation – RSA" defined in Common Criteria Part 2 and as specified below.

FCS_COP.1/RSA	Cryptographic operation – RSA
Hierarchical to	No other components.
FCS_COP.1.1	The TSF shall perform *encryption, decryption*, *signature generation and signature verification*[45] in accordance with a specified cryptographic algorithm *"Rivest-Shamir-Adleman" (RSA)*[46] and cryptographic key sizes *512 – 2048 in steps of 32*

[44] [assignment: list of management functions to be provided by the TSF]
[45] [assignment: list of cryptographic operations]
[46] [assignment: cryptographic algorithm]

bits[47] that meet the following:

Encryption:

- *According to RSAEP in PKCS V2.1 RFC3447, section 5.1.1.*
- *According to RSAES-PKCS1-V1_5-ENCRYPT in PKCS V2.1 RFC3447, section 7.2.1. The hash algorithm is limited to SHA1 and SHA256.*
- *According to RSAES-OAEP-ENCRYPT in PKCS V2.1 RFC3447, section 7.1.1. The hash algorithm is limited to SHA1 and SHA256.*

Decryption:

- *According to RSADP in PKCS V2.1 RFC3447, section 5.1.2 without 5.1.1.2.b (ii, v).*
- *According to RSAES-PKCS1-V1_5-DECRYPT in PKCS V2.1 RFC3447, section 7.2.2. The hash algorithm is limited to SHA1 and SHA256.*
- *Decryption: According to RSAES-OAEP-DECRYPT in PKCS V2.1 RFC3447, section 7.1.2. The hash algorithm is limited to SHA1 and SHA256.*

[47] [assignment: cryptographic key sizes]

Signature generation:

- *SHA-1 or SHA-256 hashed messages: According to RSASP1 in PKCS V2.1 RFC3447, section 5.2.1 without 5.1.1.2.b (ii, v).*
- *SHA-1 or SHA-256 hashed messages: According to RSASSA-PKCS1-V1_5-SIGN in PKCS V2.1 RFC3447, section 8.2.1.*
- *SHA-1 or SHA-256 hashed messages: According to RSASSA-PSS-SIGN in PKCS V2.1 RFC3447, section 8.2.1.*
- *SHA-1 hashed messages only: According to "Signing a message" in ISO/IEC 9796-2:2010, section 7.2. For 7.2.3 only scheme 1 as specified in section 8 is used.*
- *SHA-1 hashed messages only: According to Digital Signature Scheme 1 in ISO/IEC 9796-2:2010, section 8. For 8.2.2 only the option t=1 is supported. The scheme is supported with and without Message Recovery.*

Signature verification:

- *SHA-1 or SHA-256 hashed messages: According to RSAVP1 in PKCS V2.1 RFC3447, section 5.2.2.*
- *SHA-1 or SHA-256 hashed messages: According to RSASA-PKCS1-V1_5-VERIFY in PKCS V2.1 RFC3447, section 8.2.2.*
- *SHA-1 or SHA-256 hashed messages: According to RSASSA-PSS-VERIFY in PKCS V2.1 RFC3447, section 8.1.2.*
- *SHA-1 hashed messages only: According to "Verifying a signature" in ISO/IEC 9796-2:2010, section 7.3. For 7.3.3 only scheme 1 as specified in section 8 is used.*[48]
- *SHA-1 hashed messages only: According to Digital Signature Scheme 1 in ISO/IEC 9796-2:2010, section 8. For 8.2.2 only the option t=1 is supported. The scheme is supported with and without Message Recovery.*

Dependencies [FDP_ITC.1 Import of user data without security attributes, or

[48] [assignment: list of standards]

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

Refinement None.

6.1.2.8 FCS_CKM.1/RSA

The Modular Arithmetic Operation of the TOE shall meet the requirement "Cryptographic key generation (Rivest-Shamir-Adleman)" as defined in Common Criteria Part 2 and as specified below.

FCS_CKM.1/RSA Cryptographic key generation (Rivest-Shamir-Adleman)

Hierarchical to No other components.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Generation of Random Primes that are Probably Prime*[49] and specified cryptographic key sizes *512 bit to 2048 bit in steps of 32 bits*[50] that meet the following:

U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), Digital Signature Standard (DSS), FIPS PUB 186-3, section B3.3 "Generation of Random Primes that are Probably Prime" with following changes

a. For step 1, nLen is allowed to be between 512 and 2048 and shall be a multiple of 32.

b. For step 4.4, $\sqrt{2}$ *is replaced by 1.5.*

[49] [assignment: cryptographic key generation algorithm]
[50] [assignment: cryptographic key sizes]

c. *For step 5.5, $\sqrt{2}$ is replaced by 1.5.*

d. *The primality tests are enhanced.*

Random prime numbers p and q shall be generated as described above. The random prime numbers p and q are also used to generate the public key (n, e), private key (n, d) and CRT key (p, d, dP, dQ, qInv). The public key is calculated according to PKCS#1 V2_1 2002 section 3.1 "RSA public key". The public key element e is an input parameter for the FW.SPS_Crypto API, while n is the product of p and q. The private keys are calculated according to PKCS#1 V2_1 2002 section 3.2 "RSA private key". For CRT key representation, the sequence of triplets is empty.[51]

Dependencies	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
Refinement	None.

6.1.2.9 FCS_COP.1/ECDSA

The TOE shall meet the requirement “Cryptographic operation – ECDSA” defined in Common Criteria Part 2 and as specified below.

FCS_COP.1/ECDSA	Cryptographic operation – ECDSA
Hierarchical to	No other components.
FCS_COP.1.1	The TSF shall perform *ECDSA signature generation and ECDSA signature verification*[52] in accordance with a specified cryptographic algorithm *Elliptic Curve Digital Signature Algorithm (ECDSA)*[53] and cryptographic key sizes *192,*

[51] [assignment: list of standards].
[52] [assignment: list of cryptographic operations]
[53] [assignment: cryptographic algorithm]

	223, 256, 384, 512, 521 bits[54] that meet the following: *ECDSA signature generation: According to ANSI X9.62-2005, section 7.3. The underlying hash functions NONE, SHA-1, SHA224, SHA256, SHA384 and SHA512 are supported.* *ECDSA signature verification: According to ANSI X9.62-2005, section 7.4. The underlying hash functions NONE, SHA-1, SHA224, SHA256, SHA384 and SHA512 are supported.* *Supported Elliptic Curves:* • *Brainpool curves [Brainpool]: brainpoolP192r1, brainpoolP192t1, brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1 and brainpoolP512t1.* • *NIST curves [NIST]: secp192r1, NIST secp224r1, NIST secp256r1, NIST secp384r1 and NIST secp521r1.*[55]
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
Refinement	None.

6.1.2.10 FCS_COP.1/ECDH

The TOE shall meet the requirement “Cryptographic operation – ECDH” defined in Common Criteria Part 2 and as specified below.

[54] [assignment: cryptographic key sizes]
[55] [assignment: list of standards]

FCS_COP.1/ECDH	Cryptographic operation – ECDH
Hierarchical to	No other components.
FCS_COP.1.1	The TSF shall perform *Key Exchange* [56] in accordance with a specified cryptographic algorithm *Elliptic Curve Diffie-Hellman Key Exchange (ECDH)*[57] and cryptographic key sizes *192, 223, 256, 384, 512, 521 bits* [58] that meet the following: *According to ANSI X9.63 -2001, section 5.4.1. The implementation returns the x- and y-coordinates of the shared secret rather than the x-coordinate only.* *Supported Elliptic Curves:* • *Brainpool curves [Brainpool]: brainpoolP192r1, brainpoolP192t1, brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1 and brainpoolP512t1.* • *NIST curves [NIST]: secp192r1, NIST secp224r1, NIST secp256r1, NIST secp384r1 and NIST secp521r1.*[59]
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
Refinement	None.

[56] [assignment: list of cryptographic operations]
[57] [assignment: cryptographic algorithm]
[58] [assignment: cryptographic key sizes]
[59] [assignment: list of standards]

6.1.2.11 FCS_CKM.1/EC

The Modular Arithmetic Operation of the TOE shall meet the requirement "Cryptographic key generation (EC)" as defined in Common Criteria Part 2 and as specified below.

FCS_CKM.1/EC	Cryptographic key generation (EC)
Hierarchical to	No other components.
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Elliptic Curve Key Pair Generation*[60] and specified cryptographic key sizes *192, 223, 256, 384, 512, 521 bits*[61] that meet the following: *According to ANSI X9.62-2005, section A.4.3. Cofactors are not supported.* *Supported Elliptic Curves:* • *Brainpool curves [Brainpool]: brainpoolP192r1, brainpoolP192t1, brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1 and brainpoolP512t1.* • *NIST curves [NIST]: secp192r1, NIST secp224r1, NIST secp256r1, NIST secp384r1 and NIST secp521r1*[62]
Dependencies	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
Refinement	None.

[60] [assignment: cryptographic key generation algorithm]
[61] [assignment: cryptographic key sizes]
[62] [assignment: list of standards].

6.1.2.12 FCS_COP.1/HMAC

The TOE shall meet the requirement "Cryptographic operation – HMAC" defined in Common Criteria Part 2 and as specified below.

FCS_COP.1/HMAC	Cryptographic operation – HMAC
Hierarchical to	No other components.
FCS_COP.1.1	The TSF shall perform *Message Authentication Code Computation* [63] in accordance with a specified cryptographic algorithm *Keyed-Hash Message Authentication Code using SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512*[64] and cryptographic key sizes *80 – 3072 bits*[65] that meet the following: *U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), The Keyed-Hash Message Authentication Code, FIPS PUB 198-1, July 2008*[66]
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
Refinement	None.

Note: The SHA-384 and SHA-512 based HMAC implementations are not designed to withstand side-channel attacks such as DPA or similar. Therefore, side-channel analysis for these primitives is not in scope of the evaluation.

[63] [assignment: list of cryptographic operations]
[64] [assignment: cryptographic algorithm]
[65] [assignment: cryptographic key sizes]
[66] [assignment: list of standards]

6.1.2.13 FCS_COP.1/ECDSA_verify_Loader

The TOE shall meet the requirement "Cryptographic Operation ECDSA signature verification" defined in Common Criteria Part 2 and as specified below.

FCS_COP.1/ECDSA_verify_Loader	Cryptographic Operation ECDSA signature verification
Hierarchical to	No other components.
FCS_COP.1.1	The TSF shall perform *ECDSA signature verification* [67] in accordance with a specified cryptographic algorithm *Elliptic Curve Digital Signature Algorithm (ECDSA)*[68] and cryptographic key sizes *256 bits*[69] that meet the following: *ECDSA signature verification: According to ANSI X9.62-2005, section 7.4. The underlying hash function SHA256 is supported.*[70]
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
Refinement	None.

6.1.2.14 FCS_COP.1/AES_decrypt_Loader

The TOE shall meet the requirement "Cryptographic Operation AES CBC decryption" defined in Common Criteria Part 2 and as specified below.

[67] [assignment: list of cryptographic operations]
[68] [assignment: cryptographic algorithm]
[69] [assignment: cryptographic key sizes]
[70] [assignment: list of standards]

FCS_COP.1/ AES_decrypt_Loader	Cryptographic Operation AES CBC decryption
Hierarchical to	No other components.
FCS_COP.1.1	The TSF shall perform *decryption*[71] in accordance with a specified cryptographic algorithm *AES in CBC mode*[72] and cryptographic key sizes *128 bits*[73] that meet the following: [PUB197], [SP800-38A].[74]
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
Refinement	None.

6.1.2.15 FCS_CKM.4/AES_keyDest_Loader

The TOE shall meet the requirement "Cryptographic key destruction – AES decryption key" defined in Common Criteria Part 2 and as specified below.

FCS_CKM.4/ AES_keyDest_Loader	Cryptographic key destruction – AES decryption key
Hierarchical to	No other components.

[71] [assignment: list of cryptographic operations]
[72] [assignment: list of cryptographic operations]
[73] [assignment: cryptographic key sizes]
[74] [assignment: list of standards]

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *invalidation* [75] that meets the following: *None*[76].
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
Refinement	None.

6.1.3 Disclaimer Cryptographic Support

The TOE provides several hardware accelerator/coprocessors for cryptographic functions; TDES, AES, ECDSA, ECDH, RSA and HMAC /SHA. The TDES coprocessor can be used to implement single or triple DES. The TOE also provides a cryptographic library, FW.SPS_Crypto, to handle the hardware modules and in some cases to implement enhanced cryptographic functionality. The following SFRs describe the requirements associated with these hardware modules.

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But Cryptographic Functionalities with a security level of lower than 100 bits can no longer be regarded as secure **without considering the application context**. Therefore for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

[75] [assignment: cryptographic key destruction method]
[76] [assignment: list of standards]

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 bits
Cryptographic Primitive	TDES in ECB mode	[SP800-67]	|k| = 112, 168	No
	TDES in CBC mode	[SP800-67], [SP800-38A]	|k| = 112	No
	TDES in CBC mode	[SP800-67], [SP800-38A]	|k| = 168	Yes
	TDES in CBC-MAC mode	[SP800-67], [ISO 9797-1]	|k| = 112, 168	No
	TDES in Retail MAC mode	[SP800-67], [ISO 9797-1]	|k| = 2x112, 2x168	No
	TDES in Full TDES Retail MAC mode	Global Platform Card Specification 2.2.1	|k| = 2x112, 2x168	No
	AES in ECB mode AES in AES-MAC mode	[PUB197], [SP800-38A]	|k| = 128, 192, 256	No
	AES in CBC mode AES in CTR mode AES in CMAC mode	[PUB197], [SP800-38A], [ISO 9796-1], [SP800-38B]	|k| = 128, 192, 256	Yes
	SHA-1	[FIPS 180-4]	-	No
	SHA-224, 256, 384, 512	[FIPS 180-4]	-	Yes
	RSA encryption and decryption without EME-OAEP (RSAEP, RSADP)	[PKCS#1 v2.1]	512 – 2048 in steps of 32 bits	No
	RSA encryption and decryption (RSAES-PKCS1-V1_5-ENCRYPT, RSAES-PKCS1-V1_5-	[PKCS#1 v2.1]	512 – 1952 in steps of 32 bits	No

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 bits
	DECRYPT, RSAES-OAEP-ENCRYPT)			
	RSA encryption and decryption (RSAES-PKCS1-V1_5-ENCRYPT, RSAES-OAEP-ENCRYPT)	[PKCS#1 v2.1]	1984 – 2048 in steps of 32 bits	Yes
	RSA signature generation and verification (RSASP1, RSAVP1, “Signing a message”, “Verifying a signature”)	[PKCS#1 v2.1]	512 – 2048 in steps of 32 bits	No
	RSA signature generation and verification (RSASSA-PKCS1-V1_5-SIGN, RSASA-PKCS1-V1_5-VERIFY, RSASSA-PSS-SIGN, RSASSA-PSS-VERIFY)	[PKCS#1 v2.1]	512 – 1952 in steps of 32 bits	No
	RSA signature generation and verification (RSASSA-PKCS1-V1_5-SIGN, RSASA-PKCS1-V1_5-VERIFY, RSASSA-PSS-SIGN, RSASSA-PSS-VERIFY)	[PKCS#1 v2.1]	1984 – 2048 in steps of 32 bits	Yes
	ECDSA signature generation and verification	[ANSI X9.62 - 2005]	Key sizes corresponding to the used elliptic curves brainpoolP192r1,	No

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 bits
			brainpoolP192t1, and secp192r1	
	ECDSA signature generation and verification	[ANSI X9.62 - 2005]	The selected hash function output size is less than the key size of the curve. Key sizes corresponding to the used elliptic curves brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1, brainpoolP512t1, secp192r1, secp224r1, secp256r1, secp384r1 and secp521r1	No
	ECDSA signature generation and verification	[ANSI X9.62 - 2005]	The selected hash function's output size is less than the key size of the curve. Key sizes corresponding to the used elliptic curves brainpoolP224r1, brainpoolP224t1,	Yes

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 bits
			brainpoolP256r1, brainpoolP256t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1, brainpoolP512t1, secp192r1, secp224r1, secp256r1, secp384r1 and secp521r1	
	ECDH	[ANSI X9.63 - 2001]	Key sizes corresponding to the used elliptic curves brainpoolP192r1, brainpoolP192t1, and secp192r1	No
	ECDH	[ANSI X9.63 - 2001]	Key sizes corresponding to the used elliptic curves brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1, brainpoolP512t1, secp192r1, secp224r1, secp256r1, secp384r1 and secp521r1	Yes
	RSA encryption and decryption (RSAES-	[PKCS#1 v2.1]	512 – 1952 in steps of 32 bits	No

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 bits
	OAEP-ENCRYPT, RSAES-OAEP-DECRYPT)			
	RSA encryption and decryption (RSAES-OAEP-ENCRYPT, RSAES-OAEP-DECRYPT)	[PKCS#1 v2.1]	1984 – 2048 in steps of 32 bits	Yes
Integrity	HMAC with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512HMAC with SHA-1	[PUB198-1]	80 – (block size of respective hash function – 1)	No
	HMAC with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	[PUB198-1]	Block size of respective hash function – 3072	Yes
	ECDSA with SHA-256	[ANSI X9.62 - 2005]	Key sizes corresponding to the used elliptic curves secp256r1.	Yes

Table 17: TOE cryptographic functionality and security strength

6.2 Security Assurance Requirements for the TOE

This Security Target will be evaluated according to “Security Target evaluation (Class ASE)”.

The security assurance requirements for the TOE are evaluated for Evaluation Assurance Level 5 augmented (EAL5+). Augmentation of the following components is mandated by [PP]:

ALC_DVS.2 and AVA_VAN.5

The assurance requirements applicable for the TOE are listed below in Table 18. The augmentation of the assurance components compared to [PP] is highlighted by bold letters.

Class / Description	Assurance Components	Description	Refinement	Notes
ADV: Development	ADV_ARC.1	Security Architecture Description	In [PP]	
	ADV_FSP.5	Complete semi-formal functional specification with additional error information	In [PP]	
	ADV_IMP.1	Implementation representation of the TOE security functions	In [PP]	
	ADV_INT.2	Well-structured internals		
	ADV_TDS.4	Semi-formal modular design		
AGD: Guidance Documents	AGD_OPE.1	Operational user guidance	In [PP]	
	AGD_PRE.1	Preparative procedures	In [PP]	
ALC: Life Cycle Support	ALC_CMC.4	Production support, acceptance procedures and automation	In [PP]	
	ALC_CMS.5	Development tools CM coverage	In [PP]	
	ALC_DEL.1	Delivery procedures	In [PP]	
	ALC_DVS.2	Sufficiency of security measures	In [PP]	
	ALC_LCD.1	Developer-defined life cycle model		
	ALC_TAT.2	Compliance with implementation standards		
ASE: Security Target Evaluation	ASE_CCL.1	Conformance claims		
	ASE_ECD.1	Extended components definition		
	ASE_INT.1	ST Introduction		
	ASE_OBJ.2	Security Objectives		
	ASE_REQ.2	Derived Security Requirements		
	ASE_SPD.1	Security Problem Definition		
	ASE_TSS.1	TOE Summary Specification		
ATE: Tests	ATE_COV.2	Analysis of coverage	In [PP]	
	ATE_DPT.3	Testing: Modular design		
	ATE_FUN.1	Functional testing		
	ATE_IND.2	Independent Testing – Sample		
AVA: Vulnerability Assessment	AVA_VAN.5	Advanced methodical vulnerability analysis	In [PP]	

Table 18. Security Assurance Requirements

6.2.1 Refinements and Augmentations of the TOE Assurance Requirements

This Security Target claims conformance to [PP], therefore all refinements specified in [PP] are applicable. This Security Target also claims conformance to EAL5 augmented with ALC_DVS.2 and AVA_VAN.5, therefore these refinements have to be discussed here in the Security Target.

The refinement for ALC_CMS can be applied even at EAL 5 augmented with ALC_CMS.5. The assurance component ALC_CMS.4 is extended to ALC_CMS.5 with aspects regarding the configuration control system for the TOE. The refinement is not touched.

The refinement for ADV_FSP can be applied even at EAL 5 augmented with ADV_FSP.5. The assurance component ADV_FSP.4 is extended to ADV_FSP.5 with aspects regarding the descriptive level. The level is increased from informal to semi-formal including informal description. The refinement is not touched.

6.3 Security Requirements Rationale

6.3.1 Rationale for the security functional requirements

Table 19 below gives an overview of how the security functional requirements are combined to meet the security objectives. The following sections provide a detailed justification.

Objective	TOE Security Functional and Assurance Requirements
O.Ctrl_Auth_Loader	• FTP_ITC.1 “Inter-TSF trusted channel” • FDP_UCT.1 “Basic data exchange confidentiality” • FDP_UIT.1 “Data exchange integrity” • FDP_ACC.1/ Loader “Subset access control – Loader” • FDP_ACF.1/ Loader “Security attribute based access control – Loader” • FCS_COP.1/AES_decrypt_Loader • FCS_COP.1/ECDSA_verify_Loader • FCS_CKM.4/AES_keyDest_Loader
O.RND	• FCS_RNG.1 “Quality metric for random numbers” • FDP_ITT.1 “Basic internal transfer protection” • FPT_ITT.1 “Basic internal TSF data transfer protection” • FDP_IFC.1 “Subset information flow control” • FRU_FLT.2 “Limited fault tolerance” • FPT_FLS.1 “Failure with preservation of secure state” • FPT_PHP.3 “Resistance to physical attack” • FPT_TST.2 “Subset TOE security testing”
O.TDES	• FCS_COP.1/TDES “Cryptographic Operation - TDES” • FCS_CKM.4/TDES “Cryptographic key destruction – TDES”
O.AES	• FCS_COP.1/AES “Cryptographic Operation - AES” • FCS_CKM.4/AES “Cryptographic key destruction – AES”
O.SHA	• FCS_COP.1/SHA “Cryptographic Operation - SHA”
O.Mem-Access	• FDP_ACC.1 “Subset access control” • FDP_ACF.1 “Security attribute based access control” • FMT_MSA.3 “Static attribute initialization” • FMT_MSA.1 “Management of security attributes” • FMT_SMF.1 “Specification of management functions”
O.RSA	• FCS_COP.1/RSA “Cryptographic Operation - RSA” • FCS_CKM.1/RSA “Cryptographic key generation - RSA”
O.ECC	• FCS_COP.1/ECDH “Cryptographic Operation - ECDH” • FCS_COP.1/ECDSA “Cryptographic Operation - ECDSA” • FCS_CKM.1/ECC “Cryptographic key generation - ECC”

Objective	TOE Security Functional and Assurance Requirements
O.HMAC	• FCS_COP.1/HMAC “Cryptographic Operation - HMAC”
O.Leak-Inherent	• FDP_ITT.1 “Basic internal transfer protection” • FPT_ITT.1 “Basic internal TSF data transfer protection” • FDP_IFC.1 “Subset information flow control”
O.Phys-Probing	• FDP_SDC.1 “Stored data confidentiality” • FPT_PHP.3 “Resistance to physical attack”
O.Malfunction	• FRU_FLT.2 “Limited fault tolerance” • FPT_FLS.1 “Failure with preservation of secure state”
O.Phys-Manipulation	• FDP_SDI.2 “Stored data integrity monitoring and action” • FPT_PHP.3 “Resistance to physical attack” • FPT_TST.2 “Subset TOE security testing”
O.Leak-Forced	• FDP_ITT.1 “Basic internal transfer protection” • FPT_ITT.1 “Basic internal TSF data transfer protection” • FDP_IFC.1 “Subset information flow control” • FDP_SDI.2 “Stored data integrity monitoring and action” • FRU_FLT.2 “Limited fault tolerance” • FPT_FLS.1 “Failure with preservation of secure state” • FPT_PHP.3 “Resistance to physical attack” • FPT_TST.2 “Subset TOE security testing”
O.Abuse-Func	• FMT_LIM.1 “Limited capabilities” • FMT_LIM.2 “Limited availability” • FDP_ITT.1 “Basic internal transfer protection” • FPT_ITT.1 “Basic internal TSF data transfer protection” • FDP_IFC.1 “Subset information flow control” • FRU_FLT.2 “Limited fault tolerance” • FPT_FLS.1 “Failure with preservation of secure state” • FPT_PHP.3 “Resistance to physical attack” • FPT_TST.2 “Subset TOE security testing”
O.Identification	• FAU_SAS.1 “Audit storage”

Table 19. Security Requirements versus Security Objectives

For O.RND, O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced, O.Abuse-Func and O.Identification the rationale is already provided in [PP] and applies for the TOE. Additional rationale is required for mapping FPT_TST.2 to O.Phys--Manipulation. For all other Security Objectives, FPT_TST.2 is mapped as required by the [PP] is case it is already mapped to O.Phys-Manipulation. Additional rationale is required for O.TDES, O.AES, O.SHA, O.Mem-Access, , O.RSA, O.ECC and O.HMAC which are added in comparison to [PP].

The justification related to the security objective “O.Phys-Manipulation” with regard to FPT_TST.2 is as follows:

The security functional component Subset TOE security testing (FPT_TST.2) has been newly created. It allows that particular parts of the security functionality provided by the TOE can be tested after TOE Delivery. This security functional component is used instead of the functional component FPT_TST.1 from Common Criteria Part 2. For the user it is important to know which part of the security functionality can be tested. The functional component FPT_TST.1 does not mandate to explicitly specify part of the security functionality being tested. In addition, FPT_TST.1 requires verification of the integrity of TSF data and stored TSF executable code which might violate the security policy. FPT_TST.2 will detect attempts to conduce a physical manipulation on the monitoring functions of the TOE. The objective of FPT_TST.2 is therefore identical to O.Phys-Manipulation.

The justification related to the security objective “O.Mem-Access” is as follows:

The security functional requirement “Subset access control (FDP_ACC.1)” with the related Security Function Policy (SFP) “Memory Access Control Policy” exactly require to implement an area based memory access control as demanded by O.Mem-Access. The related TOE security functional requirements FDP_ACC.1, FDP_ACF.1, FMT_MSA.3, FMT_MSA.1 and FMT_SMF.1 cover this security objective.

The security functional requirement “Static attribute initialization (FMT_MSA.3)” requires that the TOE provides default values for security attributes. These default values can be overwritten by any subject (software) provided that the necessary access is allowed what is further detailed in the security functional requirement “Management of security attributes (FMT_MSA.1)”: The ability to update the security attributes is restricted to privileged subject(s). These management functions ensure that the required access control can be realized using the functions provided by the TOE.

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

The justification related to the security objective “O.TDES” is as follows:

The cryptographic operations security goals discussed for this objective are directly implemented by FCP_COP.1/TDES and FCS_CKM.4/TDES as per [PP, § 381]:

The FCS_COP.1/TDES and FCS_CKM.4/TDES meet the security objective "Cryptographic service Triple-DES (O.TDES)".

The justification related to the security objective "O.AES" is as follows:

The cryptographic operations security goals discussed for this objective are directly implemented by FCP_COP.1/AES and FCS_CKM.4/AES as per [PP, § 389]:

The FCS_COP.1/AES and FCS_CKM.4/AES meet the security objective "Cryptographic service Triple-DES (O.AES)".

The justification related to the security objective "O.SHA" is as follows:

The cryptographic operations security goals discussed for this objective are directly implemented by FCP_COP.1/SHA as per [PP, § 396]:

The FCS_COP.1/SHA meets[77] the security objective "Cryptographic service Triple-DES (O.SHA)".

The justification related to the security objective "O.RSA, "O.ECC" and "O.HMAC" is as follows:

Similar to O.AES and O.TDES as justified in the [PP], the listed SFRs directly meet the security objective O.RSA, O.ECC and O.HMAC.

The justification related to the security objective "O.Ctrl_Auth_Loader" is as follows:

The security objective Access control and authenticity for the Loader (O.Ctrl_Auth_Loader) is covered by the SFR as follows (see [PP, 372]):

- The SFR FDP_ACC.1/Loader defines the subjects, objects and operations of the Loader SFP enforced by the SFR FTP_ITC.1, FDP_UCT.1, FDP_UIT.1 and FDP_ACF.1/Loader.

- The SFR FTP_ITC.1 requires the TSF to establish a trusted channel with assured identification of its end points and protection of the channel data from modification or disclosure.

- The SFR FDP_UCT.1 requires the TSF to receive data protected from unauthorised disclosure.

[77] Editorial change by the author

- The SFR FDP_UIT.1 requires the TSF to verify the integrity of the received user data.

- The SFR FDP_ACF.1/Loader requires the TSF to implement access control for the Loader functionality.

The cited Loader SFP mandates signature verification and decryption of all received data. Therefore, FCS_COP.1/AES_decrypt_Loader has been introduced to model the decryption part, as well as FCS_COP.1/ECDSA_verify_Loader modelling the signature verification part. Furthermore, the dependency FCS_CKM.4/AES_keyDest_Loader is defined.

6.3.2 Dependencies of security functional requirements

6.3.2.1 Dependencies from [PP]

Table 20 below lists the security functional requirements defined in [PP], their dependencies and whether they are satisfied by other security requirements defined in the profile.

Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST?
FRU_FLT.2	FPT_FLS.1	Yes
FPT_FLS.1	None	No dependency
FMT_LIM.1	FMT_LIM.2	Yes
FMT_LIM.2	FMT_LIM.1	Yes
FAU_SAS.1	None	No dependency
FPT_PHP.3	None	No dependency
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	Yes
FDP_IFC.1	FDP_IFF.1	The rationale for FDP_IFC.1 is provided in [PP, §274] and applies for the TOE completely.
FPT_ITT.1	None	No dependency
FDP_SDC.1	None	No dependency
FDP_SDI.2	None	No dependency
FCS_RNG.1/PTG2	None	No dependency

Table 20. Dependencies of the Security Functional Requirements from [PP]

6.3.2.2 Additional dependencies

Table 21 lists the dependencies of the additional SFRs for this Security Target.

Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST?
FPT_TST.2	None	Yes
FCS_COP.1/AES	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Yes (by the environment) Yes
FCS_COP.1/TDES	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Yes (by the environment) Yes
FCS_COP.1/RSA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Yes Yes (by the environment)
FCS_COP.1/ECDH	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Yes Yes (by the environment)
FCS_COP.1/ECDSA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Yes Yes (by the environment)
FCS_COP.1/HMAC	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Yes (by the environment) Yes (by the environment)
FCS_CKM.1/RSA	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	Yes Yes (by the environment)
FCS_CKM.1/ECC	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	Yes Yes (by the environment)
FCS_CKM.4/AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes (by the environment)
FCS_CKM.4/TDES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes (by the environment)
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Yes Yes
FMT_MSA.1	FMT_MSA.1 FMT_SMR.1	Yes Yes – see discussion below
FMT_MSA.3	[FDP_ACC.1. or FDP_IFC.1] FMT_SMR.1	Yes

Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST?
	FMT_SMF.1	Yes – see discussion below Yes
FMT_SMF.1	None	No dependency
FTP_ITC.1	None	No dependency
FDP_UCT.1	[FTP_ITC.1, or FTP_TRP.1] [FDP_ACC.1, or FDP_IFC.1]	Yes
FDP_UIT.1	[FTP_ITC.1, or FTP_TRP.1] [FDP_ACC.1, or FDP_IFC.1]	Yes
FDP_ACC.1/Loader	FDP_ACF.1	Yes
FDP_ACF.1/Loader	FMT_MSA.3	Yes – see discussion below
FCS_COP.1/AES_decrypt_Loader	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Yes
FCS_COP.1/ECDSA_verify_Loader	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Yes
FCS_CKM.4/AES_keyDest_Loader	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes

Table 21. Additional SFR dependencies

The dependencies defined for FCS_COP.1/AES, FCS_COP.1/TDES and FCS_COP.1/HMAC in Part 2 of the Common Criteria are [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] and FCS_CKM.4. The dependency to FCS_CKM.4 is fulfilled by the TOE. The remaining dependencies shall be addressed by appropriate management of cryptographic keys used by the specified cryptographic function by the environment. The Smartcard Embedded Software is designed for a specific application context and uses the cryptographic functions provided by the TOE. Hence, there is no further requirement arising from the dependencies of FCS_COP.1/AES, FCS_COP.1/TDES and FCS_COP.1/HMAC.

The dependencies defined for FCS_COP.1/RSA, FCS_COP.1/ECDH, and FCS_COP.1/ECDSA in Part 2 of the Common Criteria are [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] and FCS_CKM.4. The dependency to FCS_CKM.1 is fulfilled by the TOE. The remaining dependency to FCS_CKM.4 shall be addressed by

appropriate management of cryptographic keys used by the specified cryptographic function by the environment. The Smartcard Embedded Software is designed for a specific application context and uses the cryptographic functions provided by the TOE. Hence, there is no further requirement arising from the dependencies of FCS_COP.1/RSA, FCS_COP.1/ECDH, and FCS_COP.1/ECDSA.

The dependencies defined for FCS_CKM.1 in Part 2 of the Common Criteria are [FCS_CKM.2 or FCS_COP.1] and FCS_CKM.4. The dependency to FCS_COP.1 is fulfilled by the TOE. The remaining dependency to FCS_CKM.4 shall be addressed by appropriate management of cryptographic keys used by the specified cryptographic function by the environment. The Smartcard Embedded Software is designed for a specific application context and uses the cryptographic functions provided by the TOE. Hence, there is no further requirement arising from the dependencies of FCS_CKM.1.

The dependencies defined for FCS_CKM.4 in Part 2 of the Common Criteria are [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]. These dependencies shall be addressed by appropriate management of cryptographic keys used by the specified cryptographic function by the environment. The Smartcard Embedded Software is designed for a specific application context and uses the cryptographic functions provided by the TOE. Hence, there is no further requirement arising from the dependencies of FCS_CKM.4.

The dependency FMT_SMR.1 introduced by the two components FMT_MSA.1 and FMT_MSA.3 is considered to be satisfied because the access control specified for the intended TOE is not role-based by enforced for each subject. Therefore, there is no need to identify roles in form of a security functional requirement FMT_SMR.1.

Part 2 of the Common Criteria defines the dependency of FDP_IFC.1 (information flow control policy statement) on FDP_IFF.1 (Simple security attributes). The specification of FDP_IFF.1 would not capture the nature of the security functional requirement nor add any detail. As stated in the Data Processing Policy referred to in FDP_IFC.1 there are no attributes necessary. The security functional requirement for the TOE is sufficiently described using FDP_ITT.1 and its Data Processing Policy (FDP_IFC.1).

FDP_ACF.1/Loader has a dependency to FMT_MSA.3. However, according to [PP, 371] the SFR FMT_MSA.3 will not be necessary if the security attributes used to enforce the Loader SFP are fixed by the IC manufacturer and no new objects under control of the Loader SFP are created. This is indeed the case for the TOE. Therefore, the dependency is not required.

6.3.3 Rationale for the Assurance Requirements

The assurance level EAL5 and the augmentation with the requirements ALC_DVS.2 and AVA_VAN.5 were chosen in order to meet the assurance expectations explained in the following paragraphs.

An assurance level EAL5 with the augmentations ALC_DVS.2 and AVA_VAN.5 are required for this type of TOE since it is intended to defend against highly sophisticated attacks. This evaluation assurance package was selected to permit a developer to gain maximum assurance from positive security engineering based on good commercial practices. In order to provide a meaningful level of assurance that the TOE provides an adequate level of defense against such attacks, the evaluators should have access to all information regarding the TOE including the TSF internals, the low level design and source code.

ALC_DVS.2 Sufficiency of security measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE.

In the particular case of a Security IC the TOE is developed and produced within a complex and distributed industrial process which must especially be protected. Details about the implementation, (e.g. from design, test and development tools as well as Initialization Data) may make such attacks easier. Therefore, in the case of a Security IC, maintaining the confidentiality of the design is very important.

This assurance component is a higher hierarchical component to EAL 5 (which only requires ALC_DVS.1). ALC_DVS.2 has no dependencies.

AVA_VAN.5 Advanced methodical vulnerability analysis

Due to the intended use of the TOE, it must be shown to be highly resistant to penetration attacks. This assurance requirement is achieved by the AVA_VAN.5 component.

Independent vulnerability analysis is based on highly detailed technical information. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing high attack potential.

AVA_VAN.5 has dependencies to ADV_ARC.1 “Security architecture description”, ADV_FSP.2 “Security enforcing functional specification”, ADV_TDS.3 “Basic modular design”, ADV_IMP.1 “Implementation representation of the TSF”, AGD_OPE.1 “Operational user guidance”, and AGD_PRE.1 “Preparative procedures”.

All these dependencies are satisfied by EAL 5.

It has to be assumed that attackers with high attack potential try to attack Security ICs like smart cards used for digital signature applications or payment systems. Therefore, specifically AVA_VAN.5 was chosen in order to assure that even these attackers cannot successfully attack the TOE.

Statement regarding Application Note 29 of [PP]:

The current versions of the technical document “Application of Attack Potential to Smartcards” is [JIL], and shall be taken as a basis for the vulnerability analysis of the TOE.

6.3.4 Rationale for security requirements internal consistency

This Security Target uses the rationale presented in [PP] as justification for the claim of internal consistency between the security requirements specified therein. The justification comprising the additional SFRs is given in the following.

The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the cryptographic algorithms implemented according to the security functional requirement FCS_COP.1. Therefore, these security functional requirements support the secure implementation and operation of FCS_COP.1.

As disturbing, manipulating during or forcing the results of the test checking the security functionality after TOE delivery, the security functional requirement FPT_TST.2 has to be protected. An attacker could aim to switch off or disturb certain sensors or filters and preserve the detection of his manipulation by blocking the correct operation of FPT_TST.2. The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the self-test functions implemented according to the security functional requirement FPT_TST.2. Therefore, these security functional requirements support the secure implementation and operation of FPT_TST.2

The implemented privilege level concept represents the area based memory access protection enforced by the processor. As an attacker could attempt to manipulate the privilege level definition as defined and present in the TOE, the functional requirement FDP_ACC.1 and the related other requirements have to be protected themselves. The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the area based memory access control function implemented according to the security functional

requirement described in the security functional requirement FDP_ACC.1 with reference to the Memory Access Control Policy and details given in FDP_ACF.1. Therefore, those security functional requirements support the secure implementation and operation of FDP_ACF.1 with its dependent security functional requirements.

The Flash Loader functionality allows the IC vendor and the IC Dedicated Support Software Developer to update the Flash memory in the field by providing a trusted communication channel that supports both confidentiality and integrity protection of the user data to be loaded. The trusted communication channel is logically distinct from all other channels and enforced by FTP_ITC.1 while access to any kind of user data is clearly regulated by FDP_ACC.1/Loader and FDP_ACF.1/Loader. FDP_UCT.1 and FDP_UIT.1 utilize the functionality defined by FCS_COP.1/AES_decrypt_Loader, FCS_COP.1/ECDSA_verify_Loader, FCS_CKM.1/Loader_keyGen_Loader and FCS_CKM.4/AES_keyDest_Loader to protect the confidentiality and integrity of any user data.

7 TOE Summary Specification

Table 22 lists the Security Functionalities the TOE provides to meet the Security Functional Requirements. The Security Functions are described in more detail in the following sections described and the relation to the security functional requirements is shown.

TOE Security Functionalities
F.Corr-Operation
F.Phys-Protection
F. Logical-Protection
F.Prev-Abuse
F.Identification
F.Crypto
F.Memory-Access
F.Flash Loader

Table 22. TOE Security Functionalities

The following description of the Security Features is a complete representation of the TSF.

7.1 F.Corr-Operation

The TOE provides the security functionality “Guarantee of Correct Operation (F.Corr-Operation)” as specified below:

F.Corr-Operation Guarantee of Correct Operation

The TOE implements various sensors and integrity monitoring components. The sensors/detectors measure the applied voltage, applied frequency, and temperature. In addition, the target address range and operation of the CPU, cryptographic accelerators, random number generator module, and SPS memories are monitored.

The covered security functional requirements are FPT_FLS.1 and FRU_FLT.2.

7.2 F.Phys-Protection

The TOE provides the security functionality “Physical Protection against Physical Probing and Manipulation (F.Phys-Protection)” as specified below.

F.Phys-Protection	Physical Protection against Physical Probing and Manipulation The protection of the TOE comprises different features of the construction which makes a tamper attack more difficult such as an active security mesh and synthesized core logic. The implemented suite of self test functions also provides a wide range of capabilities to detect and prevent tampering.

The covered security functional requirements are FPT_PHP.3, FDP_SDI.2 and FPT_TST.2.

7.3 F. Logical-Protection

The TOE provides the security functionality “Logical Protection against Leakage (F.Logical-Protection)” as specified below.

F.Logical-Protection	Logical Protection against Leakage The TOE design isolates clock domains making it very difficult to correlate signals. The TOE also provides true random numbers to allow the Security IC Embedded Software the capability to implement various techniques that prevent Differential Power Analysis (DPA) attacks.

The covered security functional requirements are FDP_ITT.1, FPT_ITT.1, FDP_IFC.1 and FDP_SDC.1.

7.4 F.Prev-Abuse

The TOE provides the security functionality “Prevent Abuse of Functionality (F.Prev-Abuse)” as specified below.

F.Prev-Abuse	Prevent Abuse of Functionality Once the TOE has been set to User mode, Test mode functions are unavailable. The User mode is designed to be irreversible.

The covered security functional requirements are FMT_LIM.1 and FMT_LIM.2.

7.5 F.Identification

The TOE provides the security functionality “TOE Identification (F.Identification)” as specified below.

F.Identification	TOE Identification During the test process Initialization Data, Pre-Personalization Data and/or supplements of the Security IC Embedded Software can be stored in the ROM and/or FLASH and/or NVM-OTP memory of the TOE.

The covered security functional requirement is FAU_SAS.1.

7.6 F.Crypto

The TOE provides the security functionality “Cryptographic Operations (F.Crypto)” as specified below.

F.Crypto	Cryptographic Operations The implemented random number generator consists of a physical true hardware random number generator (physical TRNG). The physical TRNG fulfills the requirements of the functionality class PTG.2 of [AIS31]. The TOE provides the Triple Data Encryption Standard (TDES) as defined by the National Institute of Standards and Technology (NIST). Supported by the IC Dedicated Software the TOE hardware supports various feedback modes and both Two-key as well as Three-key Triple DES. The TOE provides the Advanced Encryption Standard (AES) as defined by the National Institute of Standards and Technology (NIST). Supported by the IC Dedicated Software the TOE hardware supports AES128, AES192 and AES256 each in combination with various feedback modes. The TOE provides RSA encryption and decryption according to ISO/IEC 9796-1, Annex A, sections A.4 and A.5, and Annex C. RSA signature generation and signature verification is implemented according to ISO 9796-2. The implementation conforms to additional standards and RSA key pair generation is also supported. The IC Dedicated Software selects and combines the appropriate functions of the PKA co-processor and provides an interface for RSA computations which can be used by the Security IC Embedded Software.

The RSA private key operations can make use of standard as well as of CRT keys. Key sizes can selected from a range of 512 to 2048 in steps of 32 bits.

The TOE provides Elliptic Curve Diffie Hellman Key Exchange, ECDSA signature generation and verification and Elliptic Curve key pair generation as defined by [ANSI X9.62-2005] and [ANSI X9.63-2001]. For all elliptic curve operations Brainpool curves P192r1, P192t1, P224r1, P224t1, P256r1, P256t1, P384r1, P384t1, P512r1, P512t1 and NIST curves secp192r1, secp224r1, secp256r1, secp384r1 and secp521r1 are supported. The IC Dedicated Software selects and combines the appropriate functions of the PKA co-processor and provides an interface for EC computations which can be used by the Security IC Embedded Software.

The TOE provides the Secure Hash Algorithms SHA1, SHA224, SHA256, SHA384, SHA512 as defined by FIPS PUB 180-4. The IC Dedicated Software selects and combines the appropriate functions of the HMAC co-processor and provides an interface for SHA-Secure hashing which can be used by the Security IC Embedded Software.

The TOE provides the Hash-based Message Access Code (HMAC) as defined by FIPS PUB 198-1. As underlying hash algorithms SHA1, SHA224, SHA256, SHA384 and SHA512 can be selected. The IC Dedicated Software selects and combines the appropriate functions of the HMAC co-processor and provides an interface for HMAC-authentication which can be used by the Security IC Embedded Software. The HMAC computation using SHA-1, SHA-224 and SHA-256 implement countermeasures against side channel analysis attacks such as SPA, DPA and DFA.

The covered security functional requirements are FCS_RNG.1, FCS_COP.1/TDES, FCS_CKM.4/TDES, FCS_COP.1/AES, FCS_CKM.4/AES, FCS_COP.1/RSA and FCS_CKM.1/RSA, FCS_COP.1/ECDH, FCS_COP.1/ECDSA and FCS_CKM.1/ECC, FCS_COP.1/SHA and FCS_COP.1/HMAC.

7.7 F.Memory-Access

The TOE provides the security functionality “Area based Memory Access Control (F.Memory-Access)” as

specified below.

F.Memory-Access	Area based Memory Access Control This security function restricts the ability of a given block of executable software residing in a specific memory area to read, write, delete data and/or execute code being stored in a specific memory area. The initial settings can be configured by the embedded software developer.

The covered security functional requirements are FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3 and FMT_SMF.1.

7.8 F.Flash Loader

The TOE provides the security functionality “Secure Flash Loader (F.Flash Loader)” as specified below.

F.Flash Loader	Secure Flash Loader This security function restricts the usage of the Flash loader to a combination of the IC vendor and the Security IC Embedded Software developer. In detail 1. When updating the IC Dedicated Support Software, the package a. must be ECDSA signed by the IC vendor, and b. must not come without an update of the Security IC Embedded Software (which is itself signed by the Security IC Embedded Software developer). 2. When updating the Security IC Embedded Software, the package a. must be ECDSA signed by the Security IC Embedded Software developer, and b. must not come without an update of the IC Dedicated Support Software (which is itself signed by the IC vendor). 3. When updating the Flash bootloader itself, the package a. must be ECDSA signed by the IC vendor, and

b. must be ECDSA signed by the Security IC Embedded Software developer.
c. In addition, each update of the Flash bootloader must be followed by an update of the IC Dedicated Support Software and an update of the Security IC Embedded Software.

Furthermore, the TOE decrypts any incoming user data and by that provides means to maintain the confidentiality of all, the IC Dedicated Support Software, the Security IC Embedded Software and the Flash bootloader itself. A complex key management system is supported by the TOE that enforces that

1. the IC Dedicated Support Software and the Flash bootloader itself are encrypted using keys only known to the IC vendor, and
2. the Security IC Embedded Software is encrypted using keys only known to the Security IC Embedded Software developer.

All data is encrypted by the IC vendor or the Security IC Embedded Software developer using AES-128 in CBC mode. No other encryption mode is supported by the TOE.

The covered security functional requirements are FTP_ITC.1, FDP_ACC.1/Loader, FDP_ACF.1/Loader, FDP_UCT.1, FDP_UIT.1, FCS_COP.1/AES_decrypt_Loader, FCS_COP.1/ECDSA_verify_Loader and FCS_CKM.4/AES_keyDest_Loader.

7.9 TOE Summary Specification Rationale

Table 23 below highlights the means by which the SFRs are implemented by the TOE security functions.

SFR	TOE Security Function(s)
FRU_FLT.2	F.Corr-Operation
FPT_FLS.1	F.Corr-Operation
FPT_PHP.3	F.Phys-Protection
FDP_SDI.2	F.Phys-Protection
FPT_TST.2	F.Phys-Protection
FDP_ITT.1	F.Logical-Protection
FDP_IFC.1	F.Logical-Protection

SFR	TOE Security Function(s)
FPT_ITT.1	F.Logical-Protection
FDP_SDC.1	F.Logical-Protection
FMT_LIM.1	F.Prev-Abuse
FMT_LIM.2	F.Prev-Abuse
FAU_SAS.1	F.Identification
FCS_RNG.1	F.Crypto
FCS_COP.1/TDES	F.Crypto
FCS_CKM.4/TDES	F.Crypto
FCS_COP.1/AES	F.Crypto
FCS_CKM.4/AES	F.Crypto
FCS_COP.1/RSA	F.Crypto
FCS_CKM.1/RSA	F.Crypto
FCS_COP.1/ECDH	F.Crypto
FCS_COP.1/ECDSA	F.Crypto
FCS_CKM.1/ECC	F.Crypto
FCS_COP.1/SHA	F.Crypto
FCS_COP.1/HMAC	F.Crypto
FDP_ACC.1	F.Memory-Access
FDP_ACF.1	F.Memory-Access
FMT_MSA.1	F.Memory-Access
FMT_MSA.3	F.Memory-Access
FMT_SMF.1	F.Memory-Access
FTP_ITC.1	F.Flash Loader
FDP_ACC.1/Loader	F.Flash Loader
FDP_ACF.1/Loader	F.Flash Loader
FDP_UCT.1	F.Flash Loader
FDP_UIT.1	F.Flash Loader
FCS_COP.1/AES_decrypt_Loader	F.Flash Loader
FCS_COP.1/ECDSA_verify_Loader	F.Flash Loader
FCS_CKM.4/AES_keyDest_Loader	F.Flash Loader

Table 23. SFR Mapping to TOE Security Functions

8 Annex

8.1 References

[AIS31] Bundesamt für Sicherheit in der Informationstechnik, *Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren,* Version 2.1, 2011-12-02

[ANSI X9.62 -2005] American National Standard Institute, ANSI X9.62:2005, Public Key Cryptography for the Financial Services Industry, *The Elliptic Curve Digital Signature Algorithm (ECDSA)*, 2005.

[ANSI X9.63 -2001] American National Standard Institute, ANSI X9.63: 2001, *Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography*, 2001.

[brainpool] M. Lochter and J. Merkle, *Request for Comments (RFC) 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation*, 2010

[CC_1] *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model*; Version 3.1, Revision 4 September 2012

[CC_2] *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements*; Version 3.1, Revision 4 September 2012

[CC_3] *Common Criteria for Information Technology Security Evaluation, Part 2: Security Assurance Requirements*; Version 3.1, Revision 4 September 2012

[CEM] *Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology*; Version 3.1, Revision 4 September 2012

[FIPS 180-4] Federal Information Processing Standards Publication 180-4, *SECURE HASH STANDARD,* U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2011 February, 11

[GP] *GlobalPlatform Card Specification 2.2.1*, Section B.1.2.1

[ISO 9796-2] ISO/IEC 9796-2:2010: *Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms*, Third Edition, 2012-12-15

[ISO 9797-1] ISO/IEC 9797-1:2011, *Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher*, Second edition, 2011-03-01

[JIL] Application of Attack Potential to Smartcards, Joint Interpretation Library, Version 2.9, January 2013

[KS2011] *A proposal for: Functionality classes for random number generators*, Version 2.0, 2011-09-18

[PP] *Security IC Platform Protection Profile with Augmentation Packages*, Version 1.0, 13.01.2014, BSI-CC-PP-0084-2014, Eurosmart

[PKCS#1 v2.1] *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography*, Version 2.1, RFC 3447, RSA Laboratories, February 2003

[NIST] Certicom Research, *SEC2: Recommended Elliptic Curve Domain Parameters*, Version 1.0, 2000

[PUB 186-3] U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), *Digital Signature Standard (DSS), FIPS PUB 186-3*, July 2013

[PUB197] U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), *Advanced Encryption Standard (AES)*, FIPS PUB 197

[PUB198-1] U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), *The Keyed-Hash Message Authentication Code (HMAC)*, FIPS PUB 198-1

[SP800-38A] National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce, *Recommendation for Block Cipher*

Modes of Operation, NIST Special Publication 800-38A, Edition 2001, December 2001

[SP800-38B] National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, NIST Special Publication 800-38B, May 2005

[SP800-67] National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, NIST Special Publication 800- 67, revised January 2012