Security Target Lite of Security Chip MH1701 V05 with IC Dedicated Software

Version V1.1

北京兆讯恒达技术有限公司

Beijing Megahunt Technologies Inc.

Revision Record

DATE	Revision	Description	Author
2025-8-5	1.0	Draft completed	Zhouna
2025-8-7	1.1	Modified	Zhouna

List of Abbreviations

List of abbreviations: Explain the abbreviations used in this article, and ask for the full English name.

Abbreviations	Full Spelling
CBC	Cipher Block Chaining
CC	Common Criteria
CPU	Central Processing Unit
CRC	Checksum module
DES/TDES	Data Encryption Standard/Triple Data Encryption
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
ECB	Electronic Codebook
EDC	Error Data Check
MPU	Memory Protection Unit
FA	Fault Attack
IFD	Internal Frequency Detector
GPIO	General Purpose IO
IC	Integrated Circuit
OTP	One-Time-Programmable memory
PP	Protection Profile
RAM	Random Access Memory
ROM	Read-Only Memory
RSA	Rivest-Shamir-Adleman
SFR	Security Functional Requirements
SPA	Simple Power Analysis
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TRNG	True Random Number Generator
CL	Cryptographic libraries
DRNG	Deterministic Random Number Generator
GSM	Global System for Mobile Communication
UMTS	Universal Mobile Telecommunications System
PKE	Public Key Engine
SCP	Symmetric Co-processor
DIF	Dual Interface
ECDSA	Elliptic Curve DSA
CGU	Clock Unit
RGU	Reset Unit
T&W	Timers and Watchdog
FSMPU	Finite State Machine Power-up Unit
DMA	Direct Memory Access Controller
MEDU	Memory Encryption/Decryption Unit
EDU	Error Detection Unit
NVIC	Nested Vectored Interrupt Controller
CRAM	Cryptographic RAM
EC	Elliptic Curve
ECC	Error Correction Code
SBL	Security Boot Loader
SFs	Security Functions

Abbreviations	Full Spelling
SF	Security Feature
SF_PM	SF_PM: Protection against Malfunction
SF_PP	SF_PP: Physical Protection
SF_PF	SF_PF: Prevent abuse of Functionality
SF_RNG	SF_RNG: Random Number Generator
SF_CS	SF_CS: Cryptographic Support
SF_MAC	SF_MAC: Memory Access Control
SF_PL	SF_PL: Protection against Leakage

Table of Content

1 ST INTRODUCTION

1.1 ST Reference and TOE Reference

1.1.1 ST Reference

“Security Target Lite of Security Chip MH1701 V05 with IC Dedicated Software, Version 1.1, August 7, 2025”.

The Security Target claims a strict conformance to Eurosmart Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13th Jan. 2014, BSI-CC-PP-0084-2014.

The Protection Profile and the Security Target are built on Common Criteria version 3.1.

Common Criteria version:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017

1.1.2 TOE Reference

The TOE is named “Security Chip MH1701 with IC Dedicated Software, V05”.

In this document the TOE is abbreviated to "Security Chip MH1701".

1.2 TOE Overview

1.2.1 TOE Introduction

The TOE implements a dedicated security 32-bit RISC CPU. The controller combines the features of integrated peripheral, enhanced performance and optimized power consumption to

make it ideal for chip card applications. The TOE offer a wide range of peripherals, including ISO interface, two timers, one watchdog, a CRC module, a true random number generator (TRNG) and a deterministic random number generator (DRNG), coprocessors for symmetric and asymmetric cryptographic algorithms. Additionally, a range of communication interfaces, such as GPIO, NFC.

The TOE comprises the MEGAHUNT security chip MH1701 and IC dedicated software which includes the firmware SBL stored in ROM and software such as Cryptographic libraries (CL). The TOE can be configured as either permanently disabled for the downloader or enabled for the downloader.

1.2.2 TOE Application Scenario

The TOE offer all functions that are both required and useful in security systems, and integrated peripherals that are typically needed in chip card applications, such as information security, identification, access control, electronic banking, digital signature and multi-application cards, ID cards, transportation and e-purse applications.

1.2.3 TOE Security Functionality

The TOE is a powerful smart card IC with a large amount of memory and special peripheral devices with improved performance, optimized power consumption, at minimal chip size while implementing high security. The TOE with its integrated security features meets the security requirements of all smart card applications such as information integrity protection, access control, (U)SIM of the mobile telephone and identification card, as well as electronic funds transfer and healthcare systems. The security functionality is described as follows:

- The major components of the core system are the 32-bit CPU with security mechanisms supporting two modes: unprivileged and privilege
- Bus polarity switching
- The TOE provides a robust set of sensors for the purpose of monitoring proper chip operating conditions and detecting fault attacks. Including temperature sensor, internal

frequency sensor, voltage sensor, glitch sensor and light sensor

- AES with countermeasures against SPA, DPA, EMA, DEMA and DFA attacks
- Triple-DES with countermeasures against SPA, DPA, EMA, DEMA and DFA attacks
- RSA cryptography with countermeasures against SPA, DPA, EMA, DEMA and DFA attacks
- Elliptic Curve (EC) cryptography with countermeasures against SPA, DPA, EMA, DEMA and DFA attacks
- The TOE provides True Random Number Generator (TRNG) specially designed for smart card applications are implemented. The TRNG fulfills the requirements from the functionality class PTG.2 of AIS31
- The TOE provides Deterministic Random Number Generator (DRNG), which compliant with DRG.3 class of AIS31
- Memory access control and the enhanced Memory Protection Unit (eMPU)
- Specific active shielding that against probing and physical manipulation attacks
- Memory Encryption/Decryption Unit provides encryption of all memories inside the chip (RAM, CRAM, NVM and OTP)
- Parity check for RAM, CRAM, NVM/OTP and some critical registers
- Test mode and downloader blocking protection
- Downloader disabling and protection(only for downloader is valid)

2 TOE Description

2.1 Physical Scope of TOE

The scope of the TOE includes the IC hardware, firmware, cryptographic library and API library. The downloader in the TOE has two configurations. The first is to permanently block the downloader, the downloader cannot be used to update the user's software after delivery. The second is that the downloader is effective, the downloader can be used to update the user's software after delivery. See Table 3 for other configurations.

Table 1 Components of the TOE scope

Type	Name	Identifier	Release Version	Form of delivery
IC Hardware	Security chip MH1701	MH1701	V05	Dual Interface (DIF)Module
Security IC Dedicated Software	(overall version)		03	-
	Security Boot Loader (SBL)	C28_FW_C_SBL	V0.7 [a]	In ROM
	Cryptographic library and head files	C28_SW_C_CL	V3.0	.Lib file .a file .h file
	Security API library and head files	C28_SW_C_SAL	V3.0	.Lib file .a file .h file
Document	MH1701 Security Chip V05 Cryptographic Library Interface Manual	C28_GD_CL	V1.0	.PDF file
	MH1701 Security Chip V05 Security API Library Interface Manual	C28_GD_SAL	V1.0	.PDF file
	MH1701 Security Chip V05 Bootloader User Guidance	C28_GD_SBL	V1.0	.PDF file

	specification			
	The datasheet of MH1701 Security Chip V05	C28_GD_Datasheet	V1.0	.PDF file
	MH1701 Security Chip V05 User Operational Guidance	C28_GD_Operational Guidance	V1.0	.PDF file
	MH1701 Security Chip V05 Preparative Procedures	C28_GD_Preparative Guidance	V1.0	.PDF file

a. The version can only be checked when the downloader is valid

2.2 Logical Scope of the TOE

The logical scope of TOE hardware is the functionality of the hardware components described in the section 2.2.1. The logical scope of the IC dedicated software is described in this the section 2.2.2 and 2.2.3. The IC dedicated software includes firmware and software library two parts.

2.2.1 Hardware Description

The hardware part of the TOE (see Figure 1) as defined in this ST is comprised of:

- CPU
  - 32-bit RISC CPU
  - Enhanced Memory Protection Unit (eMPU)
- Memories
  - Read-Only Memory (ROM, for internal firmware)
  - Random Access Memory (RAM)

- Cryptographic RAM (CRAM)
- NVM memory (NVM)
- One-Time-Programmable memory (OTP)

➢ Peripherals

- ISO/IEC 7816 Interface
- ISO/IEC 14443 Interface
- SPI Interface
- I2C Interface
- General Purpose Input Output (GPIO)
- Timers and Watchdog (T&W)
- Clock Unit (CGU)
- Reset Unit (RGU)
- Direct Memory Access Controller (DMA)
- Finite State Machine Power-up Unit (FSMPU)

➢ Coprocessors and Security module

- Public Key Engine named PKE for asymmetric algorithms like RSA and EC
- Symmetric Crypto co-processor for DES/TDES and AES Standards
- Hash Functions: SHA-1, SHA-2
- True Random Number Generator (TRNG)
- Deterministic Random Number Generator (DRNG)
- Checksum module (CRC)

➢ SECMU (including Security Sensor and shield)

- Glitch Sensor
- Temperature Sensor
- Light Sensor
- Voltage Sensor
- Internal Frequency Sensor
- Active Shield

➢ Buses

- AHB Bus
- APB Bus
- DMA Bus

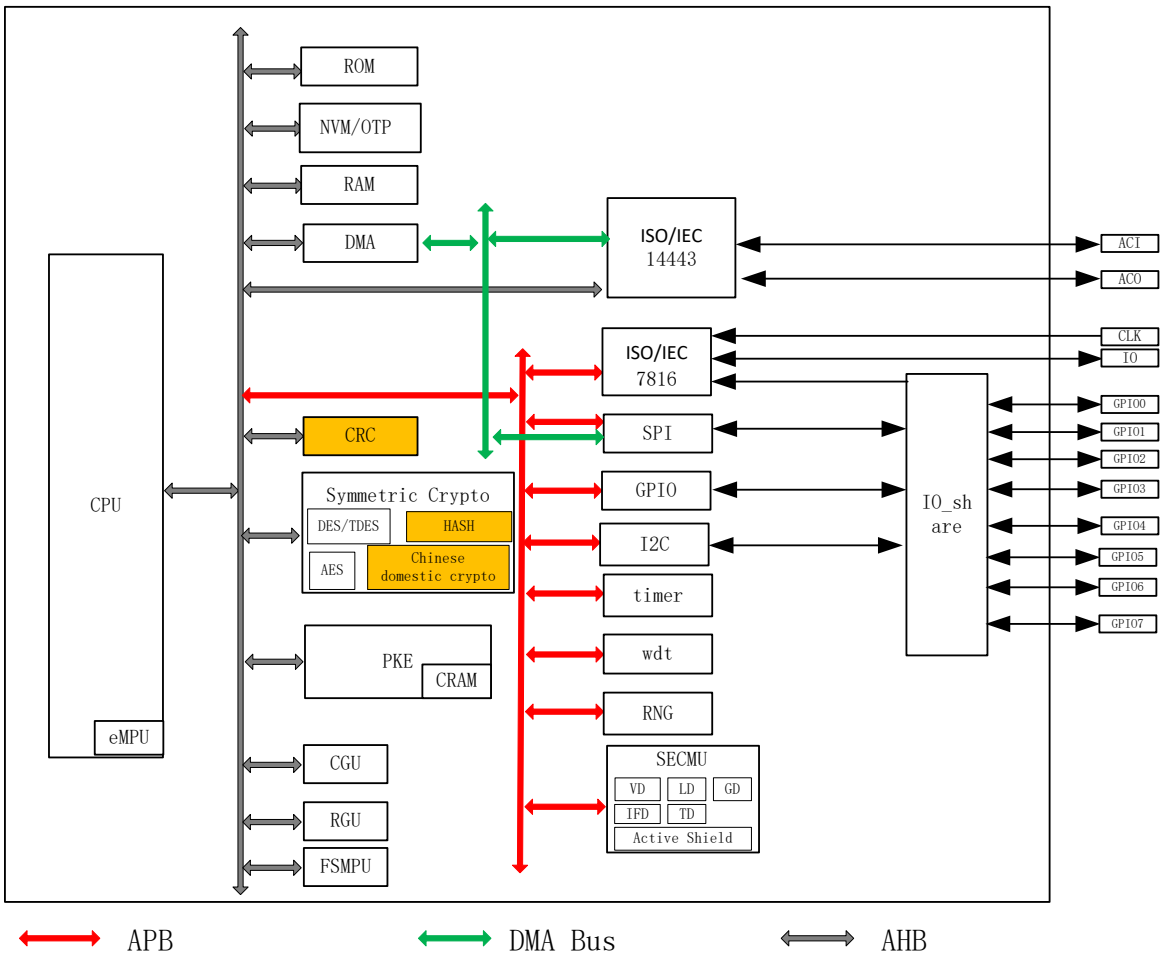

Figure 1 Hardware Boundary

The TOE contains the following functions, but these security functions are not claimed.

- Chinese domestic cryptographic function
- Single DES cryptographic function
- Hash functions for the SHA-1 and SHA-2 family
- Checksum module (CRC)

The TOE consists of smart card ICs (Security Controllers) meeting high requirements in terms of performance and security. This TOE is intended to be used in smart cards for particularly security-relevant applications and for the smart card operating system. The TOE consists of a

core system, memories, co-processors, security peripherals, control logic and peripherals.

1) The major components of the CPU (Central Processing Unit) are the 32-bit RISC CPU, the eMPU (Memory Protection Unit).

The memory model of the TOE provides two distinct, independent levels. Additionally, up to eight regions can be defined with different access rights controlled by the enhanced Memory Protection Unit (eMPU).

2) The major components of the memories are ROM, RAM, NVM and OTP.

ROM is used to stored chip firmware programs. RAM is used to store temporary data for executing programs. NVM is used to store the program and data such as the cryptographic library, OS, user applications. The chip one time programmable (OTP) memory is used to store unchangeable data, such as public key, SN, chip parameters, etc.

The CPU accesses the memory via the integrated Memory Encryption and Decryption unit (MED). All user data of the memory is encrypted, RAM, CRAM and the NVM, OTP are equipped with an error detection code (EDC).

3) The TOE contains two co-processors PKE and SCP.

The PKE for calculation of asymmetric algorithms like RSA 1024 to 4096-bits key length and scalar multiplication for Elliptic Curve (EC) cryptography with scalar length of 192, 224, 256, 384 and 521 bits and the SCP for DES, dual-key or triple-key TDES and AES (with key length of 128, 192 and 256 bits) calculations. These co-processors are especially designed for smart card applications with respect to the security and power consumption. The SCP module computes the complete AES/DES/TDES algorithm within a few clock cycles and AES algorithm is especially designed to counter attacks like SPA, DPA, EMA, DEMA and DFA. The PKE provides basic functions for the implementation of RSA and EC cryptographic libraries. The TOE also provides Chinese domestic cryptographic function and the hash functions for the SHA-1 and SHA-2 family, But, these function are not in evaluation scope.

4) The security peripherals include Security Sensor Modules, a CRC module and random number generators.

The Security Sensor Modules serve for operation within the specified range. A set of sensors (temperature sensor, backside light detector, VD, IFD, GD sensor) is used to detect excessive

deviations from the specified operational range and serve for robustness of the TOE by generating alarms. The alarms can be configured as resetting the TOE or generating the interrupts. In addition, the alarm signals of the sensors are self-tested during the power on process.

The cyclic redundancy check (CRC) module is a 16/32-bit checksum generator. It is not claimed as the security function.

Random Number Generators (TRNG/DRNG) specially designed for a smart card application is implemented. The TRNG fulfills the requirements from the functionality class PTG.2 of the AIS31 and produces true random numbers. The DRNG fulfills the requirements from the functionality class DRG.3 of the AIS31.

5) The control logic unit includes Clock Unit (CGU), Reset Unit (RGU) and Finite State Machine Power-up Unit (FSMPU).

The Clock Unit (CGU) supplies the clocks for all components of the TOE. The system clock is based on the internal oscillator clock.

The Reset Unit (RGU) supplies the resets for all components of the TOE. It generates the system reset and resets for all the subsystems and modules.

The Finite State Machine Power-up Unit (FSMPU) manage the power up procedure (including sensors self-test) of the TOE.

6) TOE has three timer modules and one WDT (WDT and TIMER)

The TOE includes three 32-bit general purpose timers.

The Timer unit is used for timer operation when clocked by the oscillator/system clock or counter operation depending on the clock source configured. The unit can be programmed for particular applications, such as measuring the time behavior of an event or outputting a clock signal at the external pin. Note also the timer events can generate interrupt requests used for interrupt service routines or peripheral event channel data transfers.

The WDT timer is a circuit that monitors controller operation by automatically initiating a reset if a specified period without an adequate response elapses after the occurrence of a hardware or software irregularity. In normal operation, the timer register or software regularity cleared by software so that no alarm occurs. However, in the situation of a hardware or software

irregularity which prevents the software from clearing the timer, a security alarm is triggered upon expiry of the WDT.

7) TOE has multiple interfaces such as ISO/IEC 14443, ISO/IEC 7816, SPI, I2C, GPIO

ISO/IEC 14443 interface and ISO/IEC 7816 interface are the interfaces available for the user. SPI, GPIO and I2C interfaces are not valid for the TOE in the DIF module format.

ISO/IEC 14443 protocol is contactless card standards protocol. The ISO/IEC 14443 module supports the contactless card ISO/IEC 14443 Type A, Type B and Mifare protocol. The Mifare protocol can not be used for security purpose. In addition, the interface also supports multiple baud rates and supports automatic calculation of the CRC.

The ISO/IEC 7816 interface provides the physical layer and data link layer processing capabilities for character frame transmission in the ISO/IEC 7816-3 protocol, and implements asynchronous serial communication character frame transmission as defined by ISO/IEC 7816-3, while providing hardware support for T0 and T1 user programs.

The serial peripheral interface (SPI) allows the chip to communicate with external devices in a half/full duplex, synchronous, serial manner. This interface can be configured in master mode and provides a communication clock for external devices. The interface can also work in a variety of master configurations.

The serial peripheral interface (I2C) allows the chip to communicate with external devices. This interface can be configured in master mode or slave mode.

The GPIO interface consists of 8 pads which can be individually configured and combined in various ways. (SPI interface, I2C interface and reset of ISO/IEC 7816 are multiplexed with 5 of GPIO pads).

8) DMA

Direct Memory Access (DMA) refers to the interface technology that external devices directly exchange data with system memory without going through the CPU. The CPU and DMA access SPI and ISO/IEC 14443 interface through arbitration mechanism

2.2.2 Firmware Description

The entire firmware of the TOE is the Security Boot Loader (SBL).

The Security Boot Loader (SBL) is the part of the IC dedicated software of the TOE which is stored in the ROM. All mandatory functions for start-up, downloading and life cycle protection are protected by a dedicated hardware firewall.

2.2.2.1 The chip Life cycle stage management

Security Boot Loader divides the chip life cycle into several stages. (Once the stage of the chip is upgraded, it will not be able to fall back to the previous stage): When the chip is delivered to customers, it is in the stages of RELEASE(downloader is enabled) or TERMINATE(downloader is disabled permanently) stage. The downloader function can be used by authenticated users in the RELEASE stage, and it must be disabled after the download is completed. Once the downloader is blocked, no one can access the sensitive operations of the chip again.

2.2.2.2 Security Boot

When the chip is powered on, SBL firstly checks the chip status, when it finds abnormal, the chip will not start. If there is no abnormality, SBL will continue to check whether there is valid Embedded Software in NVM. If there is no valid Embedded Software, the chip will not start. Otherwise, SBL configures the chip to the startup state and start the embedded software.

2.2.2.3 Security Download (Downloader is enabled)

The Security Boot Loader can receive the image of the ES and download it into the NVM memory. This downloader function has to be disabled permanently before deliver to the end user.

2.2.3 Software Library Description

The software library of the TOE consists of the cryptographic libraries including DES, AES, RSA and EC and security API library.

1) Cryptographic Libraries

The RSA Cryptographic library (CL) is used to provide a high-level interface to RSA (Rivest, Shamir, Adleman) cryptography implemented on the hardware component PKE and includes countermeasures against SPA, DPA, EMA, DEMA and DFA attacks. The routines are used for the generation of RSA key, the RSA encryption, the RSA decryption, RSA signature verification, RSA signature generation and RSA key completion. RSA key generation and RSA key completion interface are not claimed as a security function. The hardware PKE Cryptographic IP unit provides the basic long number calculations (add, subtract, multiply, power with 2048 bit numbers) with high performance. The RSA library is delivered as object code. The RSA library can perform RSA operations from 1024 to 4096 bits. Following the BSI2 recommendations, key lengths below 1976 bits are not included in the certificate.

The EC Crypto library (CL) is used to provide a high-level interface to Elliptic Curve cryptography implemented on the hardware component PKE and includes countermeasures against SPA, DPA, EMA, DEMA and DFA attacks. The routines are used for ECDSA signature generation, ECDSA signature verification, ECIES encryption, ECIES decryption, EC key generation and Elliptic Curve Diffie-Hellman key agreement. The EC library is delivered as lib files. The certification covers the standard NIST [12] and Brain pool [13] Elliptic Curves with key lengths of 192, 224, 256, 384 and 521 Bits, according to the national AIS32 regulations by the BSI.

The DES/TDES/AES Crypto library (CL) is also used to provide a high level interface to DES/TDES and AES symmetric cryptographic operations. It uses the SCP of the underlying hardware but implements also countermeasures against SPA, DPA, EMA, DEMA and DFA attacks on all known weaknesses of the SCP. The DES Crypto library is not claimed as a security function.

2) Security API Library

The security API library provides three functions: Cryptographic supporting, data security copy and security comparison, random number generation APIs (TRNG and DRNG), the TRNG is compliant with PTG.2 and the DRNG is compliant with DRG.3.

The Cryptographic supporting function includes big number calculation and Cryptographic

security configuration. The big number calculation function does not provide cryptographic function or additional security functionality as it provides only the following basic big number arithmetic and modular functions in software. The big number calculation function is deemed for software developers as support for simplified implementation of big number and modular arithmetic operations.

2.3 Interfaces of the TOE

The external interfaces of the TOE are divided into two main categories. The first category comprises the physical interfaces of the TOE and the second category comprises the interfaces of the TOE to the IC embedded software.

2.3.1 Physical interface

The TOE has the following physical interfaces to external entities in the TOE environment:

- The physical interface of the TOE to the external environment is the entire surface of the IC: Wires for Active Shield, Front side, Back side.
- The electrical interface of the TOE to the external environment is constituted by the pads of the chip:
  - The five ISO/IEC 7816 pads consist particularly of the contacted Reset, I/O, CLK lines and supply lines VCC and GND. The contact based communication is according to ISO/IEC 7816/EMV.
  - ISO/IEC 14443 interface has two pins: ANT1 and ANT2.
  - The GPIO interface consists of 8 pads which can be individually configured and combined in various ways (SPI interface, I2C interface and reset of ISO/IEC 7816 are multiplexed with 5 of GPIO pads). These interfaces only exist on the TOE in the form of bare dies, but the TOE in the form of DIF Module does not provide.
- Sensor interface: Temperature sensor, Voltage sensor, Glitch sensor, Light sensor.

2.3.2 Software interface

The TOE has the following software interfaces to the embedded software developer:

- API interface:
  - The interface to the RSA calculations is defined by the RSA Cryptographic library.
  - The interface to the EC calculations is defined by the EC Cryptographic library.
  - The interface to the DES/TDES calculations is defined by the DES/TDES Cryptographic library.
  - The interface to the AES calculations is defined by the AES Cryptographic library.
  - The interface to the true random number generation (TRNG) and deterministic random number generation (DRNG) are defined by the Security API library.
- APDU
  - The interface is a set of commands which communicated with the SBL.
- Register
  - The registers of the CPU, Co-processors and peripherals.
- CPU instruction set

2.4 Forms of delivery

The TOE can be delivered in form of complete DIF modules. The form of delivery does not affect the TOE security and it can be delivered in any form, as long as the processes applied and sites involved have been subject of the appropriate audit.

The delivery is after the end of phase4 (after module packaging) which can also include pre-personalization steps according to PP [1]. Nevertheless, in this case the TOE is finished and the extended test features are removed.

The software delivered is Cryptographic libraries and Security API Library. The following table shows the delivery methods for the TOE components.

Table 2 TOE deliveries: form and methods

TOE Component	Delivered Format	Delivery Method	Comment
MH1701	DIF modules	Postal transfer in cages	All materials are delivered to distribution centers in cages, locked.
All Firmware	-	-	Stored on the delivered hardware
All software/libraries	Cryptographic libraries (object code)	Encrypted with the user's public key and emailed to the designated person	-
	Security API Library(object code)	Encrypted with the user's public key and emailed to the designated person	-
All User Guidance documents	Personalized PDF	Encrypted with the user's public key and emailed to the designated person	-

2.5 TOE Life Cycle

The complex development and manufacturing processes can be separated into seven distinct phases. The phases 2 and 3 of the life cycle cover the IC development and production:

- IC Development (Phase 2)
  - · IC design
  - · IC Dedicated Software development
- The IC Manufacturing (Phase 3)
  - · Integration and photo mask fabrication

· IC production

· IC testing

· Preparation and pre-personalization if necessary

The life cycle phase 4 is included in the evaluation of the IC:

- The IC Packaging (Phase 4)

  · Dicing

  · Security IC packaging (and testing)

  · Pre-personalization if necessary

In addition, four important stages have to be considered in the Composite Product life cycle:

- Security IC Embedded Software Development (Phase 1)
- The Composite Product finishing process, preparation and shipping to the personalization line for the Composite Product (Composite Product Integration Phase 5)
- The Composite Product personalization and testing stage where the User Data is loaded into the Security IC's memory (Personalization Phase 6)
- The Composite Product usage by its issuers and consumers (Operational Usage Phase 7) which may include loading and other management of applications in the field

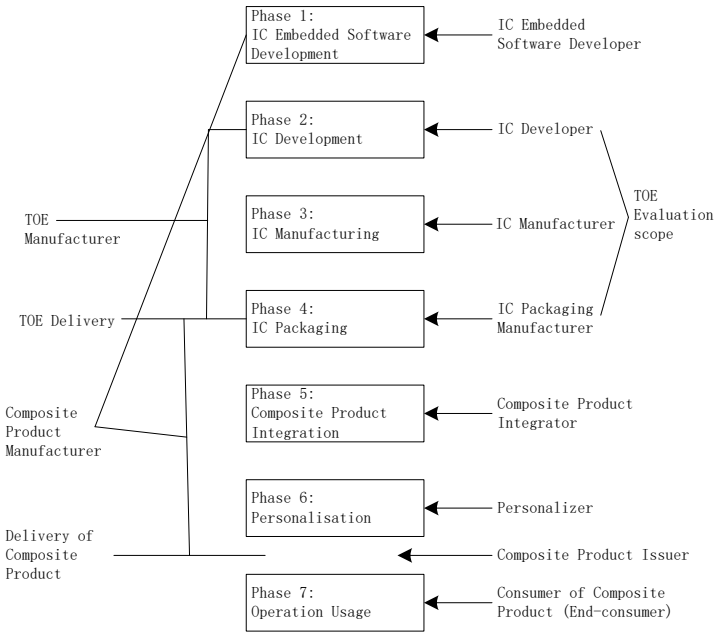

Figure 2 Definition of "TOE Delivery" and responsible Parties

The Security IC Embedded Software is developed outside the TOE development in Phase 1. The TOE is developed in Phase 2 and produced in Phase 3. After Phase 4 (module packaging),

the TOE is delivered in form of DIF modules, and the configuration of the downlaoder depends on user's requirements. The TOE evaluation scope is from Phase 2 to Phase 4.

2.6 TOE Configuration

The TOE offers different configuration options, which a customer can configure. After adding the clock adaptive mode, the clock frequency can be configured as 72MHz*4/32, 72 MHz *5/32, …, 72MHz 32/32. Users can configure different clock frequencies according to their needs. There are two kinds of memory size available, RAM and NVM. The RAM and NVM size is configurable by MEGAHUNT and the ES developer can order the TOE of different RAM and NVM size. However, the memory size is determined before delivery to the ES developer. The size of the RAM is 16KB and 10KB. The size of the NVM is 384KB and 256KB. The TOE provides the following configurations:

Table 3: TOE configuration

Number	Configuration option	Configuration value	Configurable in the field
1.	Clock Frequency	● 72 MHz ● 69.75 MHz ● … ● 11.25 MHz ● 9MHz	Yes
2.	Memory size	RAM: ● 16KB ● 10KB	No
		NVM: ● 384KB ● 256KB	No

2.7 TOE initialization with Customer Software

Please refer to the following Table 4 for how to download the Customer's software on the TOE:

Table 4: How to download user software

Download user software with downloader blocked configuration		
1	The user provides software for the download into the NVM memory to MEGAHUNT. The software is downloaded to the NVM memory during chip production. There are no user data in the ROM.	The Loader function is blocked by MEGAHUNT after downloading the user software into the NVM memory.
Download user software with downloader valid configuration		
2	The authorized user downloads the software into the NVM memory, and MEGAHUNT has not received user software	The Loader function can be activated or reactivated by the authorized user to download software into the NVM memory. In case the Loader is active, it may be either in life cycle stage "RELEASE" or "DOWNLOAD". When "DOWNLOAD", a mutual authentication needs to be performed before download can be started. In "RELEASE" a valid data block provided by Megahunt needs to be presented to enter "DOWNLOAD" stage.

2.8 Non-TOE Hardware/ Software/ Firmware

The non-TOE hardware/ software/ firmware required by the TOE is the embedded software.

3 Conformance Claim

This chapter is divided into the following sections:

3.1 CC Conformance Claim

This Security Target (ST) and the TOE claim conformance to Common Criteria version v3.1 part 1 [2], part 2 [3] and part 3 [4].

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

Conformance of this ST is claimed for:
Common Criteria part 2 extended and Common Criteria part 3 conformant.

3.2 PP Claim

This Security Target is strict compliant to the Protection Profile:
Security IC Platform Protection Profile, Version 1.0, 13th Jan. 2014, registered and certified by Bundesamtfür Sicherheitinder Informationstechnik (BSI) under the reference BSI-PP-0084.
The short term for this Protection Profile used in this document is “BSI-PP-0084” or “PP”.
Since the Security Target claims conformance to this PP, the concepts are used in the same sense. For the definition of terms refer to the BSI-PP-0084. These terms also apply to this Security Target.
The TOE provides additional functionality, which is not covered in PP. In accordance with Application Note 4 of the BSI-PP-0084, this additional functionality is added using the policy “P.Crypto-Service” (see Section 4.2 of this Security Target for details).

The following additional security functional requirements and cryptographic security services defined in the PP [1] appendix are claimed in this Security Target: The package for TDES Cryptographic from BSI-PP-0084 (chapter 7.4.1) and the Package for AES Cryptographic from BSI-PP-0084 (chapter 7.4.2).
BSI-PP-0084 section 7.3.2 “Package 2: Loader dedicated for usage by authorized users only” is only claimed in case TOE is ordered with downloader valid.
This ST does not claim conformance to any other protection profile.

3.3 Package Claim

This Security Target claims conformance to the assurance package EAL6 augmented. The augmentations to EAL6 are ALC_FLR.1
The assurance level for the TOE is EAL6 augmented with the components ALC_FLR.1.
This assurance level conforms to the Security IC Platform Protection Profile.

3.4 Conformance Claim Rationale

This Security Target claims strict conformance to the Security IC Platform Protection Profile (BSI-PP-0084).
The TOE type defined in this Security Target is secure IC which is consistent with the TOE definition in Security IC Platform Protection Profile.
All sections of this Security Target, in which security problem definition, objectives and security requirements are defined, clearly state which of these items are taken from PP and which are added in this Security Target. Therefore, this is not repeated here. Moreover, all additionally stated items in this Security Target do not contradict the items included from the BSI-PP-0084 (see the respective sections in this document). The operations done for the SFRs taken from PP are also clearly indicated.
The evaluation assurance level claimed for the target (EAL6+) is shown in section 6.2 to include respectively exceed the requirement claimed by the BSI-PP-0084.
These considerations show that the Security Target correctly claims strict conformance to PP.

4 Security Problem Definition

4.1 Description of Assets

The assets of the TOE are all assets described in section 3.1 of the BSI-PP-0084 “Security IC Protection Profile” [1].

4.2 Threats

Since this Security Target claims strict conformance to the BSI-PP-0084 “Security IC Protection Profile” the threats defined in section 3.2 of PP are valid for this Security Target. The threats defined in PP are listed below in Table 5:

Table 5: Threats according to PP [1]

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

The TOE shall avert the threat “Unauthorized Memory or Hardware Access (T.Unauthorized-Access)” as specified below.

T.Unauthorized-Access Unauthorized Memory or Hardware Access

Adverse action: An attacker may try to read, modify or execute code or data stored in restricted memory areas. And or an attacker may try to access or operate hardware resources that are restricted by executing code.

Threat agent: Attacker

Asset: Execution of code, restricted memory areas and hardware resources.

Table 6: Additional threats averted by the TOE

T.Unauthorized-Access	Unauthorized Memory or Hardware Access

4.3 Organizational Security Policies

Since this Security Target claims strict conformance to the BSI-PP-0084 “Security IC Protection Profile” the policy P.Process-TOE “Protection during TOE Development and Production” in PP is applied here as well.

In accordance with Application Note 5 in PP there are two additional policies defined in this Security Target as detailed below.

The TOE provides specific security functionality, which can be used by the Security IC Embedded Software. In the following, specific security functionality is listed, which is not derived from threats identified for the TOE’s environment. It can only be decided in the context of the application against which threats the Security IC Embedded Software will use this specific security functionality.

The IC Developer/Manufacturer therefore applies the policies as specified below:

P.Crypto-Service **Cryptographic services of the TOE**

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

- TDES encryption and decryption
- AES encryption and decryption
- RSA
- EC

The organizational security policy “Controlled usage to Loader Functionality (P.Ctlr_Loader)” applies to Loader dedicated for usage by authorized users only.

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.

4.4 Assumptions

Since this Security Target claims strict conformance to the BSI-PP-0084 “Security IC Protection Profile” the assumptions defined in section 3.4 of PP are valid for this Security Target. The following Table 7 lists these assumptions.

Table 7: Assumption according to PP [1]

Name	**Title**
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalization
A.Resp-Appl	Treatment of User Data

5 Security Objectives

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

5.1 Security Objectives for the TOE

The TOE fulfills the following security objectives, which are taken from PP [1] or newly created.

Table 8: Security Objectives for the TOE

Security Objective (SO)	Description	Security Objective Source
O.Phys-Manipulation	Protection against Physical Manipulation	From PP
O.Phys-Probing	Protection against Physical Probing	From PP
O.Malfunction	Protection against Malfunction	From PP
O.Leak-Inherent	Protection against Inherent Information Leakage	From PP
O.Leak-Forced	Protection against Forced	From PP

	Information Leakage	
O.Abuse-Func	Protection against Abuse of Functionality	From PP
O.Identification	TOE Identification	From PP
O.RND	Random Numbers	From PP
O.TDES	TDES functionality	From PP
O.AES	AES functionality	From PP
O.RSA	RSA functionality	New SO
O.EC	Scalar multiplication for EC	New SO
O.Mem-Access	Area based Memory Access Control	New SO
O.Ctrl_Auth_Loader (Opertional)	Access control and authenticity for the loader	From PP

The security objectives which the category type is “from PP” are defined and described in PP [1] section 4.1 and Annex. The other additional new security objectives are defined based on the functionality provided by the TOE as specified below:

O.RSA RSA functionality

The TOE shall provide cryptographic functionality to perform an RSA encryption and decryption to the Security IC Embedded Software.

O.EC EC functionality

The TOE shall provide cryptographic functionality to perform an EC encryption and decryption to the Security IC Embedded Software.

The TOE shall provide “Area based Memory Access Control (O.Mem-Access)” as specified below.

O.Mem-Access Area based Memory Access Control

Access by processor instructions to Area based resources (memory and hardware resources such as SF Registers) is controlled by the TOE. The TOE decides based on the area access permissions control of the enhanced Memory Protection Unit.

The TOE shall provide “Access control and authenticity for the Loader (O.Ctrl_Auth_Loader)” as specified below.

O.Ctrl_Auth_Loader Access control and authenticity for the Loader

The TSF provides trusted communication channel with authorized user, supports confidentiality protection and authentication of the user data to be loaded and access control for usage of the Loader functionality.

5.2 Security Objectives for the Security IC Embedded Software

The security objectives for the security IC embedded software development environment and the operational environment is defined in PP [1] section 4.2. The table below lists the security objectives.

Table 9: Security objectives for the embedded software according to PP [1]

OE.Resp-Appl	Treatment of User Data of Composite TOE

5.3 Security Objectives for the Operational Environment

The security objectives for the operational environment is defined in PP [1] section 4.3 and section 7.3.2.

Table 10: Security objectives for the operational environment according to PP [1]

OE.Process-Sec-IC	Protection during composite product manufacturing
OE.Loader_Usage (optional)	Secure communication and usage of the Loader

5.4 Security Objectives Rational

Section 4.4 in the BSI-PP-0084 “Security IC Protection Profile” provides a rationale how the assumptions, threats, and organizational security policies are addressed by the objectives that are specified in the BSI-PP-0084. Table 11 reproduces the table in section 4.4 and adds the mapping for P.Lim_Block_Loader from section 7.3.1 of PP [1].

Table 11: Security Objectives versus Assumptions, Threats or Policies

Assumption, Threat or Organizational Security Policy	Security Objective
A.Resp-Appl	OE.Resp-Appl
P.Process-TOE	O.Identification
A.Process-Sec-IC	OE.Process-Sec-IC
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
P.Ctlr_Loader	O.Ctrl_Auth_Loader
	OE.Loader_Usage

The following table provides the justification for the additional security objectives. They are in line with the security objectives of the BSI-PP-0084 and supplement these according to the additional threats and organizational security policies.

Table 12 provides the justification for the additional security objectives. They are in line with the security objectives of PP and supplement these according to the additional assumptions, threat and organizational security policy.

Table 12: Addition Security Objectives versus Assumptions, Threats or Policies

Assumption, Threat or Organizational Security Policy	Security Objective
T.Unauthorized-Access	O.Mem-Access
P.Crypto-Service	O.TDES O.AES O.RSA O.EC

The justification of the additional policy, threat and assumption is given in the following description.

The justification related to the threat “Unauthorized Memory or Hardware Access

(T.Unauthorized-Access)" is as follows:

According to O.Mem-Access the TOE must enforce the partitioning of memory areas so that access to memory areas is controlled. Restrictions are controlled by the hardware or eMPU. Thereby security violations caused by accidental or deliberate access to restricted data (which may include code) can be prevented (refer to T.Unauthorized-Access). The threat T.Unauthorized-Access is therefore countered if the objective is met.

The justification related to the security objectives O.TDES, O.AES, O.RSA and O.EC is as follows: Since these objectives require the TOE to implement exactly the same specific security functionality as required by P.Crypto-Service, the organizational security policy is covered by the objectives.

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

6 Extended Components Definition

There are four extended components defined and described for the TOE:

- 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 at the class FDP User data protection

The extended components FCS_RNG, FMT_LIM FAU_SAS and FDP_SDC are defined and described in the BSI-PP-0084 section 5.

7 Security Requirements

This part of the Security Target defines the detailed security requirements that shall be satisfied by the TOE. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE needs to satisfy in order to meet the security

objectives for the TOE. This chapter consists of the sections “Security Functional Requirements”, “Security Assurance Requirements” and “Security Requirements Rationale”.
The CC allows several operations to be performed on security requirements (on the component level); refinement, selection, assignment, and iteration are defined in paragraph 8.1 of Part 1 of the CC [2]. These operations are used in the PP [1] and in this Security Target, respectively.
The **refinement** operation is used to add details to requirements, and, thus, further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in **bold text** and changed words are crossed out as ~~crossed out text~~.
The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made are denoted by showing as *italic text.*
The **selection** operation is used to select one or more options provided by the PP [1] or CC in stating a requirement. Selections having been made are denoted as *underlined italic*.
The **iteration** operation is used when a component is repeated with varying operations. It is denoted by showing brackets “[iteration indicator]” and the iteration indicator within the brackets.

7.1 TOE Security Functional Requirements

The security functional requirements (SFR) for the TOE are defined and described in PP section 6.1 and in the following description.
The Table 13 provides an overview of the functional security requirements of the TOE, defined in PP [1] section 6.1. In the last column it is marked if the requirement is refined. The refinements are also valid for this ST.

Table 13: Security functional requirements defined in PP

SFR	Title	Refined in PP
FRU_FLT.2	Limited fault tolerance	Yes
FPT_FLS.1	Failure with preservation of secure state	Yes
FMT_LIM.1	Limited capabilities	No
FMT_LIM.2	Limited availability	No

FAU_SAS.1	Audit storage	No
FPT_PHP.3	Resistance to physical attack	Yes
FDP_SDI.2	Stored data integrity monitoring and action	No
FDP_SDC.1	Stored data confidentiality	No
FDP_ITT.1	Basic internal transfer protection	Yes
FPT_ITT.1	Basic internal TSF data transfer protection	Yes
FDP_IFC.1	Subset information flow control	No
FCS_RNG.1	Random Number Generation(Class PTG.2&DRG.3)	No

The components FMT_LIM.1 and FMT_LIM.2 are introduced in PP [1] to define the IT security functional requirements of the TOE as an additional family (FMT_LIM) of the Class FMT (Security Management). This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF.

The Table 14 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 Common Criteria Part 2 [3].

Table 14: Augmented security functional requirements

SFR	Title
FDP_ACC.1	Subset access control-memory access control
FDP_ACF.1	Security attribute based access control-memory 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[TDES]	Cryptographic operation
FCS_COP.1[AES]	Cryptographic operation
FCS_CKM.4[TDES]	Cryptographic key destruction
FCS_CKM.4[AES]	Cryptographic key destruction

FCS_COP.1[RSA]	Cryptographic operation
FCS_COP.1[ECDSA]	Cryptographic operation
FCS_CKM.1[EC]	Cryptographic key generation
FCS_COP.1[ECDH]	Cryptographic operation
FCS_COP.1[ECIES]	Cryptographic operation
FTP_ITC.1[Loader]	Inter-TSF trusted channel - Loader
FDP_UCT.1[Loader]	Basic data exchange confidentiality - Loader
FDP_UIT.1[Loader]	Data exchange integrity - Loader
FDP_ACC.1[Loader]	Subset access control - Loader
FDP_ACF.1[Loader]	Security attribute based access control - Loader

All assignments and selections of the security functional requirements of the TOE are done in PP [1] and in the following description.

The following sections provide extended Security Functional Requirement components, additional application notes and performed operations for the Security Functional Requirements.

7.1.1 Extended Components

The following SFRs are listed due to the assignment and refinement operations that are performed or further application note has to be provided. Other extended SFRs are not copied from the PP [1].

- **FCS_RNG**

To define the security functional requirements of the TOE an additional family (FCS_RNG) of the Class FCS (Cryptographic Support) is defined here. This family describes the functional requirements for the generation of random numbers, which may be used as secrets for cryptographic purpose or authentication.

The TOE shall meet the requirement “Quality metric for random numbers (FCS_RNG.1)” as specified below (Common Criteria Part 2 extended).

FCS_RNG.1[PTG.2] Random Number Generation (Class PTG.2)

Hierarchical to: No other components

Dependencies: No dependencies

Note: The definition of the Security Functional Requirement FCS_RNG.1 has been taken from [5]

Note: The functional requirement FCS_RNG.1 is a selection and assignment of FCS_RNG.1 defined in PP [1] according to [5]

FCS_RNG.1.1[PTG.2] The TSF shall provide a *physical* random number generator which 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.

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.

PTG.2.5: The online test procedure checks the quality of the raw random number sequence. It is triggered continuously. 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 *octets of bits* that meet:

PTG.2.6: Test procedure A 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.

FCS_RNG.1[DRG.3] Random Number Generation (Class DRG.3)

Hierarchical to: No other components

Dependencies: No dependencies

FCS_RNG.1.1[DRG.3] The TSF shall provide a *deterministic* random number generator which implements:

DRG.3.1: If initialized with a random seed using PTRNG of class PTG.2 as random source, the internal state of the RNG shall have 255 bits of entropy.

DRG3.2: The RNG provides forward secrecy.

DRG3.3: The RNG provides backward secrecy even if the current internal state is known.

FCS_RNG.1.2[DRG.3] The TSF shall provide random numbers that meet:

DRG.3.4: The RNG initialized with a random seed using PTRNG of class PTG.2 generates output for which 2^{48} strings of bit length 128 are mutually different with probability $w>1-2^{-32}$.

DRG.3.5: Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A.

- **FAU_SAS**

To define the security functional requirements of the TOE an additional family (FAU_SAS) of the Class FAU (Security Audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

The TOE shall meet the requirement “Audit storage (FAU_SAS.1)” as specified below (Common Criteria Part 2 extended).

FAU_SAS.1 Audit Storage

Hierarchical to: No other components

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide *the test process before TOE Delivery with the capability to store the Initialization Data and/or Pre-personalization Data and/or supplements of the Security IC Embedded Software in the not changeable configuration page area and non-volatile memory.*

7.1.2 Data Integrity

The TOE shall meet the requirement "Stored data integrity monitoring and action (FDP_SDI.2)" as specified below:

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for *inconsistencies between stored data and corresponding EDC* on all objects, based on the following attributes: *EDC value for the RAM, CRAM, NVM and OTP.*

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall *correct the content or trigger an alarm*".

Application note: When detection of an EDC error, the TOE will be in reset or interrupt to CPU.

7.1.3 Data Confidentiality

FDP_SDC.1 Stored data confidentiality

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_SDC.1.1The TSF shall ensure the confidentiality of the information of the user data while it is stored in the *NVM, OTP, CRAM and RAM.*

7.1.4 Malfunctions

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: *exposure to operating conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur.*

Application note: The failures will cause an alarm signals to be triggered, which will result in a special function register bit to be set and a reset (secure state).

Regarding Application Note 15 of the PP [1] generation of additional audit data is not defined for “Limited fault tolerance” (FRU_FLT.2) and “Failure with preservation of secure state” (FPT_FLS.1).

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist *physical manipulation and physical probing* to the *TSF* by responding automatically such that the SFRs are always enforced.

Application note: If a physical manipulation or physical probing attack is detected, an alarm will be automatically triggered by the hardware, which will cause the chip to be reset or generate an interrupt.

7.1.5 Memory Access Control

The security service being provided is described in the Security Function Policy (SFP) Memory Access Control Policy. The security functional requirement “Subset access control (FDP_ACC.1)” requires that this policy is in place and defines the scope were it applies. The security functional requirement “Security attribute based access control (FDP_ACF.1)” defines security attribute usage and characteristics of policies. It describes the rules for the function that implements the Security Function Policy (SFP) as identified in FDP_ACC.1. The decision whether an access is permitted or not is taken based upon attributes allocated to the software. The Smartcard Embedded Software defines the attributes and memory areas. The corresponding

permission control information is evaluated “on the-fly” by the hardware so that access is granted/effective or denied/inoperable.

The following Security Function Policy (SFP) Memory Access Control Policy is defined for the requirement “Security attribute based access control (FDP_ACF.1)”.

7.1.6 Memory Access Control Policy

The TOE shall control read, write and execute accesses of software running at boot mode or different CPU modes (privilege and un-privilege) on data including code stored in memory areas and special function registers. The TOE can also support the enhanced Memory Protection Unit. The eMPU can be used to control access to the memory based on the address.

The TOE shall meet the requirement “Subset access control (FDP_ACC.1)” as specified below.

FDP_ACC.1 Subset access control

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the *Memory Access Control Policy on all subjects: Boot program, privileged and unprivileged program, all objects: defined regions in memory and all the operations: read, write, execute defined in the Memory Access Control Policy.*

The TOE shall meet the requirement “Security attribute based access control (FDP_ACF.1)” as specified below.

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the *Memory Access Control Policy* to objects based on the following*: the subjects access the objects according to the following memory access control rules.*

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 access permission control information of the memory range of the objects during the access to determine whether the accesses can be granted to perform the operation by the subject.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none*

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none*

Application note: The rules of Memory Access Control policy is defined as follows, un-privileged mode serves as the OS's privilege isolation mechanism.

Table 15: Memory Access Control Policy

Subjects / Objects	Boot Program	Privileged Program	Un-Privileged Program
ROM	Read, execute	Not accessible	Not accessible
ROM INFO	Read, execute	Read, execute	Not accessible
CRAM	Read, write	Read, write	Not accessible
RAM	Read, write	Read, write	Read, write
NVM	ES area: Read, execute(after ES is downloaded into this area)	ES area: Read, execute(after ES is downloaded into this area)	Read, execute
	Other area: Read, write, execute	Other area: Read, write, execute	

Subjects / Objects	Boot Program	Privileged Program	Un-Privileged Program
OTP	Chip parameter area: Read / *execute, but no code in this region*	Chip parameter area: Read / *execute, but no code in this region*	Read /*execute, but no code in this region*
	User area: Read, write, execute	User area: Read, write, execute	
Critical register	Read, write	Read, write	Not accessible
Other peripheral registers	Read, write	Read, write	Read, write

The TOE shall meet the requirement "Static attribute initialization (FMT_MSA.3)" as specified below.

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 security roles

FMT_MSA.3.1 The TSF shall enforce the *Memory Access Control Policy* to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow *no subject* to specify alternative initial values to override the default values when an object or information is created.

The TOE shall meet the requirement "Management of security attributes (FMT_MSA.1)" as specified below:

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control or

FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MSA.1.1 The TSF shall enforce the *Memory Access Control Policy* to restrict the ability to *modify* the security attributes *to the privilege level program*.

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components

Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: *The privilege level program shall be able to access the configuration registers of the eMPU.*

7.1.7 Cryptographic Support

FCS_COP.1 Cryptographic operation requires a cryptographic operation to be performed in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard.

The following additional specific security functionality is implemented in the TOE:

- Advanced Encryption Standard (AES)
- Triple Data Encryption Standard (TDES)
- Elliptic Curve Cryptography (EC)
- Rivest-Shamir-Adleman (RSA)

➢ **TDES Operation**

The TDES Operation of the TOE shall meet the requirement “Cryptographic operation (FCS_COP.1)” as specified below.

FCS_COP.1 [TDES] Cryptographic operation-TDES

Hierarchical to: No other components.

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

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 [TDES] The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *TDES in ECB/CBC mode* and cryptographic key sizes *112 bits and 168 bits* that meet the following *NIST SP800-67[7] and NIST SP800-38A[8].*

FCS_CKM.4[TDES] Cryptographic key destruction - TDES

Hierarchical to: No other components.

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

FCS_CKM.4.1[TDES] The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method: *at the end of cryptographic API function, a new random number will be filled in the key register* that meets the following: *none.*

- **AES Operation**

The AES Operation of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1[AES] Cryptographic operation - AES

Hierarchical to: No other components.

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

FCS_COP.1.1[AES] The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *AES in ECB/CBC mode* and cryptographic key sizes *128 bit, 192 bit and 256 bit* that meet the following *FIPS PUB 197 [8] and NIST SP800-38A [7].*

FCS_CKM.4[AES] Cryptographic key destruction - AES

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2

Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1[AES] The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method: *at the end of cryptographic API function, a new random number will be filled in the key register* that meets the following: *none.*

- **Rivest-Shamir-Adleman (RSA) operation**

The Modular Arithmetic Operation of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1[RSA] Cryptographic operation

Hierarchical to: No other components.

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

FCS_COP.1.1[RSA] The TSF shall perform *encryption, decryption* in accordance with a specified cryptographic algorithm *Rivest-Shamir-Adleman (RSA)* and cryptographic key sizes from *1024 to 4096 bits* that meet the following: *RSA standard [9].*

- **Elliptic Curve DSA (ECDSA) operation**

The Modular Arithmetic Operation of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1 [ECDSA] Cryptographic operation

Hierarchical to: No other components.

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

FCS_COP.1.1 [ECDSA] The TSF shall perform *signature generation* and *signature*

verification in accordance with a specified cryptographic algorithm *ECDSA* and cryptographic key sizes *192, 224, 256, 384 and 521 bits* that meet the following *ANSI X9.62-2005 [11] and ANSI X9.63-2011 (R2017) [12]*

- **Elliptic Curve (EC) key generation**

The key generation for the EC shall meet the requirement "Cryptographic key generation (FCS_CKM.1)"

FCS_CKM.1 [EC] Cryptographic key generation

Hierarchical to: No other components.

Dependencies: FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 [EC] The TSF shall perform *key generation* in accordance with *Elliptic Curve EC* cryptographic key sizes *192, 224, 256, 384 and 521 bits* that meet the following *ANSI X9.62-2005 [11] and ANSI X9.63-2011 (R2017) [12]*.

- **Elliptic Curve Diffie-Hellman (ECDH) key agreement**

The Modular Arithmetic Operation of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1 [ECDH] Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, orFDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1[ECDH] The TSF shall perform *elliptic curve Diffie-Hellman key agreement* in accordance with a specified cryptographic algorithm *ECDH* and cryptographic key sizes of *192, 224, 256, 384 and 521 bits* that meet the following *ANSI X9.62-2005 [11] and ANSI X9.63-2011 (R2017) [12]*

- **Elliptic Curve Integrated Encryption Scheme (ECIES) key agreement**

The Modular Arithmetic Operation of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1 [ECIES] Cryptographic operation

Hierarchical to: No other components.

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

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 [ECIES] The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *ECIES* and cryptographic key sizes *192, 224, 256, 384 and 521 bits* that meet the following *ANSI X9.62-2005 [11] and ANSI X9.63-2011 (R2017) [12].*

7.1.8 Packages for Loader

7.1.8.1 Package 2: Loader dedicated for usage by authorized users only (Optional)

The following SFR depend on the configuration of the TOE. In case the Loader is set to be available, the following SFRs describe the use of the Loader.

The TOE Functional Requirement "Inter-TSF trusted channel (FTP_ITC.1)" is specified as follows.

FTP_ITC.1[Loader] Inter-TSF trusted channel - Loader

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1[Loader] The TSF shall provide a communication channel between itself and *Download User, Developer Mode User and Production Mode User* 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[Loader] The TSF shall permit *another trusted IT product* to initiate communication via the trusted channel.

FTP_ITC.1.3[Loader] The TSF shall initiate communication via the trusted channel for deploying Loader *functionality as described in FDP_ACF.1[Loader].*

The TOE Functional Requirement “Basic data exchange confidentiality (FDP_UCT.1)” is specified as follows.

FDP_UCT.1[Loader] Basic data exchange confidentiality - Loader

Hierarchical to: No other components.

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]

FDP_UCT.1.1[Loader] The TSF shall enforce the *Loader SFP* to *receive* user data in a manner protected from unauthorized disclosure.

The TOE Functional Requirement “Data exchange integrity (FDP_UIT.1)” is specified as follows.

FDP_UIT.1[Loader] Data exchange integrity - Loader

Hierarchical to: No other components.

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]

FDP_UIT.1.1[Loader] The TSF shall enforce the *Loader SFP* to *receive* user data in a manner protected from *modification, deletion, insertion* errors.

FDP_UIT.1.2[Loader] The TSF shall be able to determine on receipt of user data, whether *modification, deletion, insertion* has occurred.

The TOE Functional Requirement “Subset access control - Loader (FDP_ACC.1[Loader])” is specified as follows.

FDP_ACC.1[Loader] Subset access control - Loader

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control.

FDP_ACC.1.1[Loader] The TSF shall enforce the Loader SFP on

(1) the subjects *Download User, Developer Mode User, Production Mode User, and Card Operating System,*

(2) the objects user data in *Which contain Life Cycle State, Keys and Memory Segments,*

(3) the operation deployment of Loader

FDP_ACF.1[Loader] Security attribute based access control - Loader

Hierarchical to: No other components.

Dependencies: FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1[Loader] The TSF shall enforce the Loader SFP to objects based on the following:

(1) the subjects *Download User, Developer Mode User, Production Mode User, and Card Operating System* with security attributes: *none*

(2) the objects user data in *Which contain Life Cycle State, Keys and Memory Segments* with security attributes *as listed in Table 16.*

Application note: The following table describes the subjects and objects of the Loader policy.

Table 16: The subjects and objects of the Loader Policy

Identifier	Description
Subjects	
Download User	User Role to update and verify keys, download data, verify data and erase data in memory areas
Developer Mode User	User Role to switch the life cycle to Release.
Production Mode User	User Role to switch the life cycle to Terminate.
Card Operating System	The Card Operating System.
Unauthorized User	An unauthorized user.
Objects as well as related operations and attributes	

Identifier	Description
Life-Cycle State	Life Cycle State of the Loader. The only available operation is: • Switch - Switch from Download to Release, from Release to Download or from Download to Terminate. The available attributes of Life Cycle State are: • Download - Initial Life-Cycle State of the TOE which allows download operations. • Release - Previously downloaded code can be executed. Furthermore, it is possible to return to Life-Cycle State Download. • Terminate - Final state of the Loader after permanent blocking. No download operations can be performed anymore. It is not possible to switch back to another state of the Life-Cycle State.
Keys	Cryptographic keys used to identify users. The only available operation is: • Update - Update or verify a key. The only attribute is: • Permissions - Permissions associated with one key to identify subjects.

Identifier	Description
Memory Segments	Memory segments to which data or code can be downloaded. The available operations are: • Download - Download data to a memory segment. • Verify - Verifies the data downloaded to a memory segment. • Erase - Erase data within a memory segment. No attributes available.
User Data	User Data to be stored to, verified in, or removed from Memory Segments. Operations are already covered by the object Memory Segments.

FDP_ACF.1.2[Loader] The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

(1) *The Developer Mode User is allowed to switch the Life Cycle State from Download to Release.*

(2) *The Production Mode User is allowed to switch the Life Cycle State from Download to Terminate.*

(3) *The Card Operating System is allowed to switch the Life Cycle State from Release to Download.*

FDP_ACF.1.3[Loader] The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

(1) *The Download User is allowed to Download, Erase, and Verify Memory Segments if Life Cycle State Download grants this right.*

(2) *The Download User is allowed to update the keys*

Permissions of Keys if Life Cycle State Download grants this right.

FDP_ACF.1.4[Loader] The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *as stated in SFR FMT_LIM.2[Loader]*.

7.2 TOE Security Assurance Requirements

The evaluation assurance level is EAL6 augmented with ALC_FLR.1. In the following Table 17, the security assurance requirements are given.

Table 17: Assurance components

Aspect	**Acronym**	**Description**
Development	ADV_ARC.1	Security Architecture design
	ADV_FSP.5	Functional specification
	ADV_IMP.2	Implementation representation
	ADV_INT.3	TSF internals
	ADV_SPM.1	Formal model of Security Policies
	ADV_TDS.5	TOE design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support	ALC_CMC.5	CM capabilities
	ALC_CMS.5	CM scope
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Development security
	ALC_LCD.1	Life-cycle definition
	ALC_TAT.3	Tools and techniques
	ALC_FLR.1	Basic flaw remediation
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
Tests	ATE_COV.3	Analysis of coverage
	ATE_DPT.3	Depth
	ATE_FUN.2	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.5	Advanced methodical vulnerability testing

- **ADV_SPM**

The developer shall provide a formal security policy model.

ADV_SPM.1 Formal TOE security policy model

Hierarchical to: No other components.

Dependencies: ADV_FSP.4 Complete functional specification.

ADV_SPM.1.1D The developer shall provide a formal security policy model for the *Access Control Policy (FDP_ACC.1, FDP_ACF.1 with the associated dependencies).*

7.3 Security Requirements Rationale

7.3.1 Rationale for the Security Functional Requirements

The security functional requirements rationale of the TOE is defined and described in PP section 6.3 for the following security functional requirements: FDP_ITT.1, FDP_IFC.1, FPT_ITT.1, FPT_PHP.3, FDP_SDI.2, FDP_SDC.1, FPT_FLS.1, FRU_FLT.2, FMT_LIM.1, FMT_LIM.2, FCS_RNG.1, and FAU_SAS.1. In PP section 7.3.2 the rational for the following Security Functional Requirements are provided: FTP_ITC.1[Loader], FDP_UCT.1[Loader], FDP_UIT.1[Loader], FDP_ACC.1[Loader], FDP_ACF.1[Loader].

The security functional requirements FDP_ACC.1, FDP_ACF.1, FCS_COP.1, FCS_CKM.1 and FCS_CKM.4 are defined in the following description:

Table 18: Rational for Additional Security Functional Requirements in the ST

Objective	**TOE Security Functional Requirements**
O.TDES	- FCS_COP.1[TDES] “Cryptographic operation” - FCS_CKM.4[TDES] “Cryptographic key destruction”
O.AES	- FCS_COP.1[AES] “Cryptographic operation” - FCS_CKM.4[AES] “Cryptographic key destruction”
O.RSA	- FCS_COP.1[RSA] “Cryptographic operation”
O.EC	- FCS_CKM.1[EC] “Cryptographic key generation” - FCS_COP.1[ECDSA] “Cryptographic operation” - FCS_COP.1[ECDH] “Cryptographic operation” - FCS_COP.1[ECIES] “Cryptographic operation”
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.Ctrl_Auth_Loader	- FTP_ITC.1[Loader] “Inter-TSF trusted channel” - FDP_UCT.1[Loader] “Basic data exchange confidentiality” - FDP_UIT.1[Loader] “Data exchange integrity” - FDP_ACC.1[Loader] “Subset access control” - FDP_ACF.1[Loader] “Security attribute based access control”

The table above gives an overview, how the security functional requirements are combined to meet the security objectives. The detailed justification is given in the following:

The security functional requirement(s) “Cryptographic operation (FCS_COP.1)” exactly requires those functions to be implemented which are demanded by O.TDES, O.AES, O.EC and O.RSA. Therefore, FCS_COP.1 is suitable to meet the security objective.

The usage of cryptographic algorithms requires the use of appropriate keys. Otherwise these

cryptographic functions do not provide security. The keys have to be unique with a very high probability, and must have a certain cryptographic strength etc. In case of a key import into the TOE (which is usually after TOE delivery) it has to be ensured that quality and confidentiality are maintained. Keys for TDES, AES, RSA and EC are provided by the environment. In this ST the objectives for the environment OE.Resp-Appl have been clarified. The Smartcard Embedded Software defines the use of the cryptographic functions FCS_COP.1 provided by the TOE. The requirements for the environment FDP_ITC.1, FDP_ITC.2, FCS_CKM.1 and FCS_CKM.4 support an appropriate key management. These security requirements are suitable to meet OE.Resp-Appl.

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

The security functional requirement “Subset access control (FDP_ACC.1)” with the related Security Function Policy (SFP) “Memory Access Control Policy” exactly require the implementation of an area based memory access control as required 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 implementation of these functional requirements is represented by the dedicated privilege level concept.

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. Moreover, these additional security functional requirements cover the requirements by CC part 2 [3] user data protection of chapter 11 which are not refined by the PP [1].

Nevertheless, the developer of the Smartcard Embedded Software must ensure that the additional functions are used as specified and that the User Data processed by these functions are protected as defined for the application context. The TOE only provides the tool to implement the policy defined in the context of the application.

7.3.2 Dependencies of Security Functional Requirements

The dependence of security functional requirements is defined and described in PP section 6.3.2 for the following security functional requirements: FDP_ITT.1, FDP_IFC.1, FPT_ITT.1, FPT_PHP.3, FDP_SDI.2, FDP_SDC.1, FPT_FLS.1, FRU_FLT.2, FCS_RNG.1 and FAU_SAS.1.

The dependence of security functional requirements for the security functional requirements FDP_ACC.1, FDP_ACF.1, FCS_COP.1, FMT_MSA.3, FMT_MSA.1, FMT_SMF.1, FCS_CKM.4 and FDP_SDI.2 is defined in the following description.

Table 19: Dependency for cryptographic operation requirement

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FCS_COP.1[TDES]	FCS_CKM.1	No, see comment 2
	FDP_ITC.1or FDP_ITC.2 (if not FCS_CKM.1) FCS_CKM.4	No, see comment 2 Yes, CKM.4[TDES]
FCS_COP.1[AES]	FCS_CKM.1	No, see comment 2
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) FCS_CKM.4	No, see comment 2 Yes, CKM.4[AES]
FCS_CKM.4[TDES]	FCS_CKM.1	No, see comment 2
	FDP_ITC.1or FDP_ITC.2 (if not FCS_CKM.1)	No, see comment 2
FCS_CKM.4[AES]	FCS_CKM.1	No, see comment 2
	FDP_ITC.1 or FDP_ITC.2 (if not	No, see comment 2

	FCS_CKM.1)	
FCS_COP.1[RSA]	FCS_CKM.1	No, see comment 2
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) FCS_CKM.4	No, see comment 2
FCS_COP.1[ECDSA]	FCS_CKM.1	Yes, FCS_CKM.1[EC]
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) FCS_CKM.4	No, see comment 2
FCS_COP.1[ECDH]	FCS_CKM.1	Yes, FCS_CKM.1[EC]
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) FCS_CKM.4	No, see comment 2
FCS_COP.1[ECIES]	FCS_CKM.1	Yes, FCS_CKM.1[EC]
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) FCS_CKM.4	No, see comment 2
FCS_CKM.1[EC]	FCS_CKM.2 or FCS_COP.1	Yes,FCS_COP.1[ECDSA], FCS_COP.1[ECDH], FCS_COP.1[ECIES]
	FCS_CKM.4	No, see comment 2
FTP_ITC.1[Loader]	None	N/A
FDP_UCT.1[Loader]	FTP_ITC.1 or FTP_TRP.1 FDP_ACC.1 or	

	FDP_IFC.1	
FDP_UIT.1[Loader]	FDP_ACC.1 or FDP_IFC.1 FTP_ITC.1 or FTP_TRP.1	
FDP_ACC.1[Loader]	FDP_ACF.1	Yes, FDP_ACF.1[Loader]
FDP_ACF.1[Loader]	FDP_ACC.1 FMT_MSA.3	Yes, FDP_ACC.1[Loader]
FDP_ACC.1	FDP_ACF.1	Yes, FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Yes, FDP_ACC.1 Yes, FMT_MSA.3
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes, FMT_MSA.1 No, see comment 1
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes, FDP_ACC.1 No, see comment 1 Yes, FMT_SMF.1
FMT_SMF.1	None	N/A
FDP_SDI.2	None	N/A

Comment 1:

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 but enforced for each subject. Therefore, there is no need to identify roles in form of a security functional requirement FMT_SMR.1.

End of Comment

Comment 2:

The security functional requirement “Cryptographic operation (FCS_COP.1)” met by the TOE have the following 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

For the security functional requirements FCS_COP.1[TDES] and FCS_COP.1[AES], the respective dependencies FCS_CKM.1, FDP_ITC.1 and FDP_ITC.2 have to be fulfilled by the environment. That means, that the environment shall meet the requirements FCS_CKM.1 as defined in CC part 2, section 10.1 and shall meet the requirements FDP_ITC.1 or FDP_ITC.2 as defined in CC part 2, section 11.7. The TOE also fulfills FCS_CKM.4[TDES] and FCS_CKM.4[AES]

For the security functional requirements FCS_CKM.4[TDES] and FCS_CKM.4[AES], the respective dependencies FCS_CKM.1, FDP_ITC.1 or FDP_ITC.2 have to be fulfilled by the environment. That means, that the environment shall meet the requirements FCS_CKM.1 as defined in CC part 2, section 10.1 or shall meet the requirements FDP_ITC.1 or FDP_ITC.2 as defined in CC part 2, section 11.7.

For the security functional requirement FCS_COP.1[RSA], FCS_COP.1[ECDSA], FCS_COP.1[ECDH] and FCS_COP.1[ECIES], the respective dependencies FDP_ITC.1, FDP_ITC.2 have to be fulfilled by the environment. That mean, that the environment shall meet the requirements FDP_ITC.1 or FDP_ITC.2 as defined in CC part 2, section 11.7.

For the security functional requirement FCS_COP.1[RSA], FCS_COP.1[ECDSA], FCS_COP.1[ECDH], FCS_COP.1[ECIES] and FCS_CKM.1[EC], the respective dependencies FCS_CKM.4 have to be fulfilled by the environment. That mean, the environment shall meet the requirements FCS_CKM.4 as defined in CC part 2, section 10.1.

For the security functional requirements FCS_COP.1[RSA], the respective dependencies FCS_CKM.1 have to be fulfilled by the environment. For the security requirement FCS_COP.1[ECDSA], FCS_COP.1 [ECDH] and FCS_COP.1[ECIES] the respective dependency FCS_CKM.1 has to be fulfilled by the TOE with the security functional requirement FCS_CKM.1[EC] (for FCS_COP.1[ECDSA], FCS_COP.1 [ECDH] and FCS_COP.1 [ECIES]) as defined in section 7.1.7.

End of Comment

7.3.3 Rationale of the Assurance Requirements

The chosen assurance level EAL6 and the augmentation with the requirements ALC_FLR.1 were chosen in order to meet the assurance expectations explained in the following paragraphs. In Table 17: Assurance components the different assurance levels are shown as well as the augmentations. The augmentations are in compliance with the Protection Profile.

The rationale for the augmentations is the same as in the PP. The assurance level EAL6 is an elaborated pre-defined level of the CC, part 3 [4]. The assurance components in an EAL level are chosen in a way what they build a mutually supportive and complete set of components. The requirements chosen for augmentation do not add any dependencies, which are not already fulfilled for the corresponding requirements contained in EAL6. Therefore, these components add additional assurance to EAL6, but the mutual support or requirements is still guaranteed. Therefore, the augmentation with the requirement ALC_FLR.1 were chosen in order to meet the assurance expectations explained in the following paragraphs.

ALC_FLR.1 Basic flaw remediation

Flaw remediation requires that discovered security flaws be tracked and corrected by the developer. Although future compliance with flaw remediation procedures cannot be determined at the time of the TOE evaluation, it is possible to evaluate the policies and procedures that a developer has in place to track and correct flaws, and to distribute the flaw information and corrections.

ALC_FLR.1 has no dependencies.

7.3.4 Security Requirements are internally Consistent

For this chapter the PP [1] section 6.3.4 can be applied completely.

In addition to the discussion in section 6.3 of PP [1] the security functional requirement FCS_COP.1 is introduced. 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.

The implemented level concept represents the area based memory access protection enforced by the TOE or eMPU. 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.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Mem-Access 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 requirement FDP_SDI.2.1 allows detection of integrity errors of data stored in memory. FDP_SDI.2.2 in addition allows correction of one bit errors or taking further action. Both meet the security objective O.Malfunction. The requirements FRU_FLT.2, FPT_FLS.1, and FDP_ACC.1 which also meet this objective are independent from FDP_SDI.2 since they deal with the observation of the correct operation of the TOE and not with the memory content directly.

8 TOE summary specification

The TOE is equipped with following Security Features to meet the security functional requirements:

- SF_PM：Protection against Malfunction
- SF_PP：Physical Protection
- SF_PF：Prevent abuse of Functionality
- SF_RNG：Random Number Generator
- SF_CS：Cryptographic Support

- SF_MAC: Memory Access Control
- SF_PL: Protection against Leakage

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

8.1 SF_PM: Protection against Malfunction

Malfunctioning relates to the security functional requirements FRU_FLT.2, FPT_FLS.1 and FDP_SDI.2. The TOE meets these SFRs by a group of Security Functions (SFs) that guarantee correct operation of the TOE.

SFR	Security Feature	Security Function(SFs)
FRU_FLT.2 FPT_FLS.1	SF_PM: Protection against Malfunction	Temperature detection (SF1)
		Glitch detection (SF2)
		Voltage Detection (SF3)
		Internal Frequency Detection (SF4)
		Light detection (SF5)
FDP_SDI.2		Error Correction
		Error Detection (Parity check)

If one of the detectors or mechanisms detects an alarm event, the TOE will enter reset state or trigger an exception and return error message to the security IC embedded software to make sure a secure situation.

FPT_FLS.1: Failure with preservation of secure state

Failures such as frequency, voltage, temperature, light and power glitch that are out of the special range are detected by TOE's detectors. The failures will cause an alarm signals to be triggered, which will result in a special function register bit to be set and a reset or an exception (secure state).

FRU_FLT.2: Limited fault tolerance

In order to prevent malfunction, the operation signals (clock, reset, supply voltage) are

filtered/regulated. The detectors that prevent noise, glitches in the external reset pad and prevent extremely high/low internal clock frequency are implemented in the hardware.

FDP_SDI.2: Stored data integrity monitoring and action

The data stored in memory with checksum code using cyclic redundancy check algorithm to verify the stored data integrity. The check algorithm is valid in the memory areas including: NVM, RAM and CRAM.

The TOE is equipped with an error detection code (EDC) for protecting RAM, CRAM and the NVM. Thus introduced failures are securely detected. For RAM, CRAM and NVM, in case of any bit errors detected, a security alarm is triggered.

8.2 SF_PP: Physical Protection

Physical Protection relates to the security functional requirements FPT_PHP.3, FDP_SDI.2 and FDP_SDC.1. The TOE meets this SFR by implementing security features that provides physical protection against physical probing and manipulation.

SFR	Security Feature	Security Function(SFs)
FPT_PHP.3 FDP_SDC.1 FDP_SDI.2	SF_PP: Physical Protection	Active shielding (SF6)
		Memory encryption
		Error Correction
		Error Detection (Parity check)
		CRAM Bus encryption

If a physical manipulation or physical probing attack is detected, an alarm will be automatically triggered by the hardware, which will cause the chip to be reset or generate an interrupt.

FPT_PHP.3: Resistance to physical attack

This requirement focuses on the security features when the active shield is manipulated so that the features prevent the TOE from physical intrusive attacks. The TOE resets or generates an interrupt once the physical manipulations or physical probing attacks are detected.

Synthesizable processor core with glue logic makes reverse engineering and signal

identification unpractical.

Memory encryption and CRAM bus encryption prevent memory and address/data buses from probing attacks. Moreover, routing the sensitive signals such as alarm signals or buses in middle layer is effective.

FDP_SDC.1: Stored data confidentiality

All memories present on the TOE (NVM, OTP, CRAM and RAM) are encrypted using individual keys assigned by complex key management. In case of security critical error, a security alarm is generated and the TOE ends up in a secure state. All of the data that stored within memory areas are encrypted, thus the attacker can only get the cipher-text data. The encrypt algorithm is not publicity. The address of the stored data is also encrypted, so it is very difficult to get the stored data by the attacker.

The data on the CRAM bus is encrypted, which can prevent the plaintext data on the bus from being observed.

FDP_SDI.2: Stored data integrity monitoring and action

The data stored in memory with checksum code to verify the stored data integrity. The check algorithm is valid in the memory areas including: NVM, System RAM.

The TOE is equipped with an error detection code (EDC) for protecting RAM and the NVM. For NVM in case of more than one bit errors and for RAM in case of any bit errors detected, a security alarm is triggered.

8.3 SF_PF: Prevent abuse of Functionality

Prevent abuse of Functionality relates to the security requirements FMT_LIM.1, FMT_LIM.2, FAU_SAS.1. The TOE meets these SFRs by implementing a complicated test mode and download mode control mechanism that prevents abuse of test functionality delivered as part of the TOE and the download functionality after it is blocked.

SFR	Security Feature	Security Function(SFs)
FMT_LIM.1 FMT_LIM.2	SF_PF: Protection abuse of Functionality	Test mode protection (SF7)

FAU_SAS.1		
FTP_ITC.1[Loader] FDP_UCT.1[Loader] FDP_UIT.1[Loader] FDP_ACC.1[Loader] FDP_ACF.1[Loader]		Secure boot and secure download (SF17)

FAU_SAS.1: Audit storage

The manufacturing data written into the OTP area once the TOE is set from test mode to application mode.

The chip identification data (O.Identification) and TOE configuration data are also stored in the OTP area. In addition, user initialization data can be stored in the non-volatile memory during the production phase as well. During this first data programming, the TOE is still in the secure environment and in Test Mode.

FMT_LIM.1: Limited capabilities

The access to the test mode is limited. Furthermore, once the TOE is switched to application mode, the test mode is unavailable any more.

In addition, during start-up of the TOE the decision for one of the various operation modes is taken dependent on phase identifiers. The phase identifiers are stored in the OTP, the sequence of the phases is protected by the one-time program characteristics. The phase cannot be rolled back.

FMT_LIM.2: Limited availabilities

The access to the test mode is limited. Furthermore, once the TOE is switched to application mode, the test mode is unavailable any more. Only under test mode, functional test is able to be conducted.

FTP_ITC.1[Loader]: Inter-TSF trusted channel – Loader

Trusted channel for using the loader.

FDP_UCT.1[Loader]: Basic data exchange confidentiality – Loader

Protect from unauthorized disclosure.

FDP_UIT.1[Loader]: Data exchange integrity – Loader

Protect from modification, deletion, insertion.

FDP_ACC.1[Loader]: Subset access control – Loader

Defines on which Subjects and Objects the Loader SFP is applied.

FDP_ACF.1[Loader]: Security attribute based access control – Loader

Defines the Loader SFP.

8.4 SF_RNG: Random Number Generator

Random Numbers Generator relate to the security requirement FCS_RNG.1. The TOE meets this SFR by providing true random number generator (TRNG).

SFR	Security Feature	Security Function(SFs)
FCS_RNG.1	SF_RNG: Random Number Generator	Random Number Generator (SF8)

FCS_RNG.1: Random number generator

True Random Number Generator algorithm that follows the requirements and the metric of the AIS20 Class PTG.2 standard and the Deterministic Random Number Generator algorithm that follows the requirements and the metric of the AIS20 Class DRG.3 standard.

Random data is essential for cryptography as well as for security mechanisms. The TOE is equipped with a physical True Random Number Generator (TRNG, FCS_RNG.1). The random data can be used for the Smartcard Embedded Software and is also used for the security features of the TOE, like masking. The TRNG implement self-testing features. The TRNG and DRNG fulfill the requirements from the functionality class PTG.2 and DRG.3 of [5].

8.5 SF_CS: Cryptographic Support

Cryptographic Support relates the security requirements FCS_COP.1[TDES], FCS_COP.1[AES], FCS_COP.1[RSA], FSC_COP.1[ECDSA], FCS_COP.1[ECDH], FCS_COP.1[ECIES], FCS_CKM.1[EC], FCS_CKM.4[TDES] and FCS_CKM.4[AES]. The TOE meets these SFRs by providing cryptographic functionality by means of a combination of accelerating hardware and IC dedicated support software.

SFR	Security Feature	Security Function(SFs)
FCS_COP.1[TDES] FCS_CKM.4[TDES]	SF_CS: Cryptographic Support	TDES (SF9)
FCS_COP.1[AES] FCS_CKM.4[AES]		AES (SF10)
FCS_COP.1[RSA]		RSA (SF12) (Encryption, Decryption, Signature Generation and Verification)
FCS_CKM.1[EC] FCS_COP.1[ECIES] FCS_COP.1[ECDH] FSC_COP.1[ECDSA]		Elliptic Curves (SF11) (Key Generation, Encryption, Decryption, Signature Generation and Verification, Asymmetric Key Agreement)

8.5.1 TDES Function

The TOE supports the encryption and decryption in accordance with the specified cryptographic algorithm Triple Data Encryption Standard (TDES) in the Electronic Codebook Mode (ECB), Cipher Block Chaining Mode (CBC), and with cryptographic key sizes of 112 bit and 168 bit meeting the standard: NIST SP800-67[6], NIST SP800-38A [7].

The covered security functional requirements are FCS_COP.1 [TDES]

This SFR is implemented by using the interface of the CL. This library contains additional countermeasures.

Note: The TOE is delivered with the TDES CL library. The TDES CL library contains hardened TDES algorithms. The CL library needs an accessible SCP.

8.5.2 AES Function

The TSF supports the encryption and decryption in accordance with the specified cryptographic

algorithm Advanced Encryption Standard (AES) in the Electronic Codebook Mode (ECB), Cipher Block Chaining Mode (CBC) and cryptographic key sizes of 128 bit or 192 bit or 256 bit according to the standard: FIPS PUB 197 [8] and NIST SP800-38A [7].

The covered security functional requirement is FCS_COP.1[AES].

This TSF is implemented by using the interface of the CL. This library contains additional countermeasures.

Note: The TOE is delivered with the AES CL library. The AES CL library contains hardened AES algorithms. The AES library needs an accessible SCP.

8.5.3 RSA Function

The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm Rivest-Shamir-Adleman (RSA) and cryptographic key sizes 1024- 4096 bits that meet the following standards:

- Encryption:

According to section 5.1.1 RSAEP in PKCS v2.2 RFC8017 [9].

- Decryption (with or without CRT):

According to section 5.1.2 RSADP in PKCS v2.2 RFC8017 [9], for u = 2, i.e., without any (r_i, d_i, t_i), i >2, therefore without 5.1.2 (2.b) (ii)&(v), without 5.1.2 (1), 5.1.2 (2.a) only supported up to $n < 2^{4096}$.

- Signature Generation (with or without CRT):

According to section 5.2.1 RSASP1 in PKCS v2.2 RFC8017 [9], for u = 2, i.e., without any (r_i, d_i, t_i), i >2, therefore without 5.2.1 (2.b) (ii)&(v), without 5.2.1 (1), 5.2.1 (2.a) only supported up to $n < 2^{4096}$.

- Signature Verification:

According to section 5.2.2 RSAVP1 in PKCS v2.2 RFC8017 [9], without 5.2.2 (1).

The covered security functional requirement is FCS_COP.1[RSA].

Note: The TOE can also be delivered with the Cryptographic library. The Cryptographic library contains the RSA algorithms stated above. The RSA library needs an accessible PKE. If the library is not delivered, then this SFR is not applicable.

8.5.4 Elliptic Curves

The certification covers the standard NIST [12] and Brain pool [13] Elliptic Curves with key lengths of 192, 224, 256, 384 and 521 Bits, due to national AIS32 regulations by the BSI. Note that there are numerous other curve types, being also secure in terms of side channel attacks on this TOE, which can the user optionally add in the composition certification process.

8.5.4.1 Signature Generation and Verification

The TSF shall perform signature generation and signature verification in accordance with a specified cryptographic algorithm ECDSA and cryptographic key sizes 192, 224, 256, 384 and 521 that meet the following standard:

- Signature Generation:

  According to section 7.3 in ANSI X9.62 – 2005 [10]:

  Not implemented is step d) and e) thereof.

  The output of step e) has to be provided as input to our function by the caller.

  Deviation of step c) and f):

  The jumps to step a) were substituted by a return of the function with an error code, the jumps are emulated by another call to our function.

- Signature Verification:

  According to section 7.4.1 in ANSI X9.62–2005 [10]:

  Not implemented is step b) and c) thereof.

  The output of step c) has to be provided as input to our function by the caller.

  Deviation of step d):

  Beside noted calculation, our algorithm adds a random multiple of the group order n to the calculated values u1 and u2.

  The covered security functional requirement is FCS_COP.1[ECDSA].

  Note: The TOE can also be delivered with the Crypto library. The Crypto library contains the EC algorithms stated above. The EC library needs an accessible PKE. If the EC library is not delivered, then this TSF is not provided.

8.5.4.2 Asymmetric Key Generation

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Elliptic Curve EC specified in ANSI X9.62-2005[10] and specified cryptographic key sizes 192, 224, 256, 384 and 521 bits that meet the following standard:

- ECDSA Key Generation:

  According to the appendix A4.3 in ANSI X9.62-2005 [10] the co factor h is not supported.

  The covered security functional requirement is FCS_CKM.1[EC].

  Note: The TOE can also be delivered with the Crypto library. The Crypto library contains the EC algorithms stated above. The Crypto library needs an accessible PKE. If the Crypto library is not delivered, then this TSF is not provided.

8.5.4.3 Asymmetric Key Agreement

The TSF shall perform elliptic curve Diffie-Hellman key agreement in accordance with a specified cryptographic algorithm ECDH and cryptographic key sizes 192, 224 256, 384 and 521 bits that meet the following standard:

According to section 5.4.1 in X9.63–2011(R2017) [11] unlike section 5.4.1.3 our implementation not only returns the x-coordinate of the shared secret, but rather the x-coordinate and y-coordinate.

The covered security functional requirement is FCS_COP.1[ECDH].

Note: The TOE can also be delivered with the Crypto library. The Crypto library contains the EC algorithms stated above. The Crypto library needs an accessible PKE. If the Crypto library is not delivered, then this TSF is not provided.

8.5.4.4 Encryption and Decryption

The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm ECIES and cryptographic key sizes 192, 224, 256, 384 and 521 bits that meet the following standard:

- Encryption:

According to section 5.8.1 in ANSI X9.63–2011(R2017) [11]:

In step 5) and step 8) we select sha-256 as hash function which used in key derivation function and MAC scheme.

- Decryption:

According to section 5.8.2 in ANSI X9.63–2011(R2017) [11]:

In step 5) and step 8) we select sha-256 as hash function which used in key derivation function and MAC scheme.

The covered security functional requirement is FCS_COP.1[ECIES].

Note: The TOE can also be delivered with the Crypto library. The Crypto library contains the EC algorithms stated above. The EC library needs an accessible PKE. If the EC library is not delivered, then this TSF is not provided.

8.6 SF_MAC: Memory Access Control

Memory Access Control relates the security requirements FDP_ACC.1, FDP_ACF.1, FMT_MSA.3, FMT_MSA.1 and FMT_SMF.1.

SFR	Security Feature	Security Function(SFs)
FDP_ACC.1 FDP_ACF.1 FMT_MSA.3 FMT_MSA.1 FMT_SMF.1	SF_MAC: Memory Access Control	Memory access control(SF13)

FDP_ACC.1: Subset access control

The TOE implement the Memory Access Control Policy on all subjects: Boot program, privileged and unprivileged program, all objects: defined regions in memory and all the operations: read, write, execute defined in the Memory Access Control Policy.

FDP_ACF.1: Security attributes based access control

The main memory access control rules are summarized below: ROM is hidden after the completion of Boot program execution, and that prevent the embedded software to access the Security Boot Loader (SBL), CRAM can only be accessed in privileged mode; The critical

register can only be accessed in privileged mode; Table 15 provides the complete access control rules.

FMT_MSA.3: Static attributes initialization

In addition, during each start-up of the TOE the address ranges and access rights are initialized by the Security Boot Loader (SBL) with predefined values.

FMT_MSA.1: Management of security attributes

During operation within a phase the accesses to memories are granted by the eMPU controlled access rights and related levels.

FMT_SMF.1: Specification of Management Functions

The TOE clearly defines that *the privilege level program shall be able to access the configuration registers of the eMPU*.

8.7 SF_PL: Protection against Leakage

Protection against Leakage relates the security requirements FDP_ITT.1, FDP_IFC.1 and FPT_ITT.1. The TOE meets these SFRs by implementing several measures that provides logical protection against leakage.

SFR	Security Feature(SF)	Security Function(SFs)
FDP_ITT.1 FDP_IFC.1 FPT_ITT.1	SF_PL: Protection against Leakage	Bus encryption
		Bus Polarity switching
		Memory encryption
		CPU uniform instruction timing (SF14)
		CPU random branch insertion (SF16)
		Cryptographic clock randomization(SF15)

FDP_IFC.1: Subset information flow control

FDP_ITT.1: Basic internal transfer protection

FPT_ITT.1: Basic internal TSF data transfer protection

The combination of TOE features listed below achieves the effective protection of access to the internal signals.

- Address scrambling for memory
- Memory encryption
- Bus polarity switching
- Bus encryption

And the following security functions are available for ES to further prevent data leakage:

- CPU random branch insertion
- Crypto clock randomization

8.8 Assignment of Security Functional Requirements to TOE's Security Functionality

The justification and overview of the mapping between security functional requirements (SFR) and the TOE's security functionality (SF) is given in sections the sections above. The results are shown in Table 20. The security functional requirements are addressed by at least one relating security feature. The various functional requirements are often covered manifold. As described above the requirements ensure that the TOE is checked for correct operating conditions and if a not correctable failure occurs that a stored secure state is achieved, accompanied by data integrity monitoring and actions to maintain the integrity although failures occurred. An overview is given in following table:

Table 20: Mapping of SFR and Security Feature

SFR	SF_PM	SF_PP	SF_PF	SF_RNG	SF_CS	SF_MAC	SF_PL
FAU_SAS.1			√				
FMT_LIM.1			√				
FMT_LIM.2			√				
FDP_ACC.1						√	
FDP_ACF.1						√	
FTP_ITC.1[Loader]			√				
FDP_UCT.1[Loader]			√				
FDP_UIT.1[Loader]			√				

FDP_ACC.1[Loader]			√				
FDP_ACF.1[Loader]			√				
FPT_PHP.3		√					
FDP_ITT.1							√
FDP_SDC.1		√					
FDP_SDI.2	√	√					
FDP_IFC.1							√
FMT_MSA.1						√	
FMT_MSA.3						√	
FMT_SMF.1						√	
FRU_FLT.2	√						
FPT_ITT.1							√
FPT_FLS.1	√						
FCS_RNG.1				√			
FCS_COP.1[TDES]					√		
FCS_CKM.4[TDES]					√		
FCS_COP.1[AES]					√		
FCS_CKM.4[AES]					√		
FCS_COP.1[RSA]					√		
FCS_COP.1[ECDSA]					√		
FCS_COP.1[ECDH]					√		
FCS_COP.1[ECIES]					√		
FCS_CKM.1[EC]					√		

9 Bibliography

[1] Security IC Platform Protection Profile, Version 1.0, 13th Jan. 2014, registered and certified by Bundesamtfür Sicherheitinder Informationstechnik (BSI) under the reference BSI-PP-0084

[2] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model; Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

[3] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements; Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[4] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements; Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[5] Functionality classes and evaluation methodology for deterministic/physical random

number generators, version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik
[6] 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 SP800-67, Revision 1.1, revised January 2012
[7] National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce, Recommendation for Block Cipher Modes of Operation, NIST SP800-38A, December 2001
[8] U.S. Department of Commerce / National Bureau of Standards, Advanced Encryption Standard (AES), FIPS PUB 197, 2001, November 26.
[9] PKCS #1: RSA Cryptography Specifications Version 2.2, 2016
[10] American National Standard for Financial Services ANSI X9.62-2005, Public Key Cryptography for the Financial Services Industry, the Elliptic Curve Digital Signature Algorithm (ECDSA), November 16, 2005, American National Standards Institute
[11] American National Standard for Financial Services ANSI X9.63-2011 (R2017), Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, February10, 2017, American National Standards Institute
[12] NIST FIPS PUB 186-4 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION Digital Signature Standard (DSS) July 2013
[13] RFC 5639: Elliptic Curves Cryptography (ECC) Brain pool Standard Curves and Curve Generation March 2010

10 Glossary

10.1 End-user

User of the composite product in phase 7.

10.2 IC Dedicated Software

IC dedicated software which is normally recognized as IC firmware, is developed by IC

developer and embedded in a security IC. The IC dedicated software is mainly used for testing purpose (IC dedicated test software) but may provide additional services to facilitate usage of the hardware and/or to provide additional services (IC dedicated support software).

10.3 NVR

NVR is the abbreviation of Nov-Volatile Register, which is implemented by a special block of NVM. The special block of NVM will not occupy the address space which user can see.

10.4 Security IC

Composition of TOE, the security IC embedded software, user data and package (the security IC carrier).

10.5 Security IC Embedded Software

Security IC embedded software supplies the security IC application and standard services and normally is developed other than IC designer. The embedded software is designed in phase 1 and embedded into the security IC in phase 3 or later phases of the security IC product life-cycle.

10.6 Security IC Product

Integration of security IC and Embedded software is evaluated as composite target of evaluation in sense of supporting document.

10.7 TOE Delivery

The TOE is delivered in the period of in form of packaged product after packaging in phase 4.