

**IFX_CCI_00004Fh, IFX_CCI_000050h,
IFX_CCI_000051h, IFX_CCI_000052h,
IFX_CCI_000053h, IFX_CCI_000054h,
IFX_CCI_000055h, IFX_CCI_000056h,
IFX_CCI_000057h, IFX_CCI_000058h,
IFX_CCI_00005Ch S11
Security Target Lite**

Revision: v6.9

Table of Contents

Contents

| | |
|---|-----------|
| Table of Contents | 2 |
| 1 Security Target Introduction (ASE_INT) | 4 |
| 1.1 ST reference..... | 4 |
| 1.2 TOE Reference | 4 |
| 1.3 TOE Overview | 6 |
| 1.3.1 TOE Definition and Usage | 6 |
| 1.3.2 TOE major security features | 6 |
| 1.4 TOE description | 7 |
| 1.4.1 TOE components..... | 7 |
| 1.4.2 Physical scope of the TOE | 11 |
| 1.4.3 Logical scope of the TOE..... | 11 |
| 1.4.4 Interfaces of the TOE..... | 12 |
| 1.4.5 Forms of Delivery | 12 |
| 1.4.6 Production sites | 13 |
| 1.4.7 TOE Configuration..... | 13 |
| 1.4.8 TOE initialization with Customer Software..... | 14 |
| 2 Conformance Claims (ASE_CCL) | 16 |
| 2.1 Conformance Claims (ASE CCL) | 16 |
| 2.1.1 PP Claim | 16 |
| 2.1.2 Package Claim | 16 |
| 2.1.3 Conformance Rationale | 16 |
| 3 Security Problem Definition (ASE_SPD) | 18 |
| 3.1 Threats..... | 18 |
| 3.1.1 Additional Threat due to TOE specific Functionality | 18 |
| 3.1.2 Assets regarding the Threats | 19 |
| 3.2 Organizational Security Policies | 19 |
| 3.3 Assumptions | 19 |
| 4 Security objectives (ASE_OBJ) | 20 |
| 4.1 Security objectives of the TOE | 20 |
| 4.2 Security Objectives for the development and operational Environment | 21 |
| 4.3 Security Objectives Rationale | 22 |
| 5 Extended Component Definition (ASE_ECD) | 24 |
| 5.1 Component “Subset TOE security testing (FPT_TST.2)” | 24 |
| 5.2 Definition of FPT_TST.2..... | 24 |
| 5.3 TSF self test (FPT_TST)..... | 25 |
| 6 Security Requirements (ASE_REQ) | 26 |
| 6.1 TOE Security Functional Requirements | 26 |
| 6.1.1 Definition required by [PP0084] | 27 |
| 6.1.2 Support of Cipher Schemes | 28 |
| 6.1.3 Subset of TOE testing..... | 41 |
| 6.1.4 Memory access control | 42 |
| 6.1.5 Data Integrity..... | 45 |

Security Target Introduction (ASE_INT)

| | | |
|-----------|---|-----------|
| 6.1.6 | Limited Capabilities and Limited Availability | 46 |
| 6.1.7 | Support of Flash Loader..... | 47 |
| 6.1.8 | Flash Loader Policy | 47 |
| 6.1.9 | Support of Authentication of the Security IC | 51 |
| 6.2 | TOE Security Assurance Requirements | 51 |
| 6.2.1 | Refinements | 52 |
| 6.3 | Security Requirements Rationale | 53 |
| 6.3.1 | Rationale for the Security Functional Requirements | 53 |
| 6.3.2 | Rationale of the Assurance Requirements | 57 |
| 7 | TOE Summary Specification (ASE_TSS) | 58 |
| 7.1 | SF_DPM: Device Phase Management | 58 |
| 7.2 | SF_PS: Protection against Snooping..... | 58 |
| 7.3 | SF_PMA: Protection against Modifying Attacks | 58 |
| 7.4 | SF_PLA: Protection against Logical Attacks..... | 58 |
| 7.5 | SF_CS: Cryptographic Support | 58 |
| 7.6 | Assignment of Security Functional Requirements to TOE's Security Functionality..... | 58 |
| 7.7 | Security Requirements are internally consistent..... | 60 |
| 8 | References | 61 |
| 9 | Appendix: hash signatures of NRG™ SW | 63 |
| 9.1 | Hash Digests of the NrgOS.lib | 63 |
| 9.2 | Hash Digests of the NrgManagement.lib | 63 |
| 10 | Appendix: hash signatures of the HSL | 64 |
| 11 | Appendix: hash signatures of the UMSLC lib | 65 |
| 12 | Appendix: hash signatures of the SCL | 66 |
| 12.1 | SCL v2.11.003..... | 66 |
| 12.2 | SCL v2.15.000..... | 66 |
| 13 | Appendix: hash signatures of the ACL | 68 |
| 13.1 | ACL v3.02.000..... | 68 |
| 13.2 | ACL v3.33.003..... | 68 |
| 13.3 | ACL v3.35.001..... | 69 |
| 14 | Appendix: hash signatures of the RCL | 70 |
| 15 | Appendix: hash signatures of the HCL..... | 71 |
| 16 | List of Abbreviations..... | 72 |
| 17 | Glossary | 75 |
| 18 | Revision History..... | 77 |

Security Target Introduction (ASE_INT)

1 Security Target Introduction (ASE_INT)

1.1 ST reference

The ST has the revision v6.9 and is dated 2025-01-24. The title of this document IFX_CCI_00004Fh, IFX_CCI_000050h, IFX_CCI_000051h, IFX_CCI_000052h, IFX_CCI_000053h, IFX_CCI_000054h, IFX_CCI_000055h, IFX_CCI_000056h, IFX_CCI_000057h, IFX_CCI_000058h, IFX_CCI_00005Ch S11 Security Target Lite.

1.2 TOE Reference

The ST comprises an Infineon Technologies Security Controller named IFX_CCI_00004Fh, IFX_CCI_000050h, IFX_CCI_000051h, IFX_CCI_000052h, IFX_CCI_000053h, IFX_CCI_000054h, IFX_CCI_000055h, IFX_CCI_000056h, IFX_CCI_000057h, IFX_CCI_000058h, IFX_CCI_00005Ch design step S11 with firmware 80.310.03.0 and 80.310.03.1, optional NRG™ SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib v01.30.0564, optional SCL v2.15.000 and v2.11.003, optional ACL v3.33.003 and 3.35.001 and v3.02.000, optional RCL v1.10.007, optional HCL v1.13.002 and user guidance in the following called TOE (Target of evaluation).

The ST is based on the Protection Profile [PP0084].

The Protection Profile and the ST are built in compliance to CC:2022

The targeted assurance level is EAL6+.

Security Target Introduction (ASE_INT)

Table 1 Identification

| Hardware | Version | Method of identification |
|---|---|----------------------------------|
| IFX_CCI_00004Fh, IFX_CCI_000050h, IFX_CCI_000051h, IFX_CCI_000052h, IFX_CCI_000053h, IFX_CCI_000054h, IFX_CCI_000055h, IFX_CCI_000056h, IFX_CCI_000057h, IFX_CCI_000058h, IFX_CCI_00005Ch (each of the comma separated term is a Common Criteria Certification Identifier) | S11 (design step) | Non-ISO ATR |
| firmware | | |
| BOS & POWS & RFAP | 80.310.03.0 and 80.310.03.1 | Non-ISO ATR: firmware identifier |
| Flash-loader | 09.12.0003 | Flash-loader function |
| Software | | |
| NRG™ SW (optional) | 05.03.4097 | NRG™ SW function |
| HSL (optional) | v3.52.9708 | HSL function |
| UMSLC | v01.30.0564 | UMSLC function |
| SCL (optional) | v2.15.000 and v2.11.003 | SCL function |
| ACL (optional) | v3.33.003 and 3.35.001 and v3.02.000 | ACL function |
| RCL (optional) | v1.10.007 | RCL function |
| HCL (optional) | v1.13.002 | HCL function |
| User Guidance | | |
| SLC36 32-bit Security Controller - V16, Hardware Reference Manual | V5.2, 2020-12-21 | document |
| SLx1/SLx3 (40 nm) Security Controllers, Programmer's Reference Manual | V5.7, 2023-10-19 | document |
| SLC36 32-bit Security Controller - V16, Security Guidelines | v1.00-2662, 2020-10-05 | document |
| Production and Personalization Manual 32-bit security controller | v.09.12, 2023-03-02 | document |
| 32-bit Security Controller Crypto2304T V3, User Manual (optional) | V3.0, 2024-06-21 | document |
| HSL SLCx7 V16, Hardware Support Library (optional) | v3.52.9708, 2021-01-25 | document |

Security Target Introduction (ASE_INT)

| Hardware | Version | Method of identification |
|--|---|--------------------------|
| UMSLC library for SLCx7 in 40nm | v01.30.0564, 2019-08-30 | document |
| SCL37-SCP-v440-C40 Symmetric Crypto Library for SCP-v440 AES/DES/MAC (optional) | v2.11.003, 2021-06-16 & v2.15.000, 2023-07-20 | document |
| ACL37-Crypto2304T-C40 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox (optional) | v3.02.000, 2024-08-16 & v3.33.003, 2024-08-16 & v3.35.001, 2024-11-15 | document |
| RCL37-X-C40 Random Crypto Library for SCP-v440 & RNG-v3 DRBG/HWRNG 32-bit Security Controller, User interface manual (optional) | v1.10.007, 2020-06-16 | document |
| HCL37-CPU-C40 Hash Crypto Library for CPU SHA 32-bit Security Controller, User interface manual (optional) | v1.13.002, 2020-05-07 | document |

A customer shall identify the TOE. The hardware and its configuration (for details see chapter 1.4.7) is identified using the Non-ISO ATR. The Non-ISO ATR outputs a Common Criteria Certification Identifier and firmware identifier, which links the TOE to this ST. For the identification of software libraries, each library offers an API, which outputs its version. Alternatively the hashes from the Appendices of this ST can be used to check the libraries before integration. Specific firmware functions can be used to determine the exact configuration of a device from the certified range defined in Table 3.

The TOE can be ordered with a preloaded image. This image contains NVM loader functionality and is called PFL (Performance Flash Loader) with version v09.10.90.9. The PFL is intended to be used in a secured environment only and is not part of the TOE.

1.3 TOE Overview

1.3.1 TOE Definition and Usage

The TOE consists of smart card ICs (Security Controllers), firmware and user guidance meeting high requirements in terms of performance and security designed by Infineon Technologies AG. This TOE is intended to be used in smart cards for security-relevant applications and as developing platform for smart card operating systems according to the lifecycle model from [PP0084].

The term Smartcard Embedded Software is used in the following for all operating systems and applications stored and executed on the TOE. The TOE is the platform for the Smartcard Embedded Software. The Smartcard Embedded Software itself is not part of the TOE. The TOE does not require any non-TOE hardware/software/firmware.

1.3.2 TOE major security features

- Cryptographic support: TDES, AES, RSA, DH, ECDSA, ECC, ECDH, SHA-1, SHA-2, RNG (Hybrid Random Number Generator PTG.3, True Random Number Generator PTG.2, Deterministic Random Number generator DRG.3 and DRG.4 according to [BSI_RNGs])
- Memory protection unit supporting different memory access levels

Security Target Introduction (ASE_INT)

- Memory encryption
- Robust set of sensors and detectors for the purpose of monitoring proper chip operating conditions
- Redundant alarm propagation and system deactivation principle
- Register protection
- Security life control
- Program flow integrity protection
- Peripheral access control
- Bus encryption for security peripherals
- Tearing safe NVM programming
- Security optimized wiring
- Leakage control of data dependent code execution
- Device phase management supporting isolation of test features and Flash Loader accessibility
- Detection of NVM single and multi bit errors

1.4 TOE description

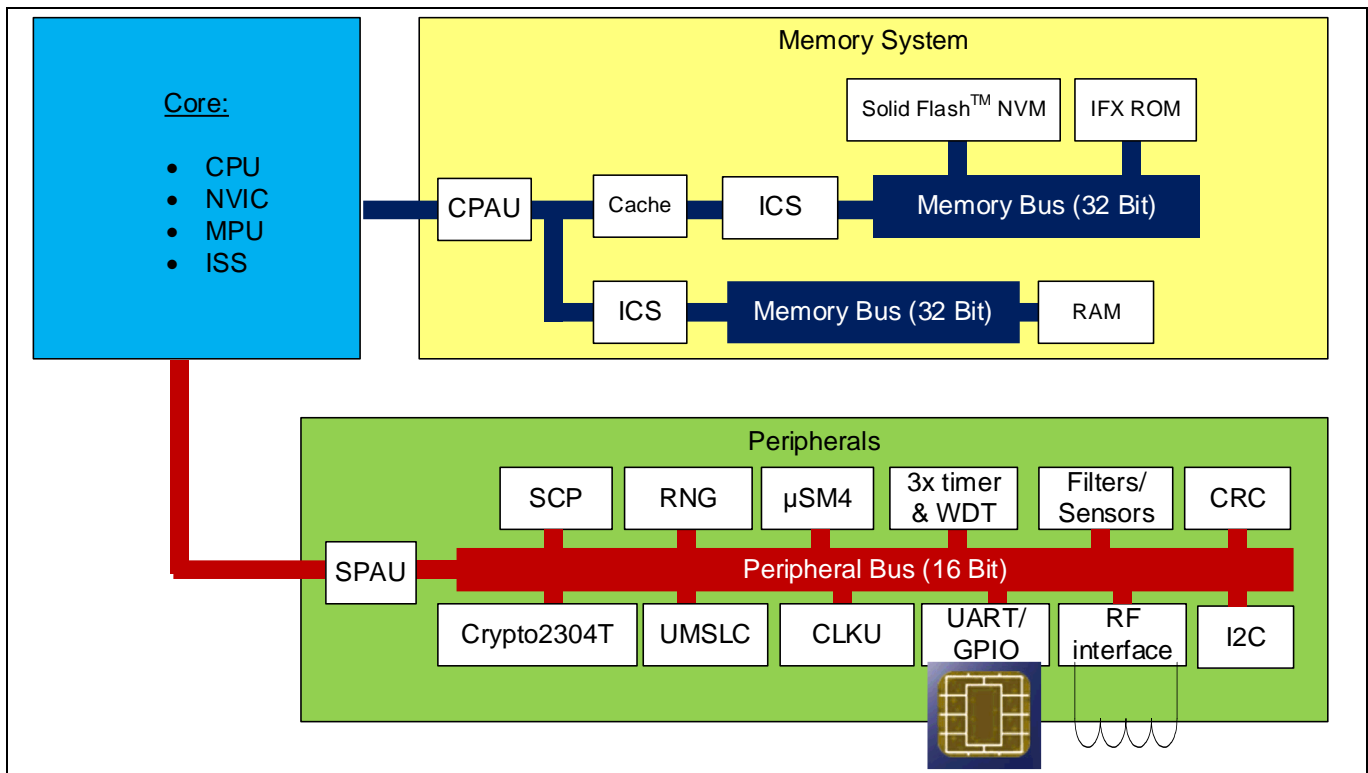
1.4.1 TOE components

1.4.1.1 Hardware components

Figure 1 shows a block diagram of the TOE hardware:

Figure 1 Block diagram of TOE hardware

Security Target Introduction (ASE_INT)



The TOE hardware consists of a core, a memory system and peripherals.

The major components of the core system are a 32-bit CPU (Central Processing Unit), an MPU (Memory Protection Unit), a Nested Vectored Interrupt Controller (NVIC) and an Instruction Stream Signature Checking (ISS).

The MPU of the core stores code and data in a linear 4-GByte memory space (32-bit range), allowing direct access without the need to swap memory segments in and out of memory using a memory protection unit.

There are two separate bus entities: a memory bus and a peripheral bus for high-speed communication with the peripherals.

The SPAU can be configured by the user to block or allow peripheral access. It can also be used to block RAM areas (For keeping Figure 1 simple, the connection between SPAU and RAM is not shown). The CPAU enables the user to block or allow unprivileged level access to NVM and specific registers of ICS and NVM.

The CPU accesses memory via the Internal Ciphering System (ICS), which encrypts/decrypts memory content. All data of the memory block is encrypted. The NVM is equipped with an error correction code (ECC). Security modules manage the alarms. Alarms may be triggered when the environmental conditions are outside the specified operational range.

A set of sensors (temperature sensor, backside light detector, glitch sensor, low frequency sensor) is used to detect excessive deviations from the specified operational range and serve for robustness of the TOE. The UMSLC function can be used to test the alarm lines.

A Random Number Generator (RNG) consists of a physical Random Number Generator with a cryptographically strong post processing unit. It can be operated in the modes as follows:

- True Random Number Generation, meeting AIS31 PTG.2
- Hybrid Random Number Generation, meeting AIS31 PTG.3

Security Target Introduction (ASE_INT)

- Deterministic Random Number Generation (DRNG) AIS31 DRG.3 and DRG.4

The Symmetric Cryptographic Processor (SCP) implements calculation of dual-key or triple-key triple-DES and AES.

The μ SM4 supports the Chinese standard encryption algorithm SM4.

The Crypto2304T co-processor provides basic means optimized for the implementation of fast and secure software of many asymmetric or public key cryptographic schemes like RSA or elliptic curve based ones. The user accessibility of the Crypto2304T is a customer ordering option

The implemented sleep mode logic (clock stop mode per ISO/IEC 7816-3) is used to reduce overall power consumption.

The TOE is able to communicate using either its contact based or contactless interface (RF interface). The contact based interface allows to use the ISO 7816 protocol via the UART. Further it offers a GPIO and an I2C slave interface. The contactless interface can be configured to RFI or ACLB mode. Both interface types support the signaling modes as follows:

- Signalling mode ISO/IEC 14443, Type A and Type B
- Signalling mode ISO/IEC 18092 passive mode, Type F
- NRG™ interface

The UMSLC enables the user software to check the activity and proper function of the system's security features.

The Clock Unit (CLKU) supplies the clocks for all components of the TOE. The Clock Unit can work in internal and external clock mode. When operating the internal clock mode the system frequency is derived from an oscillator, whereas in external clock mode, the system clock is derived from an externally supplied interface clock.

The watchdog timer triggers an event in case of a counter overflow. The timers are general purpose up-counting timers.

A CRC (Cyclic Redundancy Check) module computes a checksum value from a message or any other block of data.

The ROM is used by IFX only. The user software has to be implemented in SOLID FLASH™ memory. The user can choose, whether the software is loaded into the SOLID FLASH™ memory by Infineon Technologies AG or by the user.

The TOE uses Special Function Registers (SFRs). These SFRs are used for general purposes and chip configuration; they are located in SOLID FLASH™ memory in a configuration area page. The Online Configuration Check (OCC) function is used for register protection, i.e. controls the modification of relevant SFR settings.

In case a security violation is detected, secure state is entered by the hardware.

1.4.1.2 Firmware and software components

The TOE provides low-level firmware components: the Boot Software (BOS), the Performance Optimized Write Scheme (POWS), the contactless application programmers interface (RFAP) and the Flash Loader (FL).

The BOS firmware is used for test purposes during start-up and the FL allows downloading of user software to the NVM during the manufacturing process. All mandatory functions for start-up and internal testing are protected by a dedicated hardware firewall with two levels "BOS" and "user".

Security Target Introduction (ASE_INT)

The POWS library is an internal firmware library, i.e. not accessible by the user. It is used by the BOS and FL to store data in NVM in a tearing safe manner.

The RFAP (ROM) library provides CL interface functions. It does not implement any security functionality.

The Flash Loader allows downloading of User Software into the NVM during the manufacturing process.

The software of the TOE consists of optional packages:

- NRG™ SW: The optional NRG™ SW supports Card and Reader Mode, e.g. card creation, personalization and deletion. The NRG™ SW does not implement any security functionality
- HSL: The optional HSL provides functionality via APIs to the Smartcard Embedded Software, which contains SOLID FLASH™ NVM service routines and functionality for tearing safe programming of SOLID FLASH™ NVM.
- UMSLC lib: this library provides a wrapper around the UMSLC hardware functionality with measures to counter fault attacks.
- Symmetric Crypto Library (SCL): The optional SCL is used to provide a high level interface to the TDES and AES cryptography, which is partly implemented on the hardware component SCP and includes countermeasures against SPA, DPA and DFA attacks. The SCL is delivered as object code and in this way integrated into the user software.
- Asymmetric Crypto Library (ACL): The optional ACL implements RSA and elliptic curve based cryptographic schemes
- RCL: The Random Crypto Library offers a high-level interface for obtaining random data. This can be deterministic data or non-deterministic data that is provided by the underlying hardware.
- HCL: The Hash Crypto Library offers a high-level interface for performing cryptographic hash functions.

1.4.1.3 User Guidance components

The user guidance consists of the components as follows:

- 32-bit Security Controller – V16, Hardware Reference Manual: description of hardware features and user interfaces
- 32-bit ARM-based Security Controller, SLC 37/(40-nm Technology), Programmer's Reference Manual: description of firmware principles (including NRG™ SW) relevant for IC embedded software.
- Production and personalization 32-bit ARM-based security controller in 40 nm: contains detailed information about the usage of the Flash Loader
- 32-bit Security Controller – V16, Security Guidelines: provides the guidance and recommendations to develop secure software for and secure usage of this TOE.
- 32-bit Security Controller Crypto2304T V3, User Manual: This manual describes the functionality of the Crypto2304T module and is intended for experienced crypto library developers
- HSL SLCx7 V16, Hardware Support Library: provides an application interface (API) description and security guidelines for the optional HSL software part.
- UMSLC library for SLCx7 in 40nm User Mode Security Life Control, Version 01.00.0234: provides some guidelines, how to use the UMSLC library
- SCL37-SCP-v440-C40 Symmetric Crypto Library for SCP-v440 AES/DES/MAC: User Interface, contains all interfaces of the SCL. This document is only delivered to the user in case the SCL is part of the delivered TOE.
- ACL37-Crypto2304T-C40 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox: provides an application interface (API) description and security guidelines for the optional ACL software part
- RCL37-X-C40 Random Crypto Library for SCP-v440 & RNG-v3 DRBG/HWRNG 32-bit Security Controller, User interface manual: provides API description and security guidelines for the optional RCL part.

Security Target Introduction (ASE_INT)

- HCL37-CPU-C40 Hash Crypto Library for CPU SHA 32-bit Security Controller, User interface manual: provides API description and security guidelines for the optional HCL part.

1.4.2 Physical scope of the TOE

The physical scope of the TOE is defined by the TOE components described in chapter 1.4.1

1.4.3 Logical scope of the TOE

The logical scope of the TOE consists of the logical security features provided by the TOE. These features are listed in chapter 1.3.2. More details are provided in this chapter:

- Cryptographic support: TDES (block cipher modes ECB, CBC, CFB, CTR, Retail MAC and CMAC), AES (block cipher modes ECB, CBC, CFB, CTR and CMAC), RNG (Hybrid Random Number Generator PTG.3, True Random Number Generator PTG.2, Deterministic Random Number generator DRG.3 and DRG.4 according to [BSI_RNGs]), RSA, DH, ECC, ECDSA, ECDH, SHA-1, SHA-2.
- Memory protection unit supporting up to eight memory regions with different access rights and two privilege levels “privileged” and “user”. “User” level is more restricted in using TOE resources compared to “privileged”
- Memory encryption: all data of memories ROM, RAM and NVM are encrypted. Addresses are scrambled to disguise the location of data
- Robust set of sensors and detectors for the purpose of monitoring proper chip operating conditions consisting of a temperature sensor, backside light detector, glitch sensor and low frequency sensor.
- Redundant alarm propagation and system deactivation principle, which decreases the risk of manipulation and tampering.
- Register protection: protection of security relevant registers against fault attacks using OCC.
- Security life control: a life test on specific security features can be used by the IC embedded software to detect manipulation of these security features
- Program flow integrity protection: The Instruction Stream Signature Checking (ISS) can be employed by the IC embedded software to detect illegal program flows and trigger an alarm. The TOE also contains a watchdog, which may be used to detect program flow manipulations.
- Peripheral access control: The TOE allows the IC embedded software to lock certain peripherals dynamically.
- Bus encryption for security peripherals: All data transfers to and from dedicated peripherals are encrypted dynamically.
- Tearing safe NVM programming: the HSL provides specific routines provided for tearing safe programming. These routines prevent an unspecified interim state by either propagating the pre- or post-programming condition.
- Security optimized wiring: shield lines in combination with layout measures reduce the risk of successful manipulative attacks.
- Leakage control of data dependent code execution: dedicated measures allow the user to reduce such leakage.
- Device phase management supporting isolation of test features and Flash Loader accessibility: dedicated test features employed during production are switched off before customer delivery. The Flash Loader usage to download flash data requires either a mutual authentication or a one way user authentication depending on the order option EA. The Flash Loader supports permanent deactivation.
- Detection of NVM single and multi bit errors: Single bit errors are detected and corrected and multi bit errors detected.

Security Target Introduction (ASE_INT)

- Features, which are not mentioned here do not directly contribute to the SFRs.

1.4.4 Interfaces of the TOE

- The physical interface of the TOE to the external environment is the entire surface of the IC.
- The electrical interface of the TOE to the external environment is constituted by the pads of the chip:
 - The five ISO 7816 pads consist particularly of the contacted RES, I/O, CLK lines and supply lines VCC and GND. The contact based communication is according to ISO 7816/ETSI/EMV.
 - The I2C communication can be driven via the ISO 7816 pads. In this case no other communication using the ISO 7816 pads is possible.
- The RF interface (radio frequency power and signal interface) enables contactless communication between a PICC (proximity integration chip card) and a PCD reader/writer (proximity coupling device). Power supply is received and data are received or transmitted by an antenna which consists of a coil with a few turns directly connected to the IC.
- The data-oriented I/O interface of the TOE is represented by the I/O pad.
- The interface between firmware and hardware consists of special registers used for hardware configuration and control (Special Function Registers, SFR).
- Optional: The interface of the TOE to the operating system is covered by the optional HSL routines and by the instruction set of the TOE.
- Optional: The interface of the NRG™ SW defined by the NRG™ SW
- The interface of the UMSLC lib defined by the UMSLC lib
- Optional: The interface to the SCL calculations is defined by the SCL
- Optional: The interface to the ACL calculations is defined by the ACL
- Optional: The interface to the RCL is defined by the RCL
- Optional: The interface to the HCL is defined by the HCL

1.4.5 Forms of Delivery

The TOE can be delivered in the form of complete modules, as plain wafers in an IC case (e.g. DSO20) or in bare dies. The delivery can therefore be at the end of phase 3 or at the end of phase 4 which may also include pre-personalization steps according to [PP0084]. This means phase 4 is also part of the evaluation process. In any case the testing of the TOE is finished and the extended test features are removed. From a security policy point of view the different forms of delivery do not have any impact.

The delivery to the software developer (phase 2 → phase 1) contains the documents as described above.

Part of the software delivery is the Flash Loader program, provided by Infineon Technologies AG, running on the TOE and controlling the download of user software onto the TOE. The download is only possible after successful authentication. The user software and data must be encrypted before download. In addition, the user can permanently block further use of the Flash Loader.

The table as follows provides an overview about form and method of TOE deliveries:

Table 2 TOE deliveries: forms and methods

| TOE Component | Delivered Format | Delivery Method | Comment |
|---------------|------------------|-----------------|---------|
| Hardware | | | |

Security Target Introduction (ASE_INT)

| TOE Component | Delivered Format | Delivery Method | Comment |
|---|---------------------------------------|----------------------------------|---|
| IFX_CCI_00004Fh, IFX_CCI_000050h, IFX_CCI_000051h, IFX_CCI_000052h, IFX_CCI_000053h, IFX_CCI_000054h, IFX_CCI_000055h, IFX_CCI_000056h, IFX_CCI_000057h, IFX_CCI_000058h, IFX_CCI_00005Ch S11 | Wafer, IC case, packages | By customer order | Customer chooses delivery method. This ST describes under which circumstances transport protection is provided by the TOE. |
| Firmware | | | |
| All | – | – | stored on the delivered hardware. |
| Software | | | |
| All software libraries | L251 Library File (object code) | Secured download ¹ | – |
| PFL (not part of the TOE) | Preloaded image | Part of IC | – |
| Guidance Documentation | | | |
| All User Guidance documents | Personalized PDF | Secured download ¹ | – |

1.4.6 Production sites

The TOE may be handled at different production sites but the silicon is produced at Global Foundries fab 7 in Singapore only. The production site can be determined by the non-ISO ATR.

The delivery measures are described in the ALC_DVS aspect.

1.4.7 TOE Configuration

This TOE is represented by various configurations called products.

The module design, layout and footprint, of all products are identical.

The degree of freedom for configuring the TOE is predefined by Infineon Technologies AG. Table 3 shows the TOE hardware/firmware configurations:

Table 3 TOE hardware/firmware configuration options

| Memory | Values | Identification |
|--------------|------------------|----------------|
| SOLID FLASH™ | up to 352 kBytes | IFX-Mailbox |
| RAM | up to 16 kBytes | IFX-Mailbox |
| Peripherals | Values | Identification |

¹ Secured download is a way of delivery of documentation and TOE related software using a secure ishare connected to Infineon customer portal. The TOE user needs a DMZ Account to login (authenticate) via the Internet.

Security Target Introduction (ASE_INT)

| Memory | Values | Identification |
|---|-----------------------|-----------------------|
| Crypto2304T | Available/unavailable | Hardware register |
| μSM4 | Available/unavailable | Hardware register |
| NRG™ Crypto Module | Available/unavailable | Hardware register |
| Interface and protocol | Values | Identification |
| I2C | Available/unavailable | Hardware register |
| RFI | Available/unavailable | Hardware register |
| ACLB | Available/unavailable | Hardware register |
| Signaling mode ISO/IEC 14443 Type A | Available/unavailable | Hardware register |
| Signaling mode ISO/IEC 14443 Type B | Available/unavailable | Hardware register |
| Signaling mode ISO/IEC 18092 passive mode, Type F | Available/unavailable | Hardware register |
| ACM | Available/unavailable | Hardware register |
| AMM | Available/unavailable | Hardware register |
| AFM | Available/unavailable | Hardware register |
| Input capacitance [pF] | (27/56/78) | GCIM |
| BPU | Available/unavailable | IFX-Mailbox |
| EA | Available/unavailable | Flash loader function |

Further the Flash Loader can be configured in different ways as explained in the following section.

1.4.8 TOE initialization with Customer Software

This TOE is equipped with Flash Loader software (FL) to download user software, i.e. an operating system and applications. Various options can be chosen by the user to store software onto the SOLID FLASH™ NVM:

Table 4 Order Options to initialize the TOE with customer software

| Case | Option | Flash loader status |
|------|--|---|
| 1 | The user or/and a subcontractor downloads the software into the SOLID FLASH™ memory. Infineon Technologies does not receive any user software. | The Flash Loader can be activated or reactivated by the user or subcontractor to download software into the SOLID FLASH™ memory. In case the Flash Loader is active, it may be either in life cycle stage “Pinletter” or “Activated”. When “Activated” a mutual authentication needs to be performed or if TOE is ordered with EA available a one-way authentication from user towards Flash Loader, before download can be started. In “Pinletter” a valid Pinletter provided by Infineon Technologies AG needs to be presented to enter “Activated” stage. The PFL may be present as preloaded image. |
| 2 | The user provides software to download into the SOLID | There is no Flash Loader present. |

Security Target Introduction (ASE_INT)

| Case | Option | Flash loader status |
|------|---|---|
| | FLASH™ memory to Infineon Technologies AG. The software is loaded into the SOLID FLASH™ memory during chip production. | |
| 3 | The user provides software to download into the SOLID FLASH™ memory to Infineon Technologies AG. The software is loaded into the NVM memory during chip production. | The Flash Loader is blocked by Infineon but can be activated or reactivated by the user or subcontractor to download software into the SOLID FLASH™ memory. The user is required to provide a reactivation procedure as part of the software to Infineon Technologies AG. |
| 4 | The user provides software to download into the SOLID FLASH™ memory to Infineon Technologies AG. The software is loaded into the NVM memory during chip production. | The Flash Loader is active. The user can either download software or activate the software already present in SOLID FLASH™ memory. |
| 5 | Infineon Technologies AG preloads PFL into SOLID FLASH™. | The Flash Loader is active. The user can either download software and erase the PFL or activate the PFL present in SOLID FLASH™ memory. Note, that PFL is not part of the TOE., i.e. activating the PFL is outside of the scope of this certification. |

Conformance Claims (ASE_CCL)

2 Conformance Claims (ASE_CCL)

2.1 Conformance Claims (ASE CCL)

This ST and TOE claim conformance to CC:2022. The ST claims conformance to [CCBook3]. It is [CCBook2] extended. [CCErrata] and [CCtrans] is taken into consideration.

2.1.1 PP Claim

This ST is strictly conformant to [PP0084]. The assurance level is EAL6+. The augmentation is achieved - with regard to [CCBook5]: Security assurance components by including:

Table 5 Augmentations of the assurance level of the TOE

| Assurance Class | Assurance Family | Description |
|--------------------|------------------|------------------------|
| Life-cycle support | ALC_FLR.1 | Basic flaw remediation |

The Security IC Platform Protection Profile with Augmentation Packages is registered and certified by the Bundesamt für Sicherheit in der Informationstechnik¹ (BSI) under the reference [PP0084].

The security assurance requirements of the TOE are according to [PP0084] and [CCBook3].

2.1.2 Package Claim

This ST claims conformance to the following additional packages taken from [PP0084]:

- Package Authentication of the Security IC, section 7.2, conformant. This package is only claimed in case TOE is ordered with configuration option EA unavailable and flash loader is not permanently deactivated.
- Package Loader, Package 1: Loader dedicated for usage in secured environment only, section 7.3.1, conformant.
This package is optional and fulfilled only by TOE products with Flash Loader.
- Package Loader, Package 2: Loader dedicated for usage by authorized users only, section 7.3.2, augmented
This package is optional and fulfilled only by TOE products with Flash Loader and configuration option EA unavailable.
- Package TDES ; section 7.4.1, augmented
- Package AES ; section 7.4.2, augmented

The assurance level for the TOE is EAL6 augmented with the component ALC_FLR.1. Therefore this ST is **package-augmented** to the packages in [PP0084].

2.1.3 Conformance Rationale

The TOE is a typical security IC as defined in [PP0084] chapter 1.2.2 comprising:

- the circuitry of the IC (hardware including the physical memories),
- configuration data, initialization data related to the IC Dedicated Software and the behaviour of the security functionality

¹ Bundesamt für Sicherheit in der Informationstechnik (BSI) is the German Federal Office for Information Security

Conformance Claims (ASE_CCL)

- the IC Dedicated Software with the parts
- the IC Dedicated Test Software,
- the IC Dedicated Support Software.

The TOE is designed, produced and/or generated by the TOE Manufacturer.

With CC:2022 several SFR changes are introduced. Due to this ST claiming conformance to CC:2022 and [PP0084], rationales are provided that these changes do not affect the conformance claim to [PP0084]:

- FCS_COP.1: for this SFR dependencies are changed in CC:2022. FCS_CKM.4 is removed and instead FCS_CKM.6 added. Further FCS_CKM.5 is added for key derivation as an alternative.
- FCS_CKM.1: for this SFR dependencies are changed in CC:2022. Additionally to FCS_CKM.2 and FCS_COP.1, one further SFR is introduced as alternative: FCS_CKM.5. This SFR targets key derivation, subsequent to FCS_CKM.1. In CC:2022 key derivation would have been part of FCS_CKM.1 and thus conformance to [PP0084] can still be claimed. FCS_CKM.4 is removed and instead FCS_CKM.6 added. All other dependencies (i.e. FCS_RNG.1 or FCS_RBG.1) are in addition to the already existing ones, i.e. add stricter requirements.
- FCS_CKM.6 replaces FCS_CKM.4 and adds further requirements on the timing of key destruction. As an alternative dependency to FCS_CKM.1, FCS_CKM.5 (key derivation) can be used. As FCS_CKM.5 is neither used within [PP0084] nor within this ST, it has no relevance in this context.
- FCS_RNG.1: this SFR is taken from [CCBook2] rather than [PP0084]. The SFR is identical in [CCBook2]
- FMT_LIM.1 and FMT_LIM.2 are taken from [CCBook2] rather than [PP0084]. There is a slightly different phrasing (i.e. removing redundancy from FMT_LIM.1) and availability and capability policy mentioned in both SFR's. The meaning though is the same and therefore conformance can still be claimed.
- FIA_API.1: this SFR is taken from [CCBook2] rather than [PP0084]. The SFR requires additional information.
- FDP_SDC.1: this SFR is taken from [CCBook2] rather than [PP0084]; An assignment from [PP0084] is changed to a selection [CCbook2], which means the requirement is more stringent and thus can be considered a subset of the requirement from [PP0084].

Further with CC:2022 some SAR changes were introduced. Rationales are provided that these changes do not affect the conformance claim to [PP0084]:

- ASE_CCL.1: for CC:2022 several extensions were introduced (e.g. exact conformance to PP), which add to the already existing assurance requirements. No relaxation was introduced.
- ASE_INT.1: introduction of multi-assurance in combination with PP-configuration: not relevant for [PP0084]
- ASE_REQ.2: extended for multi assurance: not relevant for [PP0084]
- AVA_VAN.5: extension about third party components introduced. No relaxation was introduced.
- ALC_TAT.1: extension with guidance on the minimum content for an implementation standards description and rules with ADV_COMP.1. No relaxation was introduced.

3 Security Problem Definition (ASE_SPD)

The content of [PP0084] applies to this chapter completely.

3.1 Threats

The threats are directed against the assets and/or the security functions of the TOE. For example, certain attacks are only one step towards a disclosure of assets while others may directly lead to a compromise of the application security. The more detailed description of specific attacks is given later on in the process of evaluation and certification. An overview on attacks is given in [PP0084] section 3.2.

The threats to security are defined and described in [PP0084] sections 3.2 and 7.2.1.

Table 6 Threats according to [PP0084]

| | |
|---------------------|---|
| 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 |
| T.Masquerade_TOE | Masquerade the TOE |

3.1.1 Additional Threat due to TOE specific Functionality

The additional functionality of introducing sophisticated privilege levels and access control allows the secure separation between the operation system(s) and applications, the secure downloading of applications after personalization and enables multitasking by separating memory areas and performing access controls between different applications. Due to this additional functionality “area based memory access control” a new threat is introduced.

The TOE shall avert the threat “Memory Access Violation (T.Mem-Access)” as specified below:

T.Mem-Access Memory Access Violation

Parts of the Smartcard Embedded Software may cause security violations by accidentally or deliberately accessing restricted data (which may include code) or privilege levels. Any restrictions are defined by the security policy of the specific application context and must be implemented by the Smartcard Embedded Software.

“Diffusion of open samples” threat:

T.Open_Samples_Diffusion Diffusion of Open Samples

An attacker may get access to open samples of the TOE and use them to gain information about the TSF (loader, memory management unit, ROM code ...). He may also use the open samples to characterize the behavior of the IC and its security functionalities (for example: characterization of side channel profiles, perturbation cartography ...). The execution of a dedicated security features (for example: execution of a DES computation without countermeasures or by de-activating countermeasures) through the loading of an adequate code would allow this kind of characterization and the execution of enhanced attacks on the IC.

Table 7 Additional threats due to TOE specific functions and augmentations

Security Problem Definition (ASE_SPD)

| | |
|--------------------------|---------------------------|
| T.Mem-Access | Memory Access Violation |
| T.Open_Samples_Diffusion | Diffusion of Open Samples |

3.1.2 Assets regarding the Threats

The asset description from [PP0084] section 3.1 applies.

3.2 Organizational Security Policies

The organizational policies from [PP0084] sections 3.3, 7.3.1, 7.3.2 and 7.4 are applicable.

Table 8 Organizational Security Policies according [PP0084]

| | |
|--|--|
| P.Process-TOE | Protection during TOE Development and Production |
| P.Crypto-Service | Cryptographic services of the TOE |
| P.Lim_Block_Loader | Limiting and Blocking the Loader Functionality |
| P.Ctrl_Loader (only available, if Flash Loader active) | Controlled usage to Loader Functionality |

3.3 Assumptions

The TOE assumptions about the operational environment are defined and described in [PP0084] section 3.4.

Table 9 Assumption according [PP0084]

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

Security objectives (ASE_OBJ)

4 Security objectives (ASE_OBJ)

This section shows the security objectives, which are relevant to the TOE.

4.1 Security objectives of the TOE

The security objectives of the TOE are defined and described in [PP0084] sections 4.1, 7.2.1, 7.3.1, 7.3.2, 7.4.1 and 7.4.2

Table 10 Objectives for the TOE according to [PP0084]

| | |
|---|---|
| O.Phys-Manipulation | Protection against Physical Manipulation |
| O.Phys-Probing | Protection against Physical Probing |
| O.Malfunction | Protection against Malfunction |
| O.Leak-Inherent | Protection against Inherent Information Leakage |
| O.Leak-Forced | Protection against Forced Information Leakage |
| O.Abuse-Func | Protection against Abuse of Functionality |
| O.Identification | TOE Identification |
| O.RND | Random Numbers |
| O.Cap_Avail_Loader | Capability and availability of the Loader |
| O.Ctrl_Auth_Loader (only available , if Flash Loader active) | Access control and authenticity for the Loader |
| O.Authentication (only available , if Flash Loader active and TOE is ordered with configuration option EA unavailable) | Authentication to external entities |
| O.TDES | Cryptographic service Triple-DES |
| O.AES | Cryptographic service AES |

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

O.Mem-Access Area based Memory Access Control

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

The TOE shall provide TSF confidentiality protection as specified below:

O.Prot_TSF_Confidentiality **Protection of confidentiality of TSF**

The TOE must provide protection against disclosure of confidential operations of the security IC (loader, memory management unit, ...) through the use of a dedicated code loaded on open samples.

The TOE shall provide “RSA cryptographic services (O.RSA)” and “Elliptic Curve cryptographic services (O.ECC)” as specified below.

Security objectives (ASE_OBJ)

O.RSA

RSA cryptographic services

The TOE shall provide the following specific security functionality to the Smartcard Embedded Software: Rivest-Shamir-Adleman Cryptography (RSA)

O.ECC

Elliptic Curve cryptographic services

The TOE shall provide the following specific security functionality to the Smartcard Embedded Software: Elliptic Curve Cryptography (ECC)

The TOE shall provide “Cryptographic service AES-TDES-MAC (O.AES-TDES-MAC)” as specified below.

O.AES-TDES-MAC

Cryptographic service AES-TDES-MAC

The TOE provides secure cryptographic services for AES and TDES MAC generation.

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

O.HASH

Cryptographic service hash

The TOE provides secure cryptographic services for SHA-1 and SHA-2 generation .

Table 11 Additional objectives due to TOE specific functions and augmentations

| | |
|---|---------------------------------------|
| O.Mem-Access | Area based Memory Access Control |
| O.Prot_TSF_Confidentiality | Protection of confidentiality of TSF |
| O.RSA (only available, if ACL is part of the TOE and Crypto2304T user accessible) | RSA cryptographic services |
| O.ECC (only available, if ACL is part of the TOE and Crypto2304T user accessible) | Elliptic Curve cryptographic services |
| O.AES-TDES-MAC (only available, if SCL is part of the TOE) | AES-TDES-MAC cryptographic services |
| O.HASH (only available , if HCL is part of the TOE) | Hash cryptographic services |

4.2 Security Objectives for the development and operational Environment

The security objectives from [PP0084] section 4.2, 4.3, 7.2.1, 7.3.1, 7.3.2, 7.4.1 and section 7.4.2 are applicable for this TOE.

The table below lists the environmental security objectives.

Table 12 Security objectives for the environment according to [PP0084]

| Environmental objective | Description |
|---|---|
| OE.Resp-Appl | Treatment of User Data |
| OE.Process-Sec-IC | Protection during composite product manufacturing |
| OE.Lim_Block_Loader | Limitation of capability and blocking the Loader |
| OE.Loader_Usage (only applicable, if Flash Loader active and TOE is ordered with configuration option EA unavailable) | Secure communication and usage of the Loader |

Security objectives (ASE_OBJ)

| Environmental objective | Description |
|--|---|
| OE.TOE_Auth (applicable, if Flash Loader active and TOE is ordered with configuration option EA unavailable) | External entities authenticating of the TOE |

Table 13 Additional Security objectives for the environment

| Environmental objective | Description |
|---|--|
| OE.Prevent_Masquerade (only applicable, if Flash Loader active and configuration option EA available) | User is required to provide mechanisms to prevent masquerading attacks in case the TOE does not claim the package “Authentication of the Security IC”. The authorized user must further support trusted communication with the TOE by confidentiality protection and authenticity proof of data to be loaded and fulfilling the access conditions required by the Loader. |
| OE.Secure_Delivery (only applicable if Flash Loader deactivated (i.e. cases 2 and 3 from Table 4)) | When the TOE is ordered with a disabled Flash Loader, it does not provide transport protection. Therefore, technical and / or organisational security procedures (e.g. a custom mutual authentication mechanism or a security transport) should be put in place by the customer to secure the personalized TOE during delivery as required by the security needs of the loaded IC Embedded Software. |

4.3 Security Objectives Rationale

The security objectives rationale of the TOE is defined and described in [PP0084] section 4.4, 7.3.1, 7.3.2, 7.4.1 and section 7.4.2.

Compared to [PP0084] an enhancement regarding memory area protection has been established. The clear definition of privilege levels for operated software establishes the clear separation of different restricted memory areas for running the firmware, downloading and/or running the operating system and to establish a clear separation between different applications. Nevertheless, it is also possible to define a shared memory section where separated applications may exchange defined data. The privilege levels clearly define by using a hierarchical model the access right from one level to the other. These measures ensure that the threat T.Mem-Access is clearly covered by the security objective O.Mem-Access.

The objectives O.Authentication, O.Ctrl_Auth_Loader and the organizational policy P.Ctrl_Loader and the environmental objective OE.TOE_Auth as described in [PP0084] chapter 7.2 and 7.3.2 apply only to TOE products with Flash Loader enabled for software or data download by the user. In other cases the Flash Loader is not available anymore and the user software or data download is completed. If TOE is ordered with configuration option EA available the objectives O.Authentication and the environmental objective OE.TOE_Auth are not applicable for the TOE. In this case, the TOE implements a one-way authentication of users instead of a mutual authentication.

The objective OE.Prevent_Masquerade is introduced because the availability of package “Authentication of the Security IC” depends on specific order options. In case the chosen order options exclude this package, the user has to provide measures to neutralize the threat T.Masquerade_TOE. Due to the combination of these measures with the one-way authentication enforced by the Flash Loader with EA, both communication end

Security objectives (ASE_OBJ)

points are considered to be authentic. Therefore, O.Ctrl_Auth_Loader is still applicable while the objective OE.Loader_Usage is replaced by the objective OE.Prevent_Masquerade.

The objective OE.Secure_Delivery requires the customers to provide transport protection in case the TOE is delivered with flash loader deactivated (i.e. cases 2, 3 from Table 4). In that case O.Authentication is not available and needs to be compensated by customer measures. This environmental objective counters T.Open_Samples_Diffusion and T.Masquerade_TOE.

The objectives O.RSA, O.ECC, O.AES-TDES-MAC, O.HASH cover the policy P.Crypto-Service. This policy intends to allow adding various cryptographic services to the TSF.

The objective O.Prot_TSF_Confidentiality counters the threat T.Open_Samples_Diffusion. In addition T.Open_Samples_Diffusion is countered by O.Leak-Inherent and O.Leak-Forced.

Extended Component Definition (ASE_ECD)

5 Extended Component Definition (ASE_ECD)

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

- the family FAU_SAS at the class FAU Security Audit
- the component FPT_TST.2 at the class FPT Protection of the TSF

The extended family FAU_SAS is defined and described in [PP0084] section 5. The component FPT_TST.2 is defined in the following sections.

5.1 Component “Subset TOE security testing (FPT_TST.2)”

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

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

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

5.2 Definition of FPT_TST.2

The functional component “Subset TOE security testing (FPT_TST.2)” has been newly created (Common Criteria Part 2 extended). This component allows that particular parts of the security mechanisms and functions provided by the TOE can be tested after TOE Delivery or are tested automatically and continuously during normal operation transparent for the user.

This security functional component is used instead of the functional component FPT_TST.1 from Common Criteria Part 2.

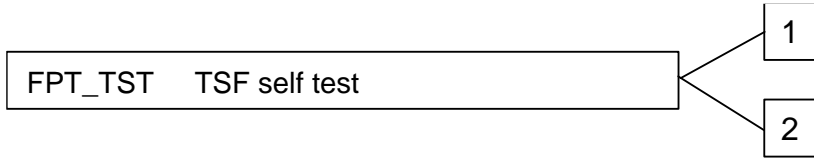
The functional component “Subset TOE testing (FPT_TST.2)” is specified as follows (Common Criteria Part 2 extended).

Extended Component Definition (ASE_ECD)

5.3 TSF self test (FPT_TST)

Family Behavior The Family Behavior is defined in [CCBook2] section 15.17.1.

Component levelling



FPT_TST.1: The component FPT_TST.1 is defined in [CCBook2] section 15.17.5.

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

Management: FPT_TST.2

The following actions could be considered for the management functions in FMT:

- management of the conditions under which subset TSF self testing occurs, such as during initial start-up, regular interval or under specified conditions
- management of the time of the interval appropriate.

Audit: FPT_TST.2

There are no auditable events foreseen.

| FPT_TST.2 | Subset TOE testing |
|------------------|--|
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies |
| FPT_TST.2.1: | The TSF shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, and/or at the conditions [assignment: conditions under which self test should occur]] to demonstrate the correct operation of [assignment: functions and/or mechanisms]. |

Security Requirements (ASE_REQ)

6 Security Requirements (ASE_REQ)

For this section [PP0084] section 6 can be applied completely.

6.1 TOE Security Functional Requirements

The security functional requirements (SFR) for the TOE are defined and described in [PP0084] and in the following description.

Table 14 provides an overview of the functional security requirements of the TOE, defined in [PP0084] section 6.1, 7.2.3, 7.3.1, 7.3.2, 7.4.1 and 7.4.2.

Table 14 Security functional requirements of the TOE defined in [PP0084]¹

| Security Functional Requirement | |
|---------------------------------|---|
| FRU_FLT.2 | “Limited fault tolerance“ |
| FPT_FLS.1 | “Failure with preservation of secure state“ |
| FMT_LIM.1 | “Limited capabilities“ |
| FMT_LIM.2 | “Limited availability“ |
| FAU_SAS.1 | “Audit storage“ |
| FDP_SDC.1 | “Stored data confidentiality“ |
| FDP_SDI.2 | “Stored data integrity monitoring and action“ |
| FPT_PHP.3 | “Resistance to physical attack“ |
| FDP_ITT.1 | “Basic internal transfer protection“ |
| FPT_ITT.1 | “Basic internal TSF data transfer protection“ |
| FDP_IFC.1 | “Subset information flow control“ |
| FCS_RNG.1/TRNG | “Random number generation - TRNG“ |
| FCS_RNG.1/DRNG | “Random number generation – DRG“ |
| FCS_RNG.1/DRNG4 | “Random number generation – DRG“ |
| FCS_RNG.1/HPRG | “Random number generation – HPRG“ |
| FCS_RNG.1/RCL/TRNG | “Random Number Generation“ |
| FCS_RNG.1/RCL/DRNG3 | “Random Number Generation“ |
| FCS_RNG.1/RCL/DRNG4 | “Random Number Generation“ |
| FCS_COP.1/SCP/TDES | “Cryptographic operation - TDES“ |
| FCS_COP.1/SCP/AES | “Cryptographic operation - AES“ |
| FCS_CKM.6/SCP | “Timing and Event of Cryptographic key destruction“ |
| FCS_COP.1/SCL/TDES | “Cryptographic operation – TDES by SCL“ |
| FCS_CKM.6/SCL | “Timing and Event of Cryptographic key destruction“ |
| FCS_COP.1/SCL/AES | “Cryptographic operation – AES by SCL“ |
| FMT_LIM.1/Loader | “Limited Capabilities – Loader“ |
| FMT_LIM.2/Loader | “Limited availability – Loader“ |
| FTP_ITC.1 | “Inter-TSF trusted channel“ |
| FDP_UCT.1 | “Basic data exchange confidentiality“ |

¹ Note: FCS_CKM.4 is replaced by FCS_CKM.6 in CC:2022

Security Requirements (ASE_REQ)

Security Functional Requirement

FDP_UIT.1 “Data exchange integrity”

FDP_ACC.1/Loader “Subset access control – Loader”

FDP_ACF.1/Loader “Security attribute based access control – Loader”

FIA_API.1 “Authentication Proof of Identity”

Table 15 provides an overview about security functional requirements, which are added to the TOE. All requirements are taken from [CCbook2] Part 2, with the exception of requirement FPT_TST.2, which is defined in this ST completely.

Table 15 Additional security functional requirements of the TOE

Security Functional Requirement

FPT_TST.2 “Subset TOE security testing”

FDP_ACC.1 “Subset access control”

FDP_ACF.1 “Security attribute based access control”

FMT_MSA.1 “Management of security attributes”

FMT_MSA.3 “Static attribute initialisation”

FMT_SMF.1 “Specification of Management functions”

FMT_SMR.1 “Security Roles”

FCS_COP.1/SCL/TDES-MAC “Cryptographic operation – TDES MAC”

FCS_COP.1/SCL/AES-MAC “Cryptographic operation – AES-MAC”

FCS_COP.1/RSA/<iteration> “Cryptographic Operation – RSA”

FCS_CKM.1/RSA/<iteration> “Cryptographic key generation - RSA”

FCS_COP.1/ECC/<iteration> “Cryptographic Operation – ECC”

FCS_CKM.1/ECC “Cryptographic key generation - ECC”

FCS_COP.1/HCL “Cryptographic key operation”

FMT_MTD.1/Loader “Management of TSF data”

FMT_SMR.1/Loader “Security roles”

FMT_SMF.1/Loader “Specification of Management Functions”

FIA_UID.2/Loader “User Identification before any action”

6.1.1 Definition required by [PP0084]

According to [PP0084] Application Note 14 the term “secure state” used by FPT_FLS.1 shall be described and a definition should be provided.

Definition of secure state:

Secure state describes three different conditions of the TOE:

1. the controller ceases operation. This condition can only be resolved by a cold or warm start of the controller. It is triggered by a security reset.
2. the controller enters a security trap. The trap handler can be defined by the user. In case no trap handler is provided the first condition is entered.
3. in case of a sudden power loss of the TOE during NVM programming (tearing): the TOE is in a condition to either restore the old NVM content or to start with the new programmed value. This condition of security

Security Requirements (ASE_REQ)

state is only provided in case the HSL is part of the TOE and one of the tearing-safe functions of the HSL is used.

Note: a security reset invalidates the RAM content.

According to [PP0084] Application Note 15, “The Common Criteria suggest that the TOE generates audit data for the security functional requirements Limited fault tolerance (FRU_FLT.2) and Failure with preservation of secure state (FPT_FLS.1).” In case of the first two conditions no Audit data are collected, because the effect entering the secure state is immediately visible. For the third condition indirect audit data is available, i.e. the user can check, whether new or old NVM data is available.

6.1.1.1 FAU_SAS

The [PP0084] defines additional security functional requirements with the family FAU_SAS of the class FAU (Security Audit). 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 <u>the test process before TOE Delivery¹</u> with the capability to store <u>the Initialization Data and/or Pre-personalization Data and/or supplements of the Security IC Embedded Software²</u> in the <u>access protected and not changeable configuration page area and non-volatile memory³</u> . |

6.1.2 Support of Cipher Schemes

6.1.2.1 True Random Number Generation, meeting AIS31 PTG.2

| | |
|-----------------------|---|
| FCS_RNG.1/TRNG | Random Number Generation |
| Hierarchical to | No other components. |
| Dependencies | No dependencies |
| FCS_RNG.1/TRNG | Random numbers generation Class PTG.2 according to [BSI_RNGs] |
| FCS_RNG.1.1/TRNG | The TSF shall provide a <u>physical⁴</u> random number generator that implements: |
| <u>PTG.2.1</u> | <u>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.</u> |
| <u>PTG.2.2</u> | <u>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</u> |

¹ [assignment: list of subjects]

² [assignment: list of audit information]

³ [assignment: type of persistent memory]

⁴ [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]

Security Requirements (ASE_REQ)

| | |
|-------------------------|--|
| | <u>raw random numbers that have been generated after the total failure of the entropy source.</u> |
| <u>PTG.2.3</u> | <u>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.</u> |
| <u>PTG.2.4</u> | <u>The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.</u> |
| <u>PTG.2.5</u> | <u>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.¹</u> |
| <u>FCS_RNG.1.2/TRNG</u> | The TSF shall provide numbers in the format 32-bit ² that meet |
| <u>PTG.2.6</u> | <u>Test procedure A, as defined in [BSI_RNGs] does not distinguish the internal random numbers from output sequences of an ideal RNG.</u> |
| <u>PTG.2.7</u> | <u>The average Shannon entropy per internal random bit exceeds 0.997.³</u> |

6.1.2.2 Hybrid Random Number Generation, meeting AIS31 PTG.3

| | |
|-------------------------|---|
| FCS_RNG.1/HPRG | Random Number Generation |
| Hierarchical to | No other components. |
| Dependencies | No dependencies |
| FCS_RNG.1/HPRG | Random numbers generation Class PTG.3 according to [BSI_RNGs] |
| <u>FCS_RNG.1.1/HPRG</u> | The TSF shall provide a <u>hybrid physical⁴</u> random number generator that implements: |
| <u>PTG.3.1</u> | <u>A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure has been detected no random numbers will be output.</u> |
| <u>PTG.3.2</u> | <u>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.</u> |
| <u>PTG.3.3</u> | <u>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 and the seeding of the DRG.3 post-processing algorithm have been finished successfully or when a defect has been detected.</u> |
| <u>PTG.3.4</u> | <u>The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.</u> |

¹ [assignment: list of security capabilities]² [selection: bit, octets of bits, numbers [assignment: format of the numbers]]³ [assignment: a defined quality metric]⁴ [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]

Security Requirements (ASE_REQ)

| | |
|-------------------------|---|
| <u>PTG.3.5</u> | <p><u>The online test procedure checks 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.</u></p> <p><u>Note:</u> <u>Continuously means that the raw random bits are scanned continuously.</u> <u>The algorithmic post-processing belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function. The output data rate of the post-processing algorithm shall not exceed its input data rate.</u> <u>End of note.</u></p> |
| <u>PTG.3.6</u> | <p><u>The algorithmic post-processing algorithm belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function, and the output data rate of the post-processing algorithm shall not exceed its input data rate.¹</u></p> |
| <u>FCS_RNG.1.2/HPRG</u> | <p>The TSF shall provide <u>numbers in the format 32-bit²</u> that meet</p> |
| <u>PTG.3.7</u> | <p><u>Statistical test suites cannot practically distinguish the internal random numbers from output sequences of an ideal RNG. The internal random numbers must pass test procedure A.</u></p> |
| <u>PTG.3.8</u> | <p><u>The internal random numbers shall use the PTRNG of class PTG.2 as random source for the post processing.³</u></p> |

Note: The internal random numbers produced by the employed PTG.2-conform PTRNG are adaptively compressed raw bits, where the compression rate is controlled by a so-called entropy estimator. The concept ensures that the random numbers provided by the PTRNG have high entropy, i.e., each delivered random byte will have more the 7.976 bit of entropy. In addition, the PTRNG produced random numbers have been tested against test procedures A and B under varying environment conditions.

6.1.2.3 Deterministic Random Number Generation (DRNG) AIS31 DRG.3

| | |
|-------------------------|---|
| FCS_RNG.1/DRNG | Random Number Generation |
| Hierarchical to | No other components. |
| Dependencies | No dependencies |
| FCS_RNG.1/DRNG | Random numbers generation Class DRG.3 according to [BSI_RNGs] |
| <u>FCS_RNG.1.1/DRNG</u> | The TSF shall provide a <u>deterministic⁴</u> random number generator that implements: |
| <u>DRG.3.1</u> | <p><u>If initialized with a random seed using a PTRNG of class PTG.2 as random source the internal state of the RNG shall have at least 100 bit of entropy.</u></p> <p><u>Note:</u> <u>Furthermore, the length of the internal state shall have at least 200 bit. (For the DRG.3 under consideration, the internal state has 351 bit.). The seed is provided</u></p> |

¹ [assignment: list of security capabilities]

² [selection: bit, octets of bits, numbers [assignment: format of the numbers]]

³ [assignment: a defined quality metric]

⁴ [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]

Security Requirements (ASE_REQ)

| | |
|-------------------------|---|
| | by a certified PTG.2 physical TRNG with guaranteed 7,976 bit of entropy per byte. <u>End of note.</u> |
| <u>DRG.3.2</u> | <u>The RNG provides forward secrecy.</u> |
| <u>DRG.3.3</u> | <u>The RNG provides backward secrecy even if the current internal state is known.¹</u> |
| <u>FCS_RNG.1.2/DRNG</u> | The TSF shall provide <u>numbers in the format 32-bit²</u> that meet |
| <u>DRG.3.4</u> | <u>The RNG, initialized with a random seed, where the seed has at least 100 bit of entropy and is derived by a PTG.2 certified PTRNG. The RNG generates output for which any consecutive 2³⁴ strings of bit length 128 are mutually different with a probability that is greater than $1 - 2^{(-16)}$.</u> |
| <u>DRG3.5</u> | Statistical test suites cannot practically distinguish the random numbers from the output sequences of an ideal RNG. The random numbers must pass test procedure A and the U.S. National Institute of Standards and Technology (NIST) test suite for RNGs used for cryptographic purposes [N800-22] containing following 16 tests: <u>Frequency (Monobit) Test, Frequency Test within a Block, Runs Tests, Test for the Longest-Run-of-Ones in a Block, Binary Matrix Rank Test, Discrete Fourier Transform (Spectral) Test, Non-overlapping (Aperiodic) Template Matching Test, Overlapping (Periodic) Template Matching Test, Maurer's "Universal Statistical" Test, Liner Complexity Test, Serial Test, Approximate Entropy Test, Cumulative Sums (Cusums) Test, Random Excursions Test and Random Excursions Variant Test.³</u> |

6.1.2.4 Deterministic Random Number Generation (DRNG) AIS31 DRG.4

| | |
|--------------------------|--|
| FCS_RNG.1/DRNG4 | Random Number Generation |
| Hierarchical to | No other components. |
| Dependencies | No dependencies |
| FCS_RNG.1/DRNG4 | Random numbers generation Class DRG.4 according to [BSI_RNGs] |
| <u>FCS_RNG.1.1/DRNG4</u> | The TSF shall provide a <u>hybrid deterministic⁴</u> random number generator that implements: |
| <u>DRG.4.1</u> | <u>The internal state of the RNG shall use PTRNG of class PTG.2 as random source</u> |
| <u>DRG.4.2</u> | <u>The RNG provides forward secrecy.</u> |
| <u>DRG.4.3</u> | <u>The RNG provides backward secrecy even if the current internal state is known.</u> |
| <u>DRG.4.4</u> | <u>The RNG provides enhanced forward secrecy on demand.</u> |
| <u>DRG.4.5</u> | <u>The internal state of the RNG is seeded by an PTRNG of class PTG.2.⁵</u> |
| <u>FCS_RNG.1.2/DRNG4</u> | The TSF shall provide <u>numbers in the format 32-bit⁶</u> that meet |

¹ [assignment: list of security capabilities]² [selection: bit, octets of bits, numbers [assignment: format of the numbers]]³ [assignment: a defined quality metric]⁴ [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]⁵ [assignment: list of security capabilities]⁶ [selection: bit, octets of bits, numbers [assignment: format of the numbers]]

Security Requirements (ASE_REQ)

| | |
|----------------|--|
| <u>DRG.4.6</u> | <u>The RNG generates output for which any consecutive 2^{34} strings of bit length 128 are mutually different with a probability that is greater than $1 - 2^{(-16)}$.</u> |
| <u>DRG4.7</u> | <u>Statistical test suites cannot practically distinguish the random numbers from the output sequences of an ideal RNG. The random numbers must pass test procedure A.¹</u> |

Note: The enhanced forward secrecy is assured by reseeding the internal state, which may be initiated on user demand (at any time).

6.1.2.5 RNG's provided by RCL

The RCL provides a shell around the hardware RNG for PTG.2:

| | |
|-----------------------------|--|
| FCS_RNG.1/RCL/TRNG | Random Number Generation |
| Hierarchical to | No other components. |
| Dependencies | No dependencies |
| FCS_RNG.1/RCL/TRNG | Random numbers generation Class PTG.2 according to [BSI_RNGs] |
| <u>FCS_RNG.1.1/RCL/TRNG</u> | <u>The TSF shall provide a <u>physical²</u> random number generator that implements:</u> |
| <u>PTG.2.1</u> | <u>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.</u> |
| <u>PTG.2.2</u> | <u>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.</u> |
| <u>PTG.2.3</u> | <u>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.</u> |
| <u>PTG.2.4</u> | <u>The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.</u> |
| <u>PTG.2.5</u> | <u>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.³</u> |
| <u>FCS_RNG.1.2/RCL/TRNG</u> | <u>The TSF shall provide <u>numbers in the format n x 32-bit⁴</u> that meet</u> |
| <u>PTG.2.6</u> | <u>Test procedure A, as defined in [BSI_RNGs] does not distinguish the internal random numbers from output sequences of an ideal RNG.</u> |
| <u>PTG.2.7</u> | <u>The average Shannon entropy per internal random bit exceeds 0.997.⁵</u> |

¹ [assignment: a defined quality metric]

² [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]

³ [assignment: list of security capabilities]

⁴ [selection: bit, octets of bits, numbers [assignment: format of the numbers]]

⁵ [assignment: a defined quality metric]

Security Requirements (ASE_REQ)

The RCL implements an RNG of class DRG.3 of [BSI_RNGs] as follows:

| FCS_RNG.1/RCL/DRNG3 | Random Number Generation |
|----------------------------|--|
| Hierarchical to | No other components. |
| Dependencies | No dependencies |
| FCS_RNG.1/RCL/DRNG3 | Random numbers generation Class DRG.3 according to [BSI_RNGs] |
| FCS_RNG.1.1/RCL/DRNG3 | The TSF shall provide a <u>deterministic</u> ¹ random number generator that implements: [N800-90A] ² |
| FCS_RNG.1.2/RCL/DRNG.3 | The TSF shall provide random numbers that meet: <u>Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG.</u> ³ |

Note: To fulfill the requirements defined in [BSI_RNGs] a refinement of the functional requirement FCS_RNG.1 is provided below:

| | |
|----------------------------|---|
| FCS_RNG.1/RCL/DRNG3 | Random numbers generation Class DRG.3 according to [BSI_RNGs] |
| FCS_RNG.1.1/RCL/DRNG3 | The TSF shall provide a <u>deterministic</u> ⁴ random number generator that implements: [N800-90A] |
| <u>DRG.3.1</u> | <u>If initialized with a random seed using a PTRNG of class PTG.2 as random source the internal state of the RNG shall have at least 100 bit of entropy and implements: [N800-90A].</u> |
| <u>DRG.3.2</u> | <u>The RNG provides forward secrecy.</u> |
| <u>DRG.3.3</u> | <u>The RNG provides backward secrecy even if the current internal state is known.</u> ⁵ |
| FCS_RNG.1.2/RCL/DRNG3 | The TSF shall provide random numbers that meet |
| <u>DRG.3.4</u> | <u>The RNG, initialized with a random seed, during every startup and after 2^{31} requests of minimal 128 bits using PTRNG of class PTG.2, generates output for which more than 2^{34} strings of bit length 128 are mutually different with probability $w > 1 - 2^{-16}$.</u> |
| <u>DRG3.5</u> | <u>Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A.</u> ⁶ |

The RCL implements an RNG of class DRG.4 of [BSI_RNGs] as follows:

| FCS_RNG.1/RCL/DRNG4 | Random Number Generation |
|----------------------------|---------------------------------|
| Hierarchical to | No other components. |

¹ [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]

² [assignment: list of security capabilities]

³ [assignment: a defined quality metric]

⁴ [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]

⁵ [assignment: list of security capabilities]

⁶ [assignment: a defined quality metric]

Security Requirements (ASE_REQ)

| | |
|----------------------------|--|
| Dependencies | No dependencies |
| FCS_RNG.1/RCL/DRNG4 | Random numbers generation Class DRG.4 according to [BSI_RNGs] |
| FCS_RNG.1.1/RCL/DRNG4 | The TSF shall provide a <u>hybrid deterministic</u> ¹ random number generator that implements: [N800-90A] ² |
| FCS_RNG.1.2/RCL/DRNG.4 | The TSF shall provide random numbers that meet: <u>Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG.</u> ³ |

Note: To fulfill the requirements defined in [BSI_RNGs] a refinement of the functional requirement FCS_RNG.1 is provided below:

| | |
|----------------------------|--|
| FCS_RNG.1/RCL/DRNG4 | Random numbers generation Class DRG.4 according to [BSI_RNGs] |
| FCS_RNG.1.1/RCL/DRNG4 | The TSF shall provide a <u>hybrid deterministic</u> ⁴ random number generator that implements: [N800-90A] |
| <u>DRG.4.1</u> | <u>The internal state of the RNG shall use PTRNG of class PTG.2 as random source</u> |
| <u>DRG.4.2</u> | <u>The RNG provides forward secrecy.</u> |
| <u>DRG.4.3</u> | <u>The RNG provides backward secrecy even if the current internal state is known.</u> |
| <u>DRG.4.4</u> | <u>The RNG provides enhanced forward secrecy on demand.</u> |
| <u>DRG.4.5</u> | <u>The internal state of the RNG is seeded by an PTRNG of class PTG.2.</u> ⁵ |
| FCS_RNG.1.2/RCL/DRNG4 | The TSF shall provide random numbers that meet |
| <u>DRG.4.6</u> | <u>The RNG, initialized with a random seed, during every startup and after each request of random data up to 4096 Bits using PTRNG of class PTG.2, generates output for which more than 2^{34} strings of bit length 128 are mutually different with probability $w > 1 - 2^{-16}$.</u> |
| <u>DRG4.7</u> | <u>Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A.</u> ⁶ |

Note: The enhanced forward secrecy is assured by reseeding the internal state, which may be initiated on user demand (at any time).

6.1.2.6 Cipher schemes provided by the SCP

| | |
|------------------------------------|--|
| FCS_COP.1/<iteration> | 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, or |

¹ [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]

² [assignment: list of security capabilities]

³ [assignment: a defined quality metric]

⁴ [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]

⁵ [assignment: list of security capabilities]

⁶ [assignment: a defined quality metric]

Security Requirements (ASE_REQ)

| | |
|-------------------------|--|
| | FCS_CKM.5 Cryptographic key derivation] |
| | FCS_CKM.6 Timing and event of cryptographic key destruction |
| FCS_COP.1.1/<iteration> | The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards] |

The operations performed in this SFR are defined in the following table. Please note that <iteration> is a placeholder for different SFR iterations defined in the first column.

Table 16 Cryptographic table for FCS_COP.1

| <iteration> | [assignment: list of cryptographic operations] | [assignment: cryptographic algorithm] | [assignment: cryptographic key sizes] | [assignment: list of standards] |
|-------------|--|---------------------------------------|---------------------------------------|--------------------------------------|
| SCP/TDES | encryption and decryption | TDES in ECB mode, CBC mode | 112 bit, 168 bit | [N800-67B], [N800-38A], [ISO18033_3] |
| SCP/AES | encryption and decryption | AES in ECB mode, CBC mode | 128 bit, 192 bit, 256 bit | [N197], [N800-38A], [ISO18033_3] |

| FCS_CKM.6/SCP | Timing and event of cryptographic key destruction |
|------------------|---|
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation] |
| FCS_CKM.6.1/SCP | The TSF shall destroy <u>cryptographic SCP registers</u> ¹ when <u>a user overwrites these registers</u> ² . |
| FCS_CKM.6.2/SCP | The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method <u>overwriting or zeroing</u> ³ that meets the following: <u>None</u> ⁴ |

Note: The key destruction can be done by overwriting the key register interfaces or by software reset of the SCP which provides immediate zeroing of all SCP key registers.

6.1.2.7 Cipher schemes provided by the SCL

| FCS_COP.1/<iteration> | Cryptographic operation |
|-----------------------|-------------------------|
| Hierarchical to: | No other components. |

¹ [assignment: list of cryptographic keys (including keying material)]

² [selection: no longer needed, [assignment: other circumstances for key or keying material destruction]]

³ [assignment: cryptographic key destruction method]

⁴ [assignment: list of standards]

Security Requirements (ASE_REQ)

| | |
|-------------------------|---|
| 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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction |
| FCS_COP.1.1/<iteration> | The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes of [assignment: cryptographic key sizes] that meet the following standards: [assignment: list of standards] |

The operations performed in this SFR are defined in the following table. Please note that <iteration> is a placeholder for different SFR iterations defined in the first column.

Table 17 Cryptographic table for FCS_COP.1

| <iteration> | [assignment: list of cryptographic operations] | [assignment: cryptographic algorithm] | [assignment: cryptographic key sizes] | [assignment: list of standards] |
|--------------|--|---|---------------------------------------|--|
| SCL/TDES | encryption and decryption | TDES in ECB mode, CBC mode, CTR mode, CFB mode | 112 bit, 168 bit | [N800-67B], [N800-38A] |
| SCL/AES | encryption and decryption | AES in ECB mode, CBC mode, CTR mode, CFB mode | 128 bit, 192 bit, 256 bit | [N197], [N800-38A] |
| SCL/TDES-MAC | MAC generation | TDES in CMAC mode and Retail MAC mode (Algorithm 3) | 112 Bit, 168 Bit | [N800-67B] (TDES), [N800-38B] (MAC), [ISO9797B] (Retail MAC) |
| SCL/AES-MAC | MAC generation | AES in CMAC mode | 128 Bit, 192 Bit, 256 Bit | [N197] (AES), [N800-38B] (MAC) |

FCS_CKM.6/SCL Timing and event of cryptographic key destruction

| | |
|------------------|---|
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation] |
| FCS_CKM.6.1/SCL | The TSF shall destroy <u>cryptographic keys stored in RAM</u> ¹ when <u>the cipher operation is closed</u> ² . |
| FCS_CKM.6.2/SCL | The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method <u>overwrite with zero or random data</u> ³ that meets the following: <u>None</u> ⁴ |

¹ [assignment: list of cryptographic keys (including keying material)]

² [selection: no longer needed, [assignment: other circumstances for key or keying material destruction]]

³ [assignment: cryptographic key destruction method]

⁴ [assignment: list of standards]

Security Requirements (ASE_REQ)

Note: The TOE can be delivered with or without the SCL. If the user decides not to use the SCL, the SFRs in this chapter are not part of the TOE.

6.1.2.8 Rivest-Shamir-Adleman (RSA)

For cryptographic RSA functionality, the TOE shall meet the requirement cryptographic operation (FCS_COP.1) and cryptographic key construction (FCS_CKM .1) as specified below:

| FCS_COP.1/RSA/<iteration> | 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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic destruction |
| FCS_COP.1.1/RSA/<iteration> | The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes of [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards] |

Table 18 Cryptographic table for FCS_COP.1/RSA

| <iteration> | [assignment: list of cryptographic operations] | [assignment: cryptographic algorithm] | [assignment: cryptographic key sizes] | [assignment: list of standards] |
|----------------------------|---|--|--|--|
| ENC_v3.02.000 | RSA encryption | RSAEP, IFEP-RSA | 1024 – 2112 Bits | [RSA-PKCSB], ch. 5.1.1 [IEEE1363], ch. 8.2.2 |
| ENC_v3.33.003 and 3.35.001 | RSA encryption | RSAEP, IFEP-RSA | 1024 – 4224 Bits | [RSA-PKCSB], ch. 5.1.1 [IEEE1363], ch. 8.2.2 |
| DEC | RSA decryption | RSADP, IFDP-RSA | 1024 – 2112 Bits | [RSA-PKCSB], ch. 5.1.2 [IEEE1363], ch. 8.2.1(I) and 8.2.3 |
| DEC_CRT | RSA decryption | RSADP (CRT), IFDP-RSA (CRT) | 1024 – 4224 Bits | [RSA-PKCSB], ch. 5.1.2 [IEEE1363], ch. 8.2.1(II) and 8.2.3 |
| SIG | RSA signature generation | RSASP1 IFSP-RSA1 | 1024 – 2112 Bits | [RSA-PKCSB], ch. 5.2.1 [IEEE1363], ch. 8.2.1(I) and 8.2.4 |
| SIG_CRT | RSA signature generation | RSASP1 (CRT) IFSP-RSA1 (CRT) | 1024 – 4224 Bits | [RSA-PKCSB], ch. 5.2.1 [IEEE1363], ch. 8.2.1(II) and 8.2.4 |

Security Requirements (ASE_REQ)

| <iteration> | [assignment: list of cryptographic operations] | [assignment: cryptographic algorithm] | [assignment: cryptographic key sizes] | [assignment: list of standards] |
|---|--|---------------------------------------|---------------------------------------|--|
| VER | RSA signature verification | RSAPV1 IFVP-RSA1 | 1024 – 4224 Bits | [RSA-PKCSB], ch. 5.2.2 [IEEE1363], ch. 8.2.5 |
| RSA_DH (only applicable for ACL v3.33.003 and 3.35.001) | key agreement | DH key agreement | Modulus length = 1024 – 4224 Bits | [N186-4], ch.5.5 [RSA-PKCSB], ch. 5.2.1 and ch. 5.1.2 [IEEE1363], ch. 8.2.4 and ch.8.2.3 |

Note: RSA CRT is with 2 primes only, i.e. always with $u = 2$ in [RSA-PKCSB]

| FCS_CKM.1/RSA/<iteration> | Cryptographic key generation |
|-----------------------------|---|
| Hierarchical to: | No other components. |
| Dependencies: | [FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction |
| FCS_CKM.1.1/RSA/<iteration> | The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards] |

Table 19 Cryptographic table for FCS_CKM.1/RSA/

| <iteration> | [assignment: cryptographic key generation algorithm] | [assignment: cryptographic key sizes] | [assignment: list of standards] |
|-------------------------------------|---|---------------------------------------|---|
| CRT (prime generation not included) | IFX RSA CRT key generation; prime generation not included | Modulus length= 1024 – 4224 Bits | [RSA-PKCSB], ch. 3.1 and 3.2 (2) [IEEE1363], ch. 8.1.3.1(2) |
| n_d (prime generation not included) | IFX RSA key generation (i.e. without CRT) and return of (n, d); prime generation not included | Modulus length = 1024 – 2112 Bits | [RSA-PKCSB], ch. 3.1 and 3.2 (1) [IEEE1363], ch. 8.1.3.1(1) |
| p_q_d (including prime generation) | IFX RSA key generation (i.e. without CRT) and return of (p, q, d) including prime generation | Modulus length = 1024 – 2112 Bits | [IEEE1363], ch. 8.1.3.1(3) [N186-4] B.3.3: (only for prime Bitlength ≥ 1024 ; in case prime Bitlength < 1024 identical algorithm is used, but considered proprietary) |

Security Requirements (ASE_REQ)

| <iteration> | [assignment: cryptographic key generation algorithm] | [assignment: cryptographic key sizes] | [assignment: list of standards] |
|---|---|---|--|
| PRIME_GEN (only applicable for v3.35.001) | Prime number generation (in the context of an RSA key generation) | length of prime number = 512 – 2112 Bits | n.a. |
| 2PRIME_GEN (only applicable for v3.33.003 and v3.35.001) | Prime number generation | length of prime number = 512 – 2064 Bits | [N186-4] B.3.3: (only for prime Bitlength >= 1024; in case prime Bitlength < 1024 identical algorithm is used, but considered proprietary) [N186-4] C.3.1 |
| PRIME_CHECK_MASK | Primality test (in the context of an RSA key generation) | length of prime number = 512 – 2064 Bits | [N186-4] C3.1 and C3.2 |
| PRIME_CHECK | Primality test (in the context of an RSA key generation) | length of prime number = 512 – 2112 Bits | n.a. |

Note: RSA CRT is with 2 primes only, i.e. always with $u = 2$ in [RSA-PKCSB]

Note: The TOE can be delivered with or without the optional RSA library. If the RSA library is not delivered, the TOE does not provide this SFR. In case of a blocked Crypto@2304T the optionally delivered cryptographic RSA library cannot be used and therefore the SFRs of this chapter are also not applicable.

Note: (applicable to ACL v3.02.000 and v3.33.003) :

CryptoGeneratePrime can only be performed in trustworthy environments. See corresponding documents “ACL37-Crypto2304T-C40 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox” for detail.

6.1.2.9 Elliptic Curve Cryptography (ECC)

For cryptographic ECC functionality, the TOE shall meet the requirement cryptographic operation (FCS_COP.1) and cryptographic key construction (FCS_CKM .1) as specified below:

| FCS_COP.1/ECC/<iteration> | 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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction |
| FCS_COP.1.1/ECC/<iteration> | The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards] |

Security Requirements (ASE_REQ)

Table 20 Cryptographic table for FCS_COP.1/ECC

| <iteration> | [assignment: list of cryptographic operations] | [assignment: cryptographic algorithm] | [assignment: cryptographic key sizes] | [assignment: list of standards] |
|--|--|---------------------------------------|---------------------------------------|---|
| SIG | EC signature generation | ECDSA ECSP-DSA | 160 – 521 Bits | [ANSX9.62], ch. 7.3 [IEEE1363], ch. 7.2.7 |
| VER | EC signature verification | ECDSA ECVP-DSA | 160 – 521 Bits | [ANSX9.62], ch. 7.4.1 [IEEE1363], ch. 7.2.8 |
| DH | ECDH key agreement | ECDH ECSVHDP-DH | 160 – 521 Bits | [ANSX9.63], ch. 5.4.1 [ISO11770_3], appendix D.6 [IEEE1363], ch. 7.2.1 |
| PACE_IM_ECDH (only applicable for ACL v3.33.003 and 3.35.001) | Pace integrated mapping | PACE integrated mapping | 160 – 521 Bits | [ICAO_11] , Appendix B2 |

Note: The following ECC curves are in scope of this evaluation:

- all Brainpool curves from [IETF5639]
- all NIST curves over prime fields from [N186-4]

Note: For the /SIG iteration, the following deviations from the standards apply:

- In [ANSX9.62]:
Step d) is not supported

Note: For the /VER iteration, the following deviations from the standards apply:

- In [ANSX9.62]:
Step b) is not supported.
Beside noted calculation, our algorithm adds a random multiple of order of the basepoint to the calculated values u_1 and u_2 .

Note: For the /DH iteration, the implementation always returns the y-coordinate in addition to the x-coordinate.

Note: Cofactor multiplication is not supported

| FCS_CKM.1/ECC | Cryptographic key generation |
|-----------------|---|
| Hierarchical to | No other components. |
| Dependencies | [FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction |

Security Requirements (ASE_REQ)

| | |
|-----------------|---|
| FCS_CKM.1.1/ECC | The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm <u>EC key generation</u> ¹ and specified cryptographic key sizes of <u>160-521 bits</u> ² that meet the following: <u>[ANSX9.62], ch. A4.3 and [IEEE1363], ch. A.16.9.</u> ³ |
|-----------------|---|

Note: The following ECC curves are in scope of this evaluation:

- all Brainpool curves from [IETF5639]
- all NIST curves from [N186-4]

Note: The TOE can be delivered with or without the optional ECC library. If the ECC library is not delivered, the TOE does not provide the SFRs of this chapter. In case of a blocked Crypto@2304T the optionally delivered cryptographic ECC library cannot be used and therefore this SFR is also not applicable. .

6.1.2.10 HCL Hash Cryptographic Library (without Hash HW module)

For hash cryptographic operations the TOE shall meet the requirement Cryptographic operation (FCS_COP.1) as specified below:

| FCS_COP.1/HCL | 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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction |
| FCS_COP.1.1/HCL | The TSF shall perform <u>cryptographic hash digest computation</u> ⁴ in accordance with a specified cryptographic algorithm <u>SHA-1 and SHA-2 with digest length 160 (SHA-1 only), 224, 256, 384, 512, 512/224 and 512/256</u> ⁵ with cryptographic key sizes of <u>none</u> ⁶ that meet the following: <u>[N180-4]</u> ⁷ |

6.1.3 Subset of TOE testing

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

The TOE shall meet the requirement “Subset TOE testing (FPT_TST.2)” as specified below (Common Criteria Part 2 extended).

¹ [assignment: list of cryptographic operations]

² [assignment: cryptographic key sizes]

³ [assignment: list of standards]

⁴ [assignment: list of cryptographic operations]

⁵ [assignment: cryptographic algorithm]

⁶ [assignment: cryptographic key sizes]

⁷ [assignment: list of standards]

Security Requirements (ASE_REQ)

| FPT_TST.2 | Subset TOE testing |
|------------------|---|
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies |
| FPT_TST.2.1 | <p>The TSF shall run a suite of self tests <u>at the conditions request of the Security IC Embedded Software¹</u> to demonstrate the correct operation of <u>the alarm lines and/or the environmental sensor mechanisms:</u></p> <ul style="list-style-type: none"> • <u>Please refer to the confidential Security Target²</u> |

6.1.4 Memory access control

Usage of multiple applications in one Smartcard often requires code and data separation in order to prevent that one application can access code and/or data of another application. For this reason the TOE provides Area based Memory Access Control. The underlying Memory Protection Unit (MPU) is documented in Appendix B3.5 of the ARMv7 M architecture reference manual [ARMv7M].

In particular, the MPU provides full support for:

- Protection regions.
- Overlapping protection regions, with ascending region priority:
 - Region 7 = highest priority.
 - Region 0 = lowest priority.
- Access permissions.
- MPU mismatches and permission violations invoke the programmable-priority MemManage fault handler.

The MPU can be used to:

- Enforce privilege rules, preventing user applications from corrupting operating system data.
- Separate processes, blocking the active task from accessing other tasks' data.
- Enforce access rules, allowing memory regions to be defined as read-only or detecting unexpected memory accesses.

The SFRs are provided by the **Memory Access Control Policy** (FDP_ACC.1 and dependencies).

6.1.4.1 Subjects, objects and operations of the Memory Access Control Policy

Subjects:

- MPU

Objects:

- memory/code addresses

Operations:

- Read a/o write a/o execute access

¹ [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, and/or at the conditions [assignment: conditions under which self test should occur]]

² [assignment: functions and/or mechanisms]

Security Requirements (ASE_REQ)

6.1.4.2 Security attributes of the Memory Access Control Policy

Security Attribute which define the roles for Subject MPU:

- Npriv flag defining privilege/non-privilege mode

Security Attribute which control the behavior of the Subject MPU:

- MPU enable/disable bit.
- 8 regions with the following attributes
 - a unique priority
 - the enable bit
 - the xn (execute never) bit
 - the start address and size
 - an access matrix which defines if an Operation of the MPU (Subject) to a memory/code address (Object) lying in the region is allowed or denied
- A bit defining the access behavior of the default region, i.e. memory/code addresses not covered by one of the 8 MPU regions.

Security Attributes for objects:

There are no security attributes for objects.

6.1.4.3 Access control rules of the Memory Access Control Policy

The following generic rules shall apply in case the MPU is enabled. In case the MPU is disabled, a privileged and unprivileged code has full read/write/execute rights to all addresses.

- overlapping regions, have access to other regions with ascending region priority: region 7 = highest priority, region 0 = lowest priority. This means, if an address is contained in multiple enabled regions, then the region with the highest priority defines the access rights.
- If an address is contained in no region then the default region defines the access rights.
- The region defining the access rights checks if the Subject has access to the Object with respect to the desired Operation. In case the access is denied the MPU throws an access violation exception. The checks are done according to the access matrix in Table 21.
- execution of code is bound to the read access of Table 21 and the xn bit. If the xn bit is cleared and read access is enabled then execution of code is defined by Table 21. If the xn bit is set then execution is never allowed.

Table 21 Access matrix for read(execute)/write access

| Privileged Mode Permissions | User Mode Permissions | Description |
|-----------------------------|-----------------------|---|
| No access | No access | All accesses in user mode and privileged mode generate a permission fault |
| Read/write | No access | Privilege mode has read/write access while any access from user mode leads to a permission fault. |

Security Requirements (ASE_REQ)

| Privileged Mode Permissions | User Mode Permissions | Description |
|-----------------------------|-----------------------|--|
| Read/write | Read | Privileged mode has read/write access while the user mode has read access only. |
| Read/write | Read/write | Privileged and user mode have read and write access. |
| Read | No access | Privileged mode has read access, while any access from user mode leads to a permission fault |
| Read | Read | Both modes have read access |

6.1.4.4 SFRs of the Memory Access Control Policy

| | |
|------------------|--|
| 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 <u>Memory Access Control Policy</u> ¹ on the list of subjects, objects, and operations among subjects and objects covered by the SFP as defined in section 6.1.4.1 ² . |
| 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 <u>Memory Access Control Policy</u> ³ to objects based on the following: <u>Attributes as specified in section 6.1.4.2</u> ⁴ . |
| FDP_ACF.1.2 | The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: <u>As specified in the section 6.1.4.3</u> ⁵ . |
| FDP_ACF.1.3 | The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: <u>none</u> ⁶ . |
| FDP_ACF.1.4 | The TSF shall explicitly deny access of subjects to objects based on the following additional rules: <u>none</u> ⁷ . |

¹ [assignment: access control SFP]² [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]³ [assignment: access control SFP]⁴ [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]⁵ [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]⁶ [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]⁷ [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

Security Requirements (ASE_REQ)

| | |
|------------------|---|
| 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 <u>Memory Access Control Policy</u> ¹ to provide <u>restrictive</u> ² default values for security attributes that are used to enforce the SFP. |
| FMT_MSA.3.2 | The TSF shall allow the <u>privilege mode</u> ³ to specify alternative initial values to override the default values when an object or information is created. |
| 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 <u>Memory Access Control Policy</u> ⁴ to restrict the ability to <u>modify</u> ⁵ the security attributes <u>Security Attribute which control the behavior of the Subject MPU</u> ⁶ to the <u>privilege mode</u> ⁷ . |
| 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: <u>modifying the security attributes</u> ⁸ . |
| FMT_SMR.1 | Security roles |
| Hierarchical to: | No other components. |
| Dependencies: | FIA_UID.1 Timing of identification |
| FMT_SMR.1.1 | The TSF shall maintain the roles <u>privilege mode and non-privilege mode</u> ⁹ . |
| FMT_SMR.1.2 | The TSF shall be able to associate users with roles. |

6.1.5 Data Integrity

| | |
|------------------|---|
| FDP_SDI.2 | Stored data integrity monitoring and action |
| Hierarchical to: | FDP_SDI.1 stored data integrity monitoring |

¹ [assignment: access control SFP, information flow control SFP]

² [selection, choose one of: restrictive, permissive, [assignment: other property]]

³ [assignment: the authorised identified roles]

⁴ [assignment: access control SFP(s), information flow control SFP(s)]

⁵ [selection: change_default, query, modify, delete, [assignment: other operations]]

⁶ [assignment: list of security attributes]

⁷ [assignment: the authorised identified roles]

⁸ [assignment: list of management functions to be provided by the TSF]

⁹ [assignment: the authorised identified roles]

Security Requirements (ASE_REQ)

| | |
|------------------|--|
| Dependencies: | No dependencies |
| FDP_SDI.2.1 | The TSF shall monitor user data stored in containers controlled by the TSF for <u>data integrity and one- and/or more-bit-errors</u> ¹ on all objects, based on the following attributes: <u>error correction ECC for the SOLID FLASH™ NVM</u> ² . |
| FDP_SDI.2.2 | Upon detection of a data integrity error, the TSF shall <u>correct 1 bit errors in the SOLID FLASH™ NVM automatically and inform the user about other bit errors</u> ³ . |
| FDP_SDC.1 | Stored data confidentiality |
| Hierarchical to: | No other components |
| Dependencies: | No dependencies |
| FDP_SDC.1.1 | The TSF shall ensure the confidentiality of <u>the information of all user data</u> ⁴ while it is stored in the <u>any memory</u> ⁵ . |

6.1.6 Limited Capabilities and Limited Availability

The SFR's FMT_LIM.1 and FMT_LIM.2 from [PP0084] are adapted due to CC:2022.

| | |
|------------------|---|
| FMT_LIM.1 | Limited Capabilities |
| Hierarchical to: | No other components. |
| Dependencies: | FMT_LIM.2: Limited availability |
| FMT_LIM.1.1 | The TSF shall limit its capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: <u>Deploying Test Features after TOE Delivery does not allow user data of the Composite TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks</u> ⁶ . |
| FMT_LIM.2 | Limited availability |
| Hierarchical to: | No other components. |
| Dependencies: | FMT_LIM.1 Limited capabilities. |
| FMT_LIM.2.1 | The TSF shall be designed in a manner that limits its availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: <u>Deploying Test Features after TOE Delivery does not allow user data of the Composite TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks</u> ⁷ . |

¹ [assignment: integrity errors]

² [assignment: user data attributes]

³ [assignment: action to be taken]

⁴ [selection: all user data, the following user data[assignment: list of user data]]

⁵ [selection: temporary memory, persistent memory, any memory]

⁶ [assignment: Limited capability and availability policy]

⁷ [assignment: Limited capability and availability policy]

Security Requirements (ASE_REQ)

6.1.7 Support of Flash Loader

The TOE provides a Flash Loader to download user data into the SOLID FLASH™ NVM, either during production of the TOE or at customer site. Depending on the configuration option EA the Flash Loader claims different sets of SFRs. [PP0084] section 7.3.1 “Package 1: Loader dedicated for usage in secured environment only” is claimed for both options. [PP0084] section 7.2 Package “Authentication of the Security IC” and [PP0084] section 7.3.2 “Package 2: Loader dedicated for usage by authorized users only” is only claimed in case TOE is ordered with EA unavailable, however a subset of SFRs from loader package 2 is also claimed, if TOE is ordered with EA available.

6.1.8 Flash Loader Policy

The table as follows shows the Flash Loader SFR claims in dependency of the order option EA.

Table 22 Flash loader SFR claims

| EA unavailable | EA available |
|---|---|
| Limited capabilities (FMT_LIM.1/Loader) | Limited capabilities (FMT_LIM.1/Loader) |
| Limited availability – Loader (FMT_LIM.2/Loader) | Limited availability – Loader (FMT_LIM.2/Loader) |
| Authentication Proof of Identity (FIA_API.1) | - |
| Inter-TSF trusted channel (FTP_ITC.1) | - |
| Basic data exchange confidentiality (FDP_UCT.1) | Basic data exchange confidentiality (FDP_UCT.1) |
| Data exchange integrity (FDP_UIT.1) | Data exchange integrity (FDP_UIT.1) |
| Subset access control – Loader (FDP_ACC.1/Loader) | Subset access control – Loader (FDP_ACC.1/Loader) |
| Security attribute based access control – Loader (FDP_ACF.1/Loader) | Security attribute based access control – Loader (FDP_ACF.1/Loader) |
| Management of TSF data – Loader (FMT_MTD.1/Loader) | Management of TSF data – Loader (FMT_MTD.1/Loader) |
| Security Roles – Loader (FMT_SMR.1/Loader) | Security Roles – Loader (FMT_SMR.1/Loader) |
| Specification of Management Functions – Loader (FMT_SMF.1/Loader) | Specification of Management Functions – Loader (FMT_SMF.1/Loader) |
| User Identification before any action – Loader (FIA_UID.2/Loader) | User Identification before any action – Loader (FIA_UID.2/Loader) |

The TOE shall meet the loader SFRs as specified below:

| FMT_LIM.1/Loader | Limited Capabilities - Loader |
|--------------------|---|
| Hierarchical to: | No other components. |
| Dependencies: | FMT_LIM.2: Limited availability |
| FMT_LIM.1.1/Loader | The TSF shall limit its capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: <u>Deploying Loader functionality after permanent deactivation does not allow stored user data to be disclosed or</u> |

Security Requirements (ASE_REQ)

manipulated by unauthorized user. The TSF prevents deploying the Loader functionality after permanent deactivation¹.

FMT_LIM.2/Loader Limited availability - Loader

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

FMT_LIM.2.1/Loader The TSF shall be designed in a manner that limits its availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: Deploying Loader functionality after permanent deactivation does not allow stored user data to be disclosed or manipulated by unauthorized user. The TSF prevents deploying the Loader functionality after permanent deactivation².

Regarding FMT_LIM.1.1/Loader the User Guidance requires the Flash Loader to be permanently deactivated prior delivery to the end user (Phase 7).

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and administrator user, or Download operator user³, that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit another trusted IT product⁴ to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for deploying Loader for downloading user data⁵.

FDP_UCT.1 Basic data exchange confidentiality

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 The TSF shall enforce the Loader SFP⁶ to receive⁷ user data in a manner protected from unauthorised disclosure.

FDP_UIT.1 Data exchange integrity

Hierarchical to: No other components.

¹ [assignment: Limited capability and availability policy]

² [assignment: Limited capability and availability policy]

³ [assignment: users authorized for using the Loader]

⁴ [selection: the TSF, another trusted IT product]

⁵ [assignment: list of functions for which a trusted channel is required]

⁶ [assignment: access control SFP(s) and/or information flow control SFP(s)]

⁷ [selection: transmit, receive]

Security Requirements (ASE_REQ)

| | |
|---------------|---|
| 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 | The TSF shall enforce the <u>Loader SFP¹</u> to <u>receive²</u> user data in a manner protected from <u>modification, deletion, insertion³</u> errors. |
| FDP_UIT.1.2 | The TSF shall be able to determine on receipt of user data, whether <u>modification, deletion, insertion⁴</u> has occurred. |

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 <u>Loader SFP⁵</u> on <ul style="list-style-type: none"> • <u>the subjects Administrator User, Download Operator User and Image Provider,</u> • <u>the objects user data in SOLID FLASH™ NVM memory of the TOE,</u> • <u>the operation deployment of Loader⁶</u> |

FDP_ACF.1/Loader Security attribute based access control - Loader

| | |
|--------------------|---|
| Hierarchical to: | No other components. |
| Dependencies: | FMT_MSA.3 Static attribute initialisation |
| FDP_ACF.1.1/Loader | FDP_ACF.1.1 The TSF shall enforce the <u>Loader SFP⁷</u> to objects based on the following: <u>the subjects and objects of FDP_ACC.1.1/Loader without security attributes⁸</u> |
| FDP_ACF.1.2/Loader | FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: <u>The authenticated Administrator User or authenticated Download Operator User can modify the user data by new user data when the new user data is authorized by the Image Provider⁹</u> |
| FDP_ACF.1.3/Loader | FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: <u>none¹⁰</u> . |

¹ [assignment: access control SFP(s) and/or information flow control SFP(s)]

² [selection: transmit, receive]

³ [selection: modification, deletion, insertion, replay]

⁴ [selection: modification, deletion, insertion, replay]

⁵ [assignment: access control SFP]

⁶ [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

⁷ [assignment: access control SFP]

⁸ [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

⁹ [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

¹⁰ [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

Security Requirements (ASE_REQ)

| | |
|--------------------|---|
| FDP_ACF.1.4/Loader | The TSF shall explicitly deny access of subjects to objects based on the following additional rules: <u>none</u> ¹ . |
|--------------------|---|

The following SFRs have been added to the SFRs from Flash Loader package 2 of [PP0084] in order to describe the management of the various Flash Loader authentication keys.

| | |
|-------------------------|--|
| FMT_MTD.1/Loader | Management of TSF data |
| Hierarchical to: | No other components. |
| Dependencies: | FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions |
| FMT_MTD.1.1/Loader | The TSF shall restrict the ability to <u>change default, modify, delete</u> ² the <u>Authentication keys for Administrator User, Download Operator User and Image Provider</u> ³ to <u>Administrator User, Download Operator User</u> ⁴ . |

Note: The Administrator User can manage the keys for Administration User, Download Operator User and Image Provider. The Download Operator User can delete the key for Image Provider and Download Operator, otherwise manage the keys for the Download Operator User only. The image provider cannot modify any keys or perform authentication with the Flash Loader. It can simply built authentic loadable images.

| | |
|-------------------------|---|
| FMT_SMR.1/Loader | Security roles |
| Hierarchical to: | No other components. |
| Dependencies: | FIA_UID.1 Timing of identification |
| FMT_SMR.1.1/Loader | The TSF shall maintain the roles <u>Administrator User, Download Operator User, Image provider</u> ⁵ . |
| FMT_SMR.1.2/Loader | The TSF shall be able to associate users with roles. |

| | |
|-------------------------|---|
| FMT_SMF.1/Loader | Specification of Management Functions |
| Hierarchical to: | No other components. |
| Dependencies: | FIA_UID.1 Timing of identification |
| FMT_SMF.1.1/Loader | The TSF shall be capable of performing the following management functions: <u>Change Key, Invalidate Key</u> ⁶ . |

Note: “Change Key” of this SFR combines the “Change default” and “modify” operations from SFR FMT_MTD.1/Loader. “Invalidate Key” of this SFR is equivalent to the “delete” operation from SFR FMT_MTD.1/Loader.

| | |
|-------------------------|--|
| FIA_UID.2/Loader | User Identification before any action |
|-------------------------|--|

¹ [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

² [selection: change_default, query, modify, delete, clear, [assignment: other operations]]

³ [assignment: list of TSF data]

⁴ [assignment: the authorised identified roles]

⁵ [assignment: the authorised identified roles]

⁶ [assignment: list of management functions to be provided by the TSF]

Security Requirements (ASE_REQ)

| | |
|--------------------|--|
| Hierarchical to: | FIA_UID.1 |
| Dependencies: | No dependencies. |
| FIA_UID.2.1/Loader | The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. |

Note: The security functional requirements FIA_API.1, FTP_ITC.1, FDP_UCT.1, FDP_UIT.1, FDP_ACC.1/Loader, FDP_ACF.1/Loader, FMT_MTD.1/Loader, FMT_SMR.1/Loader, FMT_SMF.1/Loader and FIA_UID.2/Loader apply only to TOE products with activated Flash Loader. In other cases the Flash Loader is not available anymore and the user data download is completed.

6.1.9 Support of Authentication of the Security IC

The Flash Loader provides a security IC authentication service.

| FIA_API.1 | Authentication Proof of Identity |
|------------------|--|
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FIA_API.1.1 | The TSF shall provide an <u>authentication mechanism according to [ISO9798 2] section 6.2.2 Mechanism 4: Three-pass authentication¹</u> to prove the identity of <u>the TOE²</u> by including the following properties <u>proof of knowledge of Flash Loader administrator or download operator credentials³</u> to an external entity. |

This security functional requirement applies only to TOE products with Flash Loader activated and TOE is ordered with EA unavailable.

6.2 TOE Security Assurance Requirements

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

Table 23 Assurance components

| Aspect | Acronym | Description | Refinement |
|---------------|----------------|---|-------------------|
| Development | ADV_ARC.1 | Security Architecture Description | [PP0084] |
| | ADV_FSP.5 | Complete semi-formal functional specification with additional error information | [PP0084] |
| | ADV_IMP.2 | Complete mapping of the implementation representation of the TSF | [PP0084] |
| | ADV_INT.3 | Minimally complex internals | |
| | ADV_TDS.5 | Complete semi-formal modular design | |
| | ADV_SPM.1 | Formal TOE security policy model | |

¹ [assignment: authentication mechanism]

² [selection: TOE, [assignment: object, authorized user or role]]

³ [assignment: list of properties]

Security Requirements (ASE_REQ)

| Aspect | Acronym | Description | Refinement |
|--------------------------|-----------|--|------------|
| Guidance Documents | AGD_OPE.1 | Operational user guidance | [PP0084] |
| | AGD_PRE.1 | Preparative procedures | [PP0084] |
| Life-Cycle Support | ALC_CMC.5 | Advanced support | [PP0084] |
| | ALC_CMS.5 | Development tools CM coverage | [PP0084] |
| | ALC_DEL.1 | Delivery procedures | [PP0084] |
| | ALC_DVS.2 | Sufficiency of security measures | [PP0084] |
| | ALC_LCD.1 | Developer defined life-cycle model | |
| | ALC_TAT.3 | Compliance with implementation standards – all parts | |
| ST 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 | Rigorous analysis of coverage | [PP0084] |
| | ATE_DPT.3 | Testing: modular design | |
| | ATE_FUN.2 | Ordered functional testing | |
| | ATE_IND.2 | Independent testing - sample | |
| Vulnerability Assessment | AVA_VAN.5 | Advanced methodical vulnerability analysis | [PP0084] |

6.2.1 Refinements

Some refinements are taken unchanged from [PP0084]. Table 23 provides an overview.

Some refinements from [PP0084] have to be discussed here in the ST, as the assurance level is increased.

6.2.1.1 Implementation representation (ADV_IMP)

The refinement of [PP0084] requires the evaluator to check for completeness. In case of ADV_IMP.2 the entire implementation representation has to be provided anyhow. A check for completeness is also applicable in case the entire implementation representation is provided.

6.2.1.2 Life cycle support (ALC_CMS)

The refinement from [PP0084] can also be applied to the assurance level EAL 6 augmented with ALC_CMS.5. The assurance package ALC_CMS.4 is extended to ALC_CMS.5 with aspects regarding the configuration control system for the TOE. The refinement is still valid.

6.2.1.3 Configuration management capabilities (ALC_CMC)

The refinement from [PP0084] details, how configuration management has to be also applied to production. This is also applicable for ALC_CMC.5. ALC_CMC.5 is not specifically focused on production.

Security Requirements (ASE_REQ)

6.2.1.4 Test Coverage (ATE_COV)

The refinement in [PP0084] clarifies, how to deal with testing of security mechanisms for physical protection. It further requests the TOE to be tested under different operating conditions. These refinements are also applicable for ATE_COV.3, which requires complete TSFI coverage.

6.2.1.5 Functional Specification (ADV_FSP)

The refinement from [PP0084] can also be applied to the assurance level EAL 6 augmented with ADV_FSP.5. The assurance package ADV_FSP.4 is extended to ADV_FSP.5 with aspects regarding the level of description. ADV_FSP.5 requires a semi-formal description in addition. The refinement is still valid.

For refinement details see [PP0084].

6.3 Security Requirements Rationale

6.3.1 Rationale for the Security Functional Requirements

While the security functional requirements rationale of the TOE are defined and described in [PP0084] section 6.3.1, 7.2.3, 7.3.1, 7.3.2, 7.4.1 and 7.4.2, the additional introduced SFRs are discussed below:

Table 24 Rational for additional SFR in the ST

| Objective | TOE Security Functional Requirements |
|----------------------------|---|
| O.Phys-Manipulation | - FPT_TST.2 „ Subset TOE security testing “ |
| O.Mem-Access | - FDP_ACC.1 “Subset access control” - FDP_ACF.1 “Security attribute based access control” - FMT_MSA.3 “Static attribute initialisation” - FMT_MSA.1 “Management of security attributes” - FMT_SMF.1 “Specification of Management Functions” - FMT_SMR.1 “Security Roles” |
| O.AES-TDES-MAC | FCS_COP.1/SCL/TDES, FCS_COP.1/SCL/TDES-MAC, FCS_CKM.6/SCL, FCS_COP.1/SCL/AES, FCS_COP.1/SCL/AES-MAC, |
| O.AES | FCS_CKM.6/SCL, FCS_COP.1/SCL/AES |
| O.TDES | FCS_COP.1/SCL/TDES, FCS_CKM.6/SCL |
| O.RSA | FCS_COP.1/RSA/<iteration>, FCS_CKM.1/RSA/<iteration> |
| O.ECC | FCS_COP.1/ECC/<iteration>, FCS_CKM.1/ECC |
| O.HASH | FCS_COP.1/HCL |
| O.Prot_TSF_Confidentiality | - FTP_ITC.1 Inter-trusted-TSF channel - FDP_ACC.1/Loader Subset access control –Loader - FDP_ACF.1/Loader Security attribute based access control – Loader |
| O.Ctrl_Auth_Loader | FMT_MTD.1/Loader, FMT_SMR.1/Loader, FMT_SMF.1/Loader, FIA_UID.2/Loader |

The table above gives an overview how the security functional requirements are combined to meet the security objectives. This table has to be read in addition to [PP0084] table 2 “Security Requirements versus Security Objectives”. The detailed justification is given in the following:

Security Requirements (ASE_REQ)

The security functional component Subset TOE security testing (FPT_TST.2) has been newly created (Common Criteria Part 2 extended). This component allows that particular parts of the security mechanisms and functions provided by the TOE can be tested after TOE Delivery. This security functional component is used instead of the functional component FPT_TST.1 from Common Criteria Part 2. For the user it is important to know which security functions or mechanisms can be tested. The functional component FPT_TST.1 does not mandate to explicitly specify the security functions being tested. In addition, FPT_TST.1 requires verification of the integrity of TSF data and stored TSF executable code which might violate the security policy.

The security functional requirement FPT_TST.2 detects attempts to conduct a physical manipulation on the monitoring functions of the TOE. The objective of FPT_TST.2 is O.Phys-Manipulation.

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, FMT_SMF.1 and FMT_SMR.1 cover this security objective. The implementation of these functional requirements is represented by the dedicated privilege level concept.

The additional SCL related SFRs support standard TDES and AES encryption and decryption. It also offers MAC services based on these cryptographic primitives.

The additional cryptographic SFRs related to RSA and ECC are mapped to the respective RSA and ECC objectives.

The additional HCL related SFR supports standard SHA-1 and SHA-2 algorithms and is mapped to the respective hash objective.

The additional loader SFRs describe the Flash Loader roles and the access rules. Therefore these additional SFRs are mapped to O.Ctrl_Auth_Loader contributing to the aspect “access control for usage of the loader functionality” as described in [PP0084]. In case EA is chosen, FTP_ITC.1 is not part of the TOE and therefore not mapped to O.Ctrl_Auth_Loader. However due to the confidentiality and integrity protection of downloaded user data and one-way authentication from user towards Flash Loader, the loader can still be controlled in an effective way and prevent misuse of unauthorized usage.

The loader SFR FTP_ITC.1, FDP_ACC.1/Loader and FDP_ACF.1/Loader describe the requirement of a trusted channel with role based access control in order to use the loader functionality. This prevents loading of unauthorized software by unauthorized subjects and maps to O.Prot_TSF_Confidentiality. In case EA is chosen, the Flash Loader requests a one-way authentication instead of a mutual authentication. FTP_ITC.1 is not part of the TOE. However the objective is still met, because the one-way authentication and role based access control together with the environmental objective OE.Prevent_Masquerade prevent unauthorized and manipulative usage.

The justification of the security objective and the additional requirements show that they do not contradict the rationale already given in [PP0084] for the assumptions, policy and threats defined there.

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.

6.3.1.1 Dependencies of Security Functional Requirements

The dependencies of security functional requirements are defined and described in [PP0084] section 6.3.2, 7.2.3, 7.3.1, 7.3.2, 7.4.1 and section 7.4.2 for the following security functional requirements: FDP_SDC.1, FDP_SDI.2, FDP_ITT.1, FDP_IFC.1, FPT_ITT.1, FPT_PHP.3, FPT_FLS.1, FRU_FLT.2, FMT_LIM.1, FMT_LIM.2,

Security Requirements (ASE_REQ)

FCS_RNG.1, FAU_SAS.1, FIA_API.1, FMT_LIM.1/Loader, FMT_LIM.2/Loader, FTP_ITC.1, FDP_UCT.1, FDP_UIT.1, FDP_ACC.1/Loader, FDP_ACF.1/Loader.

The dependencies of the additional security functional requirements (the functional requirements in addition to the ones defined in [PP0084]) are analysed in the following description.

Table 25 Dependency for cryptographic operation requirement

| Security Functional Requirement | Dependencies | Fulfilled by security requirements |
|---------------------------------|--|---|
| FPT_TST.2 | None | n.a. |
| FDP_ACC.1 | FDP_ACF.1 | Yes |
| FDP_ACF.1 | FDP_ACC.1 FMT_MSA.3 | Yes Yes |
| FMT_MSA.3 | FMT_MSA.1 FMT_SMR.1 | Yes Yes |
| FMT_MSA.1 | FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1 | Yes Yes Yes |
| FMT_SMF.1 | None | n.a. |
| FMT_SMR.1 | FIA_UID.1 | No, see comment 1 |
| FCS_COP.1/SCP/<iteration> | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] FCS_CKM.6 | No, see comment 2 Yes, FCS_CKM.6/SCP |
| FCS_COP.1/SCL/<iteration> | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] FCS_CKM.6 | No, see comment 2 Yes, FCS_CKM.6/SCL |
| FCS_COP.1/RSA/<iteration> | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] FCS_CKM.6 | Yes, FCS_CKM.1/RSA/<iteration> No, see comment 6 |
| FCS_COP.1/ECC/<iteration> | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] FCS_CKM.6 | Yes, FCS_CKM.1/ECC No. see comment 6 |
| FCS_COP.1/HCL | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] FCS_CKM.6 | No, see comment 2 No, see comment 5 |

Security Requirements (ASE_REQ)

| Security Functional Requirement | Dependencies | Fulfilled by security requirements |
|---------------------------------|--|--|
| FCS_CKM.6/SCL | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] | No, see comment 2 |
| FCS_CKM.6/SCP | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] | No, see comment 2 |
| FCS_CKM.1 | [FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1] | Yes, FCS_COP.1 |
| | [FCS_RBG.1 or FCS_RNG.1] | Yes, FCS_RNG.1 |
| | FCS_CKM.6 | No, see comment 6 |
| FDP_UCT.1 | [FTP_ITC.1 or FTP_TRP.1] | Yes in case EA unavailable No in case EA available, see comment 4 |
| FDP_UIT.1 | [FTP_ITC.1 or FTP_TRP.1] | Yes in case EA unavailable No in case EA available, see comment 4 |
| FDP_ACF.1/Loader | FMT_MSA.3 | No, see comment 3 |
| FMT_MTD.1/Loader | FMT_SMR.1, FMT_SMF.1 | Yes |
| FMT_SMR.1/Loader | FIA_UID.1 | Yes, met by FIA_UID.2 (hierarchical to FIA_UID.1) |
| FMT_SMF.1/Loader | FIA_UID.1 | Yes, met by FIA_UID.2 (hierarchical to FIA_UID.1) |

Comment 1:

As the privileged mode and the non-privileged mode identified in FMT_SMR.1 are implicitly identified by the MPU, the dependency to FIA_UID.1 is not applicable.

End of comment.

Comment 2:

All of the SFR's mentioned in the dependency:

[FDP_ITC.1 or
FDP_ITC.2 or
FCS_CKM.1 or
FCS_CKM.5]

address the appropriate import/generation of cryptographic keys used by the specified cryptographic function. These requirements concerning keys shall be fulfilled by the environment since the Smartcard Embedded Software is designed for a specific application context and uses the cryptographic functions provided by the TOE.

Security Requirements (ASE_REQ)

The security functional requirement FCS_COP.1/HCL describes keyless hash operations. For this reason there are no dependencies regarding key import/generation.

End of comment.

Comment 3:

There are no security attributes defined for the loader. Access is purely role based.

End of comment.

Comment 4:

The user data to be downloaded are encrypted and integrity protected with the image provider key. Only an authentic TOE knows this image provider key and is able to decrypt the encrypted user data. Therefore a trusted channel is not necessary to keep user data confidential.

End of comment

Comment 5:

Secure hash is a keyless operation

End of comment

Comment 6:

The TOE does not provide services to destroy RSA or ECC keys. This is done by the embedded software for the composite TOE

End of comment

6.3.2 Rationale of the Assurance Requirements

The chosen assurance level EAL6 is augmented by ALC_FLR.1 in order to meet the assurance expectations explained in the following paragraphs. In Table 23 the different assurance levels are shown as well as the augmentations. The augmentations are in compliance with the Protection Profile.

An assurance level EAL6 with the augmentations ALC_FLR.1 is required for this type of TOE since it is intended to defend against highly sophisticated attacks without protective environment. This evaluation assurance package was selected to permit a developer to gain maximum assurance from positive security engineering based on good commercial practices. In order to provide a meaningful level of assurance that the TOE provides an adequate level of defence against such attacks, the evaluators should have access to all information regarding the TOE including the TSF internals, the low level design and source code including the testing of the modular design. Additionally the mandatory technical document [JIL_ATT] shall be taken as a basis for the vulnerability analysis of the TOE.

TOE Summary Specification (ASE_TSS)

7 TOE Summary Specification (ASE_TSS)

The product overview is given in Section 1.3.1. The Security Features are described below and the relation to the security functional requirements is shown.

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

Table 26 TOE Security Features

| | |
|--------|---|
| SF_DPM | Device Phase Management |
| SF_PS | Protection against Snooping |
| SF_PMA | Protection against Modification Attacks |
| SF_PLA | Protection against Logical Attacks |
| SF_CS | Cryptographic Support |

The following description of the security features is a complete representation of the TSF.

7.1 SF_DPM: Device Phase Management

The life cycle of the TOE is split up into several phases.

7.2 SF_PS: Protection against Snooping

The TOE uses various means to protect from snooping of memories and busses and prevents single stepping.

7.3 SF_PMA: Protection against Modifying Attacks

This TOE implements protection against modifying attacks of memories, alarm lines, sensors and instruction execution order.

7.4 SF_PLA: Protection against Logical Attacks

Memory access of the TOE is controlled by a Memory Protection Unit (MPU), which implements different privilege levels. The MPU decides, whether access to a physical memory location is allowed based on access rights.

7.5 SF_CS: Cryptographic Support

The TOE is equipped with an asymmetric and a symmetric hardware accelerator and also software modules to support several symmetric and asymmetric cryptographic operations. It further provides random numbers to meet FCS_RNG.1.

7.6 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 the sections above. The results are shown in Table 27. The security functional requirements are addressed by at least one related security feature.

Table 27 Mapping of SFR and SF

| SFR | SF_DPM | SF_PS | SF_PMA | SF_PLA | SF_CS |
|-----------|--------|-------|--------|--------|-------|
| FRU_FLT.2 | | | x | | |

TOE Summary Specification (ASE_TSS)

| | | | | | |
|---------------------------|---|---|---|---|---|
| FPT_FLS.1 | | x | x | | x |
| FMT_LIM.1 | x | | | | |
| FMT_LIM.2 | x | | | | |
| FAU_SAS.1 | x | | | | |
| FDP_SDC.1 | | x | | | |
| FDP_SDI.2 | | | x | | |
| FPT_PHP.3 | | x | x | | x |
| FDP_ITT.1 | x | x | x | | x |
| FPT_ITT.1 | x | x | x | | x |
| FDP_IFC.1 | | x | x | | |
| FCS_COP.1/SCP/<iteration> | | | | | x |
| FCS_CKM.6/SCP | | | | | x |
| FCS_COP.1/SCL/<iteration> | | | | | x |
| FCS_CKM.6/SCL | | | | | x |
| FCS_COP.1/RSA/<iteration> | | | | | x |
| FCS_CKM.1/RSA/<iteration> | | | | | x |
| FCS_COP.1/ECC/<iteration> | | | | | x |
| FCS_CKM.1/ECC | | | | | x |
| FCS_COP.1/HCL | | | | | x |
| FCS_RNG.1/TRNG | | | | | x |
| FCS_RNG.1/HPRG | | | | | x |
| FCS_RNG.1/DRNG | | | | | x |
| FCS_RNG.1/DRNG4 | | | | | x |
| FCS_RNG.1/RCL/TRNG | | | | | x |
| FCS_RNG.1/RCL/DRNG3 | | | | | x |
| FCS_RNG.1/RCL/DRNG4 | | | | | x |
| FMT_LIM.1/Loader | x | | | | |
| FMT_LIM.2/Loader | x | | | | |
| FTP_ITC.1 | x | | | | |
| FDP_UCT.1 | x | | | | |
| FDP_UIT.1 | x | | | | |
| FDP_ACC.1/Loader | x | | | | |
| FDP_ACF.1/Loader | x | | | | |
| FMT_MTD.1/Loader | x | | | | |
| FMT_SMR.1/Loader | x | | | | |
| FMT_SMF.1/Loader | x | | | | |
| FIA_UID.2/Loader | x | | | | |
| FIA_API.1 | x | | | | |
| FPT_TST.2 | | | x | | |
| FDP_ACC.1 | | | | x | |

TOE Summary Specification (ASE_TSS)

| | | | | | |
|-----------|--|--|--|---|--|
| FDP_ACF.1 | | | | x | |
| FMT_MSA.1 | | | | x | |
| FMT_MSA.3 | | | | x | |
| FMT_SMF.1 | | | | x | |
| FMT_SMR.1 | | | | x | |

7.7 Security Requirements are internally consistent

For this chapter [PP0084] section 6.3.4 can be applied completely.

The functional requirement FPT_TST.2 requires further protection to prevent manipulation of test results, while checking the security functions of the TOE. An attacker could aim to switch off or disturb certain sensors or filters and prevent the detection of distortion by blocking the correct operation of FPT_TST.2. The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the security functional requirement FPT_TST.2. Therefore, the related security functional requirements support the secure implementation and operation of FPT_TST.2.

The requirement FPT_TST.2 allows testing of some security mechanisms by the Smartcard Embedded Software after delivery.

The implemented privilege level concept represents the area based memory access protection enforced by the MPU. As an attacker could attempt to manipulate the level concept as defined and present in the TOE, the functional requirement FDP_ACC.1 and the related other requirements have to be protected. The security functional requirements necessary to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the area based memory access control function implemented according to the security functional requirement described in the security functional requirement FDP_ACC.1 with reference to the Memory Access Control Policy and details given in FDP_ACF.1. Therefore, those security functional requirements support the secure implementation and operation of FDP_ACF.1 with its dependent security functional requirements.

References

8 References

| Reference Name | Standard Description |
|----------------|--|
| [ANSX9.62] | American National Standard for Financial Services ANS 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 |
| [ANSX9.63] | American National Standard for Financial Services X9.63-2001, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, November 20, 2001, American National Standards Institute |
| [ARMv7M] | ARMv7-M Architecture Reference Manual, ARM DDI 0403D ID021310, 12. February 2010, ARM Limited |
| [BSI_RNGs] | A proposal for: Functionality classes for random number generators, Wolfgang Killmann, Werner Schindler, Version 2.0, 18 Sept 2011 |
| [CCBook2] | Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 2: Security functional components |
| [CCBook3] | Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 3: Security assurance components |
| [CCBook5] | Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, November 2022, CC:2022, Revision 1 |
| [CCErrata] | Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), V1.0, 2024-02-01 |
| [ICAO_11] | ICAO Doc 9303, Machine Readable Travel Document, seventh edition, 2015, Part 11: Security Mechanisms for MRTDs |
| [IETF5639] | IETF: RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010, http://www.ietf.org/rfc/rfc5639.txt |
| [IEEE1363] | IEEE 1363 Standard Specification for Public Key Cryptography, January 2000 |
| [ISO11770_3] | ISO/IEC 11770-3: 2009 - Information Technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques, Technical Corrigendum 1 |
| [ISO18033_3] | ISO/IEC 18033-3: 2005 - Information Technology - Security techniques - Encryption algorithms - Part 3: Block ciphers (for AES) |
| [ISO9797B] | ISO/IEC 9797-1: 2011 - Information Technology - Security techniques - Message Authentication Codes - Part 1: Mechanisms using block cipher |
| [ISO9798_2] | ISO/IEC 9798-2: 2008 - Information Technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms |
| [JIL_ATT] | Joint Interpretation Library, Application of Attack Potential to Smartcards, Version 3.2, November 2022 |
| [N180-4] | NIST: FIPS publication 180-4: Secure Hash Standard (SHS), August 2015 |
| [N186-4] | NIST: FIPS publication 186-4: Digital Signature Standard (DSS), July 2013 |
| [N197] | Federal Information Processing Standards Publication, U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), Advanced Encryption Standard (AES), FIPS PUB 197, as of 26st November 2001 |

References

| | |
|-------------|---|
| [N800-22] | National Institute of Standards and Technology(NIST), Technology Administration, US Department of Commerce, Special Publication, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, in the revision 1a as of April 2010 |
| [N800-38A] | National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Data Encryption Standard, NIST Special Publication 800-38A, Edition 2001 |
| [N800-38B] | National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Data Encryption Standard, NIST Special Publication 800-38B, Edition 2005 with updates as of 2016-10-06 |
| [N800-67B] | National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce, NIST Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Revised November 2017, Revision 2 |
| [N800-90A] | NIST Special Publication 800-90A Revision 1 Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015 |
| [PP0084] | Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13.01.2014, BSI-CC-PP-0084-2014 |
| [RSA-PKCSB] | PKCS #1: RSA Cryptography Standard, v2.2, October 27, 2012, RSA Laboratories |

Note that the versions of these documents are listed in the certification report.

Appendix: hash signatures of NRG™ SW**9 Appendix: hash signatures of NRG™ SW****9.1 Hash Digests of the NrgOS.lib**

| | |
|---------|--|
| MD5 | 9be5ee66ba20ad52f1a83c10aab501a1 |
| SHA-1 | c52cd426140b651596d1940c97489c10435d6fb4 |
| SHA-256 | 0fc29ec712b9ba5a8a0f7541118702768b53ed43b8109df8584b8ef2539a2c64 |

9.2 Hash Digests of the NrgManagement.lib

| | |
|---------|--|
| MD5 | b38c917c38d5fe685fb3031032892769 |
| SHA-1 | e08e13020682583dc2c9f70bd3fa1b088478f9f9 |
| SHA-256 | d130d7f45c8ef36de013d6132593e5279c85a172742fe45a2e7d2b3e02f8aac5 |

Appendix: hash signatures of the HSL**10 Appendix: hash signatures of the HSL**

HSL-03.52.9708-SLCx7V16a.lib

MD5 2e1ec43d5d13d27d65456cbeb7a84cc4

SHA-1 05d4e3caa916a6182aed7b06354153bcf04d82c7

SHA-256 7df825ec42763570334e641f72fc41466712d6d231a9bf75174acb5005f3869a

Appendix: hash signatures of the UMSLC lib**11 Appendix: hash signatures of the UMSLC lib**

UMSLC-01.30.0564-SLCx7V16a.lib:

MD5 b444ffaed77933be4407935f135728a7

SHA-1 c0ba8430b96a2dc7888067fd0da301ff3405736d

SHA-256 af948dfe1449b4bf20c4cdd23d6f40efb98515c84712a2526dfaf229fcda9536

12 Appendix: hash signatures of the SCL

12.1 SCL v2.11.003

SCL37-SCP-v440-C40-cipher.lib:

MD5= be3b586f0a28aa9d49aad50a2db4be1
SHA1= caf62712f4f822d2db989c14b8bc11b1098ec9a1
SHA256= 97a0c49036d07949f7d9e4da73be12b9cd2c465ee964c03af44751c9635bed2c

SCL37-SCP-v440-C40-mac.lib:

MD5= bd46c41dd39dbd7a6c4de80dea52aef4
SHA1= a25631b3f205eb8cb06abf40503153759b8f9b80
SHA256= 8e7c75b110872c698038d13ffa474f4704c908cc64e497fb6b263c768236ce47

SCL37-SCP-v440-C40-des.lib:

MD5= ffc9fe59c7332ceb08d985e5a94ffd98
SHA1= b19a97b32db533394a758a366bee535d4dbc4943
SHA256= 5e7fd5230b21a36420934841e1205bfeff46c70011095aceaa4ce8d2ed868d213

SCL37-SCP-v440-C40-aes.lib:

MD5= 852e3074775fa559fce734e86216e9e4
SHA1= 182663c8043ff906065feda20689090a1a8721fc
SHA256= 27547d8f5cfe26c89c4460e5bc254e9f1937768e9f9d681c9c04607e4f87a784

12.2 SCL v2.15.000

SCL37-SCP-v440-C40-cipher.lib:

MD5= bca577f2630f14652b8bdc361e8beb40
SHA1= 21484376c2f752715ca7316cc003c5c9abbde95e
SHA256= 39d682fd15ada5a17b636cbc27536676efe900ce894bbbeb04aa621fa9aeadd2b2

SCL37-SCP-v440-C40-mac.lib:

MD5= 034924695150657ddbfb368f9d8b5cb14
SHA1= b872f05479c6eac8d31f5b5a1d043eddbfaa190c
SHA256= 2f3e4cbc3894c11c5ab6bc04ecae5fcf94b348a825f7a0fcedd691193f596267

SCL37-SCP-v440-C40-des.lib:

MD5= ac6e98eb2d5499bb8431ab98324d4af7
SHA1= cb0d69d066f7d796e007cf2202fd6e32e90a48ea
SHA256= d0520c4fab3b676b0731246427afdb5e991c317e32aa14451ea9938db1abf314

Appendix: hash signatures of the SCL

SCL37-SCP-v440-C40-aes.lib:

MD5= 7eede832e59a09e17a7a474c9fe4ffbc

SHA1= 9c1288050930acf34ea91c73a542aadbc0a75275

SHA256= 46b26d76e9a374ec23405232e8d2c352990c1a36c8e17bf3179217cd7e9bbc7c

Appendix: hash signatures of the ACL**13 Appendix: hash signatures of the ACL****13.1 ACL v3.02.000**

ACL37-Crypto2304T-C40-base.lib:

MD5= 8760a5214c99c82f3d34fc8e8d295415
SHA1= 8cb34365b251f955e8baf7ba64950330898df8c9
SHA256= f93fa12c7bc870f681f727b4081f198174d996ef5d4fd7009ad5a3840240af6a

ACL37-Crypto2304T-C40-ecc.lib:

MD5= 8308a51c0f13accc971931512a76fd02
SHA1= 873d481fdb78c35897aa4626363b88a5b6ba9a59
SHA256= 589592b20079d53ee0d39de1f061661f6924ed3c90be22186457abcfa6b87589

ACL37-Crypto2304T-C40-rsa2k.lib:

MD5= 3285732229560b79313f54dfa4867925
SHA1= ce3d709407c8dfeac486a57d4f7299b7f1194831
SHA256= bbe1f19dc864c5ca4125f870db3cbf70067cb6d0bc27fe5948b328207c4f77d2

ACL37-Crypto2304T-C40-rsa4k.lib:

MD5= 8ef66b7a1bfd2d636e913a3723a5c82e
SHA1= dc931964805af30b0140ab4eec074f3f2f08a45b
SHA256= 17694b594b1914ddae84af86a868061dc144c181d9c78e72d7d887bf22979812

ACL37-Crypto2304T-C40-toolbox.lib:

MD5= 57e151190ade670f9a7531acedc77a10
SHA1= 0374f32135f191ef0fdb28f40c85c1468398cf22
SHA256= 8405ef906fe0ddce4a3659e00d4d9c724f0e6d18a58b1d87a6af64969b985523

13.2 ACL v3.33.003

ACL37-Crypto2304T-C40-base.lib:

MD5= f6169db959c4ea01875e365d66888176
SHA1= df35ca3b06362973ac1b00a0f1740f423ac4d111
SHA256= c16817e0c2a2364374986a38ae052d8abbe5e449dfb92ef0746cc21a398af1d6

ACL37-Crypto2304T-C40-ecc.lib:

MD5= ece5991c2a1ba0431fa1751f481e3464
SHA1= f9bdfb2acae22d1db8532697baa6c8208bee6482
SHA256= c5606d08f92390d7b7bd4acccd55fb6a2709e3f8ad5f372f47f54eb36e8b234a

Appendix: hash signatures of the ACL

ACL37-Crypto2304T-C40-rsa2k.lib:

MD5= 6bb9cf40b6722db14a644b9a97da84b2
SHA1= fe351c1fe03572f7d9f0dabaa58203dcef888e0a
SHA256= df443f26cf8b087ee7ae18a7ca5c3713bd84046af91c1d56895c694291767b6b

ACL37-Crypto2304T-C40-rsa4k.lib:

MD5= 2eb0b9fef93bd263b18caeb07ecada3e
SHA1= 70ef805a899c4a5f5a16226f15e21ad280f2a046
SHA256= bbb8debd6186e2a0156154a9e6a905ec349457f927b282b07e6014e11b24582f

ACL37-Crypto2304T-C40-toolbox.lib:

MD5= bb0ecb011bd769cd8e1729243678e55f
SHA1= 7b24c00dd411cd5ff7a04bdb134e6ae8f4e4222c
SHA256= 4ec4c1b7a0fe44332c9d7f15917239e858572a2dd0d5968eb006d89aa8147fd4

13.3 ACL v3.35.001

ACL37-Crypto2304T-C40-base.lib:

MD5= bfae96cc5a318eb8966e524e4f87c383
SHA1= 5d0b12d29322034693af01a4bc123b5699639e0c
SHA256= b725f13e182abcdf18d8be4c372b76487bc89b5ceb1860954890afaa8b96c4aa

ACL37-Crypto2304T-C40-ecc.lib:

MD5= fdd91a1c6b9c25965c669be71e713454
SHA1= edac92e96f6e22c63900d066eb5f751b840c086b
SHA256= cc201c53dfb405665033ad77cd848314fd9bf78513529de7d92097d468149a56

ACL37-Crypto2304T-C40-rsa2k.lib:

MD5= 019c3edcc62da6bae35a722581d0044f
SHA1= 6a3c50e894223123a5cc7a21052d436c08c8a3e7
SHA256= 1a6b5f363d403fbd6a8f554c2d3adcfffb46ed9483b41abb0151ca4e0a295d53f

ACL37-Crypto2304T-C40-rsa4k.lib:

MD5= d0a8800cba751c36eef4fa08df6d2b4f
SHA1= d38a66ad79089ecbefca15ee540206140a14940d
SHA256= 42b082a2019d204ab75dc383e5652f8ac2bc5b0bb8045bbb24c45ae0d03624b6

ACL37-Crypto2304T-C40-toolbox.lib:

MD5= 3ef43509ccd0abab01123bb3483ff424
SHA1= 5c591f50ea632d3aa7cdc2291c67a04d05974b12
SHA256= d6b68b7d509b3ac9cf3a0e6d092d6a63e5e74ff68789b2f6f158fbf607faece5

Appendix: hash signatures of the RCL**14 Appendix: hash signatures of the RCL**

RCL37-X-C40-rng.lib:

MD5= 150b9751d40f254063c3ebacee5ea4c9

SHA1= 49f8d26d8b6744507a24ea4db1e1f3df2c749855

SHA256= 5aa4dabe5c1e06c04b410466a6d27d4026f06e26d73fc379c26f8ec2fb085987

RCL37-X-C40-hwrng.lib:

MD5= 6b06e50a1ee78f3af610df5b1d25d7e5

SHA1= 9ec9041bd55369c7cd0c413358b69486e19bb663

SHA256= b8f5ec9ff71dd96468fd316f73b4fa31218b83bf5281b638348f26725a6eb659

RCL37-X-C40-drbg.lib:

MD5= 5e652ebefb46d5560af95578ea8a5733

SHA1= c761f1518d105c03cec7c627eb04ab6f5f2cc780

SHA256= 0c1a19c3557508084d630c59e296ab9731c63f10eabee8708792817140025cfe

Appendix: hash signatures of the HCL**15 Appendix: hash signatures of the HCL**

HCL37-CPU-C40-hash.lib:

MD5= 49c989a7afdc5ab3a74f9a1362d0da7c

SHA1= 775ec8e830463c3771e4ab68dbdfdf184a9f2493

SHA256= c0a2187cecb3c3b458815abf275c405cbd18e13a6ed0accdd81b1278d5cd674f

HCL37-CPU-C40-sha.lib:

MD5= ec592086d002d75e7652b6b7bbc4dec3

SHA1= 2ff8188e430b5f189e0eadb3b08a8fc8d4281674

SHA256= 3fdeb1b6a862130adb987f637faf39e6b69d8a5928cef9f21e3f8d116a97e474

List of Abbreviations**16 List of Abbreviations**

AES Advanced Encryption Standard

ACLB Advanced Contactless Bridge

ACM Advanced Communication Mode: The Advanced Communication Mode enables communication with bit rates above 848 kbit/s

AFM Advanced Framing Mode refers to the frame format “Frames with error correction” as defined by ISO/IEC 14443-4, applicable for Type A and Type B only.

AIS31 “Anwendungshinweise und Interpretationen zu ITSEC und CC

Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren”

AMM Advanced Mode for NRG™ SAM: The NRG™ crypto module is operated as NRG™ technology support on the reader (i.e. PCD) side, i.e., when using the security controller as Secure Application Module (SAM) embedded in the reader device

API Application Programming Interface

ATR Answer to Reset

BCM Block Cipher Mode

BLD Backside Light Detector

BPU Block to Planned Usage. Feature allowing to configure a given device to its required usage by deactivating (blocking) unused memory and/or peripherals during card personalization. Reserved for sample deliveries and under specific contractual conditions.

CC Common Criteria

CI Chip Identification Mode (STS-CI)

CPAU Code Peripheral Access Unit

CPU Central Processing Unit

Crypto2304T Asymmetric Cryptographic Processor

DPA Differential Power Analysis

DFA Differential Failure Analysis

DRNG Deterministic Random Number Generator

DSCA Differential Side Channel Analysis

EA External Authentication

EC Elliptic Curve

ECC Error Correction Code or Elliptic Curve Cryptography (depending on context)

ECDH Elliptic Curve Diffie-Hellman

ECDSA Elliptic Curve Digital Signature Algorithm

EDC Error Detection Code

List of Abbreviations

| | |
|-------|---|
| EMA | Electro magnetic analysis |
| Flash | Flash Memory |
| FSE | Frequency Sensor |
| HCL | Hash Crypto Library |
| HPRG | Hybrid Physical Random Generator |
| HSL | Hardware Support Library |
| IC | Integrated Circuit |
| ICO | Internal Clock Oscillator |
| ID | Identification |
| IMM | Interface Management Module |
| ITP | Interrupt and Peripheral Event Channel Controller |
| I/O | Input/Output |
| ITSEC | Information Technology Security Evaluation Criteria |
| MED | Memory Encryption and Decryption |
| MMU | Memory Management Unit |
| NRG™ | ISO/IEC14443-3 Type A with CRYPTO1 |
| O | Object |
| OCC | Online Configuration Check |
| OS | Operating system |
| POWS | Performance Optimized Write Scheme |
| PRNG | Pseudo Random Number Generator |
| RAM | Random Access Memory |
| RCL | Random Crypto Library |
| RNG | Random Number Generator |
| ROM | Read Only Memory |
| RSA | Rives-Shamir-Adleman Algorithm |
| SAM | Service Algorithm Minimal |
| SCL | Symmetric Cryptographic Library |
| SCP | Symmetric Cryptographic Processor |
| SPAU | System Peripheral Access Unit |
| ST | Security Target or Security Target Lite |
| TSC | TOE Security Functions Control |

List of Abbreviations

| | |
|-------|---|
| TSE | Temperature Sensor |
| TSF | TOE Security Functionality |
| UART | Universal Asynchronous Receiver/Transmitter |
| UM | User Mode (STS) |
| UMSLC | User mode Security Life Control |
| VSE | Voltage Sensor |
| WDT | Watch Dog Timer |
| TDES | Triple DES |

Glossary

17 Glossary

| | |
|--|---|
| Application Program/Data | Software which implements the actual TOE functionality provided for the user or the data required for that purpose |
| Central Processing Unit | Logic circuitry for digital information processing |
| Chip Identification Data | Data to identify the TOE |
| CPAU | Code Peripheral Access Unit |
| Generic Chip Identification Mode | Operational status phase of the TOE, in which actions for identifying the individual chip by transmitting the Chip Identification Data take place |
| Memory Encryption and Decryption | Method of encoding/decoding data transfer between CPU and memory |
| Memory | Hardware part containing digital information (binary data) |
| Microprocessor | CPU with peripherals |
| Object subjects | Physical or non-physical part of a system which contains information and is acted upon by subjects |
| Operating System operation | Software which implements the basic TOE actions necessary for operation |
| Programmable Read Only Memory read operations | Non-volatile memory which can be written once and then only permits read operations |
| Random Access Memory | Volatile memory which permits write and read operations |
| Random Number Generator | Hardware part for generating random numbers |
| Read Only Memory | Non-volatile memory which permits read operations only |
| Resource Management System testbench etc. | Part of the firmware containing NVM programming routines, AIS31 |
| Self Test Software the TOE hardware | Part of the firmware with routines for controlling the operating state and testing |
| Security Function | Part(s) of the TOE used to implement part(s) of the security objectives |
| Security Target | Description of the intended state for countering threats |
| SmartCard | Plastic card in credit card format with built-in chip |
| Software | Information (non-physical part of the system) which is required to implement functionality in conjunction with the hardware (program code) |
| SPAU | System Peripheral Access Unit |
| Subject | Entity, generally in the form of a person, who performs actions |
| Target of Evaluation | Product or system which is being subjected to an evaluation |
| Test Mode place | Operational status phase of the TOE in which actions to test the TOE hardware take place |
| Threat | Action or event that might prejudice security |

Glossary

| | |
|-----------|--|
| User Mode | Operational status phase of the TOE in which actions intended for the user takes place |
|-----------|--|

18 Revision History

Major changes since the last revision

| Version | Description of change |
|----------------|------------------------------|
| v1.2 | Initial draft version |
| v6.9 | Final version |

Trademarks of Infineon Technologies AG

AURIX™, C166™, CanPAK™, CIPOS™, CoolGaN™, CoolMOS™, CoolSET™, CoolSiC™, CORECONTROL™, CROSSAVE™, DAVE™, DI-POL™, DrBlade™, EasyPIM™, EconoBRIDGE™, EconoDUAL™, EconoPACK™, EconoPIM™, EiceDRIVER™, eupec™, FCOS™, HITFET™, HybridPACK™, Infineon™, ISOFACE™, IsoPACK™, i-Wafer™, MIPAQ™, ModSTACK™, my-d™, NovalithIC™, OmniTune™, OPTIGA™, OptiMOS™, ORIGA™, POWERCODE™, PRIMARION™, PrimePACK™, PrimeSTACK™, PROFET™, PRO-SiL™, RASIC™, REAL3™, ReverSave™, SatRIC™, SIEGET™, SIPMOS™, SmartLEWIS™, SOLID FLASH™, SPOC™, TEMPFET™, thinQ!™, TRENCHSTOP™, TriCore™.

Trademarks updated August 2015

Other Trademarks

All referenced product or service names and trademarks are the property of their respective owners.

Edition 2025-01-24

Published by

Infineon Technologies AG
81726 Munich, Germany

© 2025 Infineon Technologies AG.
All Rights Reserved.

Do you have a question about this document?

Email: erratum@infineon.com

<DOC Number>
Document reference

IMPORTANT NOTICE

The information contained in this Security Target is given as a hint for the implementation of the product only and shall in no event be regarded as a description or warranty of a certain functionality, condition or quality of the product. Before implementation of the product, the recipient of this application note must verify any function and other technical information given herein in the real application. Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind (including without limitation warranties of non-infringement of intellectual property rights of any third party) with respect to any and all information given in this Security Target.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer's technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology delivery terms and conditions and prices please contact your nearest Infineon Technologies office (www.infineon.com).

WARNINGS

Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies' products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.