IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11 Security Target Lite

Revision: v4.0

Table of Contents

Contents

1 Security Target Introduction (ASE_INT)

1.1 ST reference

The ST has the revision v4.0 and is dated 2020-10-15. The title of this document IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11 Security Target Lite.

1.2 TOE Reference

The ST comprises an Infineon Technologies Security Controller named IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh design step T11 with firmware 80.306.16.0, optional NRG™ SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib v01.30.0564, optional SCL v2.11.003, optional ACL v3.02.000and 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 Common Criteria v3.1.

The targeted assurance level is EAL6+.

Table 1 Identification

Hardware	Version	Method of identification
IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh (each of the comma separated term is a Common Criteria Certification Identifier)	T11 (design step)	Non-ISO ATR
firmware		
BOS & POWS	80.306.16.0	Non-ISO ATR: firmware identifier
Flash-loader	09.12.0005	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)	v2.11.003	SCL function
ACL (optional)	v3.02.000	ACL function
User Guidance		
32-bit Security Controller – V11, Hardware Reference Manual	V5.2, 2020-02-05	document
32-bit Security Controllers, SLx1/SLx3 Controller Family, Programmer's Reference Manual	V4.5, 2020-06-22	document
32-bit Security Controller – V11, Security Guidelines	v1.00-2661, 2020-10-05	document
Production and personalization 32-bit ARM-based security controller	v.09.12, 2020-07-03	document
32-bit Security Controller Crypto2304T V3, User Manual	V2.0, 2019-04-24	document
HSL SLCx7 V11, Hardware Support Library (optional)	v3.52.9708, 2020-02-03	document
UMSLC library for SLCx7 in 40nm,	v01.30.0564, 2019-06-19	document

Hardware	Version	Method of identification
SCL37-SCP-v440-C40 Symmetric Crypto Library for SCP-v440 AES/DES/MAC (optional)	v2.11.003, 2020-02-10	document
ACL37-Crypto2304T-C40 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox (optional)	v3.02.000, 2020-02-07	document

A customer can identify the TOE hardware and its configuration (for details see chapter 1.4.7) 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. 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, ECDSA, ECC, ECDH, 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
- 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

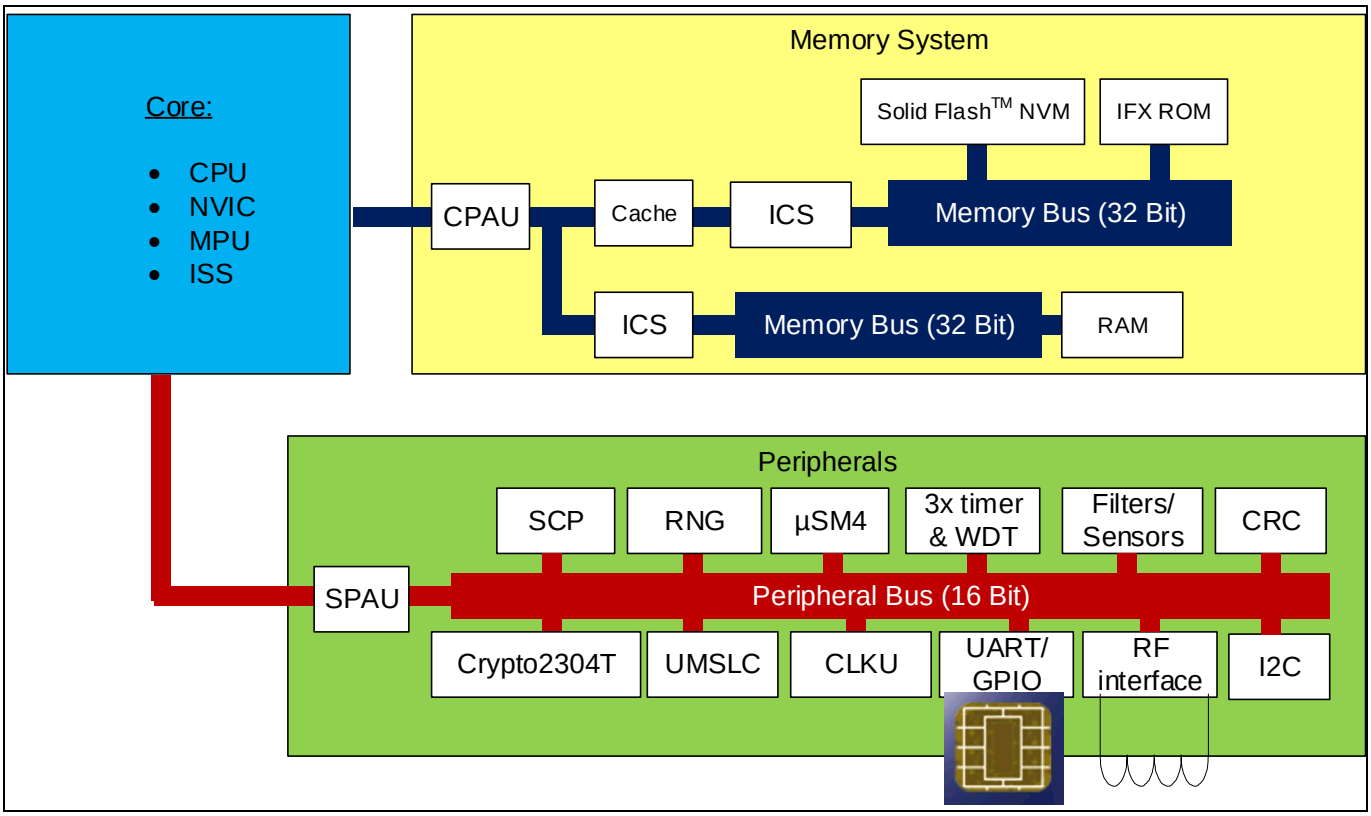
1.4 TOE description

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



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.

Security Target Introduction (ASE_INT)

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) consist 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
- 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 µSM4 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) 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”.

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 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

1.4.1.3 User Guidance components

The user guidance consists of the components as follows:

- 32-bit Security Controller – V11, Hardware Reference Manual: description of hardware features and user interfaces
- 32-bit ARM-based Securtity 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 cvontroller in 40 nm:contains detailed information about the usage of the Flash Loader
- 32-bit Security Controller – V11, 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 V11, 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.

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, 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, ECC, ECDSA, ECDH.
- 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 dependant 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.

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

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 via the UART or RF interface. 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			

TOE Component	Delivered Format	Delivery Method	Comment
IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11	Wafer, IC case, packages	Postal transfer in cages	All materials are delivered to distribution centers in cages, locked.
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 512 kBytes	IFX-Mailbox

[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.

Memory	Values	Identification
RAM	up to 16 kBytes	IFX-Mailbox
Peripherals	**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.
2	The user provides software to download into the SOLID FLASH™ memory to Infineon Technologies AG. The software is loaded into the SOLID FLASH™ memory during	There is no Flash Loader present.

Case	Option	Flash loader status
	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 preloades 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.

2 Conformance Claims (ASE_CCL)

2.1 Conformance Claims (ASE CCL)

This ST and TOE claim conformance to CC v3.1 revision 5. The ST claims conformance to [CCBook3]. It is [CCBook2] extended.

2.1.1 PP Claim

This ST is strictly conformant to [PP0084]. The assurance level is EAL6+. The augmentation is achieved - with regard to [CCBook3]: 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 Informationstechnik[1] (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.
- 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
- the IC Dedicated Software with the parts

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

Conformance Claims (ASE_CCL)

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

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

The security problem definition of [PP0084] is enhanced by adding additional threats and an environmental objective. Including these add-ons, the security problem definition of this ST is consistent with the statement of the security problem definition in [PP0084], as the ST claims strict conformance to [PP0084].

The threat memory access violation T.Mem-Access has been added, due to specific TOE memory access control functionality. This add-on has no impact on the conformance statements regarding [CCbook1] and [PP0084] with following rational:

- The security target remains conformant to [CCbook1], claim 576 as the possibility to introduce additional restrictions is given.
- The security target fulfils the strict conformance claim of [PP0084] due to the application notes 5, 6 and 7 which apply here. By those notes the addition of further security functions and security services are covered, even without deriving particular security functionality from a threat but from a policy.

The threat T.Open_Samples_Diffusion is added in case physical protection during TOE delivery to customers is omitted. This threat increases the scope of threats and does not contradict to any of the defined threats of [PP0084].

The environmental objective OE.Prevent_Masquerade is added to require the environment to add additional measures in case EA is available in order to prevent masquerading attacks. The strict conformance to [PP0084] is still met, because the ability of the TOE to prevent masquerading attacks is met by an optional package , i.e. “Package Authentication of the Security IC”. In case this package is not claimed, the TOE does not provide sufficient measures to prevent masquerading. Requesting the environment to fill this gap is an important requirement, if masquerading attacks are considered relevant. [PP0084] does not add any considerations in case the TOE does not claim this package.

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

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

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**

Security objectives (ASE_OBJ)

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 cryprographic services (O.RSA)” and “Elliptic Curve cryptographic services (O.ECC)” as specified below.

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 and verification.

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

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	Secure communication and usage of the Loader

Security objectives (ASE_OBJ)

Environmental objective	description
ordered with configuration option EA unavailable)	
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 Loade 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.

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 policiy 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 requires measures by customers to ensure the authenticity of the TOE. Due to the combination of these measures with the one-way authentication enforced by the Flash Loader with EA, both communication end 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 objectives O.RSA, O.ECC, O.AES-TDES-MAC cover the policy P.Crypto_Services. This policy intends to allow adding various cryptographic services to the TSF.

Security objectives (ASE_OBJ)

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.

The environmental 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.

5 Extended Component Definition (ASE_ECD)

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

- the family FCS_RNG at the class FCS Cryptographic Support
- the family FMT_LIM at the class FMT Security Management
- the family FAU_SAS at the class FAU Security Audit
- the family FDP_SDC at the class FDP User Data Protection
- the family FIA_API at the class FIA Identification and Authentication
- the component FPT_TST.2 at the class FPT Protection of the TSF

The extended families FCS_RNG, FMT_LIM, FAU_SAS, FDP_SDC and FIA_API are 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. 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 verifying the integrity of TSF data and stored TSF executable code which might violate the security policy.

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

5.3 TSF self test (FPT_TST)

Family Behavior The Family Behavior is defined in [CCBook3] section 15.14 (442,443).

Component levelling

FPT_TST.1: The component FPT_TST.1 is defined in [CCBook3] section 15.14 (444, 445,446).

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

Management: FPT_TST.2

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].

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]

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_COP.1/SCP/TDES	“Cryptographic operation - TDES”
FCS_COP.1/SCP/AES	“Cryptographic operation - AES”
FCS_CKM.4/SCP	“Cryptographic key destruction”
FCS_COP.1/SCL/TDES	“Cryptographic operation – TDES by SCL”
FCS_COP.1/SCL/AES	“Cryptographic operation – AES by SCL”
FCS_CKM.4/SCL	“Cryptographic key destruction”
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”	
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”	

Security Requirements (ASE_REQ)

Table 15 provides an overview about security functional requirements, which are added to the TOE. All requirements are taken from [CCbook3] 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/SCP/TDES-MAC	“Cryptographic operation – TDES MAC”
FCS_COP.1/SCP/AES-MAC	“Cryptographic operation – AES-MAC”
FCS_COP.1/RSA/<iteration> “Cryptographic Operation – RSA	
FCS_CKM.1/RSA/<iteration> “Cryptographic key management - RSA”	
FCS_CKM.4/RSA “Cryptographic key destruction - RSA”	
FCS_COP.1/ECC/<iteration> “Cryptographic Operation – ECC”	
FCS_CKM.1/ECC “Cryptographic key management - ECC”	
FCS_CKM.4/ECC “Cryptographic key destruction - ECC”	
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 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.

Security Requirements (ASE_REQ)

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.

6.1.2 Extended Components

An additional family (FCS_RNG) of the Class FCS (cryptographic support) is defined in [PP0084]. This family describes the functional requirements for random number generation used for cryptographic purposes.

The functional requirements FCS_RNG.1/TRNG, FCS_RNG.1/HPRG, FCS_RNG.1/DRNG, FCS_RNG.1/DRNG4 are iterations of the FCS_RNG.1 defined in [PP0084] refined in [BSI_RNGs].

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 physical[1] random number generator that implements:
PTG.2.1	A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.
PTG.2.2	If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.
PTG.2.3	The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.
PTG.2.4	The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.[2]
PTG.2.5	The online test procedure checks the quality of the raw random number sequence. It is triggered continuously. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.
FCS_RNG.1.2/TRNG	The TSF shall provide numbers in the format 8- or 16-bit[3] that meet
PTG.2.6	Test procedure A, as defined in [BSI_AIS31] does not distinguish the internal random numbers from output sequences of an ideal RNG.
PTG.2.7	The average Shannon entropy per internal random bit exceeds 0.997.[4]

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

[2] [assignment: list of security capabilities]

[3] [assignment: format of the numbers]

[4] [assignment: a defined quality metric]

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]
FCS_RNG.1.1/HPRG	The TSF shall provide a hybrid physical[1] random number generator that implements:
PTG.3.1	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.
PTG.3.2	If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.
PTG.3.3	The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test and the seeding of the DRG.3 post-processing algorithm have been finished successfully or when a defect has been detected.
PTG.3.4	The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.
PTG.3.5	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. Note: Continuously means that the raw random bits are scanned continuously. 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. End of note.
PTG.3.6	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.[2]
FCS_RNG.1.2/HPRG	The TSF shall provide numbers in the format 8- or 16-bit[3] that meet
PTG.3.7	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.[4]
PTG.3.8	The internal random numbers shall use the PTRNG of class PTG.2 as random source for the post processing.

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

[2] [assignment: list of security capabilities]

[3] [assignment: format of the numbers]

[4] [assignment: a defined quality metric]

Security Requirements (ASE_REQ)

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]
FCS_RNG.1.1/DRNG	The TSF shall provide a deterministic[1] random number generator that implements:
DRG.3.1	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. Note: 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 by a certified PTG.2 physical TRNG with guaranteed 7,976 bit of entropy per byte. End of note.
DRG.3.2	The RNG provides forward secrecy.
DRG.3.3	The RNG provides backward secrecy even if the current internal state is known.[2]
FCS_RNG.1.2/DRNG	The TSF shall provide numbers in the format 8- or 16-bit[3] that meet
DRG.3.4	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 $1 - 2^{(-16)}$.
DRG3.5	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: 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.[4]

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

[2] [assignment: list of security capabilities]

[3] [assignment: format of the numbers]

[4] [assignment: a defined quality metric]

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]
FCS_RNG.1.1/DRNG4	The TSF shall provide a hybrid deterministic [1] random number generator that implements:
DRG.4.1	The internal state of the RNG shall use PTRNG of class PTG.2 as random source
DRG.4.2	The RNG provides forward secrecy.
DRG.4.3	The RNG provides backward secrecy even if the current internal state is known.[2]
DRG.4.4	The RNG provides enhanced forward secrecy on demand.
DRG.4.5	The internal state of the RNG is seeded by an PTRNG of class PTG.2.
FCS_RNG.1.2/DRNG4	The TSF shall provide numbers in the format 32-bit[3] that meet
DRG.4.6	The RNG generates output for which any consecutive 234 strings of bit length 128 are mutually different with a probability that is greater than $1 - 2^{(-16)}$.
DRG4.7	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.

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 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 the test process before TOE Delivery[4] with the capability to store the Initialization Data and/or Pre-personalization Data and/or supplements of the Security IC Embedded Software[5] in the access protected and not changeable configuration page area and non-volatile memory[6].

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

[2] [assignment: list of security capabilities]

[3] [assignment: format of the numbers]

[4] [assignment: list of subjects]

[5] [assignment: list of audit information]

[6] [assignment: type of persistent memory]

6.1.3 Support of Cipher Schemes

6.1.3.1 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 of the Composite TOE without security attributes, or FDP_ITC.2 Import of user data of the Composite TOE with security attributes, or FCS_CKM.1 Cryptographic key management] FCS_CKM.4 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 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.4/SCP	Cryptographic key destruction
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1/SCP	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting or zeroing[1] that meets the following: None[2]

6.1.3.2 Cipher schemes provided by the SCL

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

[1] [assignment: cryptographic key destruction method]

[2] [assignment: list of standards]

Security Requirements (ASE_REQ)

Dependencies:	[FDP_ITC.1 Import of user data of the Composite TOE without security attributes, or FDP_ITC.2 Import of user data of the Composite TOE with security attributes, or FCS_CKM.1 Cryptographic key management] FCS_CKM.4 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	TDES in ECB mode, CBC mode, CTR mode, CFB mode	128 bit, 192 bit, 256 bit	[N197], [N800-38A]
SCL/TDES-MAC	MAC generation and verification	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 and verification	AES in CMAC mode	128 Bit, 192 Bit, 256 Bit	[N197] (AES), [N800-38B] (MAC)

FCS_CKM.4/SCL	**Cryptographic key destruction**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1/SCL	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting or zeroing[1] that meets the following: None[2]

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.

[1] [assignment: cryptographic key destruction method]

[2] [assignment: list of standards]

6.1.3.3 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 of the Composite TOE without security attributes, or FDP_ITC.2 Import of user data of the Composite TOE with security attributes, or FCS_CKM.1 Cryptographic key management] FCS_CKM.4 Cryptographic key 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 standards: [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	RSA encryption	RSAEP, IFEP-RSA	512 – 2112 Bits	[RSA-PKCSB], ch. 5.1.1 [IEEE1363], ch. 8.2.2
DEC	RSA decryption	RSADP, IFDP-RSA	512 – 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)	512 – 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	512 – 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)	512 – 4224 Bits	[RSA-PKCSB], ch. 5.2.1 [IEEE1363], ch. 8.2.1(II) and 8.2.4
VER	RSA signature verification	RSAVP1 IFVP-RSA1	512 – 4224 Bits	[RSA-PKCSB], ch. 5.2.2 [IEEE1363], ch. 8.2.5

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_COP.1 Cryptographic operation] FCS_CKM.4 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: list of cryptographic operations]and specified cryptographic key sizes of [assignment: cryptographic key sizes that meet the following: [assignment: list of standards]

Table 19 Cryptographic table for FCS_CKM.1/RSA/

<iteration>	Operation	Key size (bits)	Standards
CRT	IFX RSA CRT key generation	512 – 4224 Bits	[RSA-PKCSB], ch. 3.1 and 3.2 (2) [IEEE1363], ch. 8.1.3.1(2)
n_d	IFX RSA key generation (i.e. without CRT) and return of (n, d)	512 - 2112 Bits	[RSA-PKCSB] , ch. 3.1 and 3.2 (1) [IEEE1363] , ch. 8.1.3.1(1)
p_q_d	IFX RSA key generation (i.e. without CRT) and return of (p , q, d)	512 – 2112 Bits	[IEEE1363] , ch. 8.1.3.1(3)

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

FCS_CKM.4/RSA	Cryptographic key destruction
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1/RSA	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method destruction of RAM key during system or power on reset[1] that meets the following: None[2]

Note: The TOE can be delivered with or without the optional RSA library. If the RSA library is not deliverd, the TOE does not provide the SFRs of this chapter. 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.

6.1.3.4 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 of the Composite TOE without security attributes, or

[1] [assignment: cryptographic key destruction method]

[2] [assignment: list of standards]

	FDP_ITC.2 Import of user data of the Composite TOE with security attributes, or FCS_CKM.1 Cryptographic key management] FCS_CKM.4 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 of [assignment: cryptographic key sizes]that meet the following standards: [assignment: list of standards]

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
ADD	EC point addition	C = A+B	160 – 521 Bits	n.a.

Note: The following ECC curves are in scope of this evaluation:
- all Brainpool curves from [IETF5639]
- all NIST curves 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 u1 and u2.

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

Note: For the /ADD iteration, the elliptic curve points A, B and C are considered as secrets.

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_COP.1 Cryptographic operation]

	FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/ECC	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm EC key generation[1] and specified cryptographic key sizes of 160-521 bits[2] that meet the following: [ANSX9.62], ch. A4.3 and [IEEE1363], ch. A.16.9.[3]

Note: The following ECC curves are in scope of this evaluation:
- all Brainpool curves from [IETF5639]
- all NIST curves from [N186-4]

FCS_CKM.4/ECC	**Cryptographic key destruction**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1/ECC	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method destruction of RAM key during system or power on reset[4] that meets the following: None[5]

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

6.1.4 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).

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 at the conditions request of the Security IC Embedded Software[1] to demonstrate the correct operation of the alarm lines and/or the environmental sensor mechanisms:

[1] [assignment: list of cryptographic operations]
[2] [assignment: cryptographic key sizes
[3] [assignment: list of standards]
[4] [assignment: cryptographic key destruction method]
[5] [assignment: list of standards]

- Please refer to the confidential Security Target[2]

6.1.5 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).

6.1.5.1 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

6.1.5.2 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:

[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)

- 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 acces 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.

6.1.5.3 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.

- 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 inTable 21.
- overlapping regions, have access to other regions with ascending region priority:
  region 7 = highest priority, region 0 = lowest priority
- 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 full access while any access from user mode leads to a permission fault.
Read/write	Read(execute) only	Privileged mode has full access while the user mode has no write access rights. Execute access in User mode further depends on the xn bit.
Read/write	Read(execute)/write	Privileged mode has read and execute access rights. Write

Security Requirements (ASE_REQ)

Privileged Mode Permissions	User Mode Permissions	Description
		accesses from privileged mode lead to a permission fault. Any access of the user mode leads to a permission fault.
Read only	No access	Privileged mode has read and execute access rights. Write accesses lead to a permission fault. The same holds for the user mode, except execute access further depends on the xn bit.
Read only	Read(execute) only	All accesses in user mode and privileged mode generate a permission fault

6.1.5.4 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 Memory Access Control Policy as[1] defined in section 6.1.5.1[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 Memory Access Control Policy[3] to objects based on the following: Attributes as specified in section 6.1.5.2[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: As specified in the section 6.1.5.3[5].
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[6].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[1].

[1] editorially refined

[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]

FMT_MSA.3	Static attribute initialization
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 security roles
FMT_MSA.3.1	The TSF shall enforce the Memory Access Control Policy[2] to provide restrictive[3] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the privilege mode[4] 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 Memory Access Control Policy[5] to restrict the ability to modify[6] the security attributes Security Attribute which control the behavior of the Subject MPU[7] to the privilege mode[8].

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: modifying the security attributes[9].

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 privilege mode and non-privilege mode[10].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.1.6 Data Integrity

FDP_SDI.2	Stored data integrity monitoring and action

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

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

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

[4] [assignment: the authorised identified roles]

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

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

[7] [assignment: list of security attributes]

[8] [assignment: the authorised identified roles]

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

[10] [assignment: the authorised identified roles]

Security Requirements (ASE_REQ)

Hierarchical to:	FDP_SDI.1 stored data integrity monitoring
Dependencies:	No dependencies
FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for data integrity and one- and/or more-bit-errors[1] on all objects, based on the following attributes: error correction ECC for the SOLID FLASH™ NVM[2].
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall correct 1 bit errors in the SOLID FLASH™ NVM automatically and inform the user about other bit errors[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 the information of the user data while it is stored in the RAM and SOLID FLASH™ NVM[4].

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)

[1] [assignment: integrity errors]

[2] [assignment: user data attributes]

[3] [assignment: action to be taken]

[4] [assignment: memory area]

Security Requirements (ASE_REQ)

EA unavailable	EA available
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**
Hierarchical to:	No other components.
Dependencies:	No other components
FMT_LIM.1.1/Loader	The TSF shall be designed and implemented in a manner that limits its capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” 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[1].

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: The TSF prevents deploying the Loader functionality after permanent deactivation[2].

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 user[3], 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.

[1] [assignment: Limited capability policy]

[2] [assignment: Limited availability policy]

[3] [assignment: users authorized for using the Loader]

Security Requirements (ASE_REQ)

FTP_ITC.1.2	The TSF shall permit another trusted IT product[1] 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 data[2].

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 SFP[3] to receive[4] user data in a manner protected from unauthorised disclosure.

FDP_UIT.1	**Data exchange integrity**
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 SFP[5] to receive[6] user data in a manner protected from modification, deletion, insertion[7] errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion[8] 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 Loader SFP[9] on • the subjects Administrator User, Download Operator User and Image Provider, • the objects user data in SOLID FLASH™ NVM memory of the TOE, • the operation deployment of Loader[10]

FDP_ACF.1/Loader	**Security attribute based access control - Loader**
Hierarchical to:	No other components.

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

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

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

[4] [selection: transmit, receive]

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

[6] [selection: transmit, receive]

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

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

[9] [assignment: access control SFP]

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

Security Requirements (ASE_REQ)

Dependencies:	FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/Loader	FDP_ACF.1.1 The TSF shall enforce the Loader SFP[1] to objects based on the following: the subjects and objects of FDP_ACC.1.1/Loader without security attributes[2]
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: 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 Provider[3]
FDP_ACF.1.3/Loader	FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[4].
FDP_ACF.1.4/Loader	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[5].

Note: The security functional requirements FIA_API.1, FTP_ITC.1, FDP_UCT.1, FDP_UIT.1, FDP_ACC.1/Loader and FDP_ACF.1/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.

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 change_default, modify, delete[6] the Authentication keys for Administrator User, Download Operator User and Image Provider[7] to Administrator User, Download Operator User[8].

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.

[1] [assignment: access control SFP]

[2] [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]

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

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

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

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

[7] [assignment: list of TSF data]

[8] [assignment: the authorised identified roles]

Security Requirements (ASE_REQ)

Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1/Loader	The TSF shall maintain the roles Administrator User, Download Operator User, Image provider[1].
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: Change Key, Invalidate Key[2].

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
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.

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 a authentication mechanism according to [ISO9798_2] section 6.2.2 Mechanism 4: Three-pass authentication[3] to prove the identity of the TOE[4] 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.

[1] [assignment: the authorised identified roles]

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

[3] [assignment: authentication mechanism]

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

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	
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.

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].

6.2.2 Security policy model details

EAL6 requires the development of a formal security policy model of the TSF, and establishing a correspondence between the functional specification and this security policy model. Preserving internal consistency the security policy model is expected to formally establish the security principles from its characteristics by means of a mathematical proof.

ADV_SPM.1 Formal TOE security policy model

Hierarchical to: No other components

Dependencies: ADV_FSP.4 Complete function description

ADV_SPM.1.1D The developer shall provide a formal security policy model for the

Memory Access Control Policy and the corresponding SFRs

- FDP_ACC.1 Subset Access Control
- FDP_ACF.1 Security attribute based access control
- FMT_MSA.1 Management of Security Attributes
- FMT_MSA.3 Static Attribute Initialization.
- FMT_SMF.1 Specification of management functions
- FMT_SMR.1 Security roles

Security Requirements (ASE_REQ)

Support of Flash Loader SFRs

- FMT_LIM.1/Loader Limited Capabilities
- FMT_LIM.2/Loader Limited availability – Loader
- FTP_ITC.1 Inter-TSF trusted channel
- FDP_UCT.1 Basic data exchange confidentiality
- FDP_UIT.1 Data exchange integrity
- FDP_ACC.1/Loader Subset access control – Loader
- FDP_ACF.1/Loader Security attribute based access control – Loader
- FMT_MTD.1/Loader Management of TSF data – Loader
- FMT_SMR.1/Loader Security roles – Loader
- FMT_SMF.1/Loader Specification of Management Functions – Loader
- FIA_UID.2/Loader Use identification before any action – Loader

Support of Authentication of the Security IC SFR

- FIA_API.1 Authentication Proof of Identity

Moreover, the following SFRs shall be addressed by the formal security policy model:

- FDP_SDI.2 Stored data integrity monitoring and action
- FDP_SDC.1 Stored data confidentiality
- FDP_ITT.1 Basic Internal Transfer Protection
- FDP_IFC.1 Information Flow Control
- FPT_ITT.1 Basic internal TSF data transfer protection
- FPT_PHP.3 Resistance to physical attack
- FPT_FLS.1 Failure with preservation of secure state
- FRU_FLT.2 Limited fault tolerance
- FMT_LIM.1 Limited capabilities
- FMT_LIM.2 Limited availability
- FAU_SAS.1 Audit storage

ADV_SPM.1.2D For each policy covered by the formal security policy model, the model shall identify the relevant portions of the statement of SFRs that make up that policy.

ADV_SPM.1.3D The developer shall provide a formal proof of correspondence between the model and any formal functional specification.

ADV_SPM.1.4D The developer shall provide a demonstration of correspondence between the model and the functional specification.

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”

Security Requirements (ASE_REQ)

Objective	TOE Security Functional Requirements
	- 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.4/SCL, FCS_COP.1/SCL/AES, FCS_COP.1/SCL/AES-MAC,
O.AES	FCS_CKM.4/SCL, FCS_COP.1/SCL/AES
O.TDES	FCS_COP.1/SCL/TDES, FCS_CKM.4/SCL
O.RSA	FCS_COP.1/RSA/<iteration>, FCS_CKM.1/RSA/<iteration>, FCS_CKM.4/RSA
O.ECC	FCS_COP.1/ECC/<iteration>, FCS_CKM.1/ECC, FCS_CKM.4/ECC
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:

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 conduce 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 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 andone-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, 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	FCS_CKM.4 [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes No, see comment 2
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	No, see comment 2

Security Requirements (ASE_REQ)

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FCS_CKM.1	[FCS_CKM.2, FCS_COP.1, FCS_CKM.4]	Yes, FCS_CKM.4
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.2	Yes
FMT_SMF.1/Loader	FIA_UID.2	Yes

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:

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

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

These requirements all address the appropriate management of cryptographic keys used by the specified cryptographic function. Most requirements concerning key management 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.

For the security functional requirement FCS_COP.1/SCP/<iteration> and FCS_COP.1/SCL/<iteration> the respective dependency [FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2] has to be fulfilled by the environment.

For the security functional requirement FCS_COP.1/RSA/<iteration>, FCS_COP.1/ECC/<iteration> key generation is also supported by the ACL, therefore the dependency [FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2] is met.

The security functional requirement “Cryptographic key destruction (FCS_CKM.4)” met by the TOE has the following dependencies:

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

Security Requirements (ASE_REQ)

For the security functional requirement FCS_COP.1/SCP/<iteration> and FCS_COP.1/SCL/<iteration> the respective dependency [FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2] has to be fulfilled by the environment.

For the security functional requirement FCS_COP.1/RSA/<iteration>, FCS_COP.1/ECC/<iteration> the dependenvy is met by FCS_CKM.1.

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

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.1is 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.

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. . Different operation modes help to protect the TOE during each phase of its lifecycle.

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 priviledge 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		
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.4/SCP					x
FCS_COP.1/SCL/<iteration>					x
FCS_CKM.4/SCL					x
FCS_COP.1/RSA/<iteration>					x
FCS_CKM.1/RSA/<iteration>					x
FCS_CKM.4/RSA					x
FCS_COP.1/ECC/<iteration>					x
FCS_CKM.1/ECC					x
FCS_CKM.4/ECC					x
FCS_RNG.1/TRNG					x
FCS_RNG.1/HPRG					x
FCS_RNG.1/DRNG					x
FCS_RNG.1/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	
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.

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 Part 2: Security Functional Requirements; Version 3.1 Revision 5 April 2017, CCMB-2017-04-002
[CCBook3]	Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements; Version 3.1 Revision 5 April 2017, CCMB-2017-04-003
[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 2.9, January 2013
[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
[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

References

[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 July 2017, Revision 2
[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.

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

10 Appendix: hash signatures of the HSL

HSL-03.52.9708-SLCx7V11a.lib

MD5	2e1ec43d5d13d27d65456cbeb7a84cc4
SHA-1	05d4e3caa916a6182aed7b06354153bcf04d82c7
SHA-256	7df825ec42763570334e641f72fc41466712d6d231a9bf75174acb5005f3869a

11 Appendix: hash signatures of UMSLC lib

UMSLC-01.30.0564-SLCx7V11a.lib:

MD5	b444ffaed77933be4407935f135728a7
SHA-1	c0ba8430b96a2dc7888067fd0da301ff3405736d
SHA-256	af948dfe1449b4bf20c4cdd23d6f40efb98515c84712a2526dfaf229fcda9536

12 Appendix: hash signatures of SCL

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

MD5= be3b586f0a28aa9d49aadc50a2db4be1

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= 5e7fd5230b21a36420934841e1205beff46c70011095aceaa4ce8d2ed868d213

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

MD5= 852e3074775fa559fce734e86216e9e4

SHA1= 182663c8043ff906065feda20689090a1a8721fc

SHA256= 27547d8f5cfe26c89c4460e5bc254e9f1937768e9f9d681c9c04607e4f87a784

13 Appendix: hash signatures of ACL

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

14 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 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

BLD Backside Light Detector

BPU Block to Planned Usage. Feature allowing to configure a given device to its required usage by de-activating (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 Codem Peripheral Access Unit

CPU Central Processing Unit

Crypto2304T Asymmetric Cryptographic Processor

DPA Differential Power Analysis

DFA Differential Failure Analysis

DRNG Deterministic Random Number Generator

EA External Authentication

EC Elliptic Curve

ECC Error Correction Codeo r Elliptic Curve Cryptography (depending on context)

ECDH Elliptic Curve Diffie-Hellman

ECDSA Elliptic Curve Digital Signature Algorithm

EDC Error Detection Code

EMA Electro magnetic analysis

Flash Flash Memory

List of Abbreviations

FSE	Frequency Sensor
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
PFL	Performance Flash Loader
POWS	Performance Optimized Write Scheme
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
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
TSE	Temperatrure Sensor
TSF	TOE Security Functionality
UART	Universal Asynchronous Receiver/Transmitter

List of Abbreviations

UM	User Mode (STS)
UMSLC	User mode Security Life Control
VSE	Voltage Sensor
WDT	Watch Dog Timer
TDES	Triple DES

15 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	Physical or non-physical part of a system which contains information and is acted upon by subjects
Operating System	Software which implements the basic TOE actions necessary for operation
Programmable Read Only Memory	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	Part of the firmware containing NVM programming routines, AIS31 testbench etc.
Self Test Software	Part of the firmware with routines for controlling the operating state and testing the TOE hardware
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	Operational status phase of the TOE in which actions to test the TOE hardware take place

Glossary

Threat	Action or event that might prejudice security
User Mode	Operational status phase of the TOE in which actions intended for the user takes place

16 Revision History

Major changes since the last revision

Version	Description of change
v1.2	Initial draft version
v4.0	Final version

Edition 2020-10-15

Published by

Infineon Technologies AG

81726 Munich, Germany

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.