Public Security Target
IFX_CCI_00003Fh
IFX_CCI_000059h
IFX_CCI_00005Bh
IFX_CCI_00003Ch

G11

Common Criteria EAL6 augmented / EAL6+

Resistance to attackers with HIGH attack potential

including
Flash Loader according Package1 and Package2

Revision 1.0 as of 2020-12-07

Author: Infineon Technologies AG

DSS SQM CERT, Jürgen Noller

Table of Contents

1 Security Target Introduction (ASE_INT)

1.1 Security Target reference

The Security Target has the Revision 1.0 and is dated 2020-12-07. The title of this document is Public Security Target IFX_CCI_00003Fh IFX_CCI_000059h, IFX_CCI_00005Bh IFX_CCI_00003Ch G11.

1.2 TOE reference

The Security Target comprises an Infineon Technologies Security Controller named IFX_CCI_00003Fh IFX_CCI_000059h, IFX_CCI_00005Bh IFX_CCI_00003Ch design step G11 and with specific IC-dedicated firmware identifier 80.203.00.3 and user guidance, in the following called TOE (Target of evaluation).

The Security Target is based on the Protection Profile “Smartcard IC PlatformProtection Profile” [1]. The Protection Profile and the Security Target are built in compliance to Common Criteria v3.1.

The targeted assurance level is EAL6+.

Table 1 Identification of the TOE

Hardware	Version	Mehode of identification
IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh IFX_CCI_00003Ch (each of the comma separated term is a Common Criteria Certification Identifier)	G11 (design step)	Non-ISO ATR
Firmware		
BOS	80.203.00.3	Non-ISO ATR: firmware identifier
Flash-loader	v8.06.001	Flash-loader function
User Guidancee		
32-bit Security Controller – V20 Hardware Reference Manual for IFX_CCI_00003Fh IFX_CCI_000059h, IFX_CCI_00005Bh	Rev. 2.3	document
32-bit Security Controller – V21 Hardware Reference Manual for IFX_CCI_00003Ch	Rev. 2.3	document
ARMv7-M Architecture Reference Manual	DDI 0403D ID0 21310	document

Production and personalization 32-bit ARM-based security controller User´s manual	Rev. 3.4	document
32-bit Arm-based Security Controller SLC37 (65 nm Technology) Programmer´s Reference Manual	Rev. 4.6	document
32-bit Security Controller – V20 Security Guidelines for IFX_CCI_00003Fh IFX_CCI_000059h, IFX_CCI_00005Bh	Rev. 1.00-2621	document
32-bit Security Controller – V21 Security Guidelines for IFX_CCI_00003Ch	Rev. 1.00-2622	document
32-bit Security Controller – V20 Errata Sheet for IFX_CCI_00003Fh IFX_CCI_000059h, IFX_CCI_00005Bh	Rev. 3.0	document
32-bit Security Controller – V21 Errata Sheet for IFX_CCI_00003Ch	Rev. 3.0	document
32-bit Security Controller Crypto@2304T V3 User Manual	Rev. 2.0	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 5.

1.3 TOE overview

1.3.1 TOE definition and usage

The TOE consists of smart card IC (Security Controller), 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 lifecyclemodel from [1].

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, RNG (PTG.2, PTG.3, DRG.2, DRG.3 according to [6]
- 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
- Programflow integrity protection
- Peripheral access control
- Bus encryption for security peripherals
- Security optimized wiring
- Leakage control of data dependent code execution
- Device phasemanagement supporting isolation of test features and flash loader accessibility
- Detection of NVM single and multi bit errors

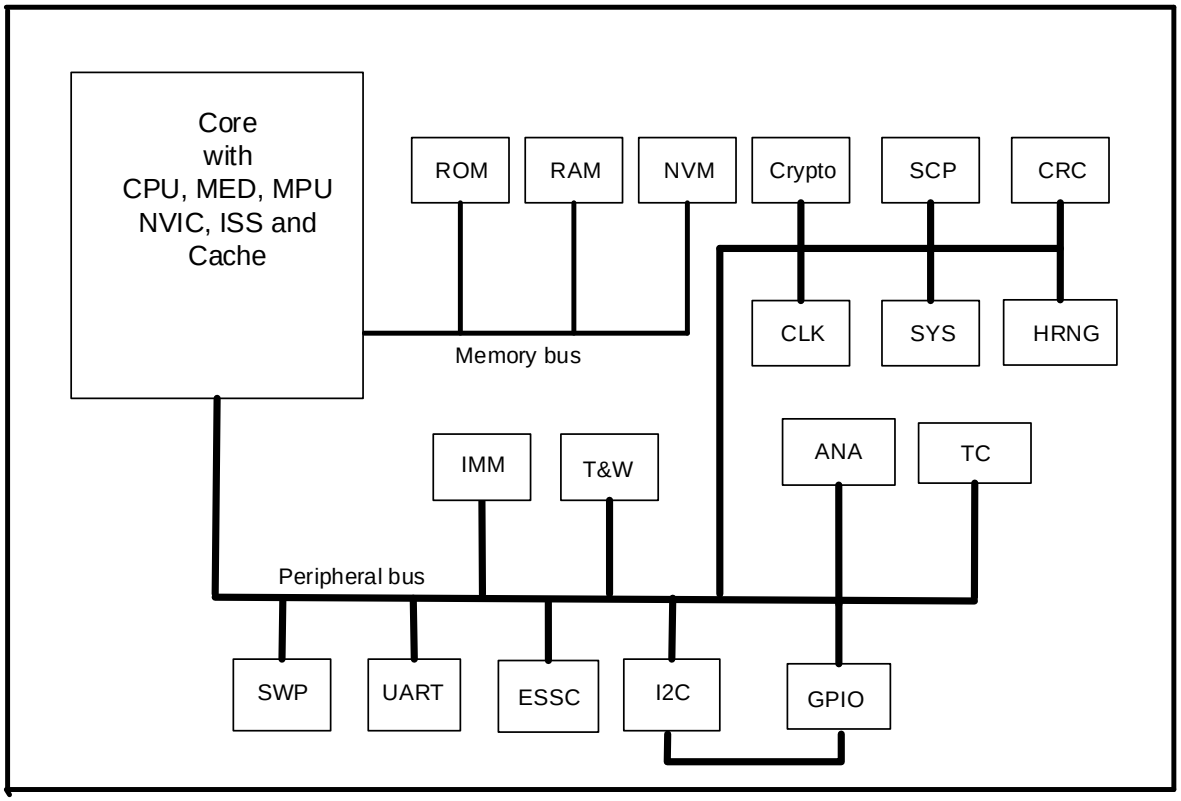
1.4 TOE description

1.4.1 TOE components

1.4.1.1 Hardware components

The Figure 1 shows a block diagram of the TOE hardware.

Figure 1 Simplified block diagram of the TOE



Core	Core System	ROM	Read Only Memory
NVM	SOLID FLASH™ NVM	RAM	Random Access Memory
CLK	Clock Unit	SYS	System Module
Crypto	Crypto2304T	SCP	Symmetric Crypto Processor
CRC	Cyclic Redundancy Check	HRNG	Hybrid Random Number Generator
T&W	Timer and Watchdog	UART	UART
I2C	Inter-Integrated Cirquit (I2C)	GPIO	General Purpose IO
SWP	Single Wire Protocol	ANA	Analog Units
IMM	Interface Management Module	TC	Tick Counter
ESSC	Enhancd Synhronous Serial Slave Controller		

The TOE hardware consists of a core, busses, coprocessors, memories, peripherals and a hybrid random number generator.

The Core

The major components of the core system are the 32-bit CPU (Central Processing Unit), the MPU (Memory Protection Unit), the MED (Memory Encryption/Decryption Unit), the Nested Vectored Interrupt Controller (NVIC), the Instruction Stream Signature Checking (ISS) and the Cache system. The CPU is compatible with the instruction set of the ARMv7_M architecture. Despite its compatibility the CPU implementation is entirely proprietary and not standard.

The CPU accesses the memory via the integrated Memory Encryption and Decryption unit (MED). The core stores both code and data in a linear 4-GByte memory space, allowing direct access without the need to swap memory segments in and out of memory using a memory protection unit. The memory model of the TOE provides two distinct, independent levels. Additionally up to eight regions can be defined with different access rights controlled by the Memory Protection Unit (MPU).

The Cache is a high-speed memory-buffer located between the CPU and the (external) main memories holding a copy of some of the memory contents to enable access, which is considerably faster than retrieving the information from the main memory. In addition to its fast access speed, the Cache also consumes less power than the main memories. The Cache is equipped with a parity protection and integrity check to verify the contents of the cache memories. The data stored in the Cache data are masked.

The Nested Vectored Interrupt Controller controls the interrupt handling and the Instruction Stream Signature Checking is an optional feature to control the program flow of the software running on the TOE.

The Busses

The bus system comprises two separate bus entities to connect the memories and the peripherals with the core: a memory bus and a peripheral bus for high-speed communication internally between the modules and to the outer world with the peripherals. The transfer of data via the memory bus is protected by means of transfering only encrypted data, and the transfer of data via the peripheral bus is protected by means of masking for the modules SCP, Crypto2304T, CRC and HRNG.

The cryptographic Coprocessors

The TOE implements two coprocessors. The Symmetric Cryptographic Coprocessor (SCP) combines both AES and DES with dual-key or triple-key hardware acceleration. The Asymmetric Cryptographic Coprocessor (Crypto2304T) provides optimized high performance calculations for the user software executing cryptographic operations. These coprocessors are especially designed for smart card applications with respect to the security and power consumption. The SCP module computes the complete DES algorithm within a few clock cycles and is especially designed to counter attacks like DPA, EMA and DFA.

Note that this TOE can come with both crypto coprocessors accessible, or with a blocked SCP, or with a blocked Crypto2304T, or with both cryptographic coprocessors blocked. The blocking depends on the customer demands prior to the production of the hardware. No accessibility of the deselected cryptographic coprocessors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic coprocessors.

The Memories

All content stored in the different memories remains encrypted. The RAM is equipped with parity error detection and the SOLID FLASH™ NVM is equipped with an error correction code (ECC) to automatically correct one-bit-errors. Additionally the addresses are protected by an address scrambling algorithm. All data of the memory blocks are encrypted.

The TOE uses also Special Function Registers SFR. These SFR registers are used for general purposes and chip configuration; the Online Configuration Check (OCC) function is used for register protection, i.e. controls the modification of relevant SFR settings.
The start-up register values are stored in the SOLID FLASH™ NVM, in the configuration page area.

The ROM is used by IFX only. The Boot Software and the Flash Loader together compose the TOE firmware stored in the ROM and in the SOLID FLASH™ NVM. All mandatory functions for internal testing, production usage and start-up behavior are grouped together in a common privilege level. Two levels are provided, the privileged level and the user level, both are protected by a hardwired Memory Protection Unit (MPU) setting.

The user software can be implemented in various options depending on the user's choice and described in section 1.1. Thereby the user software, or parts of it, can be downloaded into the SOLID FLASH™ NVM, either during production of the TOE or at customer site. In the latter case, the user downloads his software or the final parts of it at his own premises, using the Flash Loader software for downloading during the manufacturing process. The Flash Loader is dedicated for usage by authorized users only in any operation environment up to "Phase 6 Security Personalization".

The Peripherals

The Analog Modules (ANA) serve for operation within the specified range and manage the alarms. A set of sensors (temperature-, frequency-, voltage-, backside light detector) is used to detect excessive deviations from the specified operational range and serve for robustness of the TOE and specific Special Function Registers (UMSLC) can be used to test the alarm lines.

A shielding algorithm finishes the upper layers above security critical signals and wires, finally providing the so called "I2-shield".

A decentralized alarm propagation and system deactivation principle is implemented, further decreasing the risk of manipulating and tampering. Additionally, an online check of parts of the security mechanisms is available by specific Special Function Resisters (UMSLC).

Several supporting features e.g. trash register writes and instruction interrupt prevention, the optional Instruction Stream Signature Checking (ISS) are implemented as countermeasure against fault attacks and side-channel.

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

The implemented sleep mode logic (clock stop mode per ISO/IEC 7816-3) is used to reduce the overall power consumption. Several timer and watch dog modules are implemented used for example to control the communication via the UART, other interface behavior or for asynchronous wake-up and similar timed events.

The timers permits easy implementation of communication protocols such as T=1 and all other time-critical operations. The UART-controlled I/O interface allows the smart card controller and the terminal interface to be operated independently. The watch-dog timers implement a configurable time out for various purposes. More information can be found in the "32-bit Security Controller Hardware Reference Manual "[7].

The Clock Unit (CLKU) supplies the clocks for all components of the TOE. It generates the system clock and an approximately 1MHz clock for the timers. The 1MHz clock is derived from an internal oscillator, while the system clock may either be based on the internal oscillator clock (internal clock mode) or on an external clock (external clock mode). Additionally a sleep mode is available. When operating in the internal clock mode the system frequency can be configured by the user software combined with the current limitation functionality. In the external clock mode the clock is derived from the external clock and a parameter with the range of 1 to 8. The system frequency may be 1 up to 8 times the externally applied frequency but is of course limited to the maximum system frequency and can be combined with the current limitation function.

The Tick Counter (TC) module provides a 40-bit low-power counter which is fed by a 1 kHz clock. After counter reset, the value will overflow after approximately 34.8 years of continious operation.

The cyclic redundancy check (CRC) module is used to compute a checksum over any input data and allows by that explicit checking integrity of a piece of data. The CRC module is not part of the TOE Security Functionality (TSF) of this TOE.

An Interface Management module, located in the System Module (SYS), provides the TOE with the possibility to maintain two or more data interfaces simultaneously. The TOE is provided with, dependent on the configuration, different peripherals and interfaces as the SWP Slave Peripheral (SWP), the GPIO module (GPIO), the Inter-Integrated Cirquit Module (I2C), the Enhanced Synchronous Serial Slave Controller (ESSC) providing an SPI-compaible interface and the UART, providing the Standard ISO interface, to satisfy the different market requirements.

In addition to the interfaces the Hybrid Random Number Generator (HRNG) is implemented. This HRNG equals to the expression Hybrid Physical True Random Number Generator (hybrid PTRNG) as defined by the BSI. In the following, the BSI expression hybrid PTRNG is used. The hybrid PTRNG implements a true physical random source and has evidenced its conformance to different classes of AIS31 [6] as declared in section 6.1.1.

The produced genuine random numbers are available as a security service for the user and are also used for internal purposes. The hybrid PTRNG operates in the following modes of operation:

- True Random Number Generation, meeting AIS31 PTG.2
- Hybrid Random Number Generation, meeting AIS31 PTG.3
- Deterministic Random Number Generator (DRNG), meeting AIS31 DRG.3
- Key Stream Generator (KSG), stream cipher generation, meeting DRG.2

The hybrid PTRNG is deemed for any application requiring excellent physical random data entropy.

1.4.1.2 Firmware components

The TOE provides the following low-level firmware components: the Boot Software (BOS) 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 flash loader allows downloading of User Software into the NVM during the manufacturing process. It uses the SCP to download encrypted user data.

1.4.1.3 User Guidance components

The following provides a brief overview of the document set constituting the user guidance for this TOE. The user guidance is delivered in the format *.pdf or *.chm to the user. The user can download the user guidance documentation as an encrypted file from a dedicated Infineon server.
The exact document titles and versions are given in section 9.

- 32-bit Security Controller – V20 Hardware Reference Manual [7] (HRM) for the IFX_CCI_00003Fh IFX_CCI_000059h and IFX_CCI_00005Bh products or the
  32-bit Security Controller – V21 Hardware Reference Manual [7] (HRM) for the IFX_CCI_00003Ch product, both are the user data book of the TOE and contains the relevant module, function and feature description
- ARMv7-M Architecture Reference Manual [5] (ARM), is the user data book for the core of the TOE
- Production and personalization 32-bit ARM-based security controller User´s Manual [14] (PPM), contains detailed information about the usage of the Flash Loader
- 32-bit Arm-based Security Controller SLC37 (65 nm Technology) Programmer´s Reference Manual [11] (PRM), describes the usage and interfaces of the TOE
- 32-bit Security Controller – V20 Security Guidelines [23](SG) for the IFX_CCI_00003Fh IFX_CCI_000059h and IFX_CCI_00005Bh products or the
  32-bit Security Controller – V21 Security Guidelines [23](SG) for the IFX_CCI_00003Ch product,
  both providing the guidance and recommenddations to develop secure software for and secure usage of this TOE
- 32-bit Security Controller – V20 Errata Sheet [12] (ERS) for the IFX_CCI_00003Fh IFX_CCI_000059h and IFX_CCI_00005Bh products or the
  32-bit Security Controller – V21 Errata Sheet [12] (ERS) for the IFX_CCI_00003Ch product, both containing latest updates and corrections of the TOE relevant for the user and it is a kind addendum to the 32-bit Security Controller – V20/21 Hardware Reference Manual [7]. The Errata Sheet can be changed during the life cycle of the TOE. New Errata Sheet releases are reported in a monthly updated list provided from Infineon Technologies AG to the user. This list is not part of the certification process. Part of the TOE certification is the released version valid at the point in time the certificate was issued
- 32-bit Security Controller Crypto@2304T V3 User Manual [104] (CUM), provides the interface to the asymmetric cryptographic coprocessor Crypto2304T

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 the following:

- Cryptographic support: TDES, AES (block cipher modes ECB, CBC, CBC-MAC, CBC-MAC-ELB, RNG (PTG.2, PTG.3, DRG.2, DRG.3 according to [6]),
- 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 systemdeactivation 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 StreamSignature 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.
- Security optimized wiring: shield lines in combination with layout measures reduce the risk of successful manipulative attacks.
- Leakage control of data dependend 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 a mutual authentication. 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.

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 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 GPIO interface consists of 5 pads which can be individually configured and combined in various ways.
  - Also the I2C communication can be exclusively driven via the GPIO pads. In this case no other communication using the GPIO pads is possible.
  - The SWP interface is build out of one pad to support the SWP slave functionality.
  - The Serial Peripheral Interface (SPI) compatible provided by the Enhanced Synchronous Serial Controller
- The data-oriented I/O interface to the TOE is formed by the I/O pad.
- The interface to the firmware is constituted by special registers used for hardware configuration and control (Special Function Registers, SFR).
- The interface of the TOE to the operating system is constituted by the instruction set of the TOE.
- The interface of the TOE to the test routines is formed by the BOS test routine call, i.e. entry to test mode (OS TM entry).

1.4.5 Forms of Delivery

The following table illustrates all TOE components, which may be delivered to a costumer, including the identification of the delivered format (e.g. whether the user guidance document is delivered as a *.pdf or *.chm file) and the delivery method (e.g. delivery courier or PGP-encrypted Email).

Table 2 Forms of delivery

TOE Component	Delivered Format	Delivery Method	Comment
Hardware			
IFX_CCI_00003Fh IFX_CCI_000059h IFX_CCI_00005Bh IFX_CCI_00003Ch all in the design G11	- complete modules, - plain wafers, - bare dies, - in any IC case, - in what ever type of package	Postal transfer in cages	All materials are delivered to distribution centers in cages, locked
Firmware			
BOS	–	–	This firmware part of stored on the delivered hardware
Flash Loader	–	–	This firmware part of stored on the delivered hardware
Guidance Documentation (full name see section 1.4.1.3)			
ARM [5]	Personalized PDF	Secured download	
HRM [7]	Personalized PDF	Secured download	–
PPM [14]	Personalized PDF	Secured download	–
PRM [11]	Personalized PDF	Secured download	–
SG [23]	Personalized PDF	Secured download	-
ERS [12]	Personalized PDF	Secured download	–
CUM [104]	Personalized PDF	Secured download	Optional; delivered if Crypto@2304T not blocked

The 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.

The form of delivery does not affect the TOE security and it can be delivered in any type, as long as the processes applied and sites involved have been audited as compliant to the Common Criteria scheme. The delivery can therefore be at the end of phase 3 or at the end of phase 4 which can also include pre-personalization steps according to PP [1]. Nevertheless in both cases the TOE is finished and the extended test

features are removed. In this document are always both cases mentioned to avoid incorrectness but from the security policy point of view the two cases are identical.

The delivery to the software developer (phase 2 ➔ phase 1) contains the development package and is delivered in form of documentation as described above, data carriers containing the tools and emulators as development and debugging tool.
Part of the software delivery could also be the Flash Loader program, provided by Infineon Technologies AG, running on the TOE receiving the transmitted information of the user software to be loaded into the SOLID FLASH™ NVM. The download is only possible after successful mutual authentication of the TOE and the authorized user. The download process of the data uses a trusted channel to protect the integrity and confidentiality of the loaded data. In addition, the authorized user is after he finalized the download and prior deliver to third party (Phase 7 Security IC End-usage) obligated to permanently lock further use of the Flash Loader. Note that it depends on the procurement order, whether the Flash Loader program is present or not.

1.4.6 Production sites

The TOE may be handled in different production sites but the silicon of this TOE is produced in Tainan, Taiwan only, as listed below. To distinguish the different production sites of various products in the field, the site is coded into the Generic Chip Ident Mode (GCIM) data. The exact coding of the generic chip identification data is described in the “32-bit Security Controller – V20 Hardware Reference Manual” and “32-bit Security Controller – V21 Hardware Reference Manual” [7], section Chip Identification Mode.

The delivery measures are described in the ALC_DVS aspect.

Production site in chip identification

Production Site	Chip Identification
Tainan, Taiwan	byte number 13 (Fab number): $0A_H$

1.4.7 TOE configuration

This TOE is represented by a number of various products which are all based on the equal design sources. The TOE hardware and firmware remains entirely equal throughout all derivatives, but the usage for example in form of available memory sizes, availability of the various interfaces, or other functions varies by means of blocking and chip configuration. All TOE derivatives are derived from the equal hardware design results. The product IFX_CCI_00003Ch run through the Burn-In process during the production to reduce the error rate.
The TOE, referenced in Table 1 at rows Hardware and Version, can be identified with the Generic Chip Identification Mode (GCIM). The TOE hardware platform is identified by the Common Criteria Certification Identifier bytes of the GCIM as given in the “32-bit Security Controller – V20 Hardware Reference Manual “ and “32-bit Security Controller – V21 Hardware Reference Manual” [7]:
The unique hexadecimal values as stated in the title are:

- IFX_CCI_00003Fh
- IFX_CCI_000059h
- IFX_CCI_00005Bh
- IFX_CCI_00003Ch

These bytes clearly identify the hardware platform, or, in other words, the therein possible values for the TOE (without prefix IFX_CCI_) represent the equal hardware platform of this TOE. This means that the hardware entirely equals throughout all derivatives and that the differences are achieved by configuration and blocking means only. These values are unique for this hardware platform. This means that these values will not be used in any other platform or product.

The interpretation of the output GCIM data is clearly explained in the user guidance, “32-bit Security Controller – V20 Hardware Reference Manual “ and “32-bit Security Controller – V21 Hardware Reference Manual” [7] and in the “32-bit ARM-based Security Controller Programmer´s Reference Manual” [11].

This TOE is represented by a number of various products which are all based on the equal design sources. The TOE hardware and firmware remains entirely equal throughout all derivatives, but the usage for example in form of available memory sizes, availability of the various interfaces, or other functions varies by means of blocking and chip configuration. This blocking is applied by Infineon settings during the production only. Again, all TOE derivatives are derived from the equal hardware design results, the TOE.

Despite these configuration possibilities, all products are derived from the equal hardware design results, the TOE. The differences between the derivatives have no impact on the TOEs security policies. Details are explained in the user guidance “32-bit Security Controller – V20 Hardware Reference Manual“ and “32-bit Security Controller – V21 Hardware Reference Manual” [7].

All products are identically from module design, layout and footprint, but differ in their possibilities to connect to different interface options. Therefore, the TOE is represented and may be made out of different mask sets all with TOE internal and security irrelevant differences, to enable to adapt various external devices not being part of this TOE. This flexibility allows for example to connect to different types of interfaces, enables to design for different form factors and for the use of a variety of different kinds of packages with related power supply variants. Additionally there may be further package options require flexibility in design and could also depend on user requirements. In these cases one or more additional metal layer are added on top of one of the TOE mask set. These additional metal layers, it could also be more than one, just reroute the pads. Therefore, this last rerouting on top does not change the function of the TOE itself and is depending on the package only. These top metal layers are flexible in design, could depend also on user requirements and are of course not relevant for the security of the TOE. For these reasons, the metal layers are out the scope of the certification and do not belong to the TOE. Of course, in all cases passivation and isolation coating is applied on top of the last layers carrying wires.

Except this external adapt capability the TOE hardware and firmware remains entirely equal throughout all derivatives, but the usage for example in form of available memory sizes, availability of the various interfaces, or other functions varies by means of blocking and chip configuration. This blocking is applied by Infineon settings during the production only. Again, all TOE derivatives are derived from the equal hardware design results, from theTOE.

To each of the TOE relevant optional different mask set variants, an individual value is assigned, which is part of the data output of the Generic Chip Identification Mode (GCIM). By that the various hardware mask sets can be clearly identified and differentiated by the GCIM output. The interpretation of the output GCIM data is clearly explained in the user guidance [7].

There are no other differences between the mask sets the TOE is produced with, and all these changes have no impact on the TOEs security policies and related functions. Details are explained in the user guidance [7] and in the “32-bit Security Controller – V20 Errata Sheet” “32-bit Security Controller – V21 Errata Sheet” and [12].

The TOE product allows for a maximum of configuration possibilities defined by the customer order or his blocking following the market needs. For example, a TOE can come in one project with the fully available SOLID FLASH™ NVM or in another project with any other SOLID FLASH™ NVM-size below the physical implementation size, or with a different RAM size. And more, the user has the free choice, whether he needs the Symmetric Cryptographic Coprocessor SCP or not and, to be even more flexible, various interface options can be chosen as well. To sum up the major selections, the user defines by his order:

- the available memory sizes of the SOLID FLASH™ NVM and RAM,
- the availability of the Symmetric Cryptographic Coprocessor for DES and AES Standards,
- the availability of the Crypto@2304T coprocessor for RSA and EC Standards
- the availability of the Flash Loader,
- the availability of various interface options, and
- the possibility to tailor the product by blocking on his own premises (BPU),
- the possibility to apply the PIN-Letter in combination with the Flash Loader.

The degree of freedom of the chip configuration is predefined by Infineon Technologies AG and made available via the order tool.

Beside fix TOE configurations, which can be ordered as usual, this TOE implements optionally the so called Billing-Per-Use (BPU) ability. This solution enables our customer to tailor the product on his own to the required configuration –project by project. By that BPU allows for significant reduction of logistic cost at all participating parties and serves for acceleration of delivery of tailored product to the end-user.

The BPU enables our customers to block the chip on demand into the final configuration at his own premises, without further delivery or involving support by Infineon Technology AG.

The realization of it requires the presence of the Flash Loader software, enhanced with the BPU blocking software part. The presence of the BPU ability defines the customer with his order.

The user then receives this TOE in a predefined starting configuration, for example entirely unblocked. Again, the delivered starting configuration depends on the user order. After delivery, the user can put the TOE in volume on his stock and can block it down to the required sizes and features, whenever a certain configuration is required by a certain project.

Depending on the number of TOE products delivered, and their individual final blocked configuration, the customer receives a balancing payment. By that our customers are charged only for the true configurations required in their projects.

As written above, the software realizing the user allowed blocking, is implemented and delivered in the TOE – depending on the order - and is part of the evaluation and certificate. This software is an additional part of the

Flash Loader software, but also the other firmware has seen a small enhancement to enable for BPU.
If BPU is available, the blocking is done by the user at user premises, usually by taking an enhancement of the user own personalization flow and applying the according APDUs. These APDUs are predefined by Infineon Technologies and can also depend on the customer order. Only these APDUs can block the chip according to the user demands.

Infineon Technologies AG provides special software, running in parallel when doing the blocking. This software summarizes all devices and final configurations allowing for the later commercial balancing. The balancing depends on the number of chips and their individual final blockings the user has made over a defined time span. This special software can be used only for the commercial balancing, is not present on the TOE, not security relevant and therefore not part of this certificate.

All blockings are done by setting the according value in the chip configuration page, where certain parts are left available to the blocking software. Strong means of authentication are in place. The blocking software respectively BPU software is an additional part of the Flash Loader software and the only piece of software, able to manage the blocking APDUs. Therefore, the presence of the Flash Loader software is essential for the BPU ability.

The user can only apply a predefined and checksum protected set of allowed APDU configuration commands provided by Infineon Technologies AG. For this, the Flash Loader BPU software part, together with the firmware, executes one of those APDUs. After the final blocking is done and the user additionally may have downloaded his software, the entire Flash Loader including the BPU software part is permanently deactivated. This is called locking of the Flash Loader.

Of course, exclusively all security relevant settings are contained in the IFX-only part. The Flash Loader BPU software does not access and has no access to the IFX-only part.

Once the user blocking by applying the APDU has been finalized, the configuration page is no more accessible for changes. After the locking of the Flash Loader, the product is permanently fixed regarding its configurations and software. A reactivation of the Flash Loader is not possible. At the next start-up, the Boot Software (BOS) applies the made settings.

The entire configuration storage area is protected against manipulation, perturbation and false access. Note that the IFX-only part of the configuration page is already access protected prior delivery to the user and the TOE leaves the Infineon Technology premises only locked into User Mode.

The BPU software part is only present on the products which have been ordered with the BPU option. In all other cases this software is not present on the product. If a product is ordered without Flash Loader, also the Flash Loader software is disabled and the BPU configuration changes are blocked in the IFX-configuration, which renders BPU functionality unusable. Therefore, the BPU feature is only possible if the Flash Loader is active.

If the user decides to use the Flash Loader, regardless whether it is ordered with or without BPU, an additional process option can be ordered which results in an additional status of the Flash Loader. This process is called PIN-Letter and enables for simplified logistics and thereby for faster delivery of the ordered TOE products to the user. The PIN-Letter feature enabling for the PIN-Letter process is an implemented part of the Flash Loader. The resulting logistical acceleration is possible since the PIN-Letter enables for delivery of not user-specific configured, not flashed and not personalized TOE products to the user warehouse.

Extra authentication means applied in the PIN-Letter status of the Flash Loader preserve that only the intended user with the intended PIN-Letter can configure with user specific information and enable the normal Flash Loader functions in a second step. By that the user orders the products and receives - in a protected way - the belonging PIN-Letter. PIN-Letter and delivered chips must match.

By delivery the user warehouse gets filled and depending on market demands the user can immediate apply the authentication means of the PIN-Letter. If passing, the TOE products become user specific configured and the Flash Loader can be used for this specific user in a second step.

The following table outlines the different ways how the user can input his software on this TOE – a TOE without user available ROM. User software comprises usually the operating system and applications, which are for Infineon Technologies simply a user data package which is handled as a fixed data package during production. This provides high process flexibility for the user of which an overview is given in the following table:

Table 3 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™ NVM on his own. Infineon Technologies AG has not received user software and there are no user data of the Composite TOE in the ROM.	The Flash Loader can be activated by the user or subcontractor to download his software in the SOLID FLASH™ NVM – until the Flash Loader is finally deactivated by the user.
2		The user provides his complete software for the download into the SOLID FLASH™ NVM to Infineon Technologies AG. The software is downloaded to the SOLID FLASH™ NVM during chip production.	The Flash Loader is permanently disabled prior delivery.
3		The user provides software for the download into the SOLID FLASH™ NVM to Infineon Technologies AG. The software is downloaded to the SOLID FLASH™ NVM during chip production.	When leaving the Infineon Technologies AG production facility, the Flash Loader is blocked, but can be activated or reactivated by the user or subcontractor to complete the previously stored software parts in the SOLID FLASH™ NVM. Precondition is that the user has provided an own reactivation procedure in software prior chip production to Infineon Technologies AG.

For the cases with Flash Loader software on board and whenever the user has finalized his SW-download, respectively the TOE is in the final state and about to be delivered to the end-user, the user is obligated to lock the Flash Loader. The final locking of the Flash Loader results in a permanent deactivation of the Flash Loader. This means that once being in the locked status, the Flash Loader cannot be reactivated anymore.

Note that whenever a TOE comes without active Flash Loader, BPU and PIN-Letter process are not possible. All in all various delivery combinations are given and for example, a product can come with a fix configuration and with Flash Loader, to enable the user to download software, but without BPU option and with PIN-Letter. The following cases can occur:

Table 4 Options with Flash Loader, BPU and PIN-Letter

Case	Order	Option
1	Fix configuration, Flash Loader is locked	• Infineon Technologies configures and flashes all software as ordered. • The entire user software must be delivered to Infineon Technologies prior production.
2	Active Flash Loader, BPU feature blocked	• Infineon configures the chip as ordered and • the user flashes his software at his own premises. • If requested, Infineon Technologies can optionally download also shares of the user software during production. These user software shares must be delivered to Infineon Technologies prior production. The user can finalize his software package at his premises.
3	Active Flash Loader and active BPU feature	The user: • Activates the Flash Loader, • configures the chip applying the BPU feature and • flashes his software at his own premises. • If requested, Infineon Technologies can optionally download also shares of the user software during production. These user software shares must be delivered to Infineon Technologies prior production. The user can finalize his software package at his premises.
4	Active Flash Loader and PIN-Letter	Infineon configures the chip as ordered. The user receives his PIN-Letter and fills his warehouse. As required the user: • applies the PIN-Letter on the chips taken from his warehouse, gets the chips user specific configured, • activates the Flash Loader and • the user flashes his software at his own premises. If requested, Infineon Technologies can optionally download also shares of the user software during production. These user software shares must be delivered to Infineon Technologies prior production. The user can finalize his software package at his premises.
5	Active Flash Loader, active BPU and PIN-Letter	Infineon configures the chip as ordered. The user receives his PIN-Letter and fills his warehouse. As required the user: • applies the PIN-Letter on the chips taken from his warehouse, gets the chips user specific configured, • activates the Flash Loader, • applies his user specific chip configuration with the BPU feature and • flashes his software at his own premises. If requested, Infineon Technologies can optionally download also shares of the user software during production. These user software shares must be delivered to Infineon Technologies prior production. The user can finalize his software package at his premises.

The TOE can be configured within the physical limitations regarding the memory size ranges and other blocking options, focusing on the maximum respectively minimum user available limitations. Within those limitations the TOE configurations can vary under only one identical IC-hardware, regardless whether the configurations are set by Infineon or with further limitations by the user. All configurations throughout all different masksets the TOE is made off and therefore resulting derivattives have no impact on security and are covered by the certificate.

Today's predefined configurations options and respectively ranges of the TOE are listed in the Hardware Reference Manuals [7]. These predefined products come with the most requested configurations and allow to produce volumes on stock in order to simplify logistic processes.

According to the BPU option, a non-limited number of configurations of the TOE may occur in the field. The number of various configurations depends on the user and purchase contract only.

Note that the TOE answers to the Non-ISO-ATR with the Generic Chip Identification Mode (GCIM) answer. This GCIM outputs a coded clear identifier for the chip type, the design step and further configuration information. The documents Hardware Reference Manual [7] are part of the user guidance and enables for the clear interpretation of the read out GCIM data.

These GCIM data enable the user for clear identification of the TOE and also of one of the different mask sets and therewith for examination of the validity of the certificate.

In addition, dedicated special function registers (SFR) allow reading out the present configuration in detail. The output data together with the Hardware Reference Manuals [7] enables for clear identification of a product and its configuration. All these steps for gathering identification and detailed configuration information can be done by the user himself, without involving Infineon Technologies AG.

All other Smartcard Embedded Software does not belong to the TOE and is not subject of the evaluation.

2 Conformance Claims (ASE_CCL)

2.1 CC Conformance Claim

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

Conformance of this ST is claimed for:

Common Criteria part 2 **extended** [3] and Common Criteria part 3 **conformant** [4].

2.2 PP Claim

This Security Target claims **strict conformance** to the Security IC Platform Protection Profile with Augmentation Packages [1] (PP).

The Security IC Platform Protection Profile with Augmentation Packages is registered and certified by the Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference:

BSI-CC-PP-0084-2014, Version 1.0, dated 2014-01-13.

The security assurance requirements of the TOE are according to the Security IC Platform Protection Profile with Augmentation Packages [1].
They are all drawn from Part 3 of the Common Criteria version v3.1 [4].

The targeted EAL6+ level includes already the highest assurance families AVA_VAN.5 and ALC_DVS.2 from Common Criteria part 3 [4]. To achieve an additional augmentation, this Security Target is **assurance package augmented** compared to the Security IC Platform Protection Profile with Augmentation Packages [1].

The augmentation is achieved - with regard to CCv3.1 Part 3 [4]: Security assurance components by including:

Augmentations of the assurance level of the TOE

Assurance Class	Assurance Components	Description
Life-cycle support	**ALC_FLR.1**	Basic flaw remediation

2.3 Package Claim

This Security Target claims conformance to the following additional packages from the Security IC Platform Protection Profile with Augmentation Packages [1] depending on the TOE configuration:

- Package “Package 1: Loader dedicated for usage in secured environment only”, conformant, see [1] section 7.3.1,
- Furthermore, for TOE products coming with an active Flash Loader, the following packages are optional:
- Package “Package 2: Loader dedicated for usage by authorized users only” conformant, see [1] section 7.3.2,
- Package “Authentication of the Security IC” conformant, see [1] section 7.2

Note 1:
This package is optional and fulfilled only by TOE products coming with a Flash Loader. Furthermore, it should be noted that in contrast to the functional package introduced in the PP [1], the availability of the authentication mechanism is not given after locking the Flash Loader. The intended use case of the authentication is to prevent a customer from flashing user data on a non-genuine TOE. No authentication mechanism can be provided after the Flash Loader is locked.
After locking of the Flash Loader, the related threats and objectives for the operational environment and SFRs related to the TOE authentication are regarded as not applicable, due to the fact that it is out of scope of the intended use-case and the authentication functionality is no longer available.
End of note.

Depending on the availability of the optional Symmectric Cryptographic Coprocessor:

- Package “TDES” augmented; see [1] section 7.4.1
- Package “AES” augmented; see [1] section 7.4.2

These packages are optional and fulfilled by TOE products coming with an activated Symmetric Cryptographic Coprocessor.

The assurance level of this TOE is:

EAL6 augmented (EAL6+) with the component ALC_FLR.1 and additional packages

2.4 Conformance Rationale

This security target claims **strict conformance** only to the PP [1].

The Target of Evaluation (TOE) is a typical security IC as defined in PP section 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 behavior of the security functionality
- the IC Dedicated Software with the parts
- the IC Dedicated Test Software,
- the IC Dedicated Support Software
- the guidance documentation according section 0 and 8.

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

2.4.1 Security Problem Definition

Following the PP [1], the security problem definition is enhanced by adding two additional threats, an organization security policy and an augmented assumption. Including these add-ons, the security problem definition of this security target is consistent with the statement of the security problem definition in the PP [1], as the security target claimed strict conformance to the PP [1].

2.4.2 Conformance Rationale

The augmented assumption A.Key-Function, related to the usage of key-depending function, the threat memory access violation T.Mem-Access, due to specific TOE memory access control functionality, and the threat T.Open_Samples_Diffusion, due to the Flash Loader functionality have been added. These add-ons have no impact on the conformance statements regarding CC [2] and PP [1], with following rational:

- The security target remains conformant to CC [2], claim 482 as the possibility to introduce additional restrictions is given.
- The security target fulfills the strict conformance claim of the PP [1] due to the application notes 4, 5 and 6 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.

2.4.3 Adding Objectives

Due to additional security functionality coming from

- the memory access control
  - O.Mem-Access
- the objectives related to the Flash Loader
  - O.Authentication,
  - O.Cap_Avail_Loader,
  - O.Ctrl_Auth_Loader,
  - O.Prot_TSF_Confidentiality,

additional security objectives have been introduced.

These add-ons have no impact on the conformance statements regarding CC [3] and PP [1], with following rational:

- The security target remains conformant to CC [3], claim 482 as the possibility to introduce additional restrictions is given.
- The security target fulfills the strict conformance of the PP [1] due to the application note 8 applying here. This note allows the definition of high-level security goals due to further functions or services provided to the Security IC Embedded Software.

2.4.4 AES and TDES

The PP [1] implements the optional policy cryptographic services P.Crypto_Service with its packages “TDES” and “AES”. This TOE provides these optional packages requiring secure hardware based cryptographic services for the IC Embedded Software as outlined in section 0.

Due to these optional additional security functionalities the security objectives O.TDES and O.AES have been introduced. These add-ons have no impact on the conformance statements regarding CC [2] and PP [1], with following rational:

- The security target fulfills the strict conformance claim of the PP [1] due to the application notes 4, 5 and 6 which apply here. By these notes the addition of further security functions and security services are covered, even without deriving particular security functionality from a threat or a policy.

2.4.5 Loader

The PP [1] implements the optional policy for applying a Loader. The Loader is used to load data into the SOLID FLASH™ NVM.

The Loader, called Flash Loader in the following, provides the service for authentication and implements the Package for Authentication of the Security IC containing “FIA_API.1 Authentication Proof of Identity” of the TOE against a user.

This means that the user clearly can identify the TOE on his external request. This fulfills the objective “O.Authentication”, authentication to external entities, and obligates an objective to the environment “OE.TOE_Auth”, external entities authenticating of the TOE as outlined in the PP [1].

The Loader policy defines the Package 1 with its policy “P.LIM_Block_Loader” where the Loader is dedicated for usage in secured environment only and the Package 2 with its policy “P.Ctrl_Loader” where the Loader is dedicated for usage by authorized users only.

This TOE provides a Flash Loader complying with the optional packages:

- “Authentication of the Security IC”,
- “Package 1: Loader dedicated for usage in secured environment only”
- “Package 2: Loader dedicated for usage by authorized users only”

as outlined in sections 7.2 and 7.3 of the PP [1].

Due to these optional additional security functionalities the security objectives

- “O.Cap_Avail_Loader”, Capability and availability of the Loader,
- “O.Ctrl_Auth_Loader”, Access control and authenticity for the Loader,
- “OE.Loader_Usage", Secure communication and usage of the Loader,
- “O.Prot_TSF_Confidentiality”, Protection of the confidentiality of the TSF
- “OE.Lim_Block_Loader”, Limitation of capability and blocking the Loader
- and the threat
- “T.Masquerade_TOE”, Masquerade the TOE
- have been introduced.

These add-ons have no impact on the conformance statements regarding CC [2] and PP [1] as defined in section 2.4.2.

2.4.6 Summary

All of above add-ons have no impact on the conformance statements regarding CC [2] and PP [9], with following rational:

The security target fulfils the strict conformance claim of the PP [9] due to the application notes 9 applying here. By this note the addition of further security functions and security services are covered, even without deriving particular security functionality from a threat or a policy.

Due to the above rational, the security objectives of this security target are consistent with the statement of the security objectives in the PP [1], as the security target claims strict conformance to the PP [1].

All security functional requirements defined in the PP [1] are included and completely defined in this ST.

The following security functional requirements are taken from the Common Criteria Part 2 (CCP2) [3] document and respectively from the PP [1]:

Security Functional Requirements

Security Functional Requirement	Description	Source
FDP_ACC.1	Subset access control	CCP2 [3]
FDP_ACF.1	Security attribute based access contol	CCP2 [3]
FMT_MSA.1	Management of security attributes	CCP2 [3]
FMT_MSA.3	Static attribute initialization	CCP2 [3]
FMT_SMF.1	Specification of Management functions	CCP2 [3]
FCS_CKM.4/TDES (5)	Cryptographic key destruction – TDES	PP [1]
FCS_CKM.4/AES (5)	Cryptographic key destruction – AES	PP [1]
FCS_COP.1/TDES (5)	Cryptographic operation - TDES	PP [1]
FCS_COP.1/AES (5)	Cryptographic operation - AES	PP [1]
FCS_RNG.1/KSG	Generation of Random Numbers - KSG	PP [1]
FCS_RNG.1/TRNG	Generation of Random Numbers -TRNG	PP [1]
FCS_RNG.1/HPRG	Generation of Random Numbers - HPRG	PP [1]
FCS_RNG.1/DRNG	Generation of Random Numbers -DRNG	PP [1]
FDP_SDI.2	Stored data integrity monitoring and action	PP [1]
FDP_SDC.1	Stored data confidentiality	PP [1]
FMT_LIM.1	Limited capabilities	PP [1]
FMT_LIM.2	Limited availability	PP [1]

FMT_LIM.1/Loader (8)	Limited capabilities	PP [1]
FMT_LIM.2/Loader (8)	Limited availability - Loader	PP [1]
FRU_FLT.2	Limited fault tolerance	PP [1]
FPT_FLS.1	Failure with preservation of secure state	PP [1]
FPT_PHP.3	Resistance to physical attack	PP [1]
FDP_ITT.1	Basic internal transfer protection	PP [1]
FPT_ITT.1	Basic internal TSF data transfer protection	PP [1]
FDP_IFC.1	Subset information flow control	PP [1]
FIA_API.1 (7)	Authentication Proof of the Identity	PP [1]
FTP_ITC.1 (6)	Inter-TSF trusted channel	PP [1]
FDP_UCT.1 (6)	Basic data exchange confidentiality	PP [1]
FDP_UIT.1 (6)	Data exchange integrity	PP [1]
FDP_ACC.1/Loader (6)	Subset access control - Loader	PP [1]
FDP_ACF.1/Loader (6)	Security attribute based access control - Loader	PP [1]

(5) Taken from the according packages of the PP [1]: package “TDES” and package “AES”

(6) Taken from the according packages of the PP [1]: package “Package 2: Loader dedicated for usage by authorized users only”

(7) Taken from the according packages of the PP [1]: package “Authentication of Security IC”

(8) Taken from the according packages of the PP [1]: package “Package 1: Loader dedicated for usage in secured environment only”

The following security functional requirements are included and completely defined in this ST, section 5.

FPT_TST.2	Subset TOE security testing

All assignments and selections of the security functional requirements are done in the PP [1] and in this Security Target.

The Assurance Requirements of the TOE obtain the Evaluation Assurance Level 6 augmented with the assurance component **ALC_FLR.1** for the TOE.

2.5 Application Notes

The functional requirements

- FCS_RNG.1/TRNG,
- FCS_RNG.1/HPRG,
- FCS_RNG.1/DRNG,
- FCS_RNG.1/KSG

are iterations of the FCS_RNG.1 as defined in the Protection Profile [1] according to “Anwendungshinweise und Interpretationen zum Schema (AIS)” respectively “Functionality classes and evaluation methodology for physical random number generators”, AIS31 [6].

3 Security Problem Definition (ASE_SPD)

The content of the PP [1] applies to this section 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.

The threats to security are defined and described in PP [1] section 3.2 and 7.2.

Threats according PP [1]

Threat	**Name**
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

Threat Memory Access Violation

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 Smartcard Embedded Software is responsible for its User data of the Composite TOE according to the assumption “Treatment of User data of the Composite TOE (A.Resp-Appl)”. However, the Smartcard Embedded Software may comprise different parts, for instance an operating system and one or more applications. In this case, such parts may accidentally or deliberately access data (including code) of other parts, which may result in a security violation.

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.

Threat Diffusion of Open Samples

The additional functionality of a Loader as defind in the PP [1], section 7.3 requires to address the following threat, as defined in the document “PP0084: Interpretation” [PP84].

The TOE shall avert the threat “Diffusion of open samples (T.Open_Samples_Diffusion)” as specified below:

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 crytography, …). The execution of dedicated security features (for example: excecution 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.

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 primary assets concern the User data which includes the user data of the Composite TOE as well as program code (Security IC Embedded Software) stored and in operation and the provided security services. These assets have to be protected while being executed and or processed and on the other hand, when the TOE is not in operation.

This leads to four primary assets with its related security concerns:

- SC1 integrity of user data of the Composite TOE
- SC2 confidentiality of user data of the Composite TOE being stored in the TOE’s protected memory areas
- SC3 correct operation of the security services provided by the TOE for the Security IC Embedded Software
- SC4 continuous availability of random numbers

SC4 is an additional security service provided by this TOE which is the availability of random numbers.

These random numbers are generated either by a true random number or a deterministic random number generator or by both, when a true random number is used as seed for the deterministic random number generator. Note that the generation of random numbers is a requirement of the PP [1].

To be able to protect the listed assets the TOE shall protect its security functionality as well. Therefore critical information about the TOE shall be protected. Critical information includes:

- logical design data, physical design data, IC Dedicated Software, and configuration data,
- Initialization Data and Pre-personalization Data, specific development aids, test and characterization related data, material for software development support, and reticles.

The information and material produced and/or processed by the TOE Manufacturer in the TOE development and production environment (Phases 2 up to TOE Delivery) can be grouped as follows:

- logical design data,
- physical design data,
- IC Dedicated Software, Security IC Embedded Software, Initialization Data and Pre-personalization Data,
- specific development aids,
- test and characterization related data,
- material for software development support, and
- reticles and products in any form

as long as they are generated, stored, or processed by the TOE Manufacturer.

For details see PP [1] section 3.1.

3.2 Organizational Security Policies

The TOE has to be protected during the first phases of their lifecycle (phases 2 up to TOE delivery which can be after phase 3 or phase 4). Later on each variant of the TOE has to protect itself. The organizational security policy covers this aspect.

P.Process-TOE	Identification during TOE Development and Production An accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries this unique identification.

The organizational security policies are defined and described in PP [1] section 3.3.

Due to the augmentations of PP [1] and the chosen packages additional policies are introduced and described in the next section.

Organizational Security Policies according PP [1]

P.Process-TOE	Identification during TOE Development and Production

Augmented Organizational Security Policy

Due to the augmentations of the PP [1] and the chosen packages additional policies are introduced.

The TOE provides specific security functionality, which can be used by the Smartcard Embedded Software. In the following specific security functionality is listed which is not derived from threats identified for the TOE's environment because it can only be decided in the context of the smartcard application, against which threats the Smartcard Embedded Software will use the specific security functionality.

The IC Developer / Manufacturer must apply the organizational security policy "Cryptographic services of the TOE (P.Crypto-Service)" as specified below:

P.Crypto-Service	Cryptographic services of the TOE The TOE provides secure hardware based cryptographic services for the IC Embedded Software: • Triple Data Encryption Standard (TDES) • Advanced Encryption Standard (AES)

Note 2:
This TOE can come with both cryptographic coprocessors accessible, or with a blocked SCP, or with a blocked Crypto2304T, or with both cryptographic coprocessors blocked. The blocking depends on the customer demands prior to the production of the hardware. In case the SCP is blocked, no AES and DES computation supported by hardware. In case the Crypto2304T is blocked, no RSA and EC computation supported by hardware is possible. No accessibility of the deselected cryptographic coprocessor is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic coprocessors.
End of note.

The IC Developer / Manufacturer must apply the organizational security policies "Limiting and Blocking Loader Functionality" and "Controlled usage to Loader Functionality (P.Ctrl_Loader)" as specified below:

P.Lim_Block_Loader	Limiting and Blocking the Loader Functionality The composite manufacturer uses the Loader for loading of Security IC Embedded Software, user data of the Composite Product or IC Dedicated Support Software in charge of the IC Manufacturer. He limits the capability and blocks the availability of the Loader in order to protect stored data from disclosure and manipulation.

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

3.3 Assumptions

The TOE assumptions on the operational environment are defined and described in PP [1] section 3.4.

The assumptions concern the phases where the TOE has left the chip manufacturer.

The support of cipher schemas requires an additional assumption.

A.Process-Sec-IC	Protection during Packaging, Finishing and Personalization It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).
A.Resp-Appl	Treatment of User data of the Composite TOE All User data of the Composite TOE are owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant user data of the Composite TOE (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context.

3.3.1 Augmented Assumptions

The developer of the Smartcard Embedded Software must ensure the appropriate “Usage of Key-dependent Functions (A.Key-Function)” while developing this software in Phase 1 as specified below.

A.Key-Function	Usage of Key-dependent Functions Key-dependent functions (if any) shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to leakage attacks (as described under T.Leak-Inherent and T.Leak-Forced).

Note that here the routines which may compromise keys when being executed are part of the Smartcard Embedded Software. In contrast to this the threats T.Leak-Inherent and T.Leak-Forced address (i) the cryptographic routines which are part of the TOE. For details please refer to PP [1] section 3.4.

4 Security objectives (ASE_OBJ)

This section shows the subjects and objects where are relevant to the TOE.
A short overview is given in the following.

The user has the following standard high-level security goals related to the assets:

- SG1 maintain the integrity of user data (when being executed/processed and when being stored in the TOE´s memories)
- SG2 maintain the confidentiality of user data (when being executed/processed and when being stored in the TOE´s memories)
- SG3 maintain the correct operation of the security services provided by the TOE for the Security IC Embedded Software
- SG4 provision of random numbers.

4.1 Security objectives for the TOE

The security objectives of the TOE are defined and described in PP [1] section 4.1, 7.2.1, 7.3.1, 7.3.2, 7.4.1 and 7.4.2 and in this section.

Objectivs for the TOE according to PP [1]

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 - valid only for the TOE derivatives delivered with activated Flash Loader.
O.Authentication	Authentication to external entities - valid only for the TOE derivatives delivered with activated Flash Loader
O.Ctrl_Auth_Loader	Access control and authenticity for the Loader - valid only for the TOE derivatives delivered with activated Flash Loader
O.TDES	Cryptographic service Triple-DES
O.AES	Cryptographic service AES

Note 3:
The O.Cap_Avail_Loader applies to every TOE product, the objectives O. Authentication, O.Ctrl_Auth_Loader and O.Prot_TSF_Confidentiality applies only at TOE products coming with activated Flash Loader enabled for user data download by the user. In other cases the Flash Loader is not available anymore and the user data download is completed. Depending on the capabilities of the user software these objectives may then reoccur as subject of the composite TOE.
End of note.

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 additional functionality of a Loader as defind in the PP [1], section 7.3 requires to address the following objective, as defined in the document “PP0084: Interpretation” [PP84].

The TOE shall provide “Protection of the confidentiality of the TSF (O.Prot_TSF_Confidentiality)” as specified below:

O.Prot_TSF_Confidentiality	Protection of the confidentiality of the TSF The TOE must provide protection against disclosure of confidential operations of the Security IC (loader, memory management unit, …) through the use of a dedicated code loaded on open samples.

Additional objectives due to TOE specific functions and augmentation

O.Mem-Access	Area based Memory Access Control
O.Prot_TSF_Confidentiality	Protection of the confidentiality of the TSF

4.2 Security Objectives from PP for development and environment

The security objectives for the security IC embedded software development environment and the operational environment are defined in PP [1] section 4.2, 4.3, 7.2.1 and 7.3.

The operational environment of the TOE shall provide “Limitation of capability and blocking the Loader (OE.Lim_Block_Loader)”, “External entities authenticating of the TOE (OE.TOE_Auth)” and “Secure communication and usage of the Loader (OE.Loader_Usage)” as specified below:

OE.Lim_Block_Loader	Limitation of capability and blocking the Loader The Composite Product Manufacturer will protect the Loader functionality against misuse, limit the capability of the Loader and terminate irreversibly the Loader after intended usage of the Loader.

OE.TOE_Auth	External entities authenticating of the TOE The operational environment shall support the authentication verification mechanism and know authentication reference data of the TOE.

OE.Loader_Usage	Secure communication and usage of the Loader The authorized user must support the trusted communication with the TOE by confidentiality protection and authenticity proof of the data to be loaded and fulfilling the access conditions required by the Loader.

Note 4:
The objectives OE.Lim_Block_Loader, OE.TOE_Auth and OE.Loader_Usage for the development and operation environment apply only at TOE products coming with activated Flash Loader enabled for user data download by the user. In other cases the Flash Loader is not available anymore and the user data download is completed. Depending on the capabilities of the user software this objective may then reoccur as subject of the composite TOE.
End of note.

4.3 Security Objectives for the environment

OE.Resp-Appl	Treatment of User data of the Composite TOE Please refer to chapter 0 for clarification

The table below lists the security objectives.

Security Objectives for the Environment according the PP [1]

Phase 1	OE.Resp-Appl	Treatment of User data of the Composite TOE
Phase 5 – 6 optional Phase 4	OE.Process-Sec-IC	Protection during composite product manufacturing
Phase 5 – 6 optional Phase 4	OE.Lim_Block_Loader (1)	Limitation of capability and blocking the loader.
	OE.TOE_Auth (1)	Authentication to external entities
	OE.Loader_Usage (1)	Secure communication and usage of the Loader

(1) These objectives are only valid if the TOE is delivered with active Flash Loader.

4.3.1 Clarification of "Treatment of User Data (OE.Resp-Appl)"

Regarding the cryptographic services this objective of the environment has to be clarified.
By definition cipher or plain text data and cryptographic keys are user data of the Composite TOE. The Smartcard Embedded Software shall treat these data appropriately, use only proper secret keys (chosen from a large key space) as input for the cryptographic function of the TOE and use keys and functions appropriately in order to ensure the strength of cryptographic operation.
This means that keys are treated as confidential as soon as they are generated. The keys must be unique with a very high probability, as well as cryptographically strong. For example, it must be ensured that it is beyond practicality to derive the private key from a public key if asymmetric algorithms are used. If keys are imported into the TOE and/or derived from other keys, quality and confidentiality must be maintained. This implies that appropriate key management has to be realized in the environment.
Regarding the memory, software and firmware protection and the SFR and peripheral access rights handling these objectives of the environment has to be clarified. The treatment of user data of the Composite TOE is also required when a multi-application operating system is implemented as part of the Smartcard Embedded Software on the TOE. In this case the multi-application operating system should not disclose security relevant user data of one application to another application when it is processed or stored on the TOE.

4.3.2 Clarification of "Protection during Composite product manufacturing (OE.Process-Sec-IC)"

The protection during packaging, finishing and personalization includes also the personalization process (Flash Loader) and the personalization data (TOE software components) during Phase 4, Phase 5 and Phase 6.

4.4 Security Objectives Rationale

The security objectives rationale of the TOE are defined and described in PP [1] sections 4.4. The rationale regarding the objectives of the PP packages is defined and described in PP [1], section 7.2, 7.3.1, 7.3.2, 7.4.1 and 7.4.2. In the following description a rationale is provided for the organizational security policies, threats and assumptions, which are introduced in this Security Target.

Security Objective Rationale

Assumption, Threat or Organizational Security Policy	Security Objective
A.Key-Function	OE.Resp-Appl
T.Mem-Access	O.Mem-Access
T.Open_Samples_Diffusion	O.Prot_TSF_Confidentiality O.Leak-Inherent O.Leak-Forced

A.Key-Function

Compared to the PP [1] a further clarification has been made for the security objective “Treatment of user data of the Composite TOE (OE.Resp-Appl)”: By definition cipher or plain text data and cryptographic keys are user data of the Composite TOE. So, the Smartcard Embedded Software will protect such data if required and use keys and functions appropriately in order to ensure the strength of cryptographic operation. Quality and confidentiality must be maintained for keys that are imported and/or derived from other keys. This implies that appropriate key management has to be realized in the environment. That is expressed by the assumption A.Key-Function which is covered from OE.Resp–Appl. These measures make sure that the assumption A.Resp-Appl is still covered by the security objective OE.Resp-Appl.

T.Mem-Access

Compared to the PP [1] 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.

T.Open_Samples_Diffusion

The justification related to the threat “Diffusion of open Samples” (T.Open_Samples_diffusion) is as follows: Since T.Open_Samples_diffusion that the TOE resist usage of open samples, is covered exactly by the objective “Protection of the confidentiality of the TSF” (O.Prot_TSF_Confidentiality), which provides protection against disclosure of confidential operations through the use of the dedicated code loaded on open samples, and the objectice “Protection against Inherent Information Leakage” (O.Leak-Inherent), which protects confidential data against disclosure by the TOE, and the objective “Protection against Forced Information Leakage” (O.Leak-Forced), which protects the confidential data against leackge forced by malfunctions and physical manipulation by the TOE.

5 Extended Component Definition (ASE_ECD)

There are following 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 component FPT_TST.2 at the class FPT Protection of the TSF
- the family FIA_API at the class FIA Identification and Authentication

The extended components FCS_RNG, FMT_LIM, FAU_SAS and FDP_SDC are defined and described in PP [1] section 5, the extended component FIA_API is defined and described in PP [1] section 7.2. The extended component FPT_TST.2 is defined in the following.

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 [3] 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.

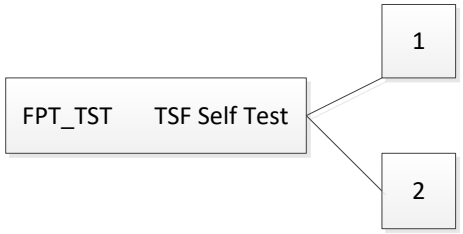
5.2 Definition of FPT_TST.2

The functional component “Subset TOE security testing (FPT_TST.2)” has been newly created (Common Criteria Part 2 extended [3]). 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 [3]. 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 [3]).

5.2.1 TSF self-test (FPT_TST)

Family Behavior	The Family Behavior is defined in [3] section 15.14 (442, 443).
Component levelling	
FPT_TST.1:	The component FPT_TST.1 is defined in [3] 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 provide a suite of self-test features [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 the PP [1] 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 the PP [1] section 6.1, 7.2, 7.3, 7.4.1, 7.4.2 and in the following description.

Following table provides an overview of the functional security requirements of the TOE, marks the source it is taken from and wether it is defined (completely done in source), refined (refinement done in source) or augmented (augmentation done in ST).

The refinements are also valid for this ST.

In the following table the abbreviation PP stands for Protection Profile and CCx for the related Common Criteria part which is indicated by the "x".

Security functional requirements defined / refined / augmented by source

Security Functional Requirement	**Description**	**Source**	**Defined in Source refined in ST / completed in ST / augmented in ST/ extended in ST**
FDP_ACC.1	"Subset access control"	CCP2 [3]	augmented
FDP_ACF.1	Security attribute based access control	CCP2 [3]	augmented
FRU_FLT.2	"Limited fault tolerance"	PP [1]	defined
FPT_FLS.1	"Failure with preservation of secure state"	PP [1]	defined
FMT_LIM.1	"Limited capabilities"	PP [1]	defined
FMT_LIM.2	"Limited availability"	PP [1]	defined
FAU_SAS.1	"Audit storage"	PP [1]	completed
FDP_SDC.1	"Stored data confidentiality"	PP [1]	completed
FDP_SDI.2	"Stored data integrity monitoring and action"	PP [1]	completed
FPT_PHP.3	"Resistance to physical attack"	PP [1]	defined
FDP_ITT.1	"Basic internal transfer protection"	PP [1]	defined
FPT_ITT.1	"Basic internal TSF data transfer protection	PP [1]	defined
FDP_IFC.1	"Subset information flow control"	PP [1]	defined
FCS_RNG.1/TRNG	"Generation of Random Numbers – TRNG"	PP [1]	completed
FCS_RNG.1/HPRG	"Generation of Random Numbers – HPRG"	PP [1]	completed
FCS_RNG.1/DRNG	"Generation of Random Numbers – DRNG"	PP [1]	completed
FCS_RNG.1/KSG	"Generation of Random Numbers – KSG"	PP [1]	completed
FMT_LIM.1/Loader	"Limited Capabilities"	PP [1]	completed
FMT_LIM.2/Loader	"Limited Availability – Loader"	PP [1]	completed

Security Functional Requirement	**Description**	**Source**	**Defined in Source refined in ST / completed in ST / augmented in ST/ extended in ST**
FIA_API.1	“Authentication Proof of Identity”	PP [1]	completed
FTP_ITC.1	“Inter-TSF trusted channel”	PP [1]	completed
FDP_UCT.1	“Basic data exchange confidentiality”	PP [1]	defined
FDP_UIT.1	“Data exchange integrity”	PP [1]	defined
FDP_ACC.1/Loader	“Subset access control – Loader”	PP [1]	completed
FDP_ACF.1/Loader	“Security attribute based access control – Loader”	PP [1]	completed
FCS_COP.1/TDES	“Cryptographic operation – TDES”	PP [1]	refined/completed
FCS_COP.1/AES	“Cryptographic operation – AES”	PP [1]	refined/completed
FCS_CKM.4/TDES	“Cryptographic key destruction – TDES”	PP [1]	completed
FCS_CKM.4/AES	“Cryptographic key destruction – AES”	PP [1]	completed
FMT_MSA.1	“Management of security attributes”	CCP2 [3]	augmented
FMT_MSA.3	“Static attribute initialization”	CCP2 [3]	augmented
FMT_SMF.1	“Specification of Management functions “	CCP2 [3]	augmented
FPT_TST.2	“TOE security testing”	CCP2 [3]	extended

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

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 applying only at TOE products coming with activated Flash Loader enabled for user data download. In other cases the Flash Loader is not available anymore and the user data download is completed. Depending on the capabilities of the user software these security functional requirements may then reoccur as subject of the composite TOE.

End of note.

6.1.1 Extended Components FCS_RNG.1 and FAU_SAS.1

6.1.1.1 FCS_RNG Generation of random numbers

To define the IT security functional requirements of the TOE an additional family (FCS_RNG) of the Class FCS (cryptographic support) is defined in the PP [1]. This family describes the functional requirements for random number generation used for cryptographic purposes.

Please note that the national regulation are outlined in PP [1] section 7.5.1 and in AIS31 and AIS20 [6]. These regulations apply for this TOE.

Note 5:
The functional requirements FCS_RNG.1/TRNG, FCS_RNG.1/HPRG, FCS_RNG.1/DRNG, FCS_RNG.1/KSG are iterations of the FCS_RNG.1 defined in the Protection Profile [1] according to “Anwendungshinweise und Interpretationen zum Schema (AIS)” respectively “A proposal for: Functionality classes for random number generators” [6].
End of note.

Note 6:
The Hybrid Physical Random Number Generator (hybrd PTRNG) implements total failure testing of the random source data and a continuous random number generator test according to:
National Institute of Standards and Technology, Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication (FIPS) 140-2, 2002-03-12 section 4.9.2.
End of note.

Together with the guidelines in [23] the hybrid PTRNG of this TOE provides random numbers conformant to several quality metrics as defined in [6]. Depending on the user configuration the TOE provide the according random number quality. For each addressed quality metric of [6] the definitions are made in the following:

6.1.1.2 True Random Number Generation, meeting [6] 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 [6]
FCS_RNG.1.1/TRNG	The TSF shall provide a physical random number generator that implements:
PTG.2.1	A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.
PTG.2.2	If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.
PTG.2.3	The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.
PTG.2.4	The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.
PTG.2.5	The online test procedure checks the quality of the raw random number sequence. It is triggered continuously. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.
FCS_RNG.1.2/TRNG	The TSF shall provide numbers in the format 8- or 16-bit that meet
PTG.2.6	Test procedure A, as defined in [6] 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.

6.1.1.3 Hybrid Random Number Generation, meeting [6] 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 [6]
FCS_RNG.1.1/HPRG	The TSF shall provide a hybrid physical 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.
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-rocessing algorithm shall not exceed its input data rate.
FCS_RNG.1.2/HPRG	The TSF shall provide numbers in the format 8- or 16-bit 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.
PTG.3.8	The internal random numbers shall use PTRNG of class PTG.2 as random source for the post-processing.

Note to PTG.3.5:
Continuously means that the raw random bits are scanned continuously.
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.
End of note.

Note to PTG.3.8:
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 conditions.
End of note.

6.1.1.4 Deterministic Random Number Generation, meeting [6] 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 [6]
FCS_RNG.1.1/DRNG	The TSF shall provide a deterministic random number generator that implements:
DRG.3.1	If initialized with a random seed using a PTRNG of class PTG.2 as random source the internal state of the RNG shall have at least 100 bit of entropy.
DRG.3.2	The RNG provides forward secrecy.
DRG.3.3	The RNG provides backward secrecy even if the current internal state is known.
FCS_RNG.1.2/DRNG	The TSF shall provide random numbers 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 2^{34} bits strings of bit length 128 are mutually different with a probability that is greater than $1 - 2^{(-16)}$.

DRG.3.5	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 Technologiy (NIST) test suite for RNGs used for cryptographic purposes [S17] 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-overlpping (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.

Note to DRG.3.1:
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.

6.1.1.5 Deterministic Random Number Generation meeting [6] DRG.2

This additional operation mode is named Key Stream Generation (KSG), which is a stream cipher generation. It is conformant to DRG.2 and implements therefore forward and additional backward secrecy.

FCS_RNG.1/KSG	**Random Number Generation**
Hierarchical to:	No other components
Dependencies:	No dependencies
FCS_RNG.1/KSG	Random numbers generation **Class DRG.2** according to [6]
FCS_RNG.1.1/KSG	The TSF shall provide a deterministic random number generator that implements:
DRG.2.1	If initialized with a random seed using a PTRNG of class PTG.2 as random source, the applied seed shall have at least 100 bits of entropy, the internal state of the RNG shall have at least the size of 200 bit - in this case the size of the internal state amounts to 351 bit, has the work factor for breaking the algorithm of 2^{127} due to the restriction on the maximum amount of keystream computed from a given seed, require guess work amounts to 2^{127} as well.
DRG.2.2	The RNG provides forward secrecy.
DRG.2.3	The RNG provides backward secrecy.
FCS_RNG.1.2/KSG	The TSF shall provide random numbers that meet:

DRG.2.4	The RNG, initialized with a random seed of length at least 100 bit delivered by an PTRNG of the class PTG.2, generates output for which any consecutive 2^{34} strings of the length 128 bits are mutually different with probability greater than $1-2^{(-16)}$.
DRG.2.5	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.

Note to DRG.2.2:
A linear complexity of the keystream of Achterbahn-128 that is lower bounded by 2^{98} (see Theorem 1 on page 27 in B. Gammel, R. Göttfert, O. Kniffler: Achterbahn-128/80, eSTREAM submission, June 2006). As a consequence an attacker needs to know at least 2 x 2^{98} = 2^{99} consecutive random bits in order to determine future random bits.
A correlation attack requires $2^{48.54}$ key stream bits along with a time complexity greater than 2119. (See R. Göttfert and B. Gammel: On the frame length of Achterbahn-128/80, Proceedings of the 2007 IEEE Information Theory Workshop on Information Theory for Wireless Networks, pp. 1-5, IEEE, 2007.) To prevent such an attack, the generator produces at most 2^{40} random bytes (=2^{43} random bits) for a given seed. Thus the required $2^{48.54}$ random bits are not available. Therefore, the property of forward secrecy is fulfilled.
End of note.

Note to DRG.2.3:
For a correlation attack knowledge of at least 2^{48} consecutive present or future random bits is required. Then, with a working factor of 2^{119} operations, the internal state can be computed. However, such an attack is not possible since the data complexity of the attack is $2^{48.54}$ and most of 2^{43} random bits are generated by the generator for each seed. Thus, the generator provides backward secrecy.
End of note.

Note to DRG.2.5:
The random numbers have been shown to fulfill all statistical tests of [6], Test Procedure A. The random numbers are in the format 8- or 16-bit.
End of note.

6.1.1.6 FAU_SAS

During testing at the end of Phase 3 before TOE Delivery, the TOE shall be able to store some data (for instance about the production history or identification data of the individual die or other data to be used after delivery). Therefore, the security functional component Audit storage (FAU_SAS.1) has been added and is described in the PP [1].

The TOE shall meet the requirement “Audit storage (FAU_SAS.1)” as specified below:

FAU_SAS.1	Audit Storage
Hierarchical to:	No dependencies
Dependencies:	No dependencies.

FAU_SAS.1.1	The TSF shall provide the test process before TOE Delivery with the capability to store the Identification Data (GCIM) of the Security IC Embedded Software in the access protected and not changeable configuration page area of the SOLID FLASH™ NVM.

6.1.2 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 [3]).

FPT_TST.2	**Subset TOE testing**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.2.1	The TSF shall provide a suite of self-test features at the request of the authorized user to demonstrate the correct operation of the alarm lines and/or following environmental sensor mechanisms: • Temperature sensor alarm • Internal Frequency Sensor alarm • Backside light detection alarm • Voltage sensor alarm • Watch Dog Timer related alarm • Software triggered alarm

6.1.3 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 section 4 in the “32-bit Security Controller Hardware Reference Manual” [7].

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

Smartcard Embedded Software defines the attributes and memory areas. The corresponding permission control information is evaluated “on-the-fly” by the hardware so that access is granted/effective or denied/inoperable.

The security functional requirement **“Static attribute initialization (FMT_MSA.3)”** ensures that the default values of security attributes are appropriately either permissive or restrictive in nature. Alternative values can be specified by any subject provided that the **Memory Access Control Policy** allows that. This is described by the security functional requirement **“Management of security attributes (FMT_MSA.1)”.** The attributes are determined during TOE manufacturing (FMT_MSA.3) or set at run-time (FMT_MSA.1).

From TOE’s point of view the different roles in the Smartcard Embedded Software can be distinguished according to the memory based access control. However the definition of the roles belongs to the user software.

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

Memory Access Control Policy

The TOE shall control operations to objects of software running at the subjects as defined below. Any access is controlled, regardless whether the access is on code or data or a jump on any other level outside the current one.

- Subjects:
  a) software running at privilege mode
  b) software running at user mode
- Objects: data including code stored in memories
- Operations: read, write and execute access

The memory model provides two distinct, independent levels separated from each other. These levels are referred to as the privileged mode and the user mode. Up to eight regions can be defined with different access rights, and additionally a privileged default background region exists. The access rights are controlled by the Memory Access Control Policy related to the following rules:

- the privilege mode has access to regions which are defined for user mode access
- the user mode has no access to the regions which are defined for privilege mode access
- overlapping regions, have access to other regions with ascending region priority:
  region 7 = highest priority, region 0 = lowest priority
- enable or disable instruction fetches

access permissions:

Privileged Mode Permissions	User Mode Permissions	Description
No access	No access	All accesses generate a permission fault
Read/write	No access	Privileged mode access only
Read/write	Read only	Writes in user mode generate a permission fault
Read/write	Read/write	Full access

Read only	No access	Privileged mode read only
Read only	Read only	Privileged and user mode read only

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

FDP_ACC.1	Subset access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1	The TSF shall enforce the Memory Access Control Policy on all subjects, all objects and all the operations defined in the Memory Access Control Policy.

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

FDP_ACF.1	Security attribute based access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1	The TSF shall enforce the Memory Access Control Policy to objects based on the following: Subject: - software running at privilege mode - software running at user mode Object: - data including code stored in memories Attributes: - the memory area where the access is performed to and the corresponding permission control information and/or - the operation to be performed.
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: evaluate the corresponding permission control information of the relevant memory range before and during the access so that accesses to be denied cannot be utilized by the subject attempting to perform the operation.

FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none.

The TOE shall meet the requirement “Static attribute initialisation (FMT_MSA.3)” as specified below.

FMT_MSA.3	Static attribute initialisation
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the Memory Access Control Policy to provide well defined(11) default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the subject - software running at privilege mode (12), to specify alternative initial values to override the default values when an object or information is created.

(11) The static definition of the access rules is documented in [7]

(12) The Smartcard Embedded Software is intended to set the memory access control policy

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

FMT_MSA.1	Management of security attributes
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MSA.1.1	The TSF shall enforce the Memory Access Control Policy to restrict the ability to change default, modify or delete the security attributes permission control information to the subject - software running at privilege mode (12).

The TOE shall meet the requirement “Specification of management functions (FMT_SMF.1)” as specified below:

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 management functions*:* the subject - software running at privilege mode (12) shall be able to access the configuration registers of the MPU.

6.1.4 Support of Cipher Schemes

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

FCS_COP.1 Cryptographic operation requires a cryptographic operation to be performed in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard; dependencies are discussed in section 6.3.1.4.

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

- Advanced Encryption Standard (AES)
- Triple Data Encryption Standard (TDES)

Note 7:
This TOE can come with both crypto coprocessors accessible, or with a blocked SCP, or with a blocked Crypto2304T, or with both cryptographic coprocessors blocked. The blocking depends on the customer demands prior to the production of the hardware. In case the SCP is blocked, no AES and DES computation supported by hardware is possible. In case the Crypto2304T is blocked, no RSA and EC computation supported by hardware is possible. No accessibility of the deselected cryptographic coprocessor is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic coprocessors.
End of note.

6.1.4.1 Preface regarding Security Level related to Cryptography

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

6.1.4.2 Triple-DES Operation

The TDES Operation the TOE shall meet the requirement “Cryptographic operation (FCS_COP.1)” and “Cryptographic key destruction” (FCS_CKM.4) as specified below:

FCS_COP.1/TDES	Cryptographic operation
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key management] FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1.1/TDES	The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm Triple Data Encryption Standard (TDES) in • the Electronic Codebook Mode (ECB) • the Cipher Block Chaining Mode (CBC) • the Cipher Block Chaining Message Authentication Code (CBC-MAC) • the Cipher Block Chaining Message Authentication Code Encrypt Last Block (CBC-MAC-ELB) and cryptographic key sizes of 112 bit or 168 bit that meet the following: • National Institute of Standards and Technology (NIST) SP 800-67 Rev. 2 [S4] • the ECB, CBC: National Institute of Standards and Technology (NIST) SP 800-38A [S5] • the CBC-MAC, CBC-MAC-ELB: ISO/IEC 9797-1 Mac Algorithm 1 and 2 respectively [S14]

Note 8:
The FCS_COP.1/TDES refers to the direct hardware DES interface of the Symmetric Crypto coprocessor (SCP).
End of note.

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

Note 9:
The key destruction can be done by overwriting the key register interfaces or by software reset of the SCP which provides immediate zeroing of all SCP key registers.
End of note.

Note 10:
The TOE can be delivered with the SCP accessible or blocked. In case the SCP is blocked, no DES computation supported by hardware is possible and the FCS_COP.1/TDES and FCS_CKM.4/TDES are not applicable.

End of note.

6.1.4.3 AES Operation

The AES Operation the TOE shall meet the requirement “Cryptographic operation (FCS_COP.1)” and “Cryptographic key destruction” (FCS_CKM.4) as specified below:

FCS_COP.1/AES	Cryptographic operation
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/AES	The TSF shall perform decryption and encryption in accordance with a specified cryptographic algorithm Advanced Encryption Standard (AES) in • the Electronic Codebook Mode (ECB) • the Cipher Block Chaining Mode (CBC) • the Cipher Block Chaining Message Authentication Code (CBC-MAC) • the Cipher Block Chaining Message Authentication Code Encrypt Last Block (CBC-MAC-ELB) and cryptographic key sizes of 128 bit or 192 bit or 256 bit that meet the following: • FIPS 197 [S8] • the ECB, CBC: National Institute of Standards and Technology (NIST) SP 800-38A [S5] • the CBC-MAC, CBC-MAC-ELB: ISO/IEC 9797-1 Mac Algorithm 1 and 2 respectively [S14]

Note 11:
The FCS_COP.1/AES refers to the direct hardware AES interface of the Symmetric Crypto coprocessor (SCP).
End of note.

FCS_CKM.4/AES	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_CKM4.1/AES	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting or zeroing that meets the following: none

Note 12:
The key destruction can be done by overwriting the key register interfaces or by software reset of the SCP which provides immediate zeroing of all SCP key registers.
End of note.

Note 13:
The TOE can be delivered with the SCP accessible or blocked. In case the SCP is blocked, no AES computation supported by hardware is possible and the FCS_COP.1/AES and FCS_CKM.4/AES are not applicable.
End of note.

6.1.5 Data Integrity

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

FDP_SDI.2	Stored data integrity monitoring and action
Hierarchical to:	FDP_SDI.1 stored data integrity monitoring
Dependencies:	No dependencies
FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for data integrity and one-bit-errors on all objects, based on the following attributes: error detection value for RAM and SOLID FLASH™ NVM and parity protection of the Cache.
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall correct one-bit-errors in the SOLID FLASH™ NVM automatically and inform the user about errors in the RAM.

The TOE shall meet the requirement “Stored data confidentiality (FDP_SDC.1)” as specified below:

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, Cache and SOLID FLASH™ NVM except the memory area of the SOLID FLASH™ NVM from address 10007000H to 100077FFH.

6.1.6 Support by the Flash Loader

The TOE provides the Flash Loader to download user data into the SOLID FLASH™ NVM, either during production of the TOE or at customer site. The Flash Loader is dedicated for usage by authorized users only in secured and insecured environment during the production up to “Phase 6 Security IC Personalisation”. The Flash Loader has to be permanently deactivated before entering “Phase 7 Security IC end-usage”. For this reason the TOE shall meet the requirements, as defind and decribed in the PP [1] section “7.3 Packages for Loader” and “7.2 Package “Authentication of the Security IC”:

- Limited capabilities (FMT_LIM.1/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),
- Data exchange integrity (FDP_UIT.1),
- Subset access control – Loader (FDP_ACC.1/Loader),
- Security attribute based access control – Loader (FDP_ACF.1/Loader)
- as defined in the PP [1], section 7.2 and 7.3.

The Flash Loader supports the following security function policy (SFP):

- Loader SFP:
  provides the mutual authentication between the TOE and the Administrator user or Download operator user, the management of keys (Kc, Kd, Kfdi) and the download of the User data into the memory of the TOE. The Loader SFP protects the downloaded data against unauthorized disclosure, modification, deletion and insertion by transferring data always in encrypted form by using Kfdi and including signature values in the data string which are checked during the download process.
- The Flash Loader supports the following subjects defined by the roles:
- Administrator user.
- Download operator user.

Deployment of loader, which covers the following Flash Loader functionality:

- The Administrator user is enabled performing mutual authentication with the keys Kc and Kd, to manage (set, exchange, delete) the keys Kc, Kd and Kfdi and to process the download of the User data into the memory of the TOE.
- Download operator user is enabled performing mutual authentication with Kd, to exchange the key Kd and to perform the download of the User data into the memory of the TOE. He can also delete Kfdi.
- The Flash Loader supports the following object:
- user data: Data loaded into the memory of the TOE.
- The Flash Loader supports the following security attributes:
- Keys Kc and Kd used for the mutual authentication process.
- Key Kfdi used to encrypt/decrypt the user data.

The TOE shall meet the requirement “Limited capabilities (FMT_LIM.1/Loader)” as specified below:

FMT_LIM.1/Loader	Limited capabilities
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability.
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.

The TOE shall meet the requirement “Limited availabilities - Loader (FMT_LIM.2/Loader)” as specified below:

FMT_LIM.2/Loader	Limited availabilities - Loader
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities.
FMT_LIM.2.1/Loader	The TSF shall be designed and implemented in a manner that limits its availability so that in conjunction with “Limited capability (FMT_LIM.1)” the following policy is enforced: The TSF prevents deploying the Loader functionality after permanent deactivation.

Note 14:
Regarding FMT_LIM.1.1/Loader it is added in the User Guidance that the Flash Loader has to be permanently deactivated prior delivery to the end user (Phase 7).
End of note.

The TOE shall meet the requirement “Authentication Proof of Identity (FIA_API.1)” as specified below:

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 ISO/IEC 9798-2 [S18], section 6.2.2 Mechanism 4 - Three-pass authentication based on the security attributes Kc and Kd to prove the identity of the TOE to an external entity.

The TOE shall meet the requirement “Inter-TSF trusted channel (FTP_ITC.1)” as specified below:

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 the Administrator user and the Download operator user as described in the Loader SFP that is logically distinct from other communication channels and provides assured identificaton of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for deploying Loader for downloading the user data.

The TOE shall meet the requirement “Basic data exchange confidentiality (FDP_UCT.1)” as specified below:

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 to receive user data in a manner protected from unauthorised disclosure.

The TOE shall meet the requirement “Data exchange integrity (FDP_UIT.1)” as specified below:

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_UIT.1.1	The TSF shall enforce the Loader SFP to receive user data in a manner protected from modification, deletion or insertion errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, wether modification, deletion or insertion has occurred.

The TOE shall meet the requirement "Subset access control - Loader (FDP_ACC.1/Loader)" as specified below:

FDP_ACC.1/Loader	Subset access control - Loader
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control.
FDP_ACC.1.1/Loader	The TSF shall enforce the Loader SFP on • (1) the subjects Administrator user and the Download operator user, • (2) the objects User data, data loaded into the SOLID FLASH™ NVM memory of the TOE, • (3) the operation deployment of the Loader.

The TOE shall meet the requirement "Security attribute based access control - Loader (FDP_ACF.1/Loader)" as specified below:

FDP_ACF.1/Loader	Security attribute based access control – Loader
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/Loader	The TSF shall enforce the Loader SFP to objects based on the following: • (1) the subjects Administrator user and the Download operator user with security attributes Kc, Kd and Kfdi • (2) the objects user data in data loaded into the SOLID FLASH™ NVM memory of the TOE with security attributes Kfdi.
FDP_ACF.1.2/Loader	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: • (1) evaluate the corresponding access control information of the relevant subject, Administrator user and Download operator user, before the access, so that accesses to be denied cannot be utilized by the subject attempting to perform the operation. The subsequent download is then protected by the key Kfdi.
FDP_ACF.1.3/Loader	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none
FDP_ACF.1.4/Loader	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none

Note 15:
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 at TOE products coming with activated Flash Loader enabled for user data download. In other cases the Flash Loader is not available anymore and the user data download is completed. Depending on the capabilities of the user software these security functional requirements may then reoccur as

subject of the composite TOE.
The permanent locking of the Flash Loader after finalizing the download and prior delivery to the end-user is covered with FMT_LIM1/Loader and FMT_LIM.2/Loader.
End of note.

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. The augmentation of the assurance components compared to the Protection Profile [1] is expressed with bold letters.

Table 5 Assurance components

Aspect	Acronym	Description	Refinement
Development	ADV_ARC.1	Security Architecture Description	in PP [1]
	ADV_FSP.5	**Complete semi-formal functional specification with additional error information**	in ST [16]
	ADV_IMP.2	**Complete mapping of the implementation representation of the TSF**	in ST [16]
	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	in PP [1]
	AGD_PRE.1	Preparative procedures	in PP [1]
Life-Cycle Support	**ALC_CMC.5**	**Advanced support**	in ST [16]
	ALC_CMS.5	**Development tools CM coverage**	in ST [16]
	ALC_DEL.1	Delivery procedures	in PP [1]
	ALC_DVS.2	Sufficiency of security measures	in PP [1]
	ALC_LCD.1	Developer defined life-cycle model	
	ALC_TAT.3	**Compliance with implementation standards – all parts**	
	ALC_FLR.1	**Basic Flaw Remediation**	
Security Target Evaluation	ASE_CCL.1	Conformance claims	
	ASE_ECD.1	Extended components definition	
	ASE_INT.1	ST introduction	
	ASE_OBJ.2	Security objectives	
	ASE_REQ.2	Derived security requirements	
	ASE_SPD.1	Security problem definition	
	ASE_TSS.1	TOE summary specification	
Tests	**ATE_COV.3**	**Rigorous analysis of coverage**	in ST [16]
	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	in PP [1]

6.2.1 Refinements

Some refinements are taken unchanged from the PP [1]. In some cases a clarification is necessary. In Table 6 an overview is given where the refinement is done.

The refinements from the PP [1] have to be discussed here in the Security Target, as the assurance level is increased. The refinements from the PP [1] are included in the chosen assurance level EAL 6 augmented with ALC_FLR.1.

6.2.1.1 Development (ADV)

ADV_IMP Implementation Representation:

The refined assurance package ADV_IMP.1 implementation representation of the TSF requires the availability of the entire implementation representation, a mapping of the design description to the implementation representation with a level of detail that the TSF can be generated without further design decisions. In addition, the correspondence of design description and implementation representation shall be demonstrated.
The covered higher assurance package ADV_IMP.2 requires a complete and not curtailed mapping of the implementation representation of the TSF, and the mapping of the design description to the entire implementation representation. In addition, the correspondence of design description and the implementation representation shall be demonstrated. The ADV_IMP.1 aspect and refinement remains therefore valid. The enhancement underlines the refinement in the PP [1] and by that the entirely complete design i.e. not curtailed representation with according mapping was provided, demonstrated and reviewed.

ADV_FSP Functional Specification:

The ADV_FSP.4 package requires a functional description of the TSFIs and there assignment to SFR-enforcing, SFR-supporting, SFR-non-interfering, including related error messages, the assurance package. The enhancement of ADV_FSP.5 requires additionally a complete semi-formal functional specification with additional error information. In addition the package includes a tracing from the functional specification to the SFRs, as well as the TSFIs descriptions including error messages not resulting from an invocation of a TSFI. These aspects from ADV_FSP.5 are independent from the ADV_FSP.4 refinements from the PP [1] but constitute an enhancement of it. By that the aspects of ADV_FSP.4 and its refinement in the PP [1] apply also here. The assurance and evidence was provided accordingly.

6.2.1.2 Life-cycle Support (ALC)

ALC_CMS Configuration Management Scope:

The Security IC embedded firmware and the optional software are part of TOE and delivered together with the TOE as the firmware and optional software are stored in the ROM and/or SOLID FLASH™ NVM. The presence of the optional parts belongs to the user order. Both, the firmware and software delivered with the TOE are controlled entirely by Infineon Technologies. In addition, the TOE offers the possibility that the user can download his software at his own premises. These parts of the software are user controlled only and are not part of this TOE. The download of this solely user controlled software into the SOLID FLASH™ NVM is protected by strong authentication means. In addition, the download itself could also be encrypted. By the augmentation of ALC_CMS.4 to ALC_CMS.5 the configuration list includes additional the development tools. The package ALC_CMS.5 is therefore an enhancement to ALC_CMS.4 and the package with its refinement in the PP [1] remains valid. The assurance and evidence was provided accordingly.

ALC_CMC Configuration Management Capabilities:

The PP refinement from the assurance package ALC_CMC.4 Production support, acceptance procedures and automation points out that the configuration items comprise all items defined under ALC_CMS to be tracked under configuration management. In addition a production control system is required guaranteeing the traceability and completeness of different charges and lots. Also the number of wafers, dies and chips must be tracked by this system as well as procedures applied for managing wafers, dies or complete chips being removed from the production process in order to verify and to control predefined quality standards and production parameters. It has to be controlled that these wafers, dies or assembled devices are returned to the same production stage from which they are taken or they have to be securely stored or destroyed otherwise. The additionally covered extended package of ALC_CMC.5 Advance Support requires advanced support considering the automatisms configuration management systems, acceptance and documentation procedures of changes, role separation with regard to functional roles of personnel, automatisms for tracking and version controlling in those systems, and includes also production control systems. The additional aspects of ADV_CMC.5 constitute an enhancement of ALC_CMC.4 and therefore the aspects and ALC_CMC.4 refinements in the PP [1] remain valid. The assurance and evidence was provided.

ALC_DVS Development Security:

The assurance package ALC_DVS.1 identification of security measures is extended to ALC_DVS.2 requiring the evidence of sufficiency of security measures. The evidence was given and reviewed that the design and implementation and its development environment is protected with regard to confidentiality and integrity. The ALC_DVS.2 package is an enhancement of ALC_DVS.1. Therefore, this package and its refinement in the PP [9] remain valid. The assurance and evidence was provided accordingly.

6.2.1.3 Tests (ATE)

ATE_COV Test Coverage:

The PP refined assurance package ATE_COV.2 Analysis of coverage addresses the extent to which the TSF is tested, and whether or not the testing is sufficiently extensive to demonstrate that the TSF operates as specified. It includes the test documentation of the TSFIs in the functional specification. In particular the refinement requires that The TOE must be tested under different operating conditions within the specified ranges. In addition, the existence and effectiveness of mechanisms against physical attacks should be covered by evidence that the TOE has the particular physical characteristics. This is furthermore detailed in the PP [1]. This assurance package ATE_COV.2 has been enhanced to ATE_COV.3 to cover the rigorous analysis of coverage. This requires the presence of evidence that exhaustive testing on rigorous entirely all interfaces as documented in the functional specification was conducted. By that ATE_COV.2 and refinements as given in the PP [1] are enhanced by ATE_COV.3 and remain as well. The TSFIs were completely tested according to ATE_COV.3 and the assurance and evidence was provided.

6.2.2 ADV_SPM Formal Security Policy Model

It is the objective of this family to provide additional assurance from 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
	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
	  • FMT_SMF.1 Specification of Management Functions
	  • FMT_LIM.1/Loader Limited capabilities
	  • FMT_LIM.2/Loader Limited availability – Loader
	  • FIA_API.1 Authentication Proof of Identity
	  • 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

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

The objectives O.Authentication and OE.TOE_Auth are discussed in the PP [1] section 7.2.1.
The objectives O.Cap_Avail_Loader and OE.Lim_Block_Loader and the covering security functional requirements FMT_LIM.1/Loader and FMT_LIM.2/Loader are discussed in the PP [1] section 7.3.1.
The policy P.Ctrl_Loader and the objectives O.Ctrl_Auth_Loader and OE.Loader_usage are discussed in the PP [1] section 7.3.2.
The additional objective O.Prot_TSF_Confidentiality is defined in section 5.1 and 5.3 of this document.
The PP [1] section 6.1 includes also the definition of FDP_SDI.2 „Stored data integrity monitoring and action“.

While the above mentioned security functional requirements rationale of the TOE are defined and described in PP [1] section 6.3.1, the additional introduced SFRs are listed and discussed below:

Table 6 Rational for additional SFR in the ST

Objective	TOE Security Functional Requirements
O.Phys-Manipulation	FPT_TST.2 “Subset TOE security testing“
O.Mem-Access	FDP_ACC.1 “Subset access control” FDP_ACF.1 “Security attribute based access control” FMT_MSA.3 “Static attribute initialisation” FMT_MSA.1 “Management of security attributes” FMT_SMF.1 “Specification of Management Functions”
O.RND	FCS_RNG.1/TRNG “Generation of Random Numbers -TRNG” FCS_RNG.1/HPRG “Generation of Random Numbers - HPRG” FCS_RNG.1/DRNG “Generation of Random Numbers -DRNG” FCS_RNG.1/KSG “Generation of Random Numbers - KSG”
O.Prot_TSF_Confidentiality	FTP_ITC.1 “Inter-TSF-trusted channel” FDP_ACC.1/Loader “Subset access control –Loader” FDP_ACF.1/Loader “Security attribute based access control – Loader” FDP_UCT.1 “Basic data exchange confidentiality” FDP_UIT.1 “Data exchange integrity”

The table above gives an overview, how the security functional requirements are combined to meet the security objectives.

6.3.1.1 Cryptographic Aspects

The developer of the Smartcard Embedded Software must ensure that the cryptographic functions are used as specified and that the User data of the Composite TOE processed by these functions are protected as defined for the application context. These issues are addressed by the specific security functional requirements:

- [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,

All these requirements have to be fulfilled to support OE.Resp-Appl for FCS_COP.1/TDES and for FCS_COP.1/AES.

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 define how to implement the specific security functionality. However, key-dependent functions could be implemented in the Smartcard Embedded Software.

The usage of cryptographic algorithms requires the use of appropriate keys. Otherwise these cryptographic functions do not provide security. The keys have to be unique with a very high probability, and must have a certain cryptographic strength etc. In case of a key import into the TOE (which is usually after TOE delivery) it has to be ensured that quality and confidentiality are maintained. Keys for DES and AES are provided by the environment.

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

6.3.1.2 Hardware related Aspects

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 tested security enforcing functions are SF_DPM Device Phase Management, SF_CS Cryptograhic Support and SF_PMA Protection against modifying attacks.

The justification related to the security objective “Protection against Physical Manipulation (O.Phys-Manipulation)” is as follows:
The security functional requirement FPT_TST.2 will detect attempts to conduce a physical manipulation on the monitoring functions of the TOE. The objective of FPT_TST.2 is O.Phys-Manipulation. The physical manipulation will be tried to overcome security enforcing functions.
The security functional requirement “Stored data integrity monitoring and action (FDP_SDI.2)” requires the implementation of an error detection mechanism which detects integrity errors of the data stored in the RAM, SOLID FLASH™ NVM and Cache memories and an error correction mechanism which corrects one-bit-errors in the SOLID FLASH™ NVM automatically and inform the user about errors in the RAM. By this the malfunction of the TOE using corrupt data is prevented. Therefore FDP_SDI.2 is suitable to meet the objective 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 and FMT_SMF.1 cover this security objective. The implementation of these functional requirements is represented by the dedicated level concept.

The justification of the security objective and the additional requirements show that they do not contradict to the rationale already given in the Protection Profile for the assumptions, policy and threats defined there. Moreover, these additional security functional requirements cover the requirements by the PP [1] User data of the Composite TOE protection of section 1.2.5 claim 35 and claim 36 which are not refined by the Protection Profile [1].
Nevertheless, the developer of the Smartcard Embedded Software must ensure that the additional functions are used as specified and that the User data of the Composite TOE 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.

The justification related to the security objective “Protection against (O.Malfunction)” is as follows:
Malfunction of the TOE might be caused by the operating conditions of the TOE. Two possibilities exists, either the operating conditions are inside the tolerated range or at least one of them is outside of this range. The second case is covered by FPT_FLS.1, because it states that a secure state is preserved in this case. The first case is covered by FRU_FLT.2 because it states that the TOE operates correctly under normal (tolerated) conditions. Therefore FPT_FLS.1 and FRU_FLT.2 are suitable to meet the objective O.Malfunction.

The presence of true random numbers is the security goal 4 (SG4) which is formalized in the objective O.RND Random Numbers. This objective must be covered by fulfillment of the security functional requirement FCS_RNG. This is defined in the PP [1] section 5.1. The rational for the functional requirement FCS_RNG is discussed in the PP [1], section 6.3.1. The requirement implements a quality metric which is defined by national regulations. The implemented random number generation fulfills the definitions of AIS31 [6] in the quality classes as outlined in section 6.1.1.1. Therefore the SFR FCS_RNG and the objective O.RND are covered.

The CC part 2 defines the component FIA_SOS.2, which is similar to FCS_RNG.1, as follows:

FIA_SOS.2	TSF Generation of secrets
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_SOS.2.1	The TSF shall provide a mechanism to generate secrets that meet [assignment: a defined quality metric].
FIA_SOS.2.2	The TSF shall be able to enforce the use of TSF generated secrets for [assignment: list of TSF functions].

6.3.1.3 Flash Loader related Aspects

The justification related to the security objective “Protection of the confidentiality of the TSF (O.Prot_TSF_Confidentiality)” is as follows:

The TOE provides protection against disclosure of confidential operations of the Security IC through the use of a dedicated code loaded on open samples with the security functional requirement FTP_ITC.1 “Inter-TSF-trusted channel”. The FTP_ITC.1 installs a communication channel between the TOE and the user which is logically distinguished from other channels. The security functional requirements FDP_UCT.1 “Basic data exchange confidentiality” and FDP_UIT.1 “Data exchange integrity” providing the confidentiality and integrity of the transferred user data with crypograhic methodes. Additionally th e security functional requirements FDP_ACC.1/Loader “Subset access control –Loader” and FDP_ACF.1/Loader “Security attribute based access control – Loader” providing the access control policy for the roles Administrator user and Download operator user.

6.3.1.4 Dependencies of Security Functional Requirements

The dependencies of the security functional requirements are defined and described in PP [1] section 6.3.2, with FDP_SDI.2, and with regard to the Flash Loader related security functional requirements, the description is given at the individual package chapters 7.2.3, 7.3.1 and 7.3.2:

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, FDP_SDI.2, FDP_SDC.1, FMT_LIM.1/Loader, FMT_LIM.2/Loader, FDP_ACC.1/Loader and FDP_AFC.1/Loader.

The security functional requirements FIA_API.1 and FTP_ITC.1 have no dependencies.
The security functional requirements FIA_API, FTP_ITC.1, FDP_UCT.1, FDP_UIT.1, FDP_ACC.1/Loader and FDP_ACF.1/Loader apply only at TOE products which are delivered with activated Flash Loader.

Further dependencies of security functional requirements are given in following table:

Table 7 Dependency for cryptographic operation requirement

Security Functional Requirement	**Dependencies**	**Fulfilled by security requirements**
FCS_COP.1/TDES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	Yes, see comment 2
FCS_CKM.4/TDES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, see comment 2
FCS_COP.1/AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM1], FCS_CKM.4	Yes, see comment 2
FCS_CKM.4/AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, see comment 2
FPT_TST.2	No dependencies	Yes
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FMT_MSA.3, FDP_ACC.1	Yes
FMT_MSA.3	FMT_MSA.1	Yes
	FMT_SMR.1	NA, see comment 1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	Yes
	FMT_SMR.1	NA, see comment 1
	FMT_SMF.1	Yes
FMT_SMF.1	None	NA
FMT_LIM.1/Loader	FMT_LIM.2/Loader	Yes
FMT_LIM.2/Loader	FMT_LIM.1/Loader	Yes
FTP_ITC.1	None	Yes, see comment 3
FDP_UCT.1	[FPT_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	Yes
FDP_UIT.1	[FPT_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	Yes
FDP_ACC.1/Loader	FMT_ACF.1/Loader	Yes
FDP_ACF.1/Loader	FMT_MSA.3	Yes, see comment 3

Comment 1:

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

End of comment.

Comment 2:

These requirements all address the appropriate management of cryptographic keys used by the specified cryptographic function and are not part of the PP [1]. 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/TDES and FCS_COP.1/AES the respective dependency FCS_CKM.4 is fulfilled by the TOE.
The cryptographic key destruction can be done by overwriting the key register interfaces or by software reset of

the SCP which provides immediate zeroing of all SCP hardware key registers.
Please refer also to the application notes 41 and 42 in the PP [1].
For the security functional requirement FCS_COP.1/TDES, FCS_COP.1/AES, FCS_CKM.4/TDES and FCS_CKM.4/AES the dependencies FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 have to be fulfilled by the environment because the TOE does not provide the accompanying functionality (e.g. generate and import keys). That mean, that the environment shall meet the requirements FCS_CKM.1, FDP_ITC.1 or FDP_ITC.2 as defined in [3], section 10.1 and 11.7.

End of comment.

Comment 3:

The inter-TSF trusted channel SFR FTP_ITC.1 has no dependency and is provided as main purpose by the Flash Loader. The Flash Loader provides a distinct and independent communication channel with authenticated end points and protection from modification or disclosure.

The dependency FMT_MSA.3 introduced by the component FDP_ACF.1/Loader is considered to be not required, because the security attributes enforcing the Loader SFP are fixed by the IC manufacturer and no new objects under the control of the Loader SFP are created. The Loader SFP also does not create any new security attributes and the security attributes are fixed during the download process. Claim 371 of PP [9] applies.

End of comment.

6.3.2 Rationale of the Assurance Requirements

The chosen assurance level EAL6 is augmentation with the requirements coming from ALC_FLR.1. In Table 8 the different assurance levels are shown as well as the augmentations. The augmentations are in compliance with the Protection Profile [1].

An assurance level EAL6 with the augmentations ALC_FLR.1 is required for this type of TOE since it is intended to defend against **highly sophisticated attacks** without protective environment over a targeted long life time. Thereby, the TOE must withstand attackers with high attack potential, which is achieved by fulfilling the assurance class AVA_VAN.5.

In order to provide a meaningful level of assurance and that the TOE provides an adequate level of defense against such high potential attacks, the evaluators 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 “Application of Attack Potential to Smartcards” [10] shall be taken as a basis for the vulnerability analysis of the TOE.

Due to the targeted long life time of the Infineon Technologies products, a comprehensive flaw remediation process and database is in place to maintain the TOE also in future. Reported flaws of any kind, meaning, regardless whether the flaws reported have a more directed towards quality, functional or security, are tracked by a dedicated database and related processes.

And more, in order to continuously improve also future products reported flaws are analyzed whether they could affect also future products. Due to its overall importance for future development, the assurance class ALC_FLR.1 is included in this certification process.

This evaluation assurance package was selected to permit a developer gaining maximum assurance from positive security engineering based on good commercial practices as well as the assurance that the TOE is maintained during its targeted life time. The evaluation assurance package follows the EAL6 assurance classes as given in [4].

6.3.2.1 ALC_FLR.1 Basic Flaw Remediation

Flaws of any kind are entered into a dedicated database with related processes to solve those.

At the point in time where a flaw is entered, it is automatically logged who entered a flaw and who is responsible for solving it. In addition, it is also documented if, when and how an individual flaw has been solved.

Flaws are prioritized and assigned to a responsibility.

The assurance class ALC_FLR.1 has no dependencies.

7 TOE Summary Specification (ASE_TSS)

The product overview is given in section 2.1. In the following the Security Features are described and the relation to the security functional requirements is shown.

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

- SF_DPM Device Phase Management
- SF_PS Protection against snooping
- SF_PMA Protection against Modifying 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 in several phases. Chip development and production (phase 2, 3, 4) and final use (phase 4-7) is a rough split-up from TOE point of view. These phases are implemented in the TOE as test mode (phase 3) and user mode (phase 4-7).

In addition, chip identification modes are implemented being active in all TOE life cycle phases. The chip identification data (O.Identification) is stored in a in the not changeable configuration page area of the SOLID FLASH™ NVM. During this first data programming, the TOE is still in the secure environment and in Test Mode.

The covered security functional requirement is FAU_SAS.1 “Audit storage”, FDP_ITT.1 “Basic internal transfer proection” and FPT_ITT.1 ”Basic internal TSF data transfer protection”.

During start-up of the TOE the decision for one of the various operation modes is taken dependent on phase identifiers. The decision of accessing a certain mode is defined as phase entry protection. The phases follow also a defined and protected sequence. The sequence of the phases is protected by means of authentication.

The covered security functional requirements are FMT_LIM.1”Limited Capabilities” and FMT_LIM.2 “Limited availability”.

During the production phase (phase 3 and 4) or after the delivery to the user (phase 5 or phase 6), the TOE provides the possibility to download, after a successful authentication process, a user specific encryption key and user data into the empty (erased) SOLID FLASH™ NVM area as specified by the associated control information of the Flash Loader software. This process is only possible after a successful mutual authentication process of the external entity and the TOE itself.
In case the user has ordered TOE derivatives without Flash Loader, the user data download by the user (phase 5 or phase 6) is disabled and all user data of the Composite TOE has been lashed (downloaded) on the TOE at Infineon premises. In both cases the integrity of the loaded data is checked with a hashing. The data to be loaded is transferred always in encrypted form.
After finalizing the load operation and prior delivery to the end-user, the Flash Loader shall be permanently deactivated. The permanent deactivation is named locking and is a user obligation documented in the user guidance. This locking removes any possibility to use or reactivate the Flash Loader.

The covered security functional requirement are FMT_LIM.1/Loader “Limited capabilities”, FMT_LIM.2/Loader “Limited availability-Loader”, FIA_API.1 “Authentication Proof of Identity”, 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” and FDP_ACF.1/Loader “Security attribute based access control – Loader”.

The Flash Loader related 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 at TOE products coming with activated Flash Loader enabled for user data download by the user. In other cases the Flash Loader is not available anymore and the user data download is completed.

In addition, during each start-up of the TOE the address ranges, belonging memory keys and access rights are initialized by the Boot Software (BOS) with predefined values. After entering a dedicated phase in the life cycle the operation of the TOE is always controlled and limited by the encryption functionality of the Memory Encryption/Decryption Unit (MED).

The covered security functional requirements are FDP_ACC.1 " Subset access control", FDP_ACF.1 " Security attribute based access contol", FMT_SMF.1 "Specification of Management functions", FMT_MSA.1 "Management of security attributes", FMT_MSA.3 "Static attribute initialization", FMT_LIM.1 "Limited capabilities" and FMT_LIM.2 "Limited capabilities".

The **SF_DPM** "Device Phase Management" covers the security functional requirements FAU_SAS.1, FMT_LIM.1, FMT_LIM.2, FDP_ITT.1, FPT_ITT.1, FMT_LIM.1/Loader, FMT_LIM.2/Loader, FIA_API.1, FTP_ITC.1, FDP_UCT.1, FDP_UIT.1, FDP_ACC.1, FDP_ACF.1, FMT_SMF.1, FMT_MSA.1, FDP_ACC.1/Loader and FDP_ACF.1/Loader.

7.2 SF_PS: Protection against Snooping

Several mechanisms protect the TOE against snooping the design or the user data during operation and even if it is out of operation (power down).

The entire design is kept in a non standard way to prevent attacks using standard analysis methods. Important parts of the chip are especially designed to counter leakage or side channel attacks like DPA/SPA or EMA/DEMA. Therefore, even the physical data gaining is difficult to perform, since timing and current consumption is independent of the processed data. In the design a number of components are automatically synthesized and mixed up to disguise an attacker and to make an analysis more difficult.

The covered security functional requirement is FPT_PHP.3 "Resistance to physical attack".

A further protective design method used is secure wiring. All security critical wires have been identified and protected by special routing measures against probing. Additionally the wires are embedded into shield lines and used as normal signal lines for operation of the chip to prevent successful probing.

The covered security functional requirements are FPT_PHP.3 "Resistance to physical attack", FPT_ITT.1 "Basic internal TSF data transfer protection", FPT_FLS.1 "Failure with preservation of secure state" and FDP_ITT.1 "Basic internal transfer protection".

All memories present on the TOE (SOLID FLASH™ NVM, ROM, RAM) are encrypted and additionally the memory addresses are scrambled, using individual keys assigned by complex key management and the Cache memory is masked. The encryption of the memory content is done by the MED using a proprietary cryptographic algorithm and a complex key management providing protection against cryptographic analysis attacks. This means that the SOLID FLASH™ NVM, RAM, ROM are encrypted with module dedicated and derived keys. The only key remaining static over the product life cycle is the specific ROM key changing from mask to mask. Additionally a chip individual scrambling of the memory addresses is active.In case of security critical error a security alarm is generated and the TOE ends up in a secure state.

The covered security functional requirements are FPT_PHP.3 "Resistance to physical attack", FDP_ITT.1 "Basic internal transfer protection", FDP_IFC.1 "Subset information flow control", FPT_ITT.1 "Basic internal TSF data transfer protection", FDP_SDC.1 "Stored data confidentiality" and FPT_FLS.1 "Failure with preservation of secure state".

In addition the data transferred over the peripheral bus to and from (bi-directional encryption) the CPU, Co-processor (Crypto2304T and SCP), the special SFRs and the peripheral devices CRC and HRNG are transported masked with an automatically dynamic mask change.
The function Trash Register Writes can be activated by the user to hide the fact if a register has been written.

The covered security functional requirements are FDP_IFC.1 “Subset information flow control“, FPT_PHP.3 “Resistance to physical attack”, FPT_ITT.1 “Basic internal TSF data transfer protection”, FPT_FLS.1 “Failure with preservation of secure state”, FDP_SDC.1 “Stored data confidentiality” and FDP_ITT.1 “Basic internal transfer protection”.

The **SF_PS** “Protection against Snooping” covers the security functional requirements FPT_PHP.3, FDP_SDC.1, FDP_IFC.1, FPT_ITT.1, FPT_FLS.1 and FDP_ITT1.

7.3 SF_PMA: Protection against Modifying Attacks

The TOE is equipped with an error detection mechanism for protecting the RAM, an error correction code (ECC) realized in the SOLID FLASH™ NVM and a parity protection for the Cache. In case of any bit errors detected in the RAM, a security alarm is triggered, in terms of single bit errors detected in the SOLID FLASH™ NVM the errors are automatically corrected. The cache has additional mechanisms implemented to detect modifications and to protect the confidentiality of the data.

The covered security functional requirements are FDP_SDC.1 “Stored data confidentiality”, FRU_FLT.2 “Limited fault tolerance“, FDP_PHP.3 “Resistance to physical attack“ and FDP_SDI.2 “Stored data integrity monitoring and action”.

The TOE is protected against fault and modifying attacks. In the case that a physical manipulation or a physical probing attack is detected, the processing of the TOE is immediately stopped and the TOE enters a secure state called security reset.

The covered security functional requirements are FPT_FLS.1 “Failure with preservation of secure state”, FPT_PHP.3 “Resistance to physical attack” and FPT_TST.2 “Subset TOE security testing“.

The Online Configuration Check (OCC) function is used for the protection of Special Function Registers (SFR), i.e. it controls the modification of relevant SFR settings. The covered security functional requirements are FPT_FLS.1 “Failure with preservation of secure state” and FPT_PHP.3 “Resistance to physical attack”.

As physical effects or manipulative attacks may also address the program flow of the user software, two watchdog timers each with a check point register function are implemented. This feature allows the user to check the correct processing time and the integrity of the program flow of the user software.
The Instruction Stream Signature Checking (ISS), which is an optional feature, calculates a hash about all executed instructions and automatically checks the correctness of this hash value. If the code execution follows an illegal path an alarm is triggered.
Another measure against modifying and perturbation respectively differential fault attacks (DFA) is the implementation of backward calculation in the SCP. By this induced errors are discovered.

The covered security functional requirements are FDP_ITT.1 “Basic internal transfer protection”, FDP_IFC.1 “Subset information flow control”, FPT_ITT.1 “Basic internal TSF data transfer protection”, FPT_FLS.1 “Failure with preservation of secure state” and FPT_PHP.3 “Resistance to physical attack”.

During start up, the TOE performs various configurations and subsystem tests. After the start up has finished, the operating system or the application can activate the testfunctions (UMSLC), provided by specific Special Function Registers, also during normal operation. These testfunctions can be used to check the alarm lines and/or functions and sensors for correct operation as given in the 32-bit Security Controller Hardware Reference Manual [7].

As attempts to modify the security features will be detected from the test, the covered security functional requirement is FPT_TST.2 “Subset TOE security testing“.

The correct function of the TOE is only given in the specified range of the environmental operating parameters. To prevent an attack exploiting that circumstance the TOE is equipped with a temperature sensor, voltage sensor, frequency sensor and backside light detection. The TOE falls into the defined secure state in case of a specified range violation. The defined secure state causes the chip internal reset process. Note that the specified range checking can only work when the TOE is running and cannot prevent reverse engineering.

The covered security functional requirements are FPT_PHP.3 “Resistance to physical attack” and FPT_FLS.1 “Failure with preservation of secure state“.

The covered security functional requirements are FPT_PHP.3 “Resistance to physical attack” and FPT_FLS.1 “Failure with preservation of secure state“.

The **SF_PMA** “Protection against Modifying Attacks” covers the security functional requirements FPT_PHP.3, FDP_IFC.1, FPT_ITT.1, FDP_ITT.1, FPT_TST.2, FDP_SDI.2, FDP_SDC.1, FRU_FLT.2 and FPT_FLS.1.

7.4 SF_PLA: Protection against Logical Attacks

The memory model of the TOE provides two distinct, independent levels called the privileged mode and user mode and the possibility to define up to eight memory regions with different access rights enforced by the Management Protection Unit (MPU). This gives the user software the possibility to define different access rights for the regions 0 to 7 at the user mode. In the case of an access violation the MPU will trigger a trap. The privileged mode has access to all regions at the user mode. The user mode has no access to the privileged mode. The policy of setting up the MPU and specifying the memory ranges for the regions (0 to 7) is defined from the user software.

The covered security functional requirements are 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”, FPT_FLS.1 “Failure with preservation of secure state” and FMT_SMF.1 “Specification of Management functions”.

The **SF_PLA** “Protection against Logical Attacks” covers the security functional requirements FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FPT_FLS.1 and FMT_SMF.1.

7.5 SF_CS: Cryptographic Support

The TOE is equipped with several hardware accelerators to support the standard symmetric cryptographic operations. This security function is introduced to include the cryptographic operation in the scope of the evaluation as the cryptographic function respectively mathematic algorithm itself is not used from the TOE security policy. On the other hand these functions are of special interest for the use of the hardware as platform for the software.

Note 16:
This TOE can come with both crypto coprocessors accessible, or with a blocked SCP, or with a blocked Crypto2304T, or with both cryptographic coprocessors blocked. The blocking depends on the customer demands prior to the production of the hardware. In case the SCP is blocked, no AES and DES computation supported by hardware is possible. In case the Crypto2304T is blocked, no RSA and EC computation supported by hardware is possible. No accessibility of the deselected cryptographic coprocessor is without impact on any

other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic coprocessors.
End of note.

7.5.1 Triple DES

The FCS_COP.1/TDES, which features are described in the following, is implemented by directly programming the hardware registers of the symmetric coprocessor. The TOE supports the encryption and decryption in accordance with the specified cryptographic algorithm Triple Data Encryption Standard (TDES) with cryptographic key sizes of 112 or 168 bit meeting the standards:

- National Institute of Standards and Technology (NIST), SP 800-67 [S4].

The TOE implements the following alternative block cipher modes for the user:

the Electronic Codebook Mode (ECB), the Cipher Block Chaining Mode (CBC), the Cipher Block Chaining Mode Message Authentication Code (CBC-MAC) and the CBC-MAC- encrypt-last-block (CBC-MAC-ELB).

The CBC-MAC and CBC-MAC-ELB complies with the standard:

- ISO/IEC 9797-1:2011, Part 1 [S14].

The implementation of ECB and CBC modes follow the standard:

- National Institute of Standards and Technology (NIST), SP 800-38A [S5].

The key destruction as required by FCS_CKM.4/TDES can be done by overwriting the key register interfaces or by software reset of the SCP which provides immediate zeroing of all SCP key registers.

Please consider also the statement of section 6.1.4.1.

The covered security functional requirements are FCS_COP.1/TDES and FCS_CKM.4/TDES.

7.5.2 AES

The FCS_COP.1/AES is implemented by directly programming the hardware registers of the symmetric coprocessor. The TOE supports the encryption and decryption in accordance with the specified cryptographic algorithm Advanced Encryption Standard (AES) and cryptographic key sizes of 128 bit or 192 bit or 256 bit that meet the standard,:

- FIPS 197 [S8].

The TOE implements the following alternative block cipher modes for the user:

the Electronic Codebook Mode (ECB), the Cipher Block Chaining Mode (CBC), the Cipher Block Chaining Mode Message Authentication Code (CBC-MAC) and the CBC-MAC- encrypt-last-block (CBC-MAC-ELB.

The implementation of CBC-MAC and CBC-MAC-ELB complies with the standard:

- ISO/IEC 9797-1:2011, Part 1 [S14].

The implementation of ECB and CBC complies with the standard:

- National Institute of Standards and Technology (NIST) SP 800-38A [S5].

The key destruction as required by FCS_CKM.4/AES can be done by overwriting the key register interfaces or by software reset of the SCP which provides immediate zeroing of all SCP key registers.

Please consider also the statement of section 6.1.4.1.

The covered security functional requirement is FCS_COP.1/AES and FCS_CKM.4/AES.

7.5.3 Random Number Generator

Random data is essential for cryptography as well as for security mechanisms. The TOE is equipped with a Hybrid Physical True Random Number Generator (hybrid PTRNG, FCS_RNG.1). The random data can be used from the Smartcard Embedded Software and is also used from the security features of the TOE, i.e. masking. The HPRNG implements various topological means, masked bus interface, is self-checking and can be actively checked by the user.

The produced genuine random numbers are available as a security service for the user and are also used for internal purposes. The hybrid PTRNG operates in the following modes of operation:

- True Random Number Generation, meeting [6] PTG.2
- Hybrid Random Number Generation, meeting [6] PTG.3
- Deterministic Random Number Generation meeting [6] DRG.3
- Key Stream Generation meeting [6] DRG.2

The hybrid PTRNG covers the security functional requirements FCS_RNG.1 “Random Number Generation” (FCS_RNG.1/TRNG, FCS_RNG.1/HPRG, FCS_RNG.1/DRNG, FCS_RNG.1/KSG), FPT_PHP.3 “Resistance to physical attack”, FDP_ITT.1 “Basic internal transfer protection”, FPT_ITT.1 “Basic internal TSF data transfer protection” and FPT_FLS.1 “Failure with preservation of secure state”.

The **SF_CS** “Cryptographic Support” covers the security functional requirements FCS_COP.1/TDES, FCS_CKM.4/TDES, FCS_COP.1/AES, FCS_CKM.4/AES, FPT_PHP.3, FDP_ITT.1, FPT_ITT.1, FPT_FLS.1, FCS_RNG.1/TRNG, FCS_RNG.1/HPRG, FCS_RNG.1/DRNG and FCS_RNG.1/KSG.

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 sections the sections above. The results are shown in the table below. The security functional requirements are addressed by at least one relating security feature.

The various functional requirements are often covered manifold. As described above the requirements ensure that the TOE is checked for correct operating conditions and if a not correctable failure occurs that a stored secure state is achieved, accompanied by data integrity monitoring and actions to maintain the integrity although failures occurred. An overview is given in the table below.

Table 8 Mapping of SFR and SFSF

Security Functional Requirement	SF_DPM	SF_PS	SF_PMA	SF_PLA	SF_CS
FAU_SAS.1	X				
FMT_LIM.1	X				
FMT_LIM.2	X				
FDP_ACC.1	X			X	
FDP_ACF.1	X			X	
FTP_ITC.1	X				
FDP_UCT.1	X				
FIA_API.1	X				
FMT_LIM.1/Loader	X				
FMT_LIM.2/Loader	X				
FDP_UIT.1	X				
FDP_ACC.1/Loader	X				
FDP_ACF.1/Loader	X				
FPT_PHP.3		X	X		X
FDP_ITT.1	X	X	X		X
FPT_ITT.1	X	X	X		X
FDP_SDC.1		X	X		
FDP_SDI.2			X		
FDP_IFC.1		X	X		
FMT_MSA.1	X			X	
FMT_MSA.3	X			X	
FMT_SMF.1	X			X	
FRU_FLT.2			X		

FPT_TST.2			X		
FPT_FLS.1		X	X	X	X
FCS_RNG.1/TRNG					X
FCS_RNG.1/HPRG					X
FCS_RNG.1/DRNG					X
FCS_RNG.1/KSG					X
FCS_COP.1/TDES					X
FCS_COP.1/AES					X
FCS_CKM.4/TDES					X
FCS_CKM.4/AES					X

7.7 Security Requirements are internally Consistent

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

In addition to the discussion in section 6.3 of PP [1] the security functional requirement FCS_COP.1 is introduced. The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the cryptographic algorithms implemented according to the security functional requirement FCS_COP.1. Therefore, these security functional requirements support the secure implementation and operation of FCS_COP.1.

As disturbing, manipulating during or forcing the results of the test checking the security functions after TOE delivery, this security functional requirement FPT_TST.2 has to be protected. An attacker could aim to switch off or disturb certain sensors or filters and preserve the detection of his manipulation by blocking the correct operation of FPT_TST.2. The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the 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. In addition, the TOE provides an automated continuous user transparent testing of certain functions.

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

8 Literature and References

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

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

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

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

[5] ARMv7-M Architecture Reference Manual, ARM DDI 0403D ID021310, 12. February 2010, ARM Limited

[6] Functionality classes and evaluation methodology for physical random number generators AIS31, Version 3.0, 2013-05-15, Bundesamt für Sicherheit in der Informationstechnik and belonging “A proposal for: Functionality classes for random number generators”, Version 2.0, 2011-09-18, Wolfgang Killmann, T-Systems GEI GmbH, Werner Schindler, Bundesamt für Sicherheit in der Informationstechnik

[7] 32-bit Security Controller – V20 Hardware Reference Manual, Infineon Technologies AG, Revision 2.3, 2020-10-15 and
32-bit Security Controller – V21 Hardware Reference Manual, Infineon Technologies AG, Revision 2.3, 2020-10-15

[10] Joint Interpretation Library, Application of Attack Potential to Smartcard, mandatory technical document, Version 3.0, April 2019, https://www.sogis.eu

[11] 32-bit ARM-based Security Controller SLC37 (65 nm Technology) Programmer’s Reference Manual, Infineon Technologies AG, Revision 4.6, 2020-10-13

[12] 32-bit Security Controller- V20 Errata Sheet, Infineon Technologies AG, Revision 3.0, 2020-10-13 and
32-bit Security Controller- V21 Errata Sheet, Infineon Technologies AG, Revision 3.0, 2020-11-02

[14] Production and personalization 32-bit ARM-based security controller User´s Manual, Infineon Technologies AG, Revision 3.4, 2018-05-14

[23] 32-bit Security Controller – V20 Security Guidelines, Version 1.00-2621, 2020-09-09, Infineon Technologies AG, and
32-bit Security Controller – V21 Security Guidelines, Version 1.00-2622, 2020-09-09, Infineon Technologies AG

[104] 32-bit Security Controller Crypto@2304T V3 User Manual, Infineon Technologies AG, Revision 2.0, 2019-04-24

[S4] National Institute of Standards and Technology (NIST), Special Publication SP 800-67 Rev.2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, November 2017, Technology Administration, U.S. Department of Commerce

[S5] National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce, NIST Special Publication SP 800-38A, 2001-12

[S8] Federal Information Processing (FIPS) Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. Department of Commerce / National Institute of Standards and Technologies, November 26, 2001

[S14] ISO/IEC 9797-1: 2011, Information technology – Security techniques–Message Authentication Codes (MACs) Part 1 Mechanisms using a block cipher, 2011-03-01

[S17] The test suite is available from the NIST RNG project website http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html statistical test suite 2010-08-11, sts.2.1.1.

[S18] ISO/IEC 9798-2:2008 Information technologies – Security techniques – Entity authentication, Part 2: Mechnisms using symmetric encripherment algorithms, Third edition 2008-12-15

[S23] Bruce SCHNEIER, Aplied Cryptography, Second Edition, John Wiley & Sons, 1996

[PP84] PP0084: Interpretations, Secretariat general de la defence et de la securite nationale, Reference: PP0084.02, 2016-04-16

[BSIG] Act on the Federal Office for Information Security (BSI-Gesetz-BSIG) of 14. August 2009, Bundesgesetzblatt I p. 2821; BSIG Section 9, Para.4, Clause 2

9 List of Abbreviations

AES	Advanced Encryption Standard
AIS31	“Anwendungshinweise und Interpretationen zu ITSEC und CC Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren”
API	Application Programming Interface
APDU	Application Protocol Data Unit
BOS	Boot Software
BSI	German: Bundesamt für Sicherheit in der Informationstechnik English: Federal Office for Information Security
CC	Common Criteria
CI	Chip Identification Mode (BOS-CI)
CIM	Chip Identification Mode (BOS-CI), same as CI
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
Crypto2304T	Asymmetric Cryptographic Coprocessor
CRT	Chinese Reminder Theorem
DES	Data Encryption Standard
DK	Deutsche Kreditwirtschaft
DPA	Differential Power Analysis
DFA	Differential Failure Analysis
DRNG	Deterministic Random Number Generator
EC	Elliptic Curve Cryptography
ECC	Error Correction Code and Elliptic Curve Cryptography depending on the context
EDC	Error Detection Code
SOLID FLASH™ NVM	Electrically Erasable and Programmable Read Only Memory
EMA	Electromagnetic analysis
FL	Flash Loader
Flash	SOLID FLASH™ Memory
HRNG	Hybrid Random Number Generator
HW	Hardware
HSL	Hardware Support Library
HSM	Hardware Security Module
IC	Integrated Circuit
ICO	Internal Clock Oscillator
ID	Identification

IMM	Interface Management Module
I/O	Input/Output
IRAM	Internal Random Access Memory
ITSEC	Information Technology Security Evaluation Criteria
MED	Memory Encryption and Decryption
MPU	Memory Protection Unit
NVM	Non Volatile Memory
O	Object
OS	Operating system
PEC	Peripheral Event Channel
PFD	Post Failure Detection Unit
PRNG	Pseudo Random Number Generator
PROM	Programmable Read Only Memory
PTRNG	Physical True Random Number Generator
RAM	Random Access Memory
RFI	Radio Frequency Interface
RMS	Resource Management System
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rives-Shamir-Adleman Algorithm
SCP	Symmetric Cryptographic Processor
SF	Security Feature
SFR	Special Function Register, as well as Security Functional Requirement The specific meaning is given in the context
SPA	Simple power analysis
SW	Software
SO	Security objective
T	Threat
TM	Test Mode (BOS)
TOE	Target of Evaluation
TRNG	True Random Number Generator
TSC	TOE Security Functions Control
TSF	TOE Security Functionality
UART	Universal Asynchronous Receiver/Transmitter
UM	User Mode (BOS)

UmSLC	User mode Security Life Control
WDT	Watch Dog Timer
XRAM	eXtended Random Access Memory
TDES	Triple DES Encryption Standard also known as TDES

10 Glossary

Application Program/Data	Software which implements the actual TOE functionality provided for the user or the data required for that purpose
Bill-Per-Use	Bill-Per-Use concept allowing the user to configure the chips
Central Processing Unit	Logic circuitry for digital information processing
Chip	Integrated Circuit
Chip Identification Data	Data stored in the SOLID FLASH™ NVM containing the chip type, lot number (including the production site), die position on wafer and production week and data stored in the ROM containing the STS version number
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
Controller	IC with integrated memory, CPU and peripheral devices
Crypto2304T	Cryptographic coprocessor for asymmetric cryptographic operations (RSA, Elliptic Curves)
Cyclic Redundancy Check	Process for calculating checksums for error detection
Electrically Erasable and Programmable Read Only Memory (SOLID FLASH™ NVM)	Non-volatile memory permitting electrical read and write operations
End User	Person in contact with a TOE who makes use of its operational capability
Firmware	Is software essential to put the chip into operation. The firmware is located in the ROM and parts of it in the SOLID FLASH™ NVM
Flash Loader	Software enabling to download software after delivery
Hardware	Physically present part of a functional system (item)
Integrated Circuit	Component comprising several electronic circuits implemented in a highly miniaturized device using semiconductor technology
Internal Random Access Memory	RAM integrated in the CPU
Mechanism	Logic or algorithm which implements a specific security function in hardware or software
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 to run the user application
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

SCP	Symmetric Cryptographic CoProcessor for symmetric cryptographic operations (TDES, AES).
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
Smart Card	Plastic card in credit card format with built-in chip. Other form factors are also possible, i.e. if integrated into mobile devices
Software	Information (non-physical part) which is required to implement functionality in conjunction with the hardware (program code)
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
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

Revision History

Figure 2 Major changes since the last revision

Version	**Description of change**
0.1	Initial version
1.0	Final version

Edition 2020-12-07

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Email: erratum@infineon.com

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

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.