Security Target Lite

Common Criteria EAL6 augmented / EAL6+

M7892 Design Step G12

Document version 4.4 as of 2024-06-20

Author: Infineon Technologies

Confidential

Edition 2024-06-20

Published by Infineon Technologies AG,

81726 Munich, Germany.

Legal Disclaimer

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics. With respect to any examples or hints given herein, any typical values stated herein and/or any information regarding the application of the device, Infineon Technologies AG 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.

Information

For further information on technology, delivery terms and conditions and prices, please contact the nearest Infineon Technologies AG Office (**www.infineon.com**).

Warnings

Due to technical requirements, components may contain dangerous substances. For information on the types in question, please contact the nearest Infineon Technologies AG Office.

Infineon Technologies AG components may be used in life-support devices or systems only with the express written approval of Infineon Technologies AG, if a failure of such components can reasonably be expected to cause the failure of that life-support device or system or to affect the safety or effectiveness of that device or system. Life support devices or systems are intended to be implanted in the human body or to support and/or maintain and sustain and/or protect human life. If they fail, it is reasonable to assume that the health of the user or other persons may be endangered.

Confidential
Miscellaneous

Trademarks of Infineon Technologies AG

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

Trademarks updated August 2015

Other Trademarks

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

Confidential

Revision History

Major changes since previous revision		
Date	**Version**	**Change Description**
2017-07-27	1.0	Initial version
2024-06-20	4.4	Final version

Table of Contents

1 Security Target Introduction (ASE_INT)

1.1 Security Target Lite and Target of Evaluation Reference

The title of this document is Security Target Lite Common Criteria EAL6 augmented / EAL6+ M7892 Design Step G12.

This document comprises the Infineon Technologies AG Security Controller (Integrated Circuit IC), M7892 Design Step G12, with specific IC dedicated firmware.

The target of evaluation (TOE) M7892 Design Step G12 is described in the following.

This Security Target Lite has the revision 4.4 and is dated 2024-06-20.

The Target of Evaluation (TOE) is the Infineon Security Controller, M7892 Design Step G12 with specific IC dedicated firmware. The design step of this TOE is G12.

The Security Target Lite is based on the Protection Profile PP-0084 “Security IC Platform Protection Profile with Augmentation Packages” [12] as publicly available for download at https://www.bsi.bund.de and certified under BSI-CC-PP-0084-2014.

The Protection Profile and the Security Target Lite are built in compliance with Common Criteria v3.1.

The Security Target Lite takes into account all relevant current final interpretations.

This TOE concept is based on the architecture, family concept and principles of the Integrity Guard implemented in the controllers by Infineon Technologies AG deemed for high security requiring applications.

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

Table 1: Identification

Object	Version	Date	Registration
Target of Evaluation			M7892 Design Step G12 With FW-Identifier 78.015.18.2 and belonging User Guidance documentation (1).
Protection Profile	1.0	2014-01-13	Security IC Platform Protection Profile with Augmentation Packages BSI-CC-PP-0084-2014
Common Criteria	3.1 Revision 5	2017-04	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Part 2: Security functional requirements Part 3: Security Assurance Components
(1) Chapter 2.2.4 describes briefly the contents of the individual documents of the User Guidance Documentation, while the individual documents are versioned and entitled in chapter 9 literature and references. The listed set of user guidance documents belongs to the TOE.			

Note also that the ROM contains no user data and the user has no access.

The user can identify the TOE and its configuration using the Non-ISO ATR in combination with firmware functions. The TOE answers the Non-ISO ATR with the Generic Chip Identification Mode (GCIM). The GCIM outputs a chip identifier byte, design step, firmware identifier version and further configuration information. The identification data and configuration details are described in the confidential Security Target and in the Family Hardware Reference Manual HRM [1].

This TOE is represented by various products, differentiated by various configuration possibilities, done either by Infineon settings during production or, after delivery, by means of blocking at customer premises.

Despite these configuration possibilities, all products are derived from the equal hardware design results, the M7892 Design Step G12. The GCIM mode is explained and detailed in the user guidance document hardware reference manual HRM [1].

All product derivatives are identically from module design, layout and footprint, but are made different in their possibilities to connect to different types of antennas or to a contact based interface only. Therefore, the TOE is represented and made out of different mask sets:

The main difference between the mask sets of the TOE is on one metal mask (M1) to implement different input capacitances in the analogue part of the radio frequency interface (RFI). This differentiation in the input capacitances allows the connection to a wider range of various antenna types, or respectively, to a contact based interface only. Note that external antennas or interfaces are not part of the TOE.

An overview upon the different mask sets is given in the Confidential Security Target.

To each of the capacitances related mask sets belonging to the TOE, an individual value is assigned, which is part of the data output of the Generic Chip Identification Mode (GCIM). This number is located in the GCIM part individual length byte to clearly differentiate between the mask sets related to the different input capacitances. Thereby, the clear identification of the silicon design step is given.

Confidential

The M7892 Design Step G12 allows for a maximum of configuration possibilities defined by the customer order or his blocking following the market needs. For example, a M7892 Design Step G12 product can come in one project with the fully available SOLID FLASH™ NVM[1] 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 coprocessor SCP, or the asymmetric coprocessor Crypto@2304T, or both, or none of them. 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.
  Note that there is no user available ROM on the TOE.
- The availability of the cryptographic coprocessors.
- The availability of various interface options.
- The degree of freedom of the chip configuration is predefined by Infineon Technologies AG and made available via the order tool.

The user has to provide the 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. I.e. there are no user data in the ROM.

The following listing contains 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. All configurations the TOE is made of and all thereof resulting derivatives have no impact on security and are covered by the certificate.
The below given configuration possibilities are valid unchanged throughout the mentioned different mask sets.

Table 2: TOE Configuration ranges

Module / Feature (User view)	Max-Value (User view)	Min-Value (User view)	User Blocking	User Blocking Step
Memories				
SOLID FLASH™ NVM	Max. 404 KByte	Min. 0 KByte	Yes	1 KByte
RAM for the user	8 KByte	1 KByte	Yes	1 KByte
Modules				
Crypto@2304T	Available	Not available	Yes	On/off
SCP	Available	Not available	Yes	On/off

[1] Infineon® SOLID FLASH™ is an Infineon Trade Mark and stands for the Infineon EEPROM working as Flash memory. The abbreviation NVM is short for Non Volatile Memory.

Confidential

Module / Feature (User view)	Max-Value (User view)	Min-Value (User view)	User Blocking	User Blocking Step
Interfaces				
ISO 7816-3 slave	Available	Not available	Yes	On/off
RFI – ISO 14443 generally	Available	Not available	Yes	On/off
ISO 14443 Type A card mode	Available	Not available	By order only	None
ISO 14443 Type B card mode	Available	Not available	By order only	None
ISO 18092 NFC passive mode	Available	Not available	By order only	None
NRG hardware support for card mode	Available	Not available	By order only	None
SW support for NRG 4k cards[1]	Available	Not available	By order only	None
SW support for NRG 1k cards[1]	Available	Not available	By order only	None

There are further communication modes and blocking options available which are outlined in the confidential Security Target and the confidential User Guidance.

All possible TOE configurations equal and/or within the physical specified ranges as outlined in the confidential Security Target and in the hardware reference manual HRM [1] are covered by the certificate.

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 such as the firmware version. The user guidance document hardware reference manual HRM [1] enables for 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 checking the validity of the certificate.

In addition, a dedicated RMS function allows reading out the present configuration in detail. Together with the programmer's reference manual (PRM) [3], this allows 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.

The TOE consists of the hardware part and the firmware part. The Smartcard Embedded Software, i.e. the operating system and applications are not part of the TOE.

[1] NRG software is not part of the TOE Security Functionality (TSF)

The firmware parts are the RMS, the Service Algorithm Minimal (SAM) the STS firmware for test purpose, the NRG software[1] interface routines. For further details regarding the firmware refer to chapter 2.2.2.Firmware patches (if there are any present) are stored in the SOLID FLASH™ NVM. The TOE has no user ROM. IFX ROM contains no user data.

Please note that the NRG software is not part of the security functionality of the TOE.

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

1.2 Target of Evaluation overview

The TOE comprises the Infineon Technologies Dual Interface Security Controller M7892 Design Step G12 with specific IC dedicated firmware.

The TOE is a member of the Infineon Technologies AG high security controller family meeting the highest requirements in terms of performance and security. A summary product description is given in this Security Target Lite (STL).

This TOE is intended to be used in any application and device requiring the highest level of security, and can be used for example not only as a secure smart card, but also as a secure element on a printed circuit board or similar. The capabilities of this TOE can be used almost everywhere, where highly secure applications are in use and of course in any other application as well. This TOE is deemed for governmental, corporate, transport and payment markets, or wherever a secure root of trust is required. Various types of applications can use this TOE in almost any device or form factor, for example in closed loop logical access controls, physical access controls, secure internet access control and internet authentication, or as multi-application token or simply as encrypted storage.

This member of the high security controller family features a security philosophy focusing on data integrity instead of numerous sensors. By that two main principles combined in close synergy are utilized in the security concept called the “Integrity Guard”. These main principles are the comprehensive error detection, including the dual CPU, and the full encrypted data path, leaving no plain data on the chip. These principles proved that they provide excellent protection against invasive and non-invasive attacks known today.

The intelligent shielding algorithm finishes the layers, finally providing the so called intelligent implicit active shielding “I^2-shield”. This provides physical protection against probing and forcing.

This dual interface controller is able to communicate using either the contact based or the contactless interface. The implemented dual interface provides a maximum flexibility in using following communication protocols respectively methods:

Contact based interfaces

- ISO 7816

  The ISO defined standard contact based communication protocol, using the pads.

Contactless interfaces

- ISO 14443 Type A and Type B

  These are ISO defined proximity contactless protocols using an external antenna and the TOE implemented analogue and digital radio frequency interface.

[1] NRG software is not part of the TOE Security Functionality (TSF)

- ISO/IEC 18092 passive mode,
  The ISO defined proximity contactless protocol using an external antenna and the TOE implemented analogue and digital radio frequency interface.
- NRG software interface,
  The proprietary proximity contactless protocol using an external antenna and the TOE implemented analogue and digital radio frequency interface, as well as the memory part reserved for NRG use.
- And various further communication modes (see Note below).
- Note: All interfaces and protocols can be made available sequentially. How the interfaces are used or combined depends exclusively on the user software. Further communication modes, details and an overview about their combinations are outlined in the confidential Security Target.

The TOE provides a real 16-bit CPU-architecture and is compatible to the MCS®251 instruction set with an execution time faster than a standard MCS®251 microcontroller at the same clock frequency. The major components of the core system are the dual CPU (Central Processing Units), acting as one, the MMU (Memory Management Unit) and MED (Memory Encryption/Decryption Unit). The dual CPU controls each other in order to detect faults and serve by this for data integrity. The TOE implements a full 16 MByte linear addressable memory space for each privilege level, a simple scalable Memory Management concept and a scalable stack size. The flexible memory concept consists of ROM- and Flash-memory as part of the non-volatile memory (NVM), respectively SOLID FLASH™ NVM. For the SOLID FLASH™ NVM the Unified Channel Programming (UCP) memory technology is used.

The RMS library providing some functionality via an API to the Smartcard Embedded Software contains for example SOLID FLASH™ NVM service routines. The Service Algorithm Minimal (SAM) provides functionality for the tearing-safe write into the SOLID FLASH™ NVM. The STS firmware is used for test purposes during start-up. The firmware parts are implemented in the ROM and in access protected areas of the SOLID FLASH™ NVM.

The BSI has changed names and abbreviations for Random Number Generators, which is clarified as follows: The Physical True Random Number Generator (PTRNG), also named True Random Number Generator (TRNG) is a physical random number generator and meets the requirements of the functionality class AIS31 PTG.2, see [16]. It is used for provision of random number generation as a security service to the user and for internal purposes. The produced genuine random numbers can be used directly or as seed for the Deterministic Random Number Generator (DRNG), formerly named as Pseudo Random Number Generator (PRNG). The DRNG respectively PRNG is not in the scope of the evaluation. The TRNG respectively PTRNG is specially designed for smart cards, but can also be used in any other application where excellent physical random data are required.

The two cryptographic coprocessors serve the need of modern cryptography: The symmetric coprocessor (SCP) combines both AES and Triple-DES with dual-key or triple-key hardware acceleration. The Asymmetric Crypto Coprocessor, called Crypto@2304T in the following, is an optimized version of the Crypto@1408 used in the SLE88-family with performance improvements for RSA-2048 bit (4096-bit with CRT) and Elliptic Curve (EC) cryptography. The Crypto@2304T does not implement any security functionality.

To fulfil the highest security standards for smartcards today and also in the future, this TOE implements a progressive digital security concept, which already has been certified in various forerunner processes and which has proven its resistance against attackers with high attack potential. This TOE utilizes digital security features to include customer friendly security, combined

with a robust design overcoming the disadvantages on analogue protection technologies. The TOE provides full on-chip encryption of the data path, covering the core including the ALUs of the CPUs, busses, memories and cryptographic coprocessors leaving no plaintext on the chip. Therefore the attractiveness for attackers is extremely reduced as encrypted signals are of no use for the attacker – neither for manipulation nor for eavesdropping.

In addition, the TOE is equipped with a full error detection capability for the complete data path. The dual CPU approach allows error detection even while processing. A comparator detects whether a calculation was performed without errors. This approach does not leave any parts of the core circuitry unprotected. The concept allows that the relevant attack scenarios are detected, whereas other conditions that would not lead to an error would mainly be ignored. That renders the TOE robust against environmental influences.

Subsequently, the TOE implements what we call intelligent implicit shielding (I^2S). These measures constitute a shield on sensitive and security relevant signals which is not recognizable as a shield. This provides excellent protection against invasive physical attacks, such as probing, forcing or similar.

In this Security Target Lite the TOE is described and a summary specification is given. The security environment of the TOE during its different phases of the lifecycle is defined. The assets are identified which have to be protected through the security policy. The threats against these assets are described. The security objectives and the security policy are defined, as well as the security requirements. These security requirements are built up of the security functional requirements as part of the security policy and the security assurance requirements. These are the steps during the evaluation and certification showing that the TOE meets the targeted requirements. In addition, the functionality of the TOE matching the requirements is described.

The assets, threats, security objectives and the security functional requirements are defined in this Security Target Lite and in the Protection Profile [12] and are referenced here. These requirements from the Protection Profile [12] build up a minimal standard common for all Smartcards.

The security functions are defined here in the Security Target Lite as property of this specific TOE. Here it is shown how this specific TOE fulfils the requirements for the common standard defined in the Common Criteria documents [13], [14], [15] and in the Security IC Platform Protection Profile [12].

2 Target of Evaluation Description

The TOE description helps to understand the specific security environment and the security policy. In this context the assets, threats, security objectives and security functional requirements can be employed. The following is a more detailed description of the TOE than in the Security IC Platform Protection Profile [12] as it belongs to the specific TOE. The Security IC Platform Protection Profile is in general often abbreviated with 'PP' and its version number.

2.1 TOE Definition

This TOE consists of a Security Dual Interface Controllers as integrated circuits (IC), meeting the highest requirements in terms of performance and security. The TOE products are manufactured by Infineon Technologies AG in a 90 nm CMOS-technology (L90).

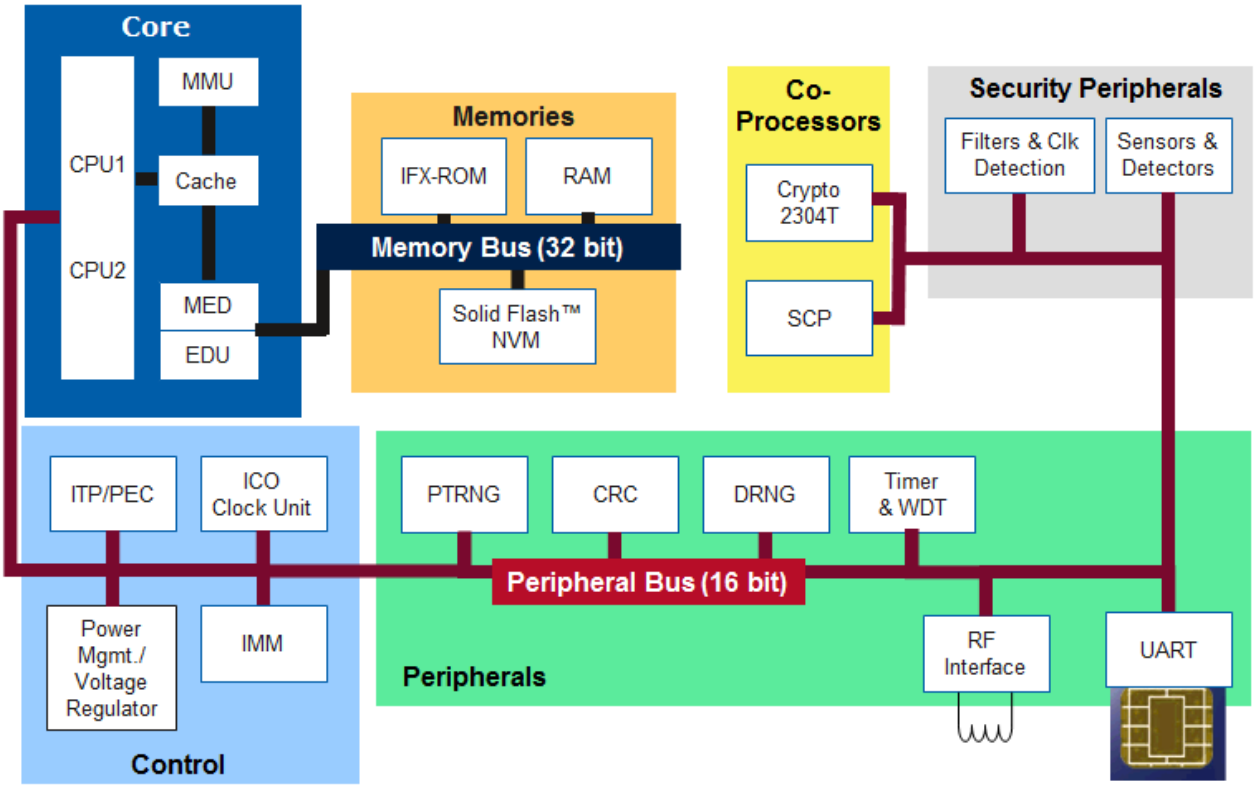
This TOE is intended to be used in smart cards and any other form factor for particularly applications requiring highest levels of security and for its previous use as developing platform for smart card operating systems according to the lifecycle model from Protection Profile [12].

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 consists of a core system, memories, coprocessors, peripherals, security peripherals and a control block.

Following diagram provides a simplified overview upon the hardware subsystems which are briefly described below:

Figure 1: Simplified block diagram of the TOE



The major components of the core system are the dual CPU (Central Processing Units) including the internal encryption leaving no plain data anywhere, the MMU (Memory Management Unit), the MED (Memory Encryption/Decryption Unit) and the CACHE memory.

The CPU – here the two processor parts (CPU1 and CPU2) are seen from functional perspective as one - is compatible with the instruction set of the forerunner family 66-PE and is therefore also compatible to the SAB 80251 instruction set (8051 is a subset hereof) and to the MCS® 251 instruction set which is enhanced. Anyhow, the dual-CPU is faster than the standard processor at the equal clock frequency. It provides additional powerful instructions for smart card or other applications. It thus meets the requirements for the new generation of operating systems. Despite its compatibility the CPU implementation is entirely proprietary and not standard.

The two processor parts of the CPU control each other in order to detect faults and maintain by this the data integrity. A comparator detects whether a calculation was performed without errors and allows error detection even while processing. Therefore the TOE is equipped with a comprehensive error detection capability, which is designed to leave no relevant parts of the circuitry unprotected.

The CPU accesses the memory via the integrated Memory Encryption and Decryption unit (MED), which transfer the data from the memory encryption schema to the CPU encryption schema without decrypting into intermediate plain data. The error detection unit (EDU) automatically manages the error detection of the individual memories and detects incorrect transfer of data between the memories by means of error code comparison.

The access rights of the firmware, user operating system and application to the memories are controlled and enforced by the memory management unit (MMU).

The CACHE memory – or simply, the CACHE – is a high-speed memory-buffer located between the CPU and the (core external) main memories holding a copy of some of the memory contents to enable access to the copy, 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. All CACHE systems own their usefulness to the principle of locality, meaning that programs are inclined to utilize a particular section of the address space for their processing over a short period of time. By including most or all of such a specific area in the CACHE, system performance can be dramatically enhanced. The implemented post failure detection identifies and manages errors if appeared during storage.

The controllers of this TOE store both code and data in a linear 16-MByte memory space, allowing direct access without the need to swap memory segments in and out of memory using a memory management unit.

The memory block contains the ROM, RAM and the SOLID FLASH™ NVM. All data of the memory block is encrypted and all memory types are equipped with an error detection code (EDC), the SOLID FLASH™ NVM in addition with an error correction code (ECC). Errors in the memories are automatically detected (EDC) and in terms of the SOLID FLASH™ NVM 1-Bit-errors are also corrected (ECC). The TOE uses also Special Function Registers (SFR). These SFR registers are used for general purposes and chip configuration. These registers are located in the SOLID FLASH™ NVM as configuration area page.

The non-volatile ROM contains the firmware parts and is accessible for Infineon only, while the RAM is a volatile memory and used by the core.

The coprocessor block contains the two coprocessors for the cryptographic operations implemented on the TOE: The Crypto@2304T for calculation of asymmetric algorithms like RSA and Elliptic Curve (EC) and the Symmetric Cryptographic Processor (SCP) for dual-key or triple-key triple-DES and AES calculations. The Crypto@2304T does not implement any security

functionality. These coprocessors are especially designed for smart card applications with respect to the security and power consumption, but can of course be used in any other application of form factor where suitable. 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 Crypto@2304T, or with both crypto 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 than the cryptographic operations provided by them; it is exactly equivalent to the situation where the user decides just not to use the cryptographic coprocessors.

The security peripherals block contains the small remaining set of sensors and filters. This small set of sensors is left in order to detect excessive deviations from the specified operational range, while not being over-sensitive. These features do not need adjustment or calibration and makes the chip even more robust. Conditions that would not be harmful for the operation would in most cases not influence the proper function. The small set of sensors is not necessary for the chip security but serve for robustness. Having the integrity guard concept in place, the sensors - except a single one - are no more required for the TOE security. The only sensor left, contributing to a security mechanism, is the frequency sensor. All other sensors are assigned to be security supporting only.

The filters are on board to make the TOE more robust against perturbations on the supply lines.

The block control is constituted out of the modules Interrupt Controller (ITP) and Peripheral Event Channel controller (PEC), the modules supplying clock (ICO) and Power Management / Voltage regulator, the Interface Management Module combined with the UmSLC. The UmSLC enables for checking the proper functions of modules and subsystems and checks the correct operation of the TOE.

The implemented clock management is optimized to reduce the overall power consumption. Contactless products provide a low-power halt mode for operation with reduced power consumption. The Clock Unit (CLKU) supplies the clocks for all components of the TOE. The Clock Unit can work in an internal and external clock mode. The system frequency can be configured and this enables a programmer to choose the best-fitting frequency for an application in consideration of a potential current limit and a demanded application performance.

The peripherals block is constituted out of PTRNG, DRNG, CRC, Timer & WDT, the RFI and the UART. The modules are briefly described in the following:

The TRNG respectively PTRNG is specially designed for smart cards, but can also be used in any other application where excellent physical random data is required. The TRNG respectively PTRNG fulfils the requirements from the functionality class PTG.2 of the AIS31 and produces genuine random numbers which then can be used directly or as seeds for the Deterministic Random Number Generator (DRNG), former named as Pseudo Random Number Generator (PRNG). The DRNG respectively PRNG is not in the scope of the evaluation.

The cyclic redundancy check (CRC) module is a checksum generator. The checksum is a unique number associated with a message or another block of data consisting of several bytes. The idea of the CRC method is to treat the input data as a binary bit stream and divide that stream by a fixed binary number. The remainder of that division is the CRC checksum.

The timer enables for easy implementation of communication protocols such as T=1 and all other time-critical operations. The timer can be programmed for particular applications, such as measuring the timing behavior of an event. Timer events can

generate interrupt requests to be used for peripheral event channel data transfers. The watchdog is implemented to provide the user some additional control of the program flow. More details are given in the hardware reference module HRM [1].

This dual interface controller is able to communicate using either the contact based or the contactless interface. The implemented dual interface provides a maximum flexibility in using following communication protocols respectively methods:

Contact based interfaces

- ISO 7816

  The ISO defined standard contact based communication protocol, using the pads.

Contactless interfaces

- ISO 14443 Type A and Type B

  The ISO defined proximity contactless protocols using an external antenna and the TOE implemented analogue and digital radio frequency interface.
- ISO/IEC 18092 passive mode

  The ISO defined proximity contactless protocol using an external antenna and the TOE implemented analogue and digital radio frequency interface.
- NRG software interface

  The proprietary proximity contactless protocol using an external antenna and the TOE implemented analogue and digital radio frequency interface, as well as the memory part reserved for NRG use.
- And various further communication modes (refer to Note).

Note: All interfaces and protocols can be made available sequentially. How the interfaces are used or combined depends exclusively on the user software. Further communication modes, details and an overview about their possible parallel usage are outlined in the confidential Security Target.

This flexibility enables for example also for bypassing the coding/decoding of the RFI and leaves its interpretation up to the software. By that further and also proprietary protocols can be implemented by the user software. Note that anything contacting from outside the chip and also any user software managing the communication are not part of this TOE.

The individual combinations of the interface options are depicted in the confidential Security Target.

Supporting a NRG software interface application requires a dedicated small space of memory. In this context and depending on user's choice, various memory sections each of 1 up to 4 kBytes can be defined. The number and location of these memory sections is simply limited by the available SOLID FLASH™ NVM space. Also these memory sections are read/write protected and are defined and generated by the user.

The bus system comprises two separate bus entities: a memory bus supporting high-speed communication between the Core and Memories, and a peripheral bus for communication with the peripherals.

Subsequently, an intelligent shielding algorithm finishes the layers, finally providing the so called intelligent implicit active shielding "I^2-shield". This provides physical protection against probing and forcing.

The STS (self-test software), RMS (Resource Management System), Service Algorithm Minimal (SAM), the NRG software interface compose the TOE's firmware stored in the ROM and the patches hereof, in the SOLID FLASH™ NVM. All mandatory functions for internal testing, production usage and start-up behavior (STS), and also the RMS and SAM functions are grouped together in a common privilege level. These privilege levels are protected by a hardwired Memory Management Unit (MMU) setting.

The TOE sets a new, improved standard of integrated security features, thereby meeting the requirements of all smart card and other related applications or form factors, such as information integrity, access control, mobile telephone and identification, as well as uses in electronic funds transfer and healthcare systems.

To sum up, the TOE is a powerful dual interface security controller with a large amount of memory and special peripheral devices with improved performance, optimized power consumption, free to choose contact based or contactless operation, at minimal chip size while implementing high security. It therefore constitutes the basis for future smart card and other related applications or form factors.

2.2 Scope of the TOE

The TOE comprises several types of hardware each differing by slight mask set changes to allow for maximum flexibility in terms of connection to antennas and implementation into different IC package and module types. All these changes have no influence on the security or any security policy related to the TOE.

Therefore, this TOE includes:

- The silicon die, respectively the Integrated Circuit (IC) respectively the hardware of this TOE.
- The TOE is also delivered in various configurations, achieved by means of blocking depending on the customer order.
- The according equal firmware on all derivatives
- User's guidance documentation including hardware, software, secure coding, and other reference manuals.

All product derivatives of this TOE, including all configuration possibilities differentiated by the GCIM data and the configuration information output, are manufactured by Infineon Technologies AG. In the following descriptions, the term "manufacturer" stands short for Infineon Technologies AG, the manufacturer of the TOE.

2.2.1 Hardware of the TOE

The hardware part of the TOE as defined in the Protection Profile [12] is comprised of:

Core System

Proprietary dual CPU implementation being comparable to the 80251 microcontroller architecture from functional perspective and with enhanced MCS® 251 instruction set

CACHE with Post Failure Detection

Memory Encryption/Decryption Unit (MED) and Error Detection Unit (EDU)

Memory Management Unit (MMU)

Memories

SOLID FLASH™ NVM, the Electrically Erasable and Programmable Read Only Memory (EEPROM) implementing the Unified Channel Programming concept (UCP)

Read-Only Memory (ROM), not available for the user

Random Access Memory (RAM)

Peripherals

True Random Number Generator (TRNG) respectively

Physical True Random Number Generator (PTRNG)

Deterministic Random Number Generator (DRNG) respectively

Pseudo Random Number Generator (PRNG)

Watchdog and Timers

Universal Asynchronous Receiver/Transmitter (UART)

Checksum module (CRC)

RF interface (radio frequency power and signal interface)

Control

Dynamic Power Management

Internal Clock Oscillator (ICO)

Interrupt and Peripheral Event Channel Controller (ITP and PEC)

Interface Management Module (IMM)

User mode Security Life Control (UmSLC)

Voltage Regulator

Coprocessors

Crypto@2304T for asymmetric algorithms like RSA and EC (optionally blocked). The Crypto@2304T does not implement any security functionality.

Symmetric Crypto Coprocessor for DES and AES Standards (optionally blocked)

Security Peripherals

Filters

Sensors

Buses

Memory Bus

Peripheral Bus

2.2.2 Firmware and software of the TOE

The entire firmware of the TOE consists of different parts:

One part comprises the RMS and SAM routines used for providing the chip resource management interface for the user. The routines are used for tearing-safe handling of the SOLID FLASH™ NVM, user testing of the security functions and error correction (Resource Management System, IC Dedicated Support Software in PP [12]). These routines are stored in a reserved area of the ROM, while belonging patches (if any) are located in the SOLID FLASH™ NVM. There is no ROM available for the user.

The second part is the STS, consisting of test and initialization routines (Self-Test Software, IC Dedicated Test Software in PP [12]). The STS routines are stored in the ROM and the belonging patch is located in the access protected SOLID FLASH™ NVM area. The STS is not accessible for the user software.

The fourth part are the NRG software interface routines. Note that these routines are always present, but deactivated, in case of the derivatives come without RF interface. Thus the user software interface is identical in both cases and consequently the related NRG interface routines can be called in each of the derivatives. In case the related NRG software interface routines are called in derivatives without RF interface, an error code is returned. In the other case the related function is performed.

All parts of the firmware above are combined together by the TOE generation process to a single file and stored then in the data files, the TOE is produced from. This comprises the firmware files for the ROM, where only Infineon Technologies AG has access, as well as the data to be flashed in the SOLID FLASH™ NVM.

2.2.3 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, particularly the contacted RES, I/O, CLK lines and supply lines VCC and GND, as well as by the contactless RF interface. The contact based communication is according to ISO 7816/ETSI/EMV.

  A further electrical interface is constituted by the La and Lb pads used for the antenna connection. More information is given in the confidential Security Target.
- The RF interface (radio frequency power and signal interface) enables contactless communication between a PICC (proximity integration chip card, PICC) and a PCD reader/writer (proximity coupling device, PCD).

  Power supply is received and data are received or transmitted by an antenna which consists of a coil with a few turns directly connected to the IC. Depending on customer orders the contactless interface options are set by means of blocking either at Infineon premises or at the premises of the user.
- The data-oriented I/O interface to the TOE is formed by the I/O pad and by the various RF options.
- 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 on one hand by the RMS routine calls and on the other by the instruction set of the TOE.
- The interface of the TOE to the test routines is formed by the STS test routine call, i.e. entry to test mode (STS-TM entry).

2.2.4 Guidance documentation

The guidance documentation consists of the listing given in the chapter 9. The exact versions of these documents are also given there, as well as the document number referenced here. The documents provide guidance as follows:

- The Hardware Reference Manual HRM [1] is the user data book of the TOE and contains the relevant module, function and feature description.
- The document Family Programmers Reference Manual PRM [3] describes the usage and interface of the Resource Management System RMS.
- The document Crypto@2304T User Manual [7] describes the architecture of cryptographic coprocessor on register level. It also provides a functional description of the register architecture, instruction set and gives programming guidance.
- The document M7892 Security Guidelines [8] represents the collection of recommendations for the software programmers.
- The document Errata sheet [9] contains the description of all interfaces of the software to the hardware relevant for programming the TOE. The SLE70 Family Errata Sheet can be changed during the life cycle of the TOE. This is reported in a monthly updated list provided from Infineon Technologies AG to the user.
- The document Advanced Mode for NRG SAM (AMM) [11] describes how to apply this type of communication. This documentation is provisioned to the user if the AMM option has been ordered and is an addendum to the Hardware Reference Manual HRM [1].

Finally the certification report may contain an overview of the recommendations to the software developer regarding the secure use of the TOE. These recommendations are also included in the ordinary documentation.

2.2.5 Forms of delivery

The TOE can be delivered in form of complete modules, with or without inlay mounting, in form of plain wafers or in any IC case (for example TSSOP28, VQFN32, VQFN40, CCS-modules, etc.) or in bare dies or whatever type of IC package or even in no package. 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 [12]. 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.

More information on the forms of delivery of the TOE components is given in the confidential Security Target.

2.2.6 Production sites

The TOE may be handled in different production sites but the silicon of this TOE is produced in dedicated production sites only. To distinguish the different production sites of various products in the field, this production site is coded into the Generic Chip Ident Mode (GCIM) data. The exact coding of the generic chip identification data is given in the confidential Security Target.

3 Conformance Claims (ASE_CCL)

3.1 CC Conformance Claim

This Security Target Lite (STL) and the TOE claim conformance to Common Criteria version v3.1 part 1 [13], part 2 [14] and part 3 [15].

Conformance of this ST is claimed for:

Common Criteria part 2 extended and Common Criteria part 3 conformant.

The extended Security Functional Requirements are defined in chapter 6.

3.2 PP Claim

The Security IC Platform Protection Profile with Augmentation Packages is registered and certified by the Bundesamt für Sicherheit in der Informationstechnik[1] (BSI) under the reference:

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 [12]. They are all drawn from Part 3 of the Common Criteria version v3.1.

The Protection Profile [12] requires the **strict conformance** for the ST claiming conformance to this PP. This is mentioned in section 2.2 of [12].

3.3 Package Claim

This Security Target Lite claims conformance to the following packages from the Security IC Protection Profile with Augmentation Packages [12]:

Depending on the availability of the optional Symmetric Crypto Coprocessor, the ST is

- "TDES" augmented; see [12], Section 7.4.1 and
- "AES" conformant; see [12], Section 7.4.2.

The Security Target Lite is augmented compared to the above mentioned packages, as it contains all SFRs included in the packages and adds additional SFRs.

The assurance level for the TOE is:

EAL6 augmented (EAL6+) with the component ALC_FLR.1.

The augmentation goes beyond the PP [12] and is achieved – with regard to CCv3.1 Part 3: Security assurance components – as follows:

Table 3: Augmentations of the assurance level of the TOE

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

The targeted EAL6+ level includes already the augmentations of the PP [12] AVA_VAN.5 and ALC_DVS.2.

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

3.4 Conformance Rationale

This Security Target Lite claims **strict conformance** to the PP [12].

The Target of Evaluation (TOE) is a typical security IC as defined in PP chapter 1.2.2 comprising:

- The circuitry of the IC (hardware including the physical memories)
- Configuration data, initialization data related to the IC Dedicated Software and the behavior of the security functionality
- The IC Dedicated Software with the parts
- The IC Dedicated Test Software,
- The IC Dedicated Support Software.
- The associated user's guidance documentation.

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

3.4.1 Security Problem Definition

Following the PP [12], the security problem definition is enhanced by adding:

- Additional threats (for details refer to 4.1.1).
- Additional organization security policy (for details refer to 4.2.1).
- And additional augmented assumption (for details refer to 4.3.1).

Aside these add-ons, the security problem definition of this Security Target Lite is consistent with the statement of the security problem definition in the PP [12], as the Protection Profile [12] demands strict conformance.

The threats and OSPs of the Security Target Lite are a superset of the ones defined in the PP [12]. Although an additional assumption is defined in the Security Target Lite compared to the PP [12], the Security Target Lite is still strict conformant to the PP [12], as the added assumption does neither mitigate a threat, which is meant to be addressed by a security objective for the TOE nor does it fulfils an OSP, which is meant to be addressed by the security objectives for the TOE.

3.4.2 Security Objective

Compared to the PP [12], the security objectives of this Security Target Lite are enhanced by adding supplemental security objectives (for details refer to 5). These modifications are necessary due to additional security functionalities, coming from the memory access control (O.Mem-Access).

The Security Target Lite is still conformant to the PP [12], as it is permissible for a Security Target Lite to contain additional security objectives compared to the PP.

3.4.3 Summary

Due to the above rationale, the Security Problem Definition (refer to section 4) and the Security Objectives (refer to section 5) are strict conformant to the PP [12].

The Security Target Lite augments the required assurance package EAL4+ augmented with AVA_VAN.5 and ALC_DVS.2 of the PP [12] to EAL6+ augmented with ALC_FLR.1. All assurance components required for the PP [12] are also contained or a hierarchically higher assurance component used in this ST.

All security functional requirements defined in the PP [12] are included and completely defined in this ST. The augmented security functional requirements are listed in Table 15.

The following security functional requirements are included and completely defined in the Extended Component Definition of this ST, section 6.

- FPT_TST.2 “Subset TOE security testing“ (Requirement from [12])

All assignments and selections of the security functional requirements are either done in the PP [12] or in this Security Target Lite (please refer to section 7.1).

3.5 Application Notes

The functional requirement FCS_RNG.1 is defined in the Protection Profile [12] and complete in this ST according to “Anwendungshinweise und Interpretationen zum Schema (AIS)” respectively “Functionality classes and evaluation methodology for physical random number generators”, AIS31 [16].

4 Security Problem Definition (ASE_SPD)

The content of the PP [12] applies to this chapter completely.

4.1 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 [12] section 3.2.

Table 4: Threats according PP [12]

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

4.1.1 Additional Threat due to TOE specific Functionality

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

The Smartcard Embedded Software is responsible for its User Data 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.

Table 5: Additional threat due to TOE specific functions and augmentations

T.Mem-Access	Memory Access Violation

4.1.2 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 deficiency of random numbers

SC4 is covered by an additional security service provided by this TOE which is the availability of random numbers. These random numbers are generated either by a physical true random number (PTRNG) or a deterministic random number (DRNG) generator or by both, if the true random number output is used as source for the seed input of the deterministic random number generator. Note that the generation of random numbers is a requirement of the PP [12].

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 photomasks.

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
- photomasks and products in any form,

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

For details see PP [12] section 3.1.

4.2 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.

Due to the augmentations of PP [12] and the chosen packages additional policies are introduced and described in the next chapter.

Table 6: Organizational Security Policy according to PP [12]

P.Process-TOE	Identification during TOE Development and Production

4.2.1 Augmented Organizational Security Policy

Due to the augmentations of the PP [12] 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 (introduced in the packages for cryptographic services of the PP [12]; section 7.4):

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:

This TOE can come with both cryptographic coprocessors accessible, or with a blocked SCP or with a blocked Crypto@2304T, 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 computational supported by hardware are possible. No accessibility of the deselected cryptographic coprocessors is without impact on any other security policy of the TOE besides the cryptographic functionality provided by the blocked component; it is exactly equivalent to the situation where the user decides just not to use the cryptographic coprocessors.

Table 7: Organizational Security Policies according to packages of the PP [12]

P.Crypto-Service	Cryptographic services of the TOE

4.3 Assumptions

The TOE assumptions on the operational environment are defined and described in PP [12] section 3.4.

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

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.

Table 8: Assumptions according to PP [12]

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

The support of cipher schemas needs to make an additional assumption.

4.3.1 Augmented Assumptions

Due to support of cipher schemas an additional assumption needs to be made compared to the PP [12].

Usage of Key-dependent Functions

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 see PP [12] section 3.4.

Table 9: Additional assumption due to TOE specific functions and augmentations

A.Key-Function	Usage of Key dependent Functions

5 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) as well as
- SG2 maintain the confidentiality of user data (when being processed and when being stored in the TOE's protected memories).
- SG3 maintain the correct operation of the security services provided by the TOE for the Security IC Embedded Software.
- SG4 provide true random numbers.

5.1 Security objectives for the TOE

The security objectives of the TOE are defined and described in PP [12] sections 4.1, 7.4.

Table 10: Objectives for the TOE according to PP [12]

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.TDES	Cryptographic service Triple-DES
O.AES	Cryptographic service AES

Note:

O.TDES and O.AES only apply if the TOE is ordered with an accessible SCP.

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.

Table 11: Additional objectives due to TOE specific functions and augmentations

O.Mem-Access	Area based Memory Access Control

5.2 Security Objectives for the Development and Operational Environment

The security objectives for the security IC Embedded Software development environment and the operational environment are defined in PP [12] section 4.2, 4.3.

Table 12: Security objectives for the environment according to PP [12]

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

5.2.1 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 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 have to be clarified. The treatment of user data of the Composite TOE is also required when a multi-application operating system is implemented as a 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.

5.3 Security Objectives Rationale

The security objectives rationale of the TOE are defined and described in PP [12] section 4.4. For the additional objectives of this ST a rational is provided below.

Table 13: Security Objective Rationale

Assumption, Threat or Organizational Security Policy	Security Objective
A.Key-Function	OE.Resp-Appl

T.Mem-Access	O.Mem-Access
P.Crypto-Service	O.TDES
	O.AES

Compared to the PP [12] 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. The user has appropriate means to generate a key in a safe environment and import it to the TOE. 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..

Compared to the PP [12] an enhancement regarding memory area protection has been established. The clear definition of privilege levels for operated software establishes the clear separation of different restricted memory areas for running the firmware, downloading and/or running the operating system and to establish a clear separation between different applications. Nevertheless, it is also possible to define a shared memory section where separated applications may exchange defined data. The privilege levels clearly define by using a hierarchical model the access right from one level to the other. These measures ensure that the threat T.Mem-Access is clearly covered by the security objective O.Mem-Access.

The PP [12] includes the organizational security policy P.Crypto-Service Cryptographic services of the TOE in a different extend as it formalizes the objectives O.TDES, O.AES.

Since O.TDES, O.AES require the TOE to implement exactly the same security functionality as required by P.Crypto-Service; the organizational security policy is covered by the objectives.

For the objective O.TDES a concrete standard reference (NIST) with operational modes is given the implementation must follow and also the cryptographic key destruction is regulated. The implementation complies to the given security functional requirements and the objective O.TDES is met.

For the objective O.AES a concrete standard reference (NIST) with a selection of key lengths is given the implementation must follow and also the cryptographic key destruction is regulated. The implementation complies to the given security functional requirements and the objective O.AES is met.

6 Extended Component Definition (ASE_ECD)

The following extended components are 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 extended components FCS_RNG, FMT_LIM, FAU_SAS and FDP_SDC are defined and described in PP [12] section 5. The component FPT_TST.2 is defined in the following.

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

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

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

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

6.2 Definition of FPT_TST.2

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

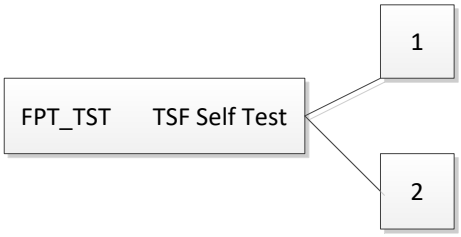
This security functional component is used instead of the functional component FPT_TST.1 from Common Criteria Part 2. For the user it is important to know which security functions or mechanisms can be tested. The functional component FPT_TST.1 does not mandate to explicitly specify the security functions being tested. In addition, FPT_TST.1 requires verifying the integrity of TSF data and stored TSF executable code which might violate the security policy.

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

6.3 TSF self-test (FPT_TST)

Family Behavior The Family Behavior is defined in [14] section 15.14 (442, 443).

Component leveling



FPT_TST.1: The component FPT_TST.1 is defined in [14] 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 security testing**
Hierarchical to:	No other components.
Dependencies:	No dependencies to other components.
FPT_TST.2.1	The TSF shall run a suite of self-tests [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, and/or at the conditions [assignment: conditions under which self-test should occur]] to demonstrate the correct operation of [assignment: functions and/or mechanisms].

7 Security Requirements (ASE_REQ)

For this section the PP [12] section 6 can be applied completely.

7.1 TOE Security Functional Requirements

The security functional requirements (SFR) for the TOE are defined and described in the PP [12] section 6.1, 7.4 and in the following description.

Following table provides an overview of the functional security requirements of the TOE, defined in the PP [12] section 6.1, 7 and 7.4. In the last column it is marked if the requirement is refined. The refinements are also valid for this ST.

Table 14: Security functional requirements defined in PP [12]

Security Functional Requirement		Refined y/n or Defined in PP [12]
FRU_FLT.2	“Limited fault tolerance“	Yes
FPT_FLS.1	“Failure with preservation of secure state”	Yes
FMT_LIM.1	“Limited capabilities”	No
FMT_LIM.2	“Limited availability”	No
FAU_SAS.1	“Audit storage”	Defined
FDP_SDC.1	“Stored data confidentiality”	Defined
FDP_SDI.2	“Stored data integrity monitoring and action”	No
FPT_PHP.3	“Resistance to physical attack”	Yes
FDP_ITT.1	“Basic internal transfer protection”	Yes
FPT_ITT.1	“Basic internal TSF data transfer protection	Yes
FDP_IFC.1	“Subset information flow control”	No
FCS_RNG.1	“Random number generation”	Defined
FCS_COP.1/TDES	“Cryptographic operation – TDES”	No
FCS_CKM.4/TDES	“Cryptographic key destruction – TDES”	No
FCS_COP.1/AES	“Cryptographic operation – AES”	No
FCS_CKM.4/AES	“Cryptographic key destruction – AES”	No

Following table provides an overview about the augmented security functional requirements, which are added additional to the TOE and defined in this ST. All requirements are taken from Common Criteria Part 2 [14], with the exception of the requirement FPT_TST.2 which is defined in this ST completely.

Table 15: Augmented security functional requirements

Security Functional Requirement	
FPT_TST.2	“Subset TOE security testing“
FDP_ACC.1	“Subset access control”

Security Functional Requirement	
FDP_ACF.1	“Security attribute based access control”
FMT_MSA.1	“Management of security attributes”
FMT_MSA.3	“Static attribute initialisation”
FMT_SMF.1	“Specification of Management functions”
FDP_SDI.1	“Stored data integrity monitoring”

All assignments and selections of the security functional requirements of the TOE are done in PP [12] and in the following description.

7.1.1 Extended Components FCS_RNG.1 and FAU_SAS.1

7.1.1.1 FCS_RNG

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 [12]. This family describes the functional requirements for random number generation used for cryptographic purposes.

Please note that the national regulation are outlined in PP [12] chapter 7.5.1 and in AIS31 [16]. These regulations apply for this TOE.

The functional requirement FCS_RNG.1 is fulfilled for FCS_RNG.1 as follows and is defined in the Protection Profile [12] according to “AIS31 Anwendungshinweise und Interpretationen zum Schema (AIS)” respectively in English language “A proposal for: Functionality classes for random number generators” [16].

FCS_RNG.1	**Random Number Generation**
Hierarchical to:	No other components
Dependencies:	No dependencies
FCS_RNG.1	Random numbers generation **Class PTG.2** according to [16]
FCS_RNG.1.1	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	The TSF shall provide *numbers in the format 8- or 16-bit* that meet
PTG.2.6	*Test procedure A, as defined in [16] 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.*

Note:

The physical random number generator 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, and chapter 4.9.2.

7.1.1.2 FAU_SAS

The PP [12] defines additional security functional requirements with the family FAU_SAS of the class FAU (Security Audit). This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

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

FAU_SAS.1	**Audit Storage**
Hierarchical to:	No other components
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide *the test process before TOE Delivery* with the capability to store *the Initialization Data and/or Pre-personalization Data and/or supplements of the Security IC Embedded Software* in the *not changeable configuration page area and non-volatile memory.*

7.1.2 Subset of TOE testing

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

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

FPT_TST.2	Subset TOE security testing
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.2.1	The TSF shall run a suite of *self-tests at the request of the authorized user to demonstrate the correct operation of the alarm lines and/or following environmental sensor mechanisms:* • *information is given in the confidential Security Target*

7.1.3 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 management unit (MMU) is documented in section 4 in the hardware reference manual HRM [1].

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 read, write, delete and execute accesses of software running at the privilege levels as defined below. Any access is controlled, regardless whether the access is on code or data or a jump on any other privilege level outside the current one.

The access rights are controlled by the MMU and related to the privilege level. More details are given in the confidential Security Target.

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 (software running at the defined and assigned privilege levels), all objects (data including code stored in memories) and all the operations defined in the Memory Access Control Policy, i.e. privilege levels*.

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 the IFX, OS1 and OS2 privilege levels required to securely operate the chip. This includes also privilege levels running interrupt routines.* *- Software running at the privilege levels containing the application software* *Object*: *- Data including code stored in memories* *Attributes*: *- The memory area where the access is performed to 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, during or after 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*[1] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow *any subject, provided that the Memory Access Control Policy is enforced and the necessary access is therefore allowed*[2], to specify alternative initial values to override the default values when an object or information is created.

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

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

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 security management functions*: access the configuration registers of the MMU*.

7.1.4 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 7.3.1.1 “Dependencies of Security Functional Requirements”.

[1] The static definition of the access rules is documented in the hardware reference manual as listed in chapter 1.1.

[2] The Smartcard Embedded Software is intended to set the memory access control policy.

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

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

Note:

This TOE can come with both crypto coprocessors accessible, or with a blocked SCP or with a blocked Crypto@2304T, or with both crypto 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 Crypto@2304T is blocked, no RSA and EC computation supported by hardware is possible. 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.

7.1.4.1 Preface regarding Security Level Related to Cryptography

The strength of the cryptographic algorithms was not rated in the course of the product certification (see [33] Section 9, Para.4, Clause 2). But cryptographic functionalities with a security level of lower than 120 bit 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.

7.1.4.2 Triple-DES Operation

The DES Operation of 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 – 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 Cryptographic key destruction
FCS_COP.1.1/TDES	The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *TDES in the Electronic Codebook Mode (ECB),* in the *Cipher Block Chaining Mode (CBC), in the Blinding Feedback Mode (BLD), and in the Recrypt Mode* and cryptographic key sizes *of 2 x 56 bit or 3 x 56 bit* that meet the following standards: • *TDES:* *National Institute of Standards and Technology (NIST) SP 800-67 Rev. 2 [20]* • *ECB, CBC:* *National Institute of Standards and Technology (NIST) SP 800-38A [21]* • *Recrypt Mode, BLD:* *Proprietary, description given in the hardware reference manual HRM [1]*

Note:

The BLD and Recrypt operation modes are described in the hardware reference manual HRM [1] while the implementations of the other modes follow the referenced standards. Also the BLD is compliant to the referenced standards but is operated in a masked way.

Note:

This SFR applies to the solely hardware-based TDES and is not applicable if the TOE is delivered with a blocked SCP. Please consider that statement in chapter 7.1.4.1.

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:

This SFR applies to the solely hardware-based TDES and is not applicable if the TOE is delivered with a blocked SCP. 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.

7.1.4.3 AES Operation

The AES Operation of 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 – AES**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/AES	The TSF shall perform *decryption and encryption* in accordance with a specified cryptographic algorithm *AES in ECB mode and CBC mode* and cryptographic key sizes of *128 bit, 192 bit and 256 bit* that meet the following standards: • *National Institute of Standards and Technology (NIST) SP 800-38A [21]* • *FIPS 197 [31]*

Note:

This SFR refers to the solely hardware-based AES calculation and is not applicable if the TOE is delivered with a blocked SCP. Please consider the statement of chapter 7.1.4.1.

FCS_CKM.4/AES	**Cryptographic key destruction – AES**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_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:

This SFR refers to the solely hardware-based AES and is not applicable if the TOE is delivered with a blocked SCP. 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.

7.1.5 Data Integrity

The TOE shall meet the requirement “Stored data integrity monitoring (FDP_SDI.1)” as specified below:

FDP_SDI.1	**Stored data integrity monitoring**
Hierarchical to:	No other components
Dependencies:	No dependencies
FDP_SDI.1.1	The TSF shall monitor user data stored in containers controlled by the TSF for *inconsistencies between stored data and corresponding EDC* on all objects, based on the following attributes: *EDC values for RAM, ROM and the SOLID FLASH™ NVM*.

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- and/or more-bit-errors* on all objects, based on the following attributes: *corresponding EDC value for the memories and error correction for the SOLID FLASH™ NVM.*
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall *correct 1 bit errors in the SOLID FLASH™ NVM automatically and inform the user about more bit errors.*

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, ROM, Cache and SOLID FLASH™ NVM.*

7.2 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 [12] is expressed with bold letters.

Table 16: Assurance Components

Aspect	Acronym	Description	Refinement
Development	ADV_ARC.1	Security Architecture Description	In PP [12]
	ADV_FSP.5	**Complete semi-formal functional specification with additional error information**	in ST
	ADV_IMP.2	**Complete mapping of the implementation representation of the TSF**	in ST
	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 [12]
	AGD_PRE.1	Preparative procedures	in PP [12]
Life-Cycle Support	**ALC_CMC.5**	**Advanced support**	in ST
	ALC_CMS.5	**Development tools CM coverage**	in ST
	ALC_DEL.1	Delivery procedures	in PP [12]
	ALC_DVS.2	Sufficiency of security measures	in PP [12]
	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	

Aspect	Acronym	Description	Refinement
	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
	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 [12]

7.2.1 Refinements

Some refinements are taken unchanged from the PP [12]. In some cases a clarification is necessary. In the table above an overview is given where the refinement is done.

The refinements from the PP [12] have to be discussed here in the Security Target Lite, as the assurance level is increased. The refinements from the PP [12] are included in the chosen assurance level EAL 6 augmented with ALC_FLR.1.

7.2.1.1 Development (ADV)

ADV_IMP Implementation Representation:

The refined assurance component 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 component 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 [12] 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 component requires a functional description of the TSFIs and there assignment to SFR-enforcing, SFR-supporting, SFR-non-interfering, including related error messages. The enhancement of ADV_FSP.5 requires additionally a complete semi-formal functional specification with additional error information. In addition the component 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 [12] but constitute an enhancement of it. By that the aspects of ADV_FSP.4 and its refinement in the PP [12] apply also here. The assurance and evidence was provided accordingly.

7.2.1.2 Life-cycle Support (ALC)

ALC_CMS Configuration Management Scope:

The Security IC embedded firmware is part of TOE and delivered together with the TOE as the firmware is stored in the ROM and/or SOLID FLASH™ NVM. The presence of the optional parts belongs to the user order. The firmware delivered with the TOE is controlled entirely by Infineon Technologies. 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 [12] 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 ALC_CMC.5 constitute an enhancement of ALC_CMC.4 and therefore the aspects and ALC_CMC.4 refinements in the PP [12] remain valid. The assurance and evidence was provided.

7.2.1.3 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 [12].

This assurance component 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 [12] 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.

7.2.2 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 Initialisation.* *Moreover, the following SFRs shall be addressed by the formal security policy model:* • *FDP_SDI.1 Stored data integrity monitoring* • *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*
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.

7.3 Security Requirements Rationale

7.3.1 Rationale for the Security Functional Requirements

The rationale for the security functional requirements are given in the PP [12] chapter 6.3.1 with a mapping of the SFRs to their objectives. The rationale for the cryptographic services is given in chapter 7.4.

The additional introduced SFRs are discussed below:

Table 17: Rationale for additional SFR in the ST

Objective	TOE Security Functional Requirements
O.Phys-Manipulation	FPT_TST.2 „Subset TOE security testing“ FDP_SDI.1 „Stored data integrity monitoring“
O.Mem-Access	FDP_ACC.1 “Subset access control” FDP_ACF.1 “Security attribute based access control” FMT_MSA.3 “Static attribute initialization” FMT_MSA.1 “Management of security attributes” FMT_SMF.1 “Specification of Management Functions”

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

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.

The justification related to the security objective “Protection against Physical Manipulation (O.Phys-Manipulation)” is as follows:

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 Cryptographic Support and SF_PMA Protection against modifying attacks.

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 (FDP_SDI.1)” requires the implementation of an Error Detection (EDC) algorithm which detects integrity errors of the data stored in all memories. By this the manipulation of the TOE using corrupt data is prevented. Therefore FDP_SDI.1 is suitable to meet the security objective O. Phys-Manipulation.

The security functional requirement “Stored data integrity monitoring and action (FDP_SDI.2)” requires the implementation of an integrity observation and correction which is implemented by the Error Detection (EDC) and Error Correction (ECC) measures. The EDC is present throughout all memories of the TOE while the ECC is realized in the SOLID FLASH™ NVM. These measures detect and inform about one and more bit errors. In case of the SOLID FLASH™ NVM 1 bit errors of the data are corrected automatically. By the ECC mechanisms it is prevented that the TOE uses corrupt data. The security reset performs an action to prevent the TOE to operate with manipulated data. Therefore FDP_SDI.2 is suitable to meet the security objective O.Phys-Manipulation.

The justification related to the security objective “Area based Memory Access Control (O.Mem-Access)” is as follows:

The security functional requirement “Subset access control (FDP_ACC.1)” with the related Security Function Policy (SFP) “Memory Access Control Policy” exactly require the implementation of an area based memory access control as required by O.Mem-Access. The related TOE security functional requirements FDP_ACC.1, FDP_ACF.1, FMT_MSA.3, FMT_MSA.1 and FMT_SMF.1 cover this security objective. The implementation of these functional requirements is represented by the dedicated privilege level concept.

The justification of the security objective and the additional requirements show that they do not contradict to the rationale already given in the Protection Profile for the assumptions, policy and threats defined there. Moreover, these additional security functional requirements cover the requirements by the PP [12] user data protection of the composite TOE protection of chapter 1.2.5 claim 35 and 36 which are not refined by the PP [12].

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

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 fulfilment of the security functional requirement FCS_RNG. This is defined in the PP [12] chapter 5.1. The requirement implements a quality metric which is defined by national regulations. The implemented random number generation fulfils the definitions of ASI31 [14] in the quality classes as outlined in chapter 7.1.1.1. Therefore the SFR FCS_RNG and the objective O.RND are covered.

The rationale for the functional requirement FCS_RNG is discussed in the PP [12], chapter 6.3.1.

7.3.1.1 Dependencies of Security Functional Requirements

The dependence of security functional requirements are defined and described in PP [12] section 6.3.2 for the following security functional requirements:

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			

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

Table 18: Dependencies for the additional Security Functional Requirements

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FCS_COP.1/TDES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, see comment 2
	FCS_CKM.4	Yes, FCS_CKM.4/TDES
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_CKM.1],	Yes, see comment 2
	FCS_CKM.4	Yes, FCS_CKM.4/AES
FCS_CKM.4/AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, see comment 2
FPT_TST.2	No dependencies	N/A
FDP_ACC.1	FDP_ACF.1	Yes, FDP_ACF.1
FDP_ACF.1	FMT_MSA.3	Yes, FMT_MSA.3
	FDP_ACC.1	Yes, FDP_ACC.1
FMT_MSA.3	FMT_MSA.1	Yes, FMT_MSA.3
	FMT_SMR.1	Not required, see comment 1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	Yes, FDP_ACC.1
	FMT_SMR.1	Not required, see comment 1
	FMT_SMF.1	Yes
FMT_SMF.1	None	N/A
FDP_SDI.1	None	N/A

Comment 1:

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

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 [12]. 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, FCS_COP.1/AES, FCS_CKM.4/TDES, FCS_CKM.4/AES the respective dependencies FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 have to be fulfilled by the environment. The meaning is that the environment shall meet the requirement FCS_CKM.1 as defined in [14], section 10.1 or shall meet the requirements FDP_ITC.1 or FDP_ITC.2 as defined in [14], section 11.7. For the security functional requirement FCS_COP.1/TDES, FCS_COP.1/AES and the respective dependencies 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 [12].

7.3.2 Rationale of the Assurance Requirements

The chosen assurance level EAL6 is augmentation with the requirements coming from ALC_FLR.1. In chapter 7.2 the different assurance levels are shown as well as the augmentations. The augmentations are in compliance with the Protection Profile [12].

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 defence 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” [17] 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 analysed 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 [15].

7.3.2.1 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.

8 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 Modification Attacks
- SF_PLA Protection against Logical Attacks
- SF_CS Cryptographic Support

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

8.1 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, a chip identification mode exists which is active in all phases. The chip identification data (O.Identification) is stored in a not-changeable configuration page area and non-volatile memory. In the same area further TOE configuration data is stored. In addition, user initialization data can be stored in the non-volatile memory during the production phase as well. During this first data programming, the TOE is still in the secure environment and in Test Mode.

The covered security functional requirement is FAU_SAS.1 “Audit storage”.

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 operation within a selected life cycle phase the accesses to memories are granted by the MMU controlled access rights and related privilege levels. The TOE operates always in a dedicated life cycle phase.

The covered security functional requirements are FDP_ACC.1 “Subset access control”, FDP_ACF.1 “Security attribute based access control” and FMT_MSA.1 “Management of security attributes”.

In addition, during each start-up of the TOE the address ranges and access rights are initialized by the STS with predefined values. The covered security functional requirement is FMT_MSA.3 “Static attribute initialisation”.

The TOE clearly defines access rights and privilege levels in conjunction with the appropriate key management in dependency of the firmware or software to be executed. By this clearly defined management functions are implemented, enforced by the MMU, and the covered security functional requirement is FMT_SMF.1 “Specification of Management Functions”.

During the testing phase in production within the secure environment the entire SOLID FLASH™ NVM is deleted. The covered security functional requirement is FPT_PHP.3 “Resistance to physical attack”.

Each operation phase is protected by means of authentication and encryption. The covered security functional requirements are FDP_ITT.1 “Basic internal transfer protection” and FPT_ITT.1 “Basic internal TSF data transfer protection”.

The **SF_DPM** “Device Phase Management” covers the security functional requirements FAU_SAS.1, FMT_LIM.1, FMT_LIM.2, FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FPT_PHP.3, FDP_ITT.1 and FPT_ITT.1.

8.2 SF_PS: Protection against Snooping

All contents of all memories of the TOE are encrypted on chip to protect against data analysis on stored data as well as on internally transmitted data. There is no plain data on the chip. In addition the data transferred over the memory bus to and from (bi-directional encryption) the CPU, Coprocessor (Crypto@2304T and SCP), the special SFRs and the peripheral devices (CRC, RNG and Timer) are encrypted as well.

The memory content and bus encryption is done by the MED using a complex key management. This means that the SOLID FLASH™ NVM, RAM, CACHE and the bus are encrypted with module dedicated and dynamic keys. Note that the ROM contains the firmware only and no user data.

Data are transferred, handled and computed only encrypted or masked anywhere on the TOE, and also the dual CPU computes entirely masked. Further protection means are described in the confidential Security Target.

The symmetric cryptographic coprocessor is entirely masked at any time and also here the masks change dynamically. The encryption and masking means covers the data processing policy and FDP_IFC.1 “Subset information flow control“. The covered security functional requirements are FPT_PHP.3 “Resistance to physical attack”, FDP_IFC.1 “Subset information flow control”, FPT_ITT.1 “Basic internal TSF data transfer protection”, FDP_ITT.1 “Basic internal transfer protection” and FDP_SDC.1 “stored data confidentiality”.

The user can define his own key for an SOLID FLASH™ NVM area to protect his data. This user individually chosen key is then delivered by the operating system and included in the dynamic SOLID FLASH™ NVM encryption. The user specified SOLID FLASH™ NVM area is then encrypted with his key and a dynamic component. The encryption of the memories is performed by the MED with a proprietary cryptographic algorithm and with a complex and dynamic key management providing protection against cryptographic analysis attacks. The few keys which have to be stored on the chip, for example the user chosen key and the chip specific ROM key, are protected against read out.

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

The proprietary implementation of the dual CPU has no standard command set and discloses therefore no possibility for deeper analysis. The covered security functional requirement is FPT_PHP.3 “Resistance to physical attack”.

The entire design is kept in a non-standard way to complicate attacks using standard analysis methods to an almost not practical condition. A proprietary CPU implementation with a non-public bus protocol is used which renders analysis very complicated and time consuming. Besides the proprietary structures also the internal timing behavior is proprietary and by this aggravating significantly the analysis in addition. 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 almost independent of the dynamically encrypted, respectively masked and/or randomized data.

In the design a number of components are automatically synthesized and mixed up to disguise and complicate analysis.

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, artificial shield lines are implemented and mixed up with normal signal lines required for chip operation, which renders probing attacks with high feasibility to not practical. This provides the so called intelligent implicit active shielding “I^2-shield”.

The covered security functional requirements are FPT_PHP.3 “Resistance to physical attack”, FPT_ITT.1“Basic internal TSF data transfer protection” and FDP_ITT.1 “Basic internal transfer protection”.

In addition to their protection during processing of code and data their storage in the SOLID FLASH™ NVM is protected against side channel attacks too: Even if users operate with direct and static addressing for storing their secrets, the addresses are always translated to virtual addresses–- if the address call is in the correct privilege level which is monitored by the MMU.

The covered security functional requirements are FPT_PHP.3 “Resistance to physical attack”, FPT_ITT.1“Basic internal TSF data transfer protection” and FDP_ITT.1 “Basic internal transfer protection”.

In contrast to the linear virtual address range the physical SOLID FLASH™ NVM pages are transparently and dynamically scrambled on every page modification. This scrambling is entirely independent from the user software and the MMU. Further information is given in the confidential Security Target.

A low system frequency sensor FSE is implemented to prevent the TOE from single stepping. The sensor is tested by the user mode security life control UMSLC and connected to the clock pad.

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

An induced error which cannot be corrected will be recognized by the Integrity Guard and leads to an alarm. In case of security critical detections a security alarm and reset is generated. The covered security functional requirement is FPT_FLS.1 “Failure with preservation of secure state”.

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

8.3 SF_PMA: Protection against Modifying Attacks

First of all we can say that all security mechanisms effective against snooping **SF_PS** apply also here since a reasonable modification of data is almost impossible on dynamically encrypted, masked, scrambled, transparently relocated, randomized and topologically protected hardware. Due to this the covered security functional requirements are FPT_PHP.3 “Resistance to physical attack”, FDP_IFC.1 “Subset information flow control”, FPT_ITT.1“Basic internal TSF data transfer protection”, FDP_ITT.1 “Basic internal transfer protection”, FDP_SDC.1 “Store d data confidentiality” and FPT_FLS.1 “Failure with preservation of secure state”.

The TOE is equipped with an error detection code (EDC) which covers the memory system of RAM, ROM and SOLID FLASH™ NVM and includes also the MED and MMU. Thus introduced failures can be detected and in terms of single bit errors in the SOLID FLASH™ NVM also automatically corrected (FDP_SDI.2 “Stored data integrity monitoring and action”).

In order to prevent accidental bit faults during production in the ROM, over the data stored in ROM an EDC value is calculated (FDP_SDI.1 “Stored data integrity monitoring”).

The covered security functional requirements are FPT_PHP.3 “Resistance to physical attack”, FDP_SDI.1 “Stored data integrity monitoring” and FDP_SDI.2 “Stored data integrity monitoring and action”.

If a user tears the card resulting in a power off situation during a SOLID FLASH™ NVM programming operation or if other perturbation is applied, no data or content loss occurs and the TOE restarts power on. The SOLID FLASH™ NVM tearing-safe write functionality covers FPT_FLS.1 “Failure with preservation of secure state”. The implemented means includes FDP_SDI.1 “Stored data integrity monitoring”.

More information is given in the confidential Security Target.

The covered security functional requirement is also FPT_PHP.3 “Resistance to physical attack“, since these measures make it difficult to manipulate the write process of the SOLID FLASH™ NVM. The covered security functional requirements are FPT_FLS.1 “Failure with preservation of secure state”, FPT_PHP.3 “Resistance to physical attack” and FDP_SDI.1 “Stored data integrity monitoring”.

The above mentioned error management in the memories and the tearing protection of the SOLID FLASH™ NVM contribute also to the security functional requirement FRU_FLT.2 “Limited fault tolerance” as induced faults are detected with high probability and the correct operation is continued by taking the appropriate action.

The TOE is protected against fault and modifying attacks. The core provides the functionality of double-computing and e.g. result comparison of all tasks to detect incorrect calculations. The detection of an incorrect calculation is stored and the TOE enters a defined secure state which causes the chip internal reset process.

The implementation of the dual CPU computing on the same data is by this one of the most important security features of this platform. As also the results of both CPU parts are compared at the end, a fault induction of modifying attacks would have to be done on both CPU parts.

More information is given in the confidential Security Target.

During start up, the STS performs various configurations and subsystem tests. After the STS has finished, the operating system or application can call on chip testing features. The testing feature checks the verity of alarm sources and testing features for correct operation as given in the HRM [1]. This test can also be released actively by the user software during normal chip operation by calling an RMS function. 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“.

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. By release of a security reset all logic and memory of the coprocessors (SCP and Crypto) immediately reset with their respectful reset values. The stored keys are overwritten with the default reset values and memory data structures are overwritten with random values. The covered security functional requirements are FCS_CKM.4 “Cryptographic key destruction”, FPT_FLS.1 “Failure with preservation of secure state”, FPT_PHP.3 “Resistance to physical attack“, and FPT_TST.2 “Subset TOE security testing“.

As physical effects or manipulative attacks may also address the program flow of the user software, a watchdog timer and a check point register are implemented. These features enable the user for checking the correct processing time and the integrity of the program flow of the user software.

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

All communication via the busses is in addition protected by a monitored hardware handshake. If the handshake was not successful an alarm can be generated.

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

The virtual memory system and privilege level model are enforced by the MMU. This controls the access rights throughout the TOE. There is a clear differentiation within the privilege levels defined. 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” and FMT_SMF1 “Specification of Management Functions”.

The **SF_PMA** “Protection against Modifying Attacks” covers the security functional requirements FCS_CKM.4, FPT_PHP.3, FDP_IFC.1, FPT_ITT.1, FDP_ITT.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FDP_ACC.1, FDP_ACF.1, FRU_FLT.2, FPT_TST.2, FDP_SDC.1, FDP_SDI.1, FDP_SDI.2 and FPT_FLS.1.

8.4 SF_PLA: Protection against Logical Attacks

The memory access control of the TOE uses a memory management unit (MMU) to control the access to the available physical memory by using virtual memory addresses and to segregate the code and data to a privilege level model. The MMU controls the address permissions of up seven privileged levels and gives the software the possibility to define different access rights for the privileged levels.

As the TOE provides support for separation of memory areas the covered security functional requirements are FDP_ACC.1 “Subset access control”, FDP_ACF.1 “Security attribute based access control”, FMT_MSA.3 “Static attribute initialization”, FMT_MSA.1 “Management of security attributes” and FMT_SMF.1 “Specification of Management functions”.

The TOE provides the possibility to protect the property rights of user code and data by the encryption of the SOLID FLASH™ NVM areas with a specific key defined by the user. Due to this key management FDP_ACF.1 is fulfilled. In addition, each memory present on the TOE is encrypted using either mask specific or chip individual or even session depending keys, assigned by a complex key management. Induced errors are recognized by the Integrity Guard concept and lead to an alarm with high feasibility. In case of security critical errors 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” and FPT_FLS.1 “Failure with preservation of secure state”.

Beside the access protection and key management, also the use of illegal operation code is detected and will release a security reset.

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_ITT.1, FDP_ITT.1, FDP_IFC.1, FPT_PHP.3, FPT_FLS.1 and FMT_SMF.1.

8.5 SF_CS: Cryptographic Support

The TOE is equipped with a coprocessor supporting the DES and AES algorithms.

8.5.1 Triple DES

The TOE supports the encryption and decryption in accordance with the specified cryptographic algorithm Triple Data Encryption Standard (TDES) with cryptographic key sizes 112 and 168 bit meeting the standard:

National Institute of Standards and Technology (NIST), SP 800-67 Rev. 2 [20]

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

- Electronic Codebook Mode (ECB)
- Cipher Block Chaining Mode (CBC)
- Blinding Feedback Mode (BLD)

- Recrypt Mode.

The Recrypt Mode and the BLD are described in the hardware reference manual HRM [1], while the implementation of ECB and CBC follow the standard:

National Institute of Standards and Technology (NIST), SP 800-38A [21].

Note that the BLD follows also the standard, but in a masked way.

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 chapter 7.1.4.1. Furthermore, this security feature is optional and is only provided if the TOE is ordered with accessible SCP.

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

Note: Using the TDES algorithm with three keys of which two keys equal is a so called two key triple DES operation. This operation can be configured and managed by the user but does not meet the national requirements issued by BSI and achieves therefore not the 100 Bits security level.

8.5.2 AES

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:

- National Institute of Standards and Technology (NIST) SP 800-38A [21]
- FIPS 197 [31]

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 chapter 7.1.4.1. Furthermore, this security feature is optional and is only provided if the TOE is ordered with accessible SCP.

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

8.5.3 PTRNG respectively TRNG

Random data is essential for cryptography as well as for security mechanisms. The TOE is equipped with a physical True Random Number Generator (PTRNG respectively TRNG, 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, like masking. The PTRNG respectively TRNG implements also self-testing features. The PTRNG respectively TRNG is compliant to the requirements of the functionality class PTG.2 of AIS31, please refer to [16].

The covered security functional requirements are FCS_RNG.1, FPT_PHP.3, FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_TST.2 and FPT_FLS.1.

8.5.4 Summary of SF_CS: Cryptographic Support

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, FDP_IFC.1, FPT_TST.2, FPT_FLS.1 and FCS_RNG.1.

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

The justification and overview of the mapping between security functional requirements (SFR) and the TOE's security functionality (SF) is given in the sections above. The results are shown in 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 19: Mapping of SFR and SF

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	X	
FDP_ACF.1	X		X	X	
FPT_PHP.3	X	X	X	X	X
FDP_ITT.1	X	X	X	X	X
FDP_SDC.1		X	X		
FDP_SDI.1			X		
FDP_SDI.2			X		
FDP_IFC.1		X	X	X	X
FMT_MSA.1	X		X	X	
FMT_MSA.3	X		X	X	
FMT_SMF.1	X		X	X	
FRU_FLT.2			X		
FPT_ITT.1	X	X	X	X	X
FPT_TST.2			X		X
FPT_FLS.1		X	X	X	X
FCS_RNG.1					X
FCS_COP.1/TDES					X
FCS_CKM.4/TDES			X		X

Security Functional Requirement	SF_DPM	SF_PS	SF_PMA	SF_PLA	SF_CS
FCS_COP.1/AES					X
FCS_CKM.4/AES			X		X

8.7 Security Requirements are internally consistent

For this chapter the PP [12] section 6.3.4 can be applied completely.

In addition to the discussion in section 6.3 of PP [12] 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 privilege level concept represents the area based memory access protection enforced by the MMU. 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.

9 Literature

The table is continued on next page regarding the referenced standards and other references.

Ref	Version	As off	Title
[1]	Rev. 3.0	2019-06-24	M7892 SOLID FLASH™ Controller for Security Applications, Hardware Reference Manual
[3]	v9.14	2019-12-03	16-bit Controller Family, SLE 70, Programmer's Reference Manual
[7]		2024-06-19	SLE70 Crypto@2304T User Manual
[8]		2024-04-23	M7892 Security Guidelines
[9]	Rev.7.1	2019-12-18	M7892 Errata Sheet
[10]	This document		Confidential Security Target for this TOE
[11]	2.0	2019-10-28	AMM Advanced Mode for NRG SAM, Addendum to M7892 Hardware Reference Manual
[12]	1.0	2014-01-13	Security IC Protection Profile PP-0084 “Security IC Platform Protection Profile with Augmentation Packages”, BSI-CC-PP-0084-2014, available at https://www.bund.bsi.de
[13]	V3.1 Rev 5	2017-04	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1 Revision 5, April 2017, CCMB-2017-04-001
[14]	V3.1 Rev 5	2017-04	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1 Revision 5, April 2017, CCMB-2017-04-002
[15]	V3.1 Rev 5	2017-04	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1 Revision 5, April 2017, CCMB-2017-04-003
[16]	3.0	2013-05-15	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
[17]	3.2	2022-11	Joint Interpretation Library, Application of Attack Potential to Smartcards
[20]	SP 800-67 Rev. 2	2017-11	National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce, NIST Special Publication 800-67
[21]	SP 800-38A	2001-12	National Institute of Standards and Technology(NIST), Technology Administration, US Department of Commerce, NIST Special Publication SP 800-38A (for AES and DES)
[30]	ISO/IEC 18033	2005	ISO/IEC 18033-3:2004, Information technology – Security techniques – Encryption algorithms– Part 3: Block ciphers [18033] (for AES)
[31]	FIPS PUB 197	2001-11-26	U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), Advanced Encryption Standard (AES), FIPS PUB 197
[33]	I	2009-08-14	Act on the Federal Office for Information Security (BSI-Gesetz - BSIG), Bundesgesetzblatt I p. 2821.
[38]	ISO/IEC 9798-2	2008-12	ISO 9798-2:2008 Information technology -- Security techniques -- Entity authentication -- Part 2: Mechanisms using symmetric encipherment algorithms; Third edition 2008-12-15

10 List of Abbreviations

AES	Advanced Encryption Standard
AIS31	“Anwendungshinweise und Interpretationen zu ITSEC und CC, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren”
AMM	Advanced Mode for NRG SAM
API	Application Programming Interface
CC	Common Criteria
CI	Chip Identification Mode (STS-CI)
CIM	Chip Identification Mode (STS-CI), same as CI
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
Crypto@2304T	Asymmetric Cryptographic Processor
CRT	Chinese Reminder Theorem
DES	Data Encryption Standard
DPA	Differential Power Analysis
DFA	Differential Failure Analysis
DTRNG	Deterministic Random Number Generator
EC	Elliptic Curve Cryptography
ECC	Error Correction Code and Elliptic Curve Cryptography depending on the context
EDC	Error Detection Code
EDU	Error Detection Unit
SOLID FLASH™ NVM	Electrically Erasable and Programmable Read Only Memory
EMA	Electromagnetic analysis
Flash	Infineon® SOLID FLASH™ Memory
IC	Integrated Circuit
ICO	Internal Clock Oscillator
ID	Identification
IMM	Interface Management Module
ITP	Interrupt and Peripheral Event Channel Controller
I/O	Input/Output
IRAM	Internal Random Access Memory
ITSEC	Information Technology Security Evaluation Criteria
M	Mechanism

MED	Memory Encryption and Decryption
MMU	Memory Management Unit
NVM	Non Volatile Memory
O	Objective (for the TOE)
OE	Objective (for the environment)
OS	Operating system
PEC	Peripheral Event Channel
PRNG	Pseudo Random Number Generator
PROM	Programmable Read Only Memory
PTRNG	Physical 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
SA	Service Algorithm Minimal
SCL	Symmetric Cryptographic Library
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
STS	Self-Test Software
SW	Software
SWIO	Software controlled Input Output
T	Threat
TM	Test Mode (STS)
TOE	Target of Evaluation
TRNG	True Random Number Generator
TSC	TOE Security Functions Control
TSF	TOE Security Functionality
UART	Universal Asynchronous Receiver/Transmitter

Confidential

UM	User Mode (STS)
UmSLC	User mode Security Life Control
WDT	Watch Dog Timer
XRAM	eXtended Random Access Memory
TDES	Triple DES Encryption Standard

11 Glossary

Application Program/Data	Software which implements the actual TOE functionality provided for the user or the data required for that purpose
Central Processing Unit	Logic circuitry for digital information processing
Chip	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
Crypto@2304T	Cryptographic coprocessor for asymmetric cryptographic operations (RSA, Elliptic Curves)
Cyclic Redundancy Check	Process for calculating checksums for error detection
EEPROM or NVM or SOLID FLASH™ NVM	Electrically Erasable and Programmable Read Only Memory, the Non-Volatile Memory (NVM) 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 and provides specific routines for the user software. The firmware is located in the ROM and parts of it in the SOLID FLASH™ NVM
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
Mutual Authentication Extension	Implementation allowing to mutually authenticate production equipment and the TOE

NRG	ISO/IEC14443-3 Type A with CRYPTO1
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
Resource Management System	Part of the firmware containing SOLID FLASH™ NVM programming routines, AIS31 test bench etc.
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 of the system) 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