Security Target Lite

M7892 B11

Recertification

Common Criteria CCv3.1 EAL6 augmented (EAL6+)

Resistance to attackers with HIGH attack potential

Document version 3.0 as of 2017-11-10

Dr. Oleg Rudakov

Chipcard & Security

Edition 2017-11-10

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 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.

Public

Miscellaneous

The term "Mifare" in this document is only used as an indicator of product compatibility to the corresponding established technology. This applies to the entire document wherever the term is used.

Trademarks of Infineon Technologies AG

Public

Revision History

Date	Version	Change Description
2017-02-15	1.0	Initial version.
2017-08-02	2.6	Final version
2017-11-10	3.0	Re-certification to include ACL v2.07.003

Table of Contents

1 Security Target Introduction (ASE_INT)

1.1 Security Target and Target of Evaluation Reference

The title of this document is Security Target Lite M7892 B11 Recertification Common Criteria CCv3.1 EAL6 augmented (EAL6+).

This document comprises the Infineon Technologies AG Security Controller (Integrated Circuit IC) M7892 B11 with specific IC dedicated firmware and optional software:

- RSA v1.02.013 or v2.07.003
- EC v1.02.013 or v2.07.003
- Toolbox v1.02.013 or v2.07.003
- Base v1.02.013 or v2.07.003
- SHA-2 v1.01
- Symmetric Crypto Library (SCL) v2.02.012.

This Security Target Lite has the revision 3.0 and is dated 2017-11-10.

The target of evaluation (TOE) M7892 B11 is described in the following.

The Target of Evaluation (TOE) is the Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013 or v2.07.003, EC v1.02.013 or v2.07.003, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013 or v2.07.003, and Toolbox v1.02.013 or v2.07.003 libraries and with specific IC dedicated software (firmware). The design step of this TOE is B11.

The Security Target is based on the Protection Profile PP-0035 “Smartcard IC Platform Protection Profile” [1] as publicly available for download at https://www.bsi.bund.de.

The Protection Profile and the Security Target are built in compliance with Common Criteria v3.1 Revision 5.

The ST takes into account all relevant current final interpretations.

Table 1: Identification

	Version	Date	Registration
Security Target Lite	3.0	2017-11-10	M7892 B11
Target of Evaluation			M7892 B11 with FW-Identifier 78.015.14.0 or FW-Identifier 78.015.14.1 or FW-Identifier 78.015.14.2 and optional SW: RSA2048 v1.02.013 or v2.07.003 (optional) RSA4096 v1.02.013 or v2.07.003 (optional) EC v1.02.013 or v2.07.003 (optional) Toolbox v1.02.013 or v2.07.003 (optional) Base v1.02.013 or v2.07.003 (optional) SHA-2 v1.01 (optional) SCL v2.02.012 (optional) and Guidance documentation(1).
Protection Profile	1.0	2007-06-15	Security IC Platform Protection Profile PP0035
Common Criteria	3.1 Revision 5	2017-04	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCMB-2017-04-001 Part 2: Security functional requirements CCMB-2017-04-002 Part 3: Security Assurance Components CCMB-2017-04-003

(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.

A customer 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 [35] and in the Family Hardware Reference Manual [6].

1.2 Remarks to the Target of Evaluation (TOE)

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 B11. The GCIM mode is explained and detailed in the user guidance document hardware reference manual HRM [6].

All product derivatives are identical in module design, basic layout and footprint, but are adapted to connect to different types of antennas or to a contact based interface only. Therefore, the TOE is represented and made out of five different mask sets with following TOE internal and security irrelevant differences:

The main difference between the mask sets of the TOE is on one metal mask (M1) to implement four different input capacitances in the analogue part of the radio frequency interface (RFI). One of the four input capacitances is zero and marks a derivative deemed for contact based communication only. 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. The derivatives without available input capacitance are deemed for contact based communication only.

The additional fifth mask set takes one of the previous four mask sets and adds an additional mask on top of the very last mask of the TOE. This last mask is deemed to produce a metal layer, just rerouting the pads for a special package type. This additional top metal layer is comparable to an outer package, which would simply reconnect the TOE pads in a different way. This last rerouting layer does not change the function of the TOE itself and is, in addition, subject of the design requirements of the users. This last layer is flexible in design, naming and is of course, not relevant for the security of the TOE. It is comparable to the scenario where someone takes a piece of wire and reconnects the pads of a smartcard in a different way.

For logistical reasons and due to user demands the TOE products produced with this fifth mask set output a different design step C1x, where “x” represents a number from 1 up to 9. The number depends on the design variants of the additional top metal layer and of the package, which can be customer specific.

To each of four capacitances related mask sets, 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. And, furthermore users can identify derivatives produced with the additional top metal layer by the design step output “C1x” as described above. On those “C1x” derivatives the GCIM part of the individual length byte remains unchanged and allows the identification of which of the other four mask sets was used to produce the TOE with the additional top metal layer. Therefore, the GCIM design step output - C11 up to C19 - of this extra top metal layer TOE products correspond always to the TOE silicon design step B11. Thereby, the clear identification of the silicon design step is given.

There are no other differences between the mask sets the TOE is produced with. Details are explained in the user guidance hardware reference manual HRM [6] and in the errata sheet [15].

The M7892 B11 product allows for a maximum of configuration possibilities defined by the customer order following the market needs. For example, a M7892 B11 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

[1] SOLID FLASH™ NVM is an Infineon Trade Mark and stands for the Infineon EEPROM working as Flash memory.

coprocessor Crypto@2304T, or both, or none of them. In addition, the user decides, whether the TOE comes with a free combination of software libraries or without any. And, to be even more flexible, various interface options can be chosen as well. To sum up the major selections, the user defines by his order:

- The available memory sizes of the SOLID FLASH™ NVM and RAM.
  Note that there is no user available ROM on the TOE.
- The availability of the cryptographic coprocessors.
- The user has the free choice for combinations of optional cryptographic libraries. The TOE can be delivered with either v1.02.013 or v2.07.003 (or none) of these libraries, but it is not possible to combine different versions within the TOE.
- The availability of the Flash Loader for available interfaces like ISO-7816, contactless ISO-14443.
- The availability of various interface options.
- The possibility to tailor the product by blocking on his own premises.
- The degree of freedom of the chip configuration is predefined by Infineon Technologies AG and made available via the order tool.

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

The blocking information can be modified by the users applying specific APDUs. Once final locking is done, further modifications are disabled.

The BPU software part is only present on predefined products, which have been ordered with the BPU option. In all other cases this software is not present on the product. More details can be obtained in the Confidential Security Target [35].

In addition, after strong and successful authentication, the Flash Loader firmware part allows the download of user software, or just parts of it, to the SOLID FLASH™ NVM. By this the user is free to decide:

- whether Infineon downloads (flashes) the user software entirely during the TOE production phase,
- or if this is done by the user himself after Infineon has delivered the TOE without user software,
- or Infineon downloaded only parts of the user software and the user completes his software at his own premises.

If Infineon is required to download the user software or parts of it, the user is of course required to provide Infineon the code deemed for the download, prior production of the TOE. This user software transfer to Infineon is done by a secure channel, of course being also part of this certificate.

Therefore, the user is entirely flexible in his process, regardless whether he intends to flash his code entirely on his own, or sends his complete code or just parts of it to Infineon for high parallel flashing during production. After the flashing steps have been completed, the Flash Loader firmware is permanently deactivated. A reactivation is then no more possible.

Beside all configuration possibilities, it is self-evident that of course, exclusively all security relevant settings are contained in the IFX-only part. The Flash Loader BPU software does not access and has no access to the IFX-only part.

Once the user blocking by applying the APDU has been finalized, the configuration page is no more accessible for changes. After the final deactivation of the Flash Loader the product is permanently fixed regarding its configurations and software. A reactivation of the Flash Loader is not possible. At the next start-up, the STS apply the settings, and, if called, a RMS-function can output the finally made chip configuration for verification and information purposes.

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

Beside the various TOE configurations further possibilities of how the user inputs his software on the TOE, i.e. the operating system and applications, are in place. This provides a maximum of flexibility and for the entire process of how users keep and manage their data. An overview is given in the following table:

Table 2: Options to implement user software at Infineon production premises

1.	The user or/and a subcontractor downloads the software into the SOLID FLASH™ NVM on his own. Infineon Technologies AG has not received user software and there is no user data in the ROM.	The Flash Loader can be activated or reactivated by the user or subcontractor to download his software in the SOLID FLASH™ NVM – until the Flash Loader is finally deactivated by the user.
2	The user provides 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 is no user data in the ROM.	There is no Flash Loader present.
3	The user provides software for the download into the SOLID FLASH™ NVM to Infineon Technologies AG. The software is downloaded to the SOLID FLASH™ NVM during chip production. I.e. there is no user data in the ROM.	The Flash Loader is blocked afterwards but can be activated or reactivated by the user or subcontractor to download his software in the SOLID FLASH™ NVM. Precondition is that the user has provided an own reactivation procedure in software prior chip production to Infineon Technologies AG.

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

The following listing contains a selection of configuration possibilities. More information is given in the Confidential Security Target [35]. Note that within those limitations the TOE configurations can vary under only one equal IC-hardware and one development code – the M7892 B11 – and without impact on security.

Note also that following configuration possibilities are valid unchanged throughout all different mask sets.

Public

Table 3: Configuration ranges and blocking options for the user

Module / Feature (User view)	Max-Value (User view)	Min-Value (User view)	Blocking possible	Blocking Step
Memories				
SOLID FLASH™ NVM	Max. 404 kBytes	Min. 0 kBytes	Yes	1 kBytes
ROM	Not available	Not available	No	None
RAM for the user	8 kBytes	1 kBytes	Yes	1kBytes
Modules				
Crypto@2304T	Available	Not available	Yes	On/off
SCP	Available	Not available	Yes	On/off
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
Mifare hardware support for card mode	Available	Not available	By order only	None
SW support for Mifare compatible 4k cards (1)	Available	Not available	By order only	None
SW support for Mifare compatible 1k cards (1)	Available	Not available	By order only	None

(1) Mifare emulation

All possible TOE configurations equal and/or within the below specified ranges are covered by the certificate.

Note that there is no user available on-chip ROM module anymore. The user software and data are now located in a dedicated and protected part of the SOLID FLASH™ NVM. The long life storage endurance, the automatic management of often used memory pages, together with the means for error detection and correction serves at least for equal or even higher reliability and endurance, compared to a dedicated ROM.

Beside the above listed flexible ranges, the user guidance contains a number of predefined configurations for those customers not making use of the BPU option. All of these configurations belong to the TOE as well and are of course made of the equal hardware and are inside the above declared ranges.

Today’s predefined configurations of the TOE are listed in the hardware reference manual [6]. These predefined products come with the most requested configurations and allow to produce volumes on stock in order to simplify logistic processes.

According to the BPU option, a not limited number of configurations of the TOE may occur in the field. The number of various configurations depends on the user and purchase contract only.

Note that the TOE answers to the Non-ISO-ATR with the Generic Chip Identification Mode (GCIM) answer. This GCIM outputs a coded clear identifier for the type of the GCIM, the platform identifier, the design step and further configuration information. The hardware reference manual [6], being part of the user guidance, enables then for the clear interpretation of the read out GCIM data.

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

In addition, a dedicated RMS function allows reading out the present configuration in detail. Again, together with hardware reference manual [6], 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, the firmware parts and the optional software parts.

The firmware parts are the RMS library, the Service Algorithm Minimal (SAM), the STS firmware for test purpose (see chapter 2.2.2), providing some functionality via an API to the Smartcard Embedded Software, the Flash Loader for downloading user software to the SOLID FLASH™ NVM and the Mifare compatible software interface. The firmware is located in the ROM and the belonging patches are stored in the SOLID FLASH™ NVM. The ROM contains no user data.

The software parts are differentiated into:

The cryptographic libraries RSA[1], EC[2] SHA-2[3], and the symmetric cryptographic library (SCL), as well as the supporting libraries Toolbox and Base.

The TOE can be delivered including - in free combinations - or not including any of the functionality of the cryptographic libraries EC, RSA, SHA-2, SCL and the supporting Toolbox library. The Base library is used internally by the RSA, the EC and the Toolbox library, thus if one of the aforementioned libraries is ordered, the Base library will be automatically included in the delivery.

If the user decides not to use one or all of the crypto library(s), the specific library(s) is (are) not delivered to the user and the accompanying “Additional Specific Security Functionality (O.Add-Functions)” *Rivest-Shamir-Adleman (RSA*) and/ or *EC and/or SHA-2* and SCL based *Advanced Encryption Standard (AES)* and/or SCL based *Triple Data Encryption Standard (TDES)* is/are not provided by the TOE.

The Toolbox library provides the user optionally basic arithmetic and modular arithmetic operations, in order to support user software development using long integer operations. These basic arithmetic operations do not provide any security functionality, implement no security mechanism, and do not proved additional specific security functionality - as defined for the cryptographic libraries.

The user developed software using the Toolbox basic operations is not part of the TOE.

[1] Rivest-Shamir-Adleman asymmetric cryptographic algorithm

[2] The Elliptic Curve Cryptography is abbreviated with EC only in the further, in order to avoid conflicts with the abbreviation for the Error Correction Code ECC.

[3] SHA Secure Hash Algorithm

Deselecting one of the libraries does not include the code implementing functionality, which the user decided not to use. Not including the code of the deselected functionality has no impact of any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the functionality.

The SCL, RSA, EC, SHA-2, Base and Toolbox libraries can be loaded, together with the Smartcard Embedded software, into the SOLID FLASH™ NVM. The Smartcard Embedded Software, i.e. the operating system and applications are not part of the TOE and thus not subject of the evaluation.

1.3 Target of Evaluation Overview

The TOE comprises the Infineon Technologies AG Dual Interface Security Controller M7892 B11 with specific IC dedicated firmware and optional SCL, RSA, EC, SHA-2, Base and Toolbox libraries.

The TOE is a member of the Infineon Technologies AG high security controller family SLE70 meeting the highest requirements in terms of performance and security. A summary product description is given in this Security Target Lite (ST).

The SLE70 family provides a common architecture upon which specific products can be tailored for markets ranging from basic security applications (SLE76) up to high security and contactless applications (SLE78).

The TOE is intended to be used in any applications and devices with highest security requirements. For example in smart cards and also in other applications, such as secure element in various devices. This new product family features a progressive security philosophy focusing on data integrity. By that three main principles combined in close synergy are utilized in the new security concept called the “Integrity Guard”. The Integrity Guard implements the main principles full error detection, full encryption and intelligent active shielding.

With these capabilities 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, 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 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: ISO 7816-3, ISO 14443 Type A and Type B, ISO/IEC 18092 NFC passive mode, Mifare compatible software Interface as well as further communication modes, allowing also the implementation of user defined concepts for contact based or contactless communication. More details are given in the confidential Security Target [35] and the hardware reference manual [6].

In order to increase the contactless interface performance even more, the RFI can be configured in terms of baud rates for reception and transmission and the setting of the sub-carrier frequency used for the load modulation. More details are given in the hardware reference manual [6].

Table 4: Interface combinations excerpt of the TOE

Interface Options in brief					
Protocol	ISO7816	ISO14443 A	ISO14443 B	ISO18092 NFC passive mode	Mifare compatible interface

Further details and options are described in the Confidential Security Target [35].

The TOE provides a real 16-bit CPU-architecture and is compatible to the Intel 80251 architecture. The major components of the core system are the two CPUs (Central Processing Units), the MMU (Memory Management Unit) and MED (Memory Encryption/Decryption Unit). The two CPUs control 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 provides functionality for the tearing save write into the SOLID FLASH™ NVM. The STS firmware is used for test purposes during start-up and the Flash Loader allows downloading user software to the SOLID FLASH™ NVM during the manufacturing process. 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 [5]. 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), former 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 performance optimized for RSA-2048 bit (4096-bit with CRT) and Elliptic Curve (EC) cryptography.

The software part of the TOE consists of the cryptographic RSA-, EC-, SCL and the SHA-2 libraries and the supporting Toolbox and Base libraries. The Base library is used internally by the RSA, the EC and the Toolbox library, thus if one of the aforementioned libraries is ordered, the Base library will be automatically included in the delivery. The Base library does not provide any additional specific security functionality.

The RSA library is used to provide a high level interface to RSA (Rivest, Shamir, Adleman) cryptography implemented on the hardware component Crypto@2304T and includes countermeasures against SPA, DPA and DFA attacks. The routines are used for the RSA keys generation (only in v2.07.003), RSA signature verification, the RSA signature generation and the RSA modulus recalculation. The hardware Crypto@2304T unit provides the basic long number calculations (add, subtract, multiply, square with 1100 bit numbers) with high performance. The RSA library is delivered as object code and in this way integrated in the user software. The RSA library can perform RSA operations from 512 to 4096 bits.

Following the BSI[1] recommendations, key lengths below 1976 bit are not included in the certificate.

The EC library is used to provide a high level interface to Elliptic Curve cryptography implemented on the hardware component Crypto@2304T and includes countermeasures against SPA, DPA and DFA attacks. The routines are used for ECDSA signature generation, ECDSA signature verification, ECDSA key generation and Elliptic Curve Diffie-Hellman key agreement. In addition, the EC library provides an additional function for calculating primitive elliptic curve operations like EC Add and EC Double. EC curves over prime field Fp, as well as over GF(2^n) finite field are supported too.

The EC library is delivered as object code and in this way integrated in the user software. The certification covers the standard NIST [17] and Brainpool [18] Elliptic Curves with key lengths of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits, due to national AIS32 regulations by the BSI. Note that there are further uncounted side-channel-secure curve types which the user can optionally add in the composition certification process.

The SHA-library provides the calculation of a hash value of freely chosen data input in the CPU. The SHA-library is delivered as object code and is in this way available for the user software.

This secure hash-algorithm SHA-2 is intended to be used for signature generation, verification and generic data integrity checks. The use for keyed hash operations like HMAC or similar security critical operations involving keys, is not subject of this TOE and requires specific security improvements and DPA analysis including the operating system, which is not part of this TOE. Further essential information about the usage is given in the confidential user guidance [11].

The toolbox library does not provide cryptographic support or additional security functionality as it provides only the following basic long integer arithmetic and modular functions in software, supported by the cryptographic coprocessor: Addition, subtraction, division, multiplication, comparison, reduction, modular addition, modular subtraction, modular multiplication, modular inversion and modular exponentiation. No security relevant policy, mechanism or function is supported. The toolbox library is deemed for software developers as support for simplified implementation of long integer and modular arithmetic operations.

The SCL Library offers a high-level interface for performing symmetric cryptography algorithms using SCP coprocessor. The SCL has implemented block repetitions, dummy calculations, backward calculation rounds and known-answer test security functions using 128, 192 and 256 AES algorithm, and TDES or DES algorithms. The SCL also supports ECB, CBC, CTR, CFB and PCBC block cipher modes, however the PCBC mode is not a part of this evaluation. The SCL provides public API [10] containing cipher block management functions (Cipher*), block cipher mode encryption/decryption functions (BCM*), cipher block instantiation helper functions CipAlg_*_Sec1 and CipAlg_*_Sec2, however the CipAlg_*_Sec1 functions are not a part of this evaluation.

Note that 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 user’s choice. 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.

If the Crypto@2304T is blocked the user will not be able to use the functionality of the EC, the RSA and the Toolbox

[1] BSI Bundesamt für Sicherheit in der Informationstechnik – Federal office for information security

library, as these optional software libraries perform their basic arithmetic operations of the asymmetric cryptographic coprocessor. If the SCP is blocked the user will not be able to use the hardware based AES and TDES calculations and furthermore he will not be able to use the functionality of the SCL, as this optional software library is based on the symmetric cryptographic coprocessor.

The TOE can be also be delivered without a specific optional software library. In this case the TOE does not provide the additional specific security functionality Rivest-Shamir-Adleman Cryptography (RSA) or/and Elliptic Curve Cryptography (EC) or/and SHA-2 or/and SCL based Advanced Encryption Standard (AES) or/and SCL based Triple Data Encryption Standard (TDES).

To fulfill 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. Thereby, 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 covering the complete core, 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 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. And more, the TOE is equipped with signal protection implemented by an Infineon-specific shielding combined with secure wiring and shielding of security critical signals.

In the Confidential Security Target [35] 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 and in the Protection Profile (PP) [1] and are referenced here. These requirements build up a minimal standard common for all Smartcards.

The security functions are defined here in the Security Target as property of this specific TOE. Here it is shown how this specific TOE fulfills the requirements for the standard defined in the Protection Profile [1].

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 PP [1] as it belongs to the specific TOE.

2.1 TOE Definition

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

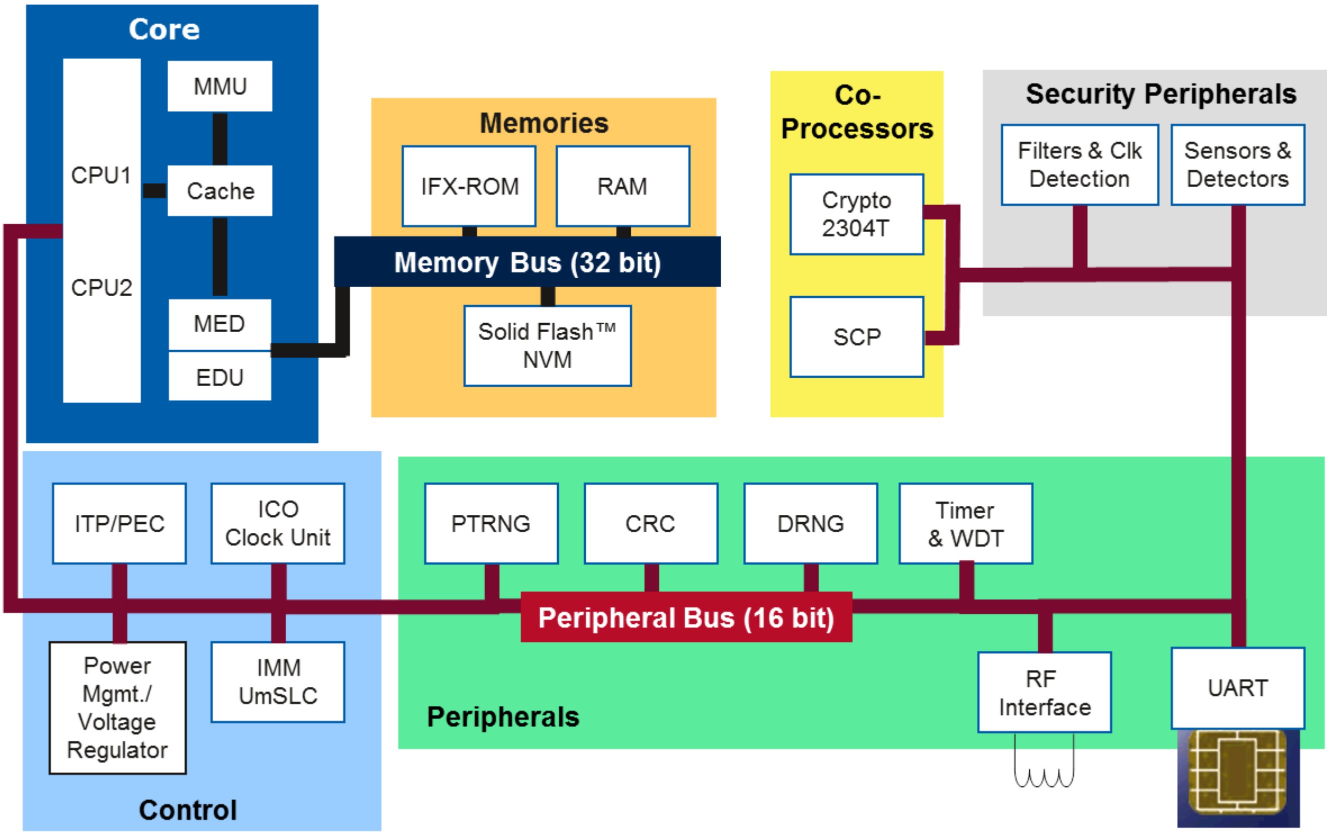
This TOE is intended to be used in smart cards for particularly security-relevant applications and for its previous use as developing platform for smart card operating systems according to the lifecycle model from the PP [1].

The term Smartcard Embedded Software is used in the following for all operating systems and applications stored and executed on the TOE regardless whether it is a smartcard or another application of form factor. 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 modules and analogue peripherals.

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. 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 (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 certain 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 cryptographic operations are implemented on the TOE: The Crypto2304T 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. 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 Crypto2304T, or with both crypto coprocessors blocked. The blocking depends on the customer demands prior to the production of the hardware. If the SCP is blocked the user will neither be able to use the solely hardware based AES and TDES calculations of the TOE nor the SCL based AES and TDES calculations. If the Crypto@2304T is blocked the user will not be able to use the services of the optional RSA, EC and Toolbox libraries. No accessibility of the deselected cryptographic co-processors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic coprocessors.

The 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. More details are given in the Confidential Security Target [35] and in the hardware reference manual [6].

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 are required. The TRNG respectively PTRNG fulfills the requirements from the functionality class PTG.2 of the AIS31 and produces genuine random numbers which then can be used directly or as seed 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 [6].

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 [6].

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 different communication protocols: ISO 7816, ISO 14443 Type A and Type B, ISO/IEC 18092 NFC passive mode, Mifare compatible software Interface, as well as further communication modes, allowing also implementation of user defined concepts for contact based or contactless communication. The flexibility of the communication interfaces enable for example also the use cases involving external analogue modems, which are typically deemed for applications running in mobile devices. Please note that these external parts are of course not part of this TOE. More details are given the Confidential Security Target [35] and the hardware reference manual [6].

Supporting a Mifare compatible software Interface application requires a dedicated small space of memory. In this context and depending on user’s choice, various memory sections of 1 up to 4 kByte each 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. Please note that the Mifare part does not provide any TOE security functionality.

The implemented sleep mode logic (clock stop mode per ISO/IEC 7816-3) is used to reduce the overall power consumption. Contactless products provide a low-power halt mode for operation with reduced power.

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) and Flash Loader together compose the TOE 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 user software can be implemented in various options depending on the user's choice as described in chapter 2.2.2. Thereby the user software, or parts of it, can be downloaded into the SOLID FLASH™ NVM, either during production of the TOE or at customer side. In the latter case, the user downloads his software or the final parts of it at his own premises, using the Flash Loader software.

The toolbox library does not provide cryptographic support or additional security functionality as it provides only the following basic long integer arithmetic and modular functions in software, supported by the cryptographic coprocessor: Addition, subtraction, division, multiplication, comparison, reduction, modular addition, modular subtraction, modular multiplication, modular inversion and modular exponentiation. No security relevant policy, mechanism or function is supported. The toolbox library is deemed for software developers as support for simplified implementation of long integer and modular arithmetic operations.

The RSA library is used to provide a high level interface to RSA (Rivest, Shamir, Adleman) cryptography implemented on the hardware component Crypto@2304T and includes countermeasures against SPA, DPA and DFA attacks. The routines are used for the RSA key generation (only in v2.07.003), RSA signature verification, the RSA signature generation and the RSA modulus recalculation. The hardware Crypto@2304T unit provides the basic long number calculations (add, subtract, multiply, square with 1100 bit numbers) with high performance. The RSA library is delivered as object code and in this way integrated in the user software. The RSA library can perform RSA operations from 512 to 4096 bits.

Following the BSI[1] recommendations, key lengths below 1976 bit are not included in the certificate.

The EC library is used to provide a high level interface to Elliptic Curve cryptography implemented on the hardware component Crypto@2304T and includes countermeasures against SPA, DPA and DFA attacks. The routines are used for ECDSA signature generation, ECDSA signature verification, ECDSA key generation and Elliptic Curve Diffie-Hellman key agreement. In addition, the EC library provides an additional function for calculating primitive elliptic curve operations like EC Add and EC Double. EC curves over prime field Fp, as well as over GF(2^n) finite field are supported too.

The EC library is delivered as object code and in this way integrated in the user software. The certification covers the standard NIST [17] and Brainpool [18] Elliptic Curves with key lengths of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits, due to national AIS32 regulations by the BSI. Note that there are further uncounted side-channel-secure curve types which the user can optionally add in the composition certification process.

The Base library is used internally by the RSA, the EC and the Toolbox library, thus if one of the aforementioned libraries is ordered, the Base library will be automatically included in the delivery. The Base library does not provide any additional specific security functionality.

The SHA-library provides the calculation of a hash value of freely chosen data input in the CPU. The SHA-library is delivered as object code and is in this way available for the user software.

This secure hash-algorithm SHA-2 is intended to be used for signature generation, verification and generic data integrity checks. The use for keyed hash operations like HMAC or similar security critical operations involving keys, is not subject of this TOE and requires specific security improvements and DPA analysis including the operating system, which is not part of this TOE. Further essential information about the usage is given in the confidential user guidance [11].

[1] BSI Bundesamt für Sicherheit in der Informationstechnik – Federal office for information security

Public

The SCL library provides public cipher API for user application. The Cipher API contains functionality on operation with the SCL: configuration of runtime settings, encryption and decryption of multiple data blocks using one of the built-in Block Cipher Modes: ECB, CBC, CTR, CFB and PCBC. The SCL also provides functionality of adding custom BCMs. Public AES API provides encryption and decryption of a 128-bit block using AES standard. The following key sizes are supported: 128 bits, 192 bits, 256 bits. Public DES API provides encryption and decryption of a 64-bit block using the following algorithms: DES and TDES with an effective key size of 56 bits (+ 8 parity bits) as well as 112 and 168 bits. Please note that the PCBC block cipher mode and the "*_*Sec1*"-functions of the SCL are not part of this evaluation.

Note that the TOE can be delivered without a specific optional software library. In this case the TOE does not provide the additional specific security functionality Rivest-Shamir-Adleman Cryptography (RSA) or/and Elliptic Curve Cryptography (EC) or/and SHA-2 or/and SCL based Advanced Encryption Standard (AES) or/and SCL based Triple Data Encryption Standard (TDES).

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:

The silicon die, respectively the IC or hardware, in several versions:

Each version differences from each other just by the input capacity of the radio frequency interface RFI or by the additional metal layer on top with according firmware and optional software of the security controller, as defined in the chapters above.

The TOE is also delivered in various configurations, achieved by means of blocking.

The user's guidance documentation including hardware, software, Flash Loader, secure coding, and other reference manuals.

All product derivatives of this TOE, including all configuration possibilities, regardless whether coming with or without top metal layer, are manufactured by Infineon Technologies AG. In the following descriptions, the term "manufacturer" stands short for Infineon Technologies AG, the manufacturer of the TOE.

New configurations can occur at any time, but in any case the user is able to clearly identify the TOE hardware, its configuration and proof the validity of the certificate independently, meaning without involving the manufacturer.

Entirely all means of blocking and the, for the blocking involved firmware respectively software parts have been subject of the evaluation. All resulting configurations of a TOE derivative are subject of the certificate. All resulting configurations are either at the predefined limits or within the predefined configuration ranges.

The firmware used for the TOE internal testing and TOE operation, the firmware and software parts exclusively used for the blocking, the parts of the firmware and software required for cryptographic support are part of the TOE and therefore part of the certification. The documents as described in section 2.2.4 and referenced in Table 1, are supplied as user guidance.

Not part of the TOE and not part of the certification are the Smartcard Embedded Software respectively user software, and commercial parts the Billing-Per-Use software.

2.2.1 Hardware of the TOE

The hardware part of the TOE (see Figure 1) as defined in the PP [1] is comprised of:

Core System

Proprietary CPU implementation of the Intel MCS251 standard architecture from functional perspective, represented by two CPUs from hardware perspective

CACHE with Post Failure Detection

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

Memory Management Unit (MMU)

Memories

Read-Only Memory (ROM), not user available

Random Access Memory (RAM)

SOLID FLASH™ NVM

Public

Note: The TOE has implemented an Electrical Erasable Programmable Read Only Memory (EEPROM) module. This EERPOM module is configured to act for the most part as a flash memory. Therefore, the module is called SOLID FLASH™ NVM.

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)

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

Security Peripherals

Filters

Sensors

Buses

Memory Bus

Peripheral Bus

2.2.2 Firmware and Software of the TOE

For this TOE, the user can chose between different alternative firmware packages and can also chose the optional libraries. The exact versions of firmware respectively optional software alternatives are given in Table 1.

The entire firmware of the TOE consists of different parts:

One part comprises the RMS and SAM routines for SOLID FLASH™ NVM programming, security functions test, and random number online testing (Resource Management System, IC Dedicated Support Software in the Protection Profile [1]).

The RMS and SAM routines are stored from Infineon Technologies AG in the ROM, while belonging patches (if any) are located in a protected area of the SOLID FLASH™ NVM. The ROM is only available for Infineon Technologies AG, the user has no access.

The second part is the STS, consisting of test and initialization routines (Self-Test Software, IC Dedicated Test Software in PP [1]). The STS routines are stored in the ROM and the belonging patch (if any) is located in a protected area of the SOLID FLASH™ NVM. The STS is not accessible for the user software.

The third part is the Flash Loader. This piece of software is located in the ROM, but some parts of it are also stored in the SOLID FLASH™ NVM. It enables the download of the user software or parts of it to the SOLID FLASH™ NVM. After completion of the download the Flash Loader shall be locked by the by the user.

The fourth part is the Mifare compatible software interface routines. Note that these routines are always present, but are deactivated, in case that a derivative comes without RF interface. Thus the user software interface is identical in both cases and consequently the related interface routines can be called in each of the derivatives. In case the related Mifare compatible software interface routines are called in derivatives without RF interface, an error code is returned. In the other case the related function is performed. Please note that the Mifare compatible software interface does not provide any specific TOE security functionality.

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.

The optional software part of the TOE consists of the SCL, RSA, the EC, the SHA-2, the Base and the toolbox libraries.

The SCL library is used to provide a high-level interface to DES/TDES and AES symmetric cryptographic operation. It uses the SCP of the underlying hardware and implements countermeasures against all known weaknesses of the SCP v3 (e.g. dummy calculations, block repetitions and backward calculation). The SCL library consists of three C-library files: Cipher.lib, AES.lib, and DES.lib. These files are not distributed separately, and, therefore, all three files are called together Symmetric Cryptographic Library. The SCL supports the ECB, CBC, CTR CFB and PCBC block cipher modes. Please note that the PCBC mode, as well as “*_Sec1”-functions of the SCL, are not covered by the evaluation.

The SHA-2 library provides the calculation of a hash value of freely chosen data input in the CPU. The SHA-2 library is delivered as object code and is in this way available for the user software. This secure hash-algorithm SHA-2 is intended to be used for signature generation, verification and generic data integrity checks. The use for keyed hash operations like HMAC or similar security critical operations involving keys, is not subject of this TOE and requires specific security improvements and DPA analysis including the operating system, which is not part of this TOE. Further essential information about the usage is given in the confidential user guidance.

The RSA library is used to provide a high level interface to the RSA cryptography implemented on the hardware component Crypto@2304T and includes countermeasures against SPA, DPA and DFA attacks. The routines are used for the RSA signature verification, the RSA signature generation and the RSA modulus recalculation. The module provides the basic long number calculations (add, subtract, multiply, square with 1100 bit numbers) with high performance.

The RSA library is delivered as object code and in this way integrated in the user software. The RSA library can perform RSA operations from 512 to 4096 bits. Depending on the customer’s choice, the TOE can be delivered with the 4096 code portion or with the 2048 code portion only. The 2048 code portion is included in both. Parts of the evaluation are the RSA straight operations with key length from 1976bits to 2048 bits, and the RSA CRT[1] operations with key lengths of 1976Bits to 4096 Bits.

The EC library is used to provide a high level interface to Elliptic Curve cryptography and includes countermeasures against SPA, DPA and DFA attacks. The routines are used for ECDSA signature generation, ECDSA signature verification, ECDSA key generation and Elliptic Curve Diffie-Hellman key agreement. In addition, the EC library provides an interface to an addition function for primitive elliptic curve operations like ECC Add and ECC Double. ECC curves over prime field Fp, as well as over GF(2^n) finite field are supported too.

The EC library is delivered as object code and in this way integrated in the user software. The certification covers the standard NIST [17] and Brainpool [18] Elliptic Curves with key lengths of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits, due to national AIS32 regulations by the BSI. Note that there are further uncounted side-channel-secure curve types which the user can optionally add in the composition certification process.

The toolbox library does not provide cryptographic support or additional security functionality as it provides only the following basic long integer arithmetic and modular functions in software, supported by the cryptographic coprocessor: Addition, subtraction, division, multiplication, comparison, reduction, modular addition, modular subtraction, modular multiplication, modular inversion and modular exponentiation. No security relevant policy, mechanism or function is supported. No security relevant policy, mechanism or function is supported. The toolbox library is deemed for software developers as support for simplified implementation of long integer and modular arithmetic operations.

The Base Library provides the low level interface to the asymmetric cryptographic coprocessor and is necessary in order to use the EC, RSA or Toolbox library. Thus it is automatically included in the delivery if any of the aforementioned libraries (EC, RSA, Toolbox) is ordered. The Base library does not provide any security functionality on its own.

Note:

The cryptographic libraries SCL, RSA, EC and SHA-2 are delivery options. The TOE may come with free combinations of or even without these libraries. In the case of coming without one or any combination of the cryptographic libraries SCL, RSA, EC and SHA-2, the TOE does not provide the Additional Specific Security Functionality Rivest-Shamir-Adleman Cryptography (RSA) and/or Elliptic Curve Cryptography (EC) and/or SHA-2 and/or SCL based Advanced Encryption Standard (AES) and/or SCL based Triple Data Encryption Standard (TDES).

2.2.3 Interfaces of the TOE

The interfaces are constituted out of:

- 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. Further combinations involving the pads and parts of the RF interface are also possible and described in the Confidential Security Target [35] and in the hardware reference manual [6].

[1] CRT: Chinese Remainder Theorem

- 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. Note that further interface options are available and described in the Confidential Security Target [35].
- 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).
- The interface to the RSA calculations is defined from the RSA library interface.
- The interface to the EC calculations is defined from the EC library interface
- The interface to the SHA-2 calculation is defined from the SHA-2 library interface.
- The interface to the Toolbox is defined from the Toolbox library interface.
- The interface to the symmetric crypto-operations DES/TDES/AES is defined from the SCL library interface.

Note that the interfaces to the optional software libraries (RSA, EC, Toolbox, SHA-2 and SCL) are optionally depending on the customer order.

2.2.4 Guidance Documentation

The guidance documentation consists of the listing given in the table in 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:

- M7892, Controller Family for Security Applications, Hardware Reference Manual [6].
- SLx 70 Family Production and Personalization [7] contains detailed information about the usage of the Flash Loader.
- SLE 70 Family Programmer’s Reference User’s Manual [8] describes the usage and interface of the Resource Management System RMS.
- SLE 70 Asymmetric Crypto Library for Crypto@2304T, RSA, ECC, Toolbox, User Interface (optional) [9], contains all interfaces of the cryptographic RSA- and EC libraries, as well as of the Toolbox library. This document is only delivered to the user in case the RSA library and/or the EC library and/or the Toolbox library is/are part of the delivered TOE.
- SLE 70 Asymmetric Crypto Library for Crypto@2304T, RSA, ECC, Toolbox, User Interface (optional) [35], contains all interfaces of the cryptographic RSA- and EC libraries, as well as of the Toolbox library. This document is only delivered to the user in case the RSA library and/or the EC library and/or the Toolbox library is/are part of the delivered TOE.

- SCL78 Symmetric Crypto Library for SCPv3 DES / AES 16-bit Security Controller User Interface [10]. This document contains the description of the user interface, general concepts and important security guidelines for software designers.
- SLx 70 Family, Secure Hash Algorithm SHA-2, (SHA 256/224, SHA 512/384) [11]. This document contains all interfaces of the SHA-2 library and is only delivered to the user in case the SHA-2 library is part of the delivered TOE.
- Crypto@2304T User Manual [12], describing the architecture of cryptographic coprocessor on register level. It also provides a functional description of the register architecture, instruction set and gives programming guidance.
- AMM Advanced Mode for Mifare-Compatible Technology [13], Addendum to M7892 Hardware Reference Manual. Additional user guidance how to use the Advanced Mode for Mifare Technology (AMM). This documentation is provisioned to the user if the AMM option has been ordered. This user guidance describes the interface and how to use this communication mode. This is an addendum to the HRM [6].
- M7892 Security Guidelines [14]. This document discusses and provides code examples of how the user can consider the secure programming recommendations.
- M7892 Controller Family for Security Applications, Errata Sheet [15]. It can occur that the TOE or related documentation can be updated during the life cycle. This is reported to the users by the confidential Errata Sheet.

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
- with or without inlay antenna mounting
- in form of plain wafers
- in any IC case (for example TSSOP28, VQFN32, VQFN40, CCS-modules, etc.)
- in no IC case or IC package, simply as bare dies
- or in whatever type of IC 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 subject of the appropriate audit.

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 [11]. Nevertheless in both cases the TOE is finished and the extended test features are removed. In this document are always both cases mentioned to avoid incorrectness but from the security policy point of view the two cases are identical.

The delivery to the software developer (phase 2 → phase 1) contains the development package and is delivered in form of documentation as described above, data carriers containing the tools and emulators as development and debugging tool.
Part of the software delivery could also be the Flash Loader program, provided by Infineon Technologies AG, running on the TOE and receiving the transmitted information of the user software to be loaded into the SOLID FLASH™ NVM. The download is only possible after successful authentication and the user software can also be downloaded in an encrypted way. In addition, the user is after he finalized the download and prior deliver to third party obligated to permanently lock further use of the Flash Loader. Note that it depends on the procurement order, whether Flash Loader program is present or not.

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

Table 5: Forms of Delivery

TOE Component	**Delivered Format**	**Delivery Method**[1]	**Comment**
Hardware			
M7892 B11	Wafer, IC case, packages	Postal transfer in cages	All materials are delivered to distribution centers in cages, locked.
Firmware			
STS	–	–	This firmware part of stored on the delivered hardware.
RMS	–	–	This firmware part of stored on the delivered hardware
SAM	–	–	This firmware part of stored on the delivered hardware.
Mifare compatible software interface routines	–	–	This firmware part of stored on the delivered hardware.
Flash Loader	–	–	This firmware part of stored on the delivered hardware.
Software			

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

Public

TOE Component	Delivered Format	Delivery Method[1]	Comment
RSA Library	L251 Library File (object code)	Secured download[1]	Optional; depending on order.
EC Library	L251 Library File (object code)	Secured download[1]	Optional; depending on order.
Toolbox Library	L251 Library File (object code)	Secured download[1]	Optional; depending on order.
Base Library	L251 Library File (object code)	Secured download[1]	Optional; depending on presence of RSA, EC and Toolbox.
SHA-2 Library	L251 Library File (object code)	Secured download[1]	Optional; depending on order.
SCL	L251 Library File (object code)	Secured download[1]	Optional; depending on order. Consists of three library files.
Guidance Documentation			
Hardware Reference Manual [6]	Personalized PDF	Secured download[1]	–
Production and Personalization User's Manual [7]	Personalized PDF	Secured download[1]	–
Programmer's Reference Manual [8]	Personalized PDF	Secured download[1]	–
Asymmetric Crypto Library User Interface for version v1.02.013 [9]	Personalized PDF	Secured download[1]	Optional, delivered if at least one of the RSA, EC or Toolbox libraries is ordered (v1.02.013)
Asymmetric Crypto Library User Interface for version v2.07.003 [35]	Personalized PDF	Secured download[1]	Optional, delivered if at least one of the RSA, EC or Toolbox libraries is ordered (v2.07.003)
Secure Hash Algorithm SHA-2 [11]	Personalized PDF	Secured download[1]	Optional; delivered if the SHA-2 library is ordered.
Crypto@2304T User Manual [12]	Personalized PDF	Secured download[1]	Optional, delivered if the TOE is ordered with an accessible Crypto@2304T.
M7892 B11 Security Guidelines [14]	Personalized PDF	Secured download[1]	–
M7892 B11 Errata Sheet [15]	Personalized PDF	Secured download[1]	–
AMM Advanced Mode for Mifare-Compatible Technology [13]	Personalized PDF	Secured download[1]	Optional; delivered if the AMM is ordered.

TOE Component	Delivered Format	Delivery Method[1]	Comment
Symmetric Crypto Library User Interface [10]	Personalized PDF	Secured download[1]	Optional, delivered if the SCL is ordered.

2.2.6 Production Sites

The TOE may be handled in different production sites but the silicon of this TOE is produced in Dresden, Germany only, as listed below. To distinguish the different production sites of various products in the field, the site is coded into the Generic Chip Ident Mode (GCIM) data. The exact coding of the generic hip identification data is described in the hardware reference manual, [6].

The delivery measures are described in the ALC_DVS aspect.

Table 6: Production site in chip identification

Production Site	Design Step	Chip Identification
Dresden, Germany	B11	Byte number 13: 02h

3 Conformance Claims (ASE_CCL)

3.1 CC Conformance Claim

This Security Target (ST) and the TOE claim conformance to Common Criteria version v3.1 part 1 [2], part 2 [3] and part 3 [4] following the evaluation methodology will be used for this evaluation "Common Methodology for Information Technology Security Evaluation" [33].

Furthermore 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

This Security Target is conformant to the Security IC Platform Protection Profile [1].

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

BSI-PP-0035, Version 1.0, dated 2007-06-15.

The Protection Profile [1] requires the **strict conformance** for the ST claiming conformance to this PP. This is mentioned in chapter 2.2 of [1].

3.3 Package Claim

This Security Target does not claim conformance to a package of the PP [1].

The Security Target is EAL6 augmented with the component ALC_FLR.1.

Table 7: Augmentations of the assurance level of the TOE

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

Thus the targeted EAL6+ level includes already the augmentations of the PP [1] (AVA_VAN.5 and ALC_DVS.2) and includes further augmentations compared to the predefined EAL6 assurance level (this package is defined in CC part 3).

3.4 Conformance Rationale

This Security Target claims conformance to one PP, the Security IC Platform Protection Profile [1].

The Protection Profile requires the **strict conformance** for the ST claiming conformance to this PP. This is mentioned in chapter 2.2 of [1].

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

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:

Compared to the PP [1], the security problem definition of this Security Target is enhanced by adding:

- Additional threats (for details refer to chapter 4.1.1).
- Additional organization security policies (for details refer to chapter 4.2.1).
- And additional assumptions (for details refer to chapter 4.3.1).

Aside these add-ons, the security problem definition of this Security Target is consistent with the statement of the security problem definition in the PP [1], as the Protection Profile [1] demands strict conformance.

The threats and OSPs of the Security Target are a superset of the ones defined in the PP [1]. Although an additional assumption is defined in the Security Target compared to the PP [1], the Security Target is still strict conformant to the PP [1], 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 Objectives

Compared to the PP [1], the security objectives of this Security Target are enhanced by adding supplemental security objectives (for details refer to 5.1). These modifications are necessary due to the additional security functionalities, one coming from the cryptographic libraries - O.Add-Functions, and due to the memory access control - O.Mem-Access, additional security objectives have been introduced.

The Security Target is still strict conformant to the PP [1], as it is permissible for a Security Target to contain additional security objectives compared to the PP.

3.4.3 Summary

Due to the rationale provided above the Security Problem Definition (refer to chapter 4) and the Security Objectives (refer to chapter 5) are strict conformant to the PP [1].

The Security Target enhances the required assurance package EAL4+ augmented with AVA_VAN.5 and ALC_DVS.2 of the PP [1] to EAL6+ augmented with ALC_FLR.1. Thus the Security Target contains all assurance requirements, respectively hierarchically higher assurance requirements, of the PP [1].

Furthermore all security functional requirements defined in the PP [1] are included and completely defined in the Security Target and the augmented security functional requirements are listed in Table 17.

The following security functional requirements are defined in the Extended Component Definition of the Security Target (refer to chapter 6):

- FPT_TST.2 “Subset TOE security testing” (Requirements from [1])

All open assignments and selections of the security functional requirements are either done in the PP [1] or in this Security Target (please refer to chapter 7.1).

3.5 Application Notes

The functional requirement FCS_RNG.1 is a refinement of the FCS_RNG.1 defined in the Protection Profile [1] according to AIS31, see reference [5].

4 Security Problem Definition (ASE_SPD)

The content of the PP [1] 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. An overview on attacks is given in PP [1] section 3.2.

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

Table 8: Threats according PP [1]

T.Phys-Manipulation	Physical Manipulation
T.Phys-Probing	Physical Probing
T.Malfunction	Malfunction due to Environmental Stress
T.Leak-Inherent	Inherent Information Leakage
T.Leak-Forced	Forced Information Leakage
T.Abuse-Func	Abuse of Functionality
T.RND	Deficiency of Random Numbers

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 (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 9: Additional threats 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 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 and of the Security IC Embedded Software (while being executed/processed and while being stored in the TOE's memories),
- SC2 Confidentiality of User Data and of the Security IC Embedded Software (while being processed and while being stored in the TOE's memories)
- SC3 Correct operation of the security services provided by the TOE for the Security IC Embedded Software.
- SC4 Continuous availability of random numbers

SC4 is an additional security service provided by this TOE which is the availability of random numbers. These random numbers are generated either by a true random number or a deterministic random number generator or by both, when a true random number is used as seed for the deterministic random number generator. Note that the generation of random numbers is a requirement of the PP [1].

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

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

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

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

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

For details see PP [1] section 3.1.

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

The organizational security policies are defined and described in PP [1] section 3.3. Due to the augmentations of PP [1] an additional policy is introduced and described in the next chapter.

Table 10: Organizational Security Policies according PP [1]

P.Process-TOE	Protection during TOE Development and Production

4.2.1 Augmented Organizational Security Policy

Due to the augmentations compared to the PP [1] an additional policy is 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 policy "Additional Specific Security Functionality (P.Add-Functions)" as specified below.

P.Add-Functions	Additional Specific Security Functionality The TOE shall provide the following specific security functionality to the Smartcard Embedded Software • Advanced Encryption Standard (AES) • Triple Data Encryption Standard (TDES) • Rivest-Shamir-Adleman Cryptography (RSA) • Elliptic Curve Cryptography (EC) • Secure Hash Algorithm SHA-2

Note:

The cryptographic libraries SCL, RSA, EC, SHA-2 and the Toolbox library are delivery options. Therefore the TOE may come with free combinations of or even without these libraries. In the case of coming without one or any combination of the cryptographic libraries SCL, RSA, EC and SHA-2, the TOE does not provide the Additional Specific Security Functionality Rivest-Shamir-Adleman Cryptography (RSA) and/or Elliptic Curve Cryptography (EC) and/or SHA-2 and/or SCL based Advanced Encryption Standard (AES) and/or SCL based Triple Data Encryption Standard (TDES). The Toolbox library is no cryptographic library and provides no additional specific security functionality. If RSA, EC or Toolbox are part of the shipment, the Base Library is automatically included. The Base Library does not provide additional specific security functionality.

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 TDES computation supported by hardware is possible (neither solely hardware based nor SCL based). In case the crypto@2304T is blocked, no RSA and EC computation supported by hardware is possible. The use of the SHA-2 library is also possible with both crypto coprocessors blocked. 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.

4.3 Assumptions

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

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

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.Plat-Appl	Usage of Hardware Platform The Security IC Embedded Software is designed so that the requirements from the following documents are met: (i) TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the hardware data sheet, and the hardware application notes, and (ii) findings of the TOE evaluation reports relevant for the Security IC Embedded Software as documented in the certification report.

A.Resp-Appl	Treatment of User Data All User Data are owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context.

Table 11: Assumption according PP [1]

A.Process-Sec-IC	Protection during Packaging, Finishing and Personalization
A.Plat-Appl	Usage of Hardware Platform
A.Resp-Appl	Treatment of User Data

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

4.3.1 Augmented Assumptions

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

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

Note that here the routines which may compromise keys when being executed are part of the Smartcard Embedded Software. In contrast to this the threats T.Leak-Inherent and T.Leak-Forced address (i) the cryptographic routines which are part of the TOE.

5 Security Objectives (ASE_OBJ)

This section shows the subjects and objects, which 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 and of the Security IC Embedded Software
- SG2 maintain the confidentiality of User Data and of the Security IC Embedded Software
- SG3 maintain the correct operation of the security services provided by the TOE for the Security IC Embedded Software
- SG4 provision of random numbers.

5.1 Security Objectives for the TOE

The security objectives of the TOE are defined and described in PP [1] section 4.1.

Table 12: Objectives for the TOE according to PP [1]

O.Phys-Manipulation	Protection against Physical Manipulation
O.Phys-Probing	Protection against Physical Probing
O.Malfunction	Protection against Malfunction
O.Leak-Inherent	Protection against Inherent Information Leakage
O.Leak-Forced	Protection against Forced Information Leakage
O.Abuse-Func	Protection against Abuse of Functionality
O.Identification	TOE Identification
O.RND	Random Numbers

The TOE provides “Additional Specific Security Functionality (O.Add-Functions)” as specified below.

O.Add-Functions	Additional Specific Security Functionality The TOE must provide the following specific security functionality to the Smartcard Embedded Software: • Advanced Encryption Standard (AES) • Triple Data Encryption Standard (TDES) • Rivest-Shamir-Adleman (RSA) • Elliptic Curve Cryptography (EC) • Secure Hash Algorithm (SHA-2)

Note:

The cryptographic libraries SCL, RSA, EC, SHA-2 and the Toolbox library are delivery options. Therefore the TOE may come with free combinations of or even without these libraries. In the case of coming without one or any combination of the cryptographic libraries SCL, RSA, EC and SHA-2, the TOE does not provide the Additional Specific Security Functionality Rivest-Shamir-Adleman Cryptography (RSA) and/or Elliptic Curve Cryptography (EC) and/or SHA-2 and/or SCL based Advanced Encryption Standard (AES) and/or SCL based Triple Data Encryption Standard (TDES). The Toolbox library is no cryptographic library and provides no additional specific security functionality. If RSA, EC or Toolbox are parts of the shipment, the Base Library is automatically included. The Base Library does not provide additional specific security functionality.

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 TDES computation supported by hardware is possible (neither solely hardware based nor SCL based). In case the crypto@2304T is blocked, no RSA and EC computation supported by hardware is possible. The use of the SHA-2 library is also possible with both crypto coprocessors blocked. No accessibility of the deselected cryptographic coprocessors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic Coprocessors.

The 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 13: Additional objectives due to TOE specific functions and augmentations

O.Add-Functions	Additional specific security functionality
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 is defined in PP [1] section 4.2 and 4.3. The table below lists the security objectives.

Table 14: Security objectives for the environment according to PP [1]

Phase 1	OE.Plat-Appl	Usage of Hardware Platform
	OE.Resp-Appl	Treatment of User Data
Phase 5 – 6 optional Phase 4	OE.Process-Sec-IC	Protection during composite product manufacturing

5.2.1 Clarification of “Usage of Hardware Platform (OE.Plat-Appl)”

Regarding the cryptographic services this objective of the environment has to be clarified. The TOE supports cipher schemes as additional specific security functionality. If required the Smartcard Embedded Software shall use these cryptographic services of the TOE and their interface as specified. When key-dependent functions implemented in the Smartcard Embedded Software are just being executed, the Smartcard Embedded Software must provide protection against disclosure of confidential data (User Data) stored and/or processed in the TOE by using the methods described under “Inherent Information Leakage (T.Leak-Inherent)” and “Forced Information Leakage (T.Leak-Forced)“.

The objectives of the environment regarding the memory, software and firmware protection and the SFR and peripheral-access-rights-handling have to be clarified. For the separation of different applications the Smartcard Embedded Software (Operating System) may implement a memory management scheme based upon security functions of the TOE.

5.2.2 Clarification of “Treatment of User Data (OE.Resp-Appl)”

Regarding the cryptographic services this objective of the environment has to be clarified. By definition cipher or plain text data and cryptographic keys are User Data. The Smartcard Embedded Software shall treat these data appropriately, use only proper secret keys (chosen from a large key space) as input for the cryptographic function of the TOE and use keys and functions appropriately in order to ensure the strength of cryptographic operation.

This means that keys are treated as confidential as soon as they are generated. The keys must be unique with a very high probability, as well as cryptographically strong. For example, it must be ensured that it is beyond practicality to derive the private key from a public key if asymmetric algorithms are used. If keys are imported into the TOE and/or derived from other keys, quality and confidentiality must be maintained. This implies that appropriate key management has to be realized in the environment.

Regarding the memory, software and firmware protection and the SFR and peripheral access rights handling these objectives of the environment has to be clarified. The treatment of User Data is also required when a multi-application operating system is implemented as part of the Smartcard Embedded Software on the TOE. In this case the multi-application operating system should not disclose security relevant user data of one application to another application when it is processed or stored on the TOE.

5.2.3 Clarification of “Protection during composite product manufacturing (OE.Process-Sec-IC)”

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

5.3 Security Objectives Rationale

The security objectives rationale of the TOE are defined and described in PP [1] section 4.4. For the additional objectives of this ST a rational is provided below.

Table 15: Security Objective Rationale

Assumption, Threat or Organisational Security Policy	Security Objective
P.Add-Functions	O.Add-Functions
A.Key-Function	OE.Plat-Appl OE.Resp-Appl
T.Mem-Access	O.Mem-Access

The justification related to the security objective “Additional Specific Security Functionality (O.Add-Functions)” is as follows: Since O.Add-Functions requires the TOE to implement exactly the same specific security functionality as required by P.Add-Functions; the organizational security policy is covered by the objective.

Nevertheless 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 required by P.Add-Functions. (Note that these objectives support that the specific security functionality is provided in a secure way as expected from P.Add-Functions.) Especially O.Leak-Inherent and O.Leak-Forced refer to the protection of confidential data (User Data or TSF data) in general. User Data are also processed by the specific security functionality required by P.Add-Functions.

Compared to PP [1] clarification has been made for the security objective “Usage of Hardware Platform (OE.Plat-Appl)”: If required the Smartcard Embedded Software shall use these cryptographic services of the TOE and their interface as specified. In addition, the Smartcard Embedded Software must implement functions which perform operations on keys (if any) in such a manner that they do not disclose information about confidential data. The non-disclosure due to leakage A.Key-Function attacks is included in this objective OE.Plat-Appl. This addition ensures that the assumption A.Plat-Appl is still covered by the objective OE.Plat-Appl although additional functions are being supported according to O.Add-Functions.

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

Compared to the PP [1] an enhancement regarding memory area protection has been established. The clear definition of privilege levels for operated software establishes the clear separation of different restricted memory areas for running the firmware, downloading and/or running the operating system and to establish a clear separation between different applications. Nevertheless, it is also possible to define a shared memory section where separated applications may exchange defined data. The privilege levels clearly define by using a hierarchical model the access right from one level to the other. These measures ensure that the threat T.Mem-Access is clearly covered by the security objective O.Mem-Access.

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

6 Extended Component Definition (ASE_ECD)

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

- the family **FCS_RNG** at the class FCS Cryptographic Support
- the family **FMT_LIM** at the class FMT Security Management
- the family **FAU_SAS** at the class FAU Security Audit
- the component **FPT_TST.2** at the class FPT Protection of the TSF

The extended components FCS_RNG, FMT_LIM and FAU_SAS are defined and described in PP [1] 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.

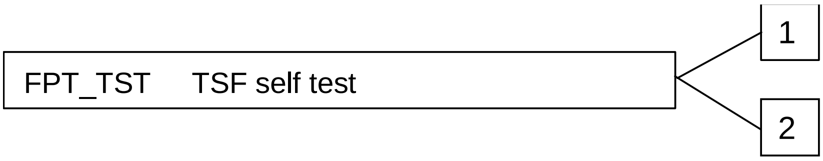
The functional component “Subset TOE testing (FPT_TST.2)” is specified as follows (Common Criteria Part 2 extended).

Public

6.2.1 TSF Self-Test (FPT_TST)

Family Behavior The Family Behavior is defined in [3] section 15.14 (442, 443).

Component leveling



FPT_TST.1 The component FPT_TST.1 is defined in [3] section 15.14 (444, 445, 446).

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

Management: FPT_TST.2

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

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

Audit: FPT_TST.2

There are no auditable events foreseen.

FPT_TST.2	**Subset TOE Testing**
Hierarchical to	No other components.
Dependencies:	No dependencies 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 [1] 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 [1] section 6.1 and in the following description.

The Table 15 provides an overview of the functional security requirements of the TOE, defined in the in PP [1] section 6.1. In the last column it is marked if the requirement is refined. The refinements are also valid for this ST.

Table 16: Security functional requirements defined in PP [1]

Security Functional Requirement		Refined in PP [1]
FRU_FLT.2	“Limited fault tolerance“	Yes
FPT_FLS.1	“Failure with preservation of secure state”	Yes
FMT_LIM.1	“Limited capabilities”	No
FMT_LIM.2	“Limited availability”	No
FAU_SAS.1	“Audit storage”	No
FPT_PHP.3	“Resistance to physical attack”	Yes
FDP_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”	No

The Table 16 provides an overview about the augmented security functional requirements, which are added supplemental to the TOE and defined in this ST. All requirements are taken from Common Criteria Part 2 [3], with the exception of the requirement FPT_TST.2, which is defined in this ST completely.

Table 17: Augmented security functional requirements

Security Functional Requirement	
FPT_TST.2	“Subset TOE security testing“
FDP_ACC.1	“Subset access control”
FDP_ACF.1	“Security attribute based access control”
FMT_MSA.1	“Management of security attributes”
FMT_MSA.3	“Static attribute initialization”
FMT_SMF.1	“Specification of Management functions”

Security Functional Requirement	
FCS_COP.1/TDES	“Cryptographic support -TDES”
FCS_COP.1/AES	“Cryptographic support - AES”
FCS_COP.1/TDES_SCL	“Cryptographic support TDES-SCL”
FCS_COP.1/AES_SCL	“Cryptographic support AES-SCL”
FCS_COP.1/RSA-v1.02.013	“Cryptographic support - RSA”
FCS_COP.1/RSA-v2.07.003	“Cryptographic support - RSA”
FCS_CKM.1/RSA-v2.07.003	“Cryptographic key management - EC”
FCS_COP.1/ECDSA-v1.02.013	“Cryptographic support - ECDSA”
FCS_COP.1/ECDSA-v2.07.003	“Cryptographic support - ECDSA”
FCS_COP.1/ECDH-v1.02.013	“Cryptographic support - ECDH”
FCS_COP.1/ECDH-v2.07.003	“Cryptographic support - ECDH”
FCS_CKM.1/EC-v1.02.013	“Cryptographic key management - EC”
FCS_CKM.1/EC-v2.07.003	“Cryptographic key management - EC”
FCS_COP.1/SHA	“Cryptographic support - SHA”
FCS_CKM.4/TDES	“Cryptographic key destruction - TDES”
FCS_CKM.4/AES	“Cryptographic key destruction - AES”
FCS_CKM.4/TDES_SCL	“Cryptographic key destruction –TDES-SCL”
FCS_CKM.4/AES_SCL	“Cryptographic key destruction - AES-SCL”
FCS_CKM.1/EC	“Cryptographic key management - EC”
FDP_SDI.1	“Stored data integrity monitoring”
FDP_SDI.2	“Stored data integrity monitoring and action”

All assignments and selections of the security functional requirements of the TOE are either done in the PP [1] or 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 as an extended component in the PP [1]. This family describes the functional requirements for random number generation used for cryptographic purposes. The PP [1] does already provide an instance of this SFR with a completed selection and a partially completed assignment. The instance of FCS_RNG.1 that will be used within this ST is completed according to AIS31 [5]. The element FCS_RNG.1.1 was subject of an editorial refinement in order to provide an easy integration of the PTG.2 class from AIS31 [5]. Furthermore the element FCS_RNG.1.2 was functionally refined, which is indicated by the underlined text. This refinement does specify the format of the provided random numbers and does not mitigate the security functional requirement, as defined in the PP [1]. The Security Target is still strict conformant to the PP [1], as the refined FCS_RNG.1 still meets the requirement as defined in the PP [1].

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 [5]
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 [5] 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 test of the random source and a continuous RNG test according to following standard:

National Institute of Standards and Technology, Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication (FIPS) 140-2 [31], 2002-12-03, chapter 4.9.2.

7.1.1.2 FAU_SAS

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

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

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

7.1.2 Subset of TOE Testing

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

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

FPT_TST.2	Subset TOE testing
Hierarchical to	No other components.
Dependencies:	No dependencies.
FPT_TST.2.1	The TSF shall run a suite of self-tests *at the request of the authorized user* to demonstrate the correct operation of the *alarm lines and/or following environmental sensor mechanisms:* Please refer to the Confidential Security Target [35].

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 of the hardware reference manual [6].

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 memory model provides distinct, independent privilege levels separated from each other in the virtual address space. More information is given in the Confidential Security Target [35].

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 can not 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 initialization (FMT_MSA.3)” as specified below.

FMT_MSA.3	Static attribute initialization
Hierarchical to	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the *Memory Access Control Policy* to provide *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*[1]*,* to specify alternative initial values to override the default values when an object or information is created.

[1] The static definition of the access rules is documented in [6]

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".

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

- Advanced Encryption Standard (AES)[2]
- Triple Data Encryption Standard (TDES)[2]
- Elliptic Curve Cryptography (EC)[3]
- Rivest-Shamir-Adleman (RSA)[3]

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

[2] The TOE provides a solely hardware based AES and TDES implementation and the AES and TDES calculations provided by the SCL.

[3] For the case the TOE comes without RSA and/or EC library, the TOE provides basic HW-related routines for RSA and/or EC calculations. For a secure library implementation the user has to implement additional countermeasures himself.

- Secure Hash Algorithm (SHA-2)

Note that the additional function of the EC library, providing the primitive elliptic curve operations, does not add specific security functionality.

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 TDES computation supported by hardware is possible (neither solely hardware based nor SCL based). In case the crypto@2304T is blocked, no RSA and EC computation supported by hardware is possible. In case of a blocked crypto@2304T the optionally delivered cryptographic and the supporting Toolbox and Base Library cannot be used in that TOE product. The use of the SHA-2 library is also possible with both crypto coprocessors blocked. 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 [27] Section 9, Para.4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functions it shall be checked whether the related cryptographic operations are appropriate for the intended system. Some further hints and guidelines can be derived from the "Technische Richtlinie BSI TR-02102", www.bsi.bund.de.

Any cryptographic functionality that is marked in the column "Security level above 100 Bits" of the following table with a "no" achieves a security level of lower than 100 Bits (in general context).

Table 18: Cryptographic TOE functionality

Cryptographic Mechanism	Standard	Key size in Bits	Security level above 100 Bits
ECDH	[20]	Key sizes corresponding to the used elliptic curves P-{192,224}, K-{163,233}, B-{233} [17], and brainpool P{160, 192, 224}r1, brainpool P{160, 192, 224}t1 [18]	No
ECDH	[21]	Key sizes corresponding to the used elliptic curves P-{256, 384, 521}, K-{409}, B-{283, 409} [17], brainpool P{256, 320, 384, 512}r1, brainpool P{256, 320, 384, 512}t1 [18]	Yes
ECDSA key generation	[25], [32]	Key sizes corresponding to the used elliptic curves P-{192,224}, K-{163,233}, B-{233} [17] and brainpool P{160, 192, 224}r1, brainpool P{160, 192, 224}t1 [18]	No

Cryptographic Mechanism	Standard	Key size in Bits	Security level above 100 Bits
ECDSA key generation	[25], [32]	Key sizes corresponding to the used elliptic curves P-{256, 384, 521}, K-{409}, B-{283, 409} [17], brainpool P{256,320,384,512}r1, brainpool P{256,320,384,512}t1 [18])	Yes
ECDSA signature generation / verification	[25], [26]	Key sizes corresponding to the used elliptic curves P-{192,224}, K-{163,233}, B-{233} [17] and brainpool P{160, 192, 224}r1, brainpool P{160, 192, 224}t1 [18]	No
ECDSA signature generation / verification	[25]], [26]	Key sizes corresponding to the used elliptic curves P-{256, 384, 521}, K-{409}, B-{283, 409} [17], brainpool P{256,320,384,512}r1, brainpool P{256,320,384,512}t1 [18])	Yes
TDES	[22]	|k| = 112 in all operating modes	No
	[22]	|k| = 168	Yes
	proprietary	|k| = 168 Blinding Feedback Mode	No
	proprietary	|k| = 168 Recrypt	Yes
	[22], [28], [34]	|k| = 168 in operating mode ECB, CBC-MAC. CBC-MAC-ELB	No
	[22], [28]	|k| = 168 in operating modes CFB, CTR, CBC	Yes
AES	[23]	|k| = 128, 192, 256	Yes
	[23], [28]	|k| = 128, 192, 256 in operating modes CBC, CFB, CTR	Yes
	proprietary	|k| = 128, 192, 256 Recrypt	Yes
	proprietary	|k| = 128, 192, 256 Operating mode: BLD	No

Cryptographic Mechanism	Standard	Key size in Bits	Security level above 100 Bits
	[23], [28], [34]	|k| = 128, 192, 256 in operating mode ECB, CBC-MAC, CBC-MAC-ELB	No
RSA encryption / decryption/ signature generation / verification (only modular exponentiation part)	[24]	Modulus length = 1976 - 4096	Yes
SHA-{256, 512}	[19]	None	n.a., keyless operation
Physical True RNG PTG.2	[5]	n.a.	n.a.

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 management] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/TDES	The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *Triple Data Encryption Standard (TDES) in the Electronic Codebook Mode (ECB), the Cipher Block Chaining Mode (CBC), the Blinding Feedback Mode (BLD), the Recrypt Mode, the Cipher Block Chaining Mode (CBC-MAC), the CBC-MAC- encrypt-last-block (CBC-MAC-ELB) mode* and cryptographic key sizes *of 2 x 56 bit or 3 x 56 bit,* that meet the following *standards*: • *Triple Data Encryption Standard (TDES):* *National Institute of Standards and Technology (NIST) SP 800-67 Rev. 1 [22].* • *Block Cipher Modes: ECB, CBC* *National Institute of Standards and Technology (NIST) SP 800-38A [28].* • *Block Cipher Modes: BLD, Recrypt* *Proprietary, a description is given in the hardware reference manual HRM [6].* • *Block Cipher Modes: CBC-MAC, CBC-MAC-ELB: [34]*

Note:

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

For more information about the implementation of CBC-MAC-ELB see [15].

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 a software reset of the SCP, which provides immediate zeroing of all SCP key registers.

FCS_COP.1/TDES_SCL	Cryptographic operation - TDES_SCL
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key management] FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1.1/TDES_SCL	The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm *Triple Data Encryption Standard (TDES) in the Electronic Codebook Mode (ECB),* in the *Cipher Block Chaining Mode (CBC), Cipher Feedback (CFB) and Counter (CTR) Modes* and cryptographic key sizes of *112 bit and 168 bit* that meet the following standards: • *Triple Data Encryption Standard (TDES):* *National Institute of Standards and Technology (NIST) SP 800-67 Rev. 1 [22].* • *Block Cipher Modes: ECB, CBC, CFB, CTR:* *National Institute of Standards and Technology (NIST) SP 800-38A [28].*

Note:

This SFR refers to the TDES calculations provided by the optional symmetric cryptographic library (SCL) and is not applicable if the TOE is delivered with a blocked TDES SCP or without SCL.

FCS_CKM.4/TDES_SCL	Cryptographic key destruction – TDES_SCL
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/TDES_SCL	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 TDES provided by the optional symmetric cryptographic library (SCL) and is not applicable if the TOE is delivered with a blocked SCP or without SCL. 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. The data object stored in the memory of the TOE can be destroyed using the "Cipher_Close()" function of the SCL.

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 *encryption and decryption* in accordance with a specified cryptographic algorithm *Advanced Encryption Standard (AES) in the Electronic Codebook Mode (ECB), the Cipher Block Chaining Mode (CBC), the Blinding Feedback Mode (BLD), the Recrypt Mode, the Cipher Block Chaining Mode (CBC-MAC), the CBC-MAC- encrypt-last-block (CBC-MAC-ELB) mode* and cryptographic key sizes of *128 bit or 192 bit or 256 bit* that meet the following standards: • *Advanced Encryption Standard (AES)* *U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL),* *Advanced Encryption Standard (AES), FIPS 197 [23]* • Block Cipher Modes: CBC, ECB *National Institute of Standards and Technology (NIST) SP 800-38A [28].* • *Block Cipher Modes: BLD, Recrypt* *Proprietary, a description is given in the hardware reference manual HRM [6].* • *Block Cipher Modes: CBC-MAC, CBC-MAC-ELB*: [34]

Note:

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

For more information about the implementation of CBC-MAC-ELB see [15].

FCS_CKM.4/AES	Cryptographic key destruction – AES
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1/AES	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key

	destruction method *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 a software reset of the SCP, which provides immediate zeroing of all SCP key registers.

FCS_COP.1/AES_SCL	Cryptographic operation – AES_SCL
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_SCL	The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *Advanced Encryption Standard (AES) in the Electronic Codebook Mode (ECB), Cipher Block Chaining Mode (CBC), Counter Mode (CTR) and Cipher Feedback Mode (CFB)* and cryptographic key sizes of *128 bit or 192 bit or 256 bit* that meet the following standards: • *Advanced Encryption Standard (AES):* *U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL),* *Advanced Encryption Standard (AES), FIPS 197 [23].* • *Block Cipher Modes: ECB, CBC, CTR, CFB* *National Institute of Standards and Technology (NIST) SP 800-38A [28]*

Note:

This SFR applies to the AES calculations provided by the optional symmetric cryptographic library (SCL) and is not applicable if the TOE is delivered with a blocked SCP or without SCL.

FCS_CKM.4/AES_SCL	Cryptographic key destruction – AES_SCL
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1/AES_SCL	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 AES provided by the optional symmetric cryptographic library (SCL) and is not applicable if the TOE is delivered with a blocked SCP or without SCL. 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. The data object stored in the memory of the TOE can be destroyed using the “Cipher_Close()” function of the SCL.

7.1.4.4 Rivest-Shamir-Adleman (RSA) Operation

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

Valid for cryptographic library version v1.02.013:	
FCS_COP.1/RSA-v1.02.013	**Cryptographic operation**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/RSA-v1.02.013	The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *Rivest-Shamir-Adleman (RSA)* and cryptographic key sizes *1024- 4096 bits* that meet the following standards: ***Encryption:*** *According to section 5.1.1 RSAEP in PKCS [22] without 5.1.1.1.* ***Decryption (with or without CRT):*** *According to section 5.1.2 RSADP in PKCS [22] for u = 2, i.e., without any (r_i, d_i, t_i), i >2, therefore without 5.1.2.2.b (ii)&(v), without 5.1.2.1. 5.1.2.2.a, only supported up to* $n < 2^{2048}$

	Signature Generation (with or without CRT): *According to section 5.2.1 RSASP1 in PKCS [22] for u = 2, i.e., without any (r_i, d_i, t_i), i >2, therefore without 5.2.1.2.b (ii)&(v), without 5.2.1.1.* *5.2.1.2.a, only supported up to* $n < 2^{2048}$ ***Signature Verification:*** *According to section 5.2.2 RSAVP1 in PKCS [22],* *without 5.2.2.1.*

	Valid for cryptographic library version v2.07.003
FCS_COP.1/RSA-v2.07.003	**Cryptographic operation - RSA**
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/RSA-v2.07.003	The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *Rivest-Shamir-Adleman (RSA)* and cryptographic key sizes *1976- 4096 bits* that meet the following standards: ***Encryption:*** *1. According to section 5.1.1 RSAEP in PKCS [22]:* • *Supported for* $n < 2^{4096 + 128}$ • *5.1.1(1) not supported* *2. According to section 8.2.2 IFEP-RSA in IEEE [28]:* *Supported for* $n < 2^{4096 + 128}$ ***Decryption (with or without CRT):*** *1. According to section 5.1.2 RSADP in PKCS [22]:* *for u = 2, i.e., without any* (r_i, d_i, t_i)*,* $i > 2$ • *5.1.2(1) not supported* • *5.1.2(2.a) not supported for* $n < 2^{2048 + 64}$ • *5.1.2(2.b) supported for* $p \times q < 2^{4096 + 128}$ • *5.1.2(2.b) (ii)&(v) not applicable due to u = 2* 2. According to section 8.2.3 IEEE [28]:

- 8.2.1(I) supported for $n < 2^{2048 + 64}$
- *8.2.1(II) supported for* $p \times q < 2^{4096 + 128}$

8.2.1(III) not supported

Signature Generation (with or without CRT):

1. According to section 5.2.1 RSASP1 in PKCS [22]:

for $u = 2$, i.e., without any (r_i, d_i, t_i), $i > 2$

- *5.2.1(1) not supported*
- *5.2.1(2.a) supported for* $n < 2^{2048 + 64}$
- *5.2.1(2b) supported for* $p \times q < 2^{4096 + 128}$
- *5.2.1(2b) (ii)&(v) not applicable due to $u = 2$*

2. According to section 8.2.4 IFSP-RSA1 in IEEE [28]:

- *8.2.1(I) supported for* $n < 2^{2048 + 64}$
- *8.2.1(II) supported for* $p \times q < 2^{4096 + 128}$

8.2.1(III) not supported

Signature Verification:

1. According to section 5.2.2 RSAVP1 in PKCS [22]:

supported for $n < 2^{4096 +128}$

- *5.2.2(1) not supported*

2. According to section 8.2.5 IEEE [28]:

- *Supported for* $n < 2^{4096 +128}$

8.2.5(1) not supported

Note:

This SFR is not applicable if the TOE is delivered with a blocked Crypto@2304T or without RSA library.

Please consider also the statement of chapter 7.1.4.1.

7.1.4.5 Rivest-Shamir-Adleman (RSA) Key generation

The key generation for the RSA shall meet the requirement “Cryptographic key generation (FCS_CKM.1)”

FCS_CKM.1/RSA-v2.07.003	Cryptographic key generation – RSA
Hierarchical to:	No other components.
Dependencies:	FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/RSA-v2.07.003	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *rsagen1* and specified cryptographic key sizes of *1976 – 4096 bits* that meet the following standard: *1. According to section 3.1 and 3.2) in PKCS [21]:* *for u=2, i.e., without any (r_i, d_i, t_i), i > 2* • *3.1 supported for n < $2^{4096 + 128}$* • *3.2(1) supported for n< $2^{2048 + 64}$* • *3.2(2) supported for p x q < $2^{4096 + 128}$* *2. According to section 8.1.3.1 in IEEE [27]:* • *8.1.3.1(1) supported for n < $2^{2048 + 64}$* • *8.1.3.1(2) supported for p x q < $2^{4096 + 128}$* • *8.1.3.1(3) supported for p x q < $2^{2048 + 64}$*

Note:

This SFR is not applicable if the TOE is delivered with a blocked Crypto@2304T or without RSA library. Please consider the statement of chapter 7.1.4.1.

Note:

For easy integration of RSA functions into the user’s operating system and/or application, the library contains single cryptographic functions respectively primitives which are compliant to the standard. The primitives are referenced above. Therefore, the library supports the user to develop an application representing the standard if required.

7.1.4.6 Generally with Regard to Elliptic Curves

The EC library is delivered as object code and in this way integrated in the user software. The certification covers the standard NIST [17] and Brainpool [18] Elliptic Curves with key lengths of of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits, due to national AIS32 regulations by the BSI. Note that there are further uncounted side-channel secure curve types, which the user can optionally add in the composition certification process.

7.1.4.7 Elliptic Curve DSA (ECDSA) Operation

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

	Valid for cryptographic library version v1.02.013
FCS_COP.1/ECDSA-v1.02.013	Cryptographic operation - ECDSA
Hierarchical to	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ECDSA-v1.02.013	The TSF shall perform *signature generation and signature verification* in accordance with a specified cryptographic algorithm ECDSA and cryptographic key sizes *of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits* that meet the following *standard:* ***Signature Generation:*** *1. According to section 7.3 in ANSI X9.62 - 2005* *Not implemented are steps d) and e) thereof.* *The output of step e) has to be provided as input to our function by the caller.* *Deviation of steps c) and f):* *The jumps to step a) were substituted by a return of the function with an error code, the jumps are emulated by another call to our function.* *2. According to sections 6.2(6.2.2+6.2.3) in ISO/IEC 15946-2:2002.* *Not implemented is section 6.2.1: the output of 5.4.2 has to be provided by the caller as input to our function.* *Standard ISO/IEC 15946-2:2002 is withdrawn.* ***Signature Verification:*** *1. According to section 7.4.1 in ANSI X9.62–2005* *Not implemented are steps b) and c) thereof.* *The output of step c) has to be provided as input to our function by the caller.* *Deviation of step d):* *Beside noted calculation, our algorithm adds a random multiple of BasepointerOrder n to the calculated values u1 and u2.* *2. According to sections 6.4(6.4.1+6.4.3+6.4.4) in ISO/IEC 15946-2:2002.* *Not implemented is section 6.4.2: the output of 5.4.2 has to be provided by the caller as input to our function.*

Standard ISO/IEC 15946-2:2002 is withdrawn.

Valid for cryptographic library version v2.07.003

FCS_COP.1/ECDSA-v2.07.003 **Cryptographic operation - ECDSA**

Hierarchical to: No other components.

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

FCS_COP.1.1/ECDSA-v2.07.003 The TSF shall perform *signature generation and signature verification* in accordance with a specified cryptographic algorithm *ECDSA* and cryptographic key sizes *160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bit* that meet the following standard:

ECDSA Signature Generation:

1. *According to section"7.3 Signing Process” in ANSI X9.62–- 2005:*
   - *Step d) and e) not supported.*
   - *The output of step e) has to be provided as input to our function by the caller.*
   - *Deviation of step c) and f):*
     - *The jumps to step a) were substituted by a return of the function with an error code, the jumps are emulated by another call to our function.*
2. *According to section"6.4.3 Signature process” in ISO/IEC 14888-3:2006:*
   - *6.4.3.3 not supported.*
   - *6.4.3.5 not supported:*
     - *the hash-code H of the message has to be provided by the caller as input to our function.*
   - *6.4.3.7 not supported.*
   - *6.4.3.8 not supported.*
3. *According to section"7.2.7 ECSP-DSA” in IEEE Std 1363-2000:*
   - *Deviation of step (3) and (4):*

The jumps to step 1, were substituted by a return of the function with an error code, the jumps are emulated by another call to our function.

ECDSA Signature Verification:

1. *According to section"7.4.1 Verification with the Public Key” in ANSI X9.62–- 2005:*
   - *Step b) and c) not supported.*
   - *The output of step c) has to be provided as input to our function by the caller.*

- *Deviation of step d):*
    - *Beside noted calculation, our algorithm adds a random multiple of BasepointOrder n to the calculated values u_1 and u_2.*

2. *According to section"6.4.4 Signature Verification Process" in ISO/IEC 14888-3:2006:*
    - *6.4.4.2 not supported.*
    - *6.4.4.3 not supported:*
        - *the hash-code H of the message has to be provided by the caller as input to our function.*
3. *According to section"7.2.8 ECVP-DSA" in IEEE Std 1363-2000.*

Note:

This SFR is not applicable if the TOE is delivered with a blocked Crypto@2304T or without the EC library.

Note:

For easy integration of EC functions into the user's operating system and/or application, the library contains single cryptographic functions respectively primitives which are compliant to the standard. The primitives are referenced above. Therefore, the library supports the user to develop an application representing the standard if required.

7.1.4.8 Elliptic Curve (EC) Key Generation

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

	Valid for cryptographic library version v1.02.013
FCS_CKM.1/EC-v1.02.013	Cryptographic key generation - EC
Hierarchical to	No other components.
Dependencies:	FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/EC-v1.02.013	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Elliptic Curve EC* and specified cryptographic key sizes *of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits* that meet the following *standard:* **ECDSA *Key Generation:*** • *According to the appendix A4.3 in ANSI X9.62-2005 [25]: The cofactor h is not supported.* • *According to section 6.1 (not 6.1.1) in ISO/IEC 15946-1:2002*

	Valid for cryptographic library version v2.07.003
FCS_CKM.1/EC-v2.07.003	**Cryptographic key generation - EC**
Hierarchical to:	No other components.
Dependencies:	FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/EC-v2.07.003	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Elliptic Curve EC* and specified cryptographic key sizes *160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bit* that meet the following standard: *ECDSA Key Generation:* 1. *According to the appendix A4.3 Elliptic Curve Key Pair Generation in ANSI X9.62-2005 [25]: The optional cofactor h is not supported.* *2. According to section 6.4.2 Generation of signature key and verification key in ISO/IEC 14888-3 [36]* 3. *According to appendix A.16.9 An algorithm for generating EC keys in IEEE Std. 1363-2000 [37]*

Note:

This SFR is not applicable if the TOE is delivered with a blocked Crypto@2304T or without EC library.

Note:

For easy integration of EC functions into the user’s operating system and/or application, the library contains single cryptographic functions respectively primitives which are compliant to the standard. The primitives are referenced above. Therefore, the library supports the user to develop an application representing the standard if required.

7.1.4.9 Elliptic Curve Diffie-Hellman (ECDH) Key Agreement

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

Valid for cryptographic library version v1.02.013	
FCS_COP.1/ECDH-v1.02.013	Cryptographic operation - ECDH
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/ECDH-v1.02.013	The TSF shall perform *elliptic curve Diffie-Hellman key agreement* in accordance with a specified cryptographic algorithm *ECDH* and cryptographic key sizes *160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits* that meet the following *standard:* *1. According to section 5.4.1 in ANSI X9.63 [20] -2001* *Unlike section 5.4.1.3 our implementation not only returns the x-coordinate of the shared secret, but rather the x-coordinate and y-coordinate.* *2. According to sections 8.4.2.1, 8.4.2.2, 8.4.2.3, 8.4.2.4 in ISO/IEC 15946-3:2002.*

Valid for cryptographic library version v2.07.003	
FCS_COP.1/ECDH-v2.07.003	**Cryptographic operation - ECDH**
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/ECDH-v2.07.003	The TSF shall perform *elliptic curve Diffie-Hellman key agreement* in accordance with a specified cryptographic algorithm *ECDH* and cryptographic key sizes *160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bit* that meet the following standard: 1. *According to section 5.4.1 Standard Diffie-Hellman Primitive in ANSI X9.63 [20] Unlike section 5.4.1(3) our implementation not only returns the x-coordinate of the shared secret, but rather the x-coordinate and the y-coordinate.* 2. *According to section Appendix D.6 Key agreement of Diffie-Hellman type in ISO/IEC 11770-3 [38] the function enables the operations described in appendix D.6.*

	3. According to section 7.2.1 ECSVHDP-DP in IEEE Std. 1363:2000 [37] Unlike section 7.2.1 our implementation not only returns the x-coordinate of the shared secret, but rather the x-coordinate and the y-coordinate.

Note:

This SFR is not applicable if the TOE is delivered with a blocked Crypto@2304T or without EC library.

Note:

The certification covers the standard NIST [17] and Brainpool [18] Elliptic Curves with key lengths of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits, due to national AIS32 regulations by the BSI. Note that there are further uncounted side-channel secure curve types, which the user can optionally add in the composition certification process.

Note:

For easy integration of EC functions into the user's operating system and/or application, the library contains single cryptographic functions respectively primitives which are compliant to the standard. The primitives are referenced above. Therefore, the library supports the user to develop an application representing the standard if required.

Note:

The EC primitives allow the selection of various curves. The selection of the curves depends to the user.

7.1.4.10 SHA-2 Operation

The SHA-2 Operation of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1/SHA	Cryptographic Operation - SHA
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/SHA	The TSF shall perform *hash-value calculation of user chosen data* in accordance with a specified cryptographic algorithm *SHA-2* and with cryptographic key sizes *of none* that meet the following *standards*: *FIPS 180-4 as of 2015-08 [19]*

Note:

This SFR is not applicable if the TOE is delivered without the SHA-2 library.

Note:

The SHA-2 cryptographic operation is a keyless operation.

Note:

The secure hash-algorithm SHA-2 is intended to be used for signature generation, verification and generic data integrity checks. The use for keyed hash operations like HMAC or similar security critical operations involving keys, is not subject of this TOE and requires specific security improvements and DPA analysis including the operating system, which is not part of this TOE. Further essential information about the usage is given in the confidential user guidance [11].

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 value for the RAM, ROM and 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 RAM, ROM and SOLID FLASH™ NVM and error correction ECC 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.*

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 [1] is expressed with bold letters.

Table 19: Assurance components

Aspect	Acronym	Description	Refinement
Development	ADV_ARC.1	Security Architecture Description	In PP [1]
	ADV_FSP.5	**Complete semi-formal functional specification with additional error information**	in ST
	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**	

Aspect	Acronym	Description	Refinement
Guidance Documents	AGD_OPE.1	Operational user guidance	in PP [1]
	AGD_PRE.1	Preparative procedures	in PP [1]
Life-Cycle Support	**ALC_CMC.5**	**Advanced support**	in ST
	ALC_CMS.5	**Development tools CM coverage**	in ST
	ALC_DEL.1	Delivery procedures	in PP [1]
	ALC_DVS.2	Sufficiency of security measures	in PP [1]
	ALC_LCD.1	Developer defined life-cycle model	
	ALC_TAT.3	**Compliance with implementation standards – all parts**	
	ALC_FLR.1	**Basic Flaw Remediation**	
Security Target Evaluation	ASE_CCL.1	Conformance claims	
	ASE_ECD.1	Extended components definition	
	ASE_INT.1	ST introduction	
	ASE_OBJ.2	Security objectives	
	ASE_REQ.2	Derived security requirements	
	ASE_SPD.1	Security problem definition	
	ASE_TSS.1	TOE summary specification	
Tests	**ATE_COV.3**	**Rigorous analysis of coverage**	In ST
	ATE_DPT.3	**Testing: modular design**	
	ATE_FUN.2	**Ordered functional testing**	
	ATE_IND.2	Independent testing - sample	
Vulnerability Assessment	AVA_VAN.5	Advanced methodical vulnerability analysis	in PP [1]

7.2.1 Refinements

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

7.2.1.1 Development (ADV)

ADV_IMP Implementation Representation:

The refined assurance package ADV_IMP.1 implementation representation of the TSF requires the availability of the entire implementation representation, a mapping of the design description to the implementation representation with a level of detail that the TSF can be generated without further design decisions. In addition, the correspondence of design description and implementation representation shall be demonstrated.

The covered higher assurance package ADV_IMP.2 requires a complete and not curtailed mapping of the implementation representation of the TSF, and the mapping of the design description to the entire implementation representation. In addition, the correspondence of design description and the implementation representation shall be demonstrated. The ADV_IMP.1 aspect and refinement remains therefore valid. The enhancement underlines the refinement in the PP [1] and by that the entirely complete design i.e. not curtailed representation with according mapping was provided, demonstrated and reviewed.

ADV_FSP Functional Specification:

The ADV_FSP.4 package requires a functional description of the TSFIs and there assignment to SFR-enforcing, SFR-supporting, SFR-non-interfering, including related error messages, the assurance package. The enhancement of ADV_FSP.5 requires additionally a complete semi-formal functional specification with additional error information. In addition the package includes a tracing from the functional specification to the SFRs, as well as the TSFIs descriptions including error messages not resulting from an invocation of a TSFI.

These aspects from ADV_FSP.5 are independent from the ADV_FSP.4 refinements from the PP [1] but constitute an enhancement of it. By that the aspects of ADV_FSP.4 and its refinement in the PP [1] apply also here. The assurance and evidence was provided accordingly.

7.2.1.2 Life-cycle Support (ALC)

ALC_CMS Configuration Management Scope:

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

ALC_CMC Configuration Management Capabilities:

The PP [1] 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 [1] remain valid. The assurance and evidence was provided.

7.2.1.3 Tests (ATE)

ATE_COV Test Coverage:

The PP [1] refined assurance package ATE_COV.2 Analysis of coverage addresses the extent to which the TSF is tested, and whether or not the testing is sufficiently extensive to demonstrate that the TSF operates as specified. It includes the test documentation of the TSFIs in the functional specification. In particular the refinement requires that The TOE must be tested under different operating conditions within the specified ranges. In addition, the existence and effectiveness of mechanisms against physical attacks should be covered by evidence that the TOE has the particular physical characteristics. This is furthermore detailed in the PP [1].

This assurance package ATE_COV.2 has been enhanced to ATE_COV.3 to cover the rigorous analysis of coverage. This requires the presence of evidence that exhaustive testing on rigorous entirely all interfaces as documented in the functional specification was conducted. By that ATE_COV.2 and refinements as given in the PP [1] are enhanced by ATE_COV.3 and remain as well. The TSFIs were completely tested according to ATE_COV.3 and the assurance and evidence was provided.

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. The assurance and evidence was provided.

ADV_SPM.1 Formal TOE security policy model

Hierarchical to: No other components

Dependencies: ADV_FSP.4 Complete function description

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

Memory Access Control Policy and the corresponding SFRs

- *FDP_ACC.1 Subset Access Control*
- *FDP_ACF.1 Security attribute based access control*
- *FMT_MSA.1 Management of Security Attributes*
- *FMT_MSA.3 Static Attribute initialization.*

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

- *FDP_SDI.1 Stored data integrity monitoring*
- *FDP_SDI.2 Stored data integrity monitoring and action*
- *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 is given in the PP [1] chapter 6.3.1, including a mapping of the SFRs to their objectives.

The additional introduced SFRs are discussed below:

Public

Table 20: Rational for additional SFR in the ST

Objective	TOE Security Functional Requirements
O.Add-Functions	- FCS_COP.1/TDES "Cryptographic operation - TDES" - FCS_COP.1/TDES_SCL "Cryptographic operation - TDES_SCL" - FCS_COP.1/AES "Cryptographic operation - AES" - FCS_COP.1/AES_SCL "Cryptographic operation - AES_SCL" - FCS_COP.1/SHA "Cryptographic operation - SHA" - FCS_COP.1/RSA-v1.02.013 "Cryptographic operation - RSA" - FCS_COP.1/RSA-v2.07.003 "Cryptographic operation - RSA" - FCS_CKM.1/RSA-v2.07.003 "Cryptographic key generation - RSA" - FCS_COP.1/ECDSA-v1.02.013 "Cryptographic operation - ECDSA" - FCS_COP.1/ECDSA-v2.07.003 "Cryptographic operation - ECDSA" - FCS_COP.1/ECDH-v1.02.013 "Cryptographic operation - ECDH" - FCS_COP.1/ECDH-v2.07.003 "Cryptographic operation - ECDH" - FCS_CKM.1/EC-v1.02.013 "Cryptographic key generation - EC" - FCS_CKM.1/EC-v2.07.003 "Cryptographic key generation - EC" - FCS_CKM.4/TDES "Cryptographic key destruction - TDES" - FCS_CKM.4/AES "Cryptographic key destruction - AES" - FCS_CKM.4/TDES_SCL "Cryptographic key destruction - TDES_SCL" - FCS_CKM.4/AES_SCL "Cryptographic key destruction - AES_SCL"
O.Phys-Manipulation	- FPT_TST.2 "Subset TOE security testing" - FDP_SDI.1 "Stored data integrity monitoring" - FDP_SDI.2 "Stored data integrity monitoring and action"
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 detailed justification is given in the following:

The justification related to the security objective "Additional Specific Security Functionality (O.Add-Functions)" is as follows:

The security functional requirement(s) “Cryptographic operation (FCS_COP.1)” exactly requires those functions to be implemented, which are demanded by O.Add-Functions. The FCS_CKM.1/EC supports the generation of EC keys needed for this cryptographic operations. Therefore, FCS_COP.1/RSA, FCS_COP.1/ECDSA, FCS_COP.1/ECDH and FCS_CKM/EC are suitable to meet the security objective. The FCS_COP.1/SHA is a keyless algorithm and has no dependencies to FCS_CKM.1.

The symmetric services demanded by O.Add-Functions are provided via the SFRs FCS_COP.1/AES, FCS_COP.1/TDES, FCS_COP.1/AES_SCL and FCS_COP.1/TDES_SCL. The TOE may not provide key generation for the symmetric cryptographic operations (for further details please refer to chapter 7.3.1.1), however the SFRs FCS_CKM.4/AES, FCS_CKM.4/TDES, FCS_CKM.4/AES_SCL and FCS_CKM.4/TDES_SCL provide the user with the possibility to destroy the keys, which are stored on the TOE.

The use of the supporting libraries Toolbox and Base has no impact on any security functional requirement nor does the use generate additional requirements.

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. This is described by the objective for the operational environment OE.Resp-Appl. Furthermore the following dependencies have to be fulfilled in order to use the security functional requirement FCS_COP.1:

- [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.

As already mentioned above, some of these dependencies are already achieved by the TOE and can optionally be achieved by the operational environment as well. However the remaining dependencies have to be fulfilled by the TOE accordingly (OE.Resp-Appl). For further details on the dependencies, which have to be achieved by the operational environment, please refer to chapter 7.3.1.1.

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 RSA, TDES and AES are provided by the environment. Keys for EC algorithms can be provided either by the TOE or the environment.

In this ST the objectives for the environment OE.Plat-Appl and OE.Resp-Appl have been clarified. The Smartcard Embedded Software defines the use of the cryptographic functions FCS_COP.1 provided by the TOE. The requirements for the environment FDP_ITC.1, FDP_ITC.2, FCS_CKM.1 and FCS_CKM.4 have to support an appropriate key management (for details on the dependencies, which have to be fulfilled by the environment, please refer to chapter 7.3.1.1). These security requirements are suitable to meet OE.Resp-Appl.

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

The security functional 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 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 [3] user data protection of chapter 11 which are not refined by the PP [1].

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

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.

7.3.1.1 Dependencies of Security Functional Requirements

The dependence of security functional requirements are defined and described in PP [1] 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 and FAU_SAS.1.

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

Table 21: Dependency for cryptographic operation requirement

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FCS_COP.1/TDES	FCS_CKM.4	Yes, FCS_CKM.4/TDES.
	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, see comment 3
FCS_COP.1/TDES_SCL	FCS_CKM.4	Yes, FCS_CKM.4/TDES_SCL.
	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, see comment 3
FCS_CKM.4/TDES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, see comment 3
FCS_CKM.4/TDES_SCL	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, see comment 3
FCS_COP.1/AES	FCS_CKM.4	Yes, FCS_CKM.4/AES.
	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, see comment 3
FCS_COP.1/AES_SCL	FCS_CKM.4	Yes, FCS_CKM.4/AES_SCL.
	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, see comment 3
FCS_CKM.4/AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, see comment 3
FCS_CKM.4/AES_SCL	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, see comment 3
FCS_COP.1/RSA-v1.02.013	FCS_CKM.4	Yes, see comment 3
	[FDP_ITC.1 or FDP_ITC.2]	Yes, see comment 3
FCS_COP.1/RSA-v2.07.003	FCS_CKM.4	Yes
	[FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2]	Yes, FCS_CKM.1/RSA-v2.07.003. See comment 3.
FCS_CKM.1/RSA-v2.07.003	FCS_CKM.2 or FCS_COP.1	Yes
	FCS_CKM.4	Yes, see comment 3
FCS_COP.1/ECDSA-v1.02.013	FCS_CKM.4	Yes, see comment 3
	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, FCS_CKM.1/EC--v1.02.013. For details see comment 3
FCS_COP.1/ECDSA-v2.07.003	FCS_CKM.4	Yes, see comment 3
	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, FCS_CKM.1/EC-v2.07.003. For details see comment 3
FCS_CKM.1/EC-v1.02.013	[FCS_CKM.2 or FCS_COP.1]	Yes, FCS_COP.1/ECDSA-v1.02.013 and FCS_COP.1/ECDH-v1.02.013
	FCS_CKM.4	Yes, see comment 3

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FCS_CKM.1/EC-v2.07.003	[FCS_CKM.2 or FCS_COP.1]	Yes, FCS_COP.1/ECDSA-v2.07.003 and FCS_COP.1/ECDH-v2.07.003
	FCS_CKM.4	Yes, see comment 3
FCS_COP.1/ECDH-v1.02.013	FCS_CKM.4	Yes, see comment 3
	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, FCS_CKM.1/EC-v1.02.013. For details see comment 3
FCS_COP.1/ECDH-v2.07.003	FCS_CKM.4	Yes, see comment 3
	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, FCS_CKM.1/EC-v2.07.003. For details see comment 3
FCS_COP.1/SHA-SW	No dependencies	N/A, see comment 4
FCS_COP.1/SHA-HW	No dependencies	N/A, see comment 4
FPT_TST.2	No dependencies, see comment 1	N/A
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1	Yes, FDP_ACC.1
	FMT_MSA.3	Yes, FMT_MSA.3
FMT_MSA.3	FMT_MSA.1	Yes, FMT_MSA.1
	FMT_SMR.1	Not required, see comment 2
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	Yes, FDP_ACC.1
	FMT_SMR.1	Yes, see comment 2
	FMT_SMF.1	Yes, FMT_SMF.1
FMT_SMF.1	None	N/A
FDP_SDI.1	None	N/A
FDP_SDI.2	None	N/A

Comment 1:

The TOE is already a platform representing the lowest level in a Smartcard. There is no lower or »underlying abstract machine« used by the TOE which can be tested. Therefore, the former dependency to FPT_AMT.1 is fulfilled without further and by that dispensable. CC in the Revision 3 considered this and dropped this dependency.

Comment 2:

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 3:

These requirements all address the appropriate management of cryptographic keys used by the specified cryptographic function and are not part of the PP [1]. Most requirements concerning key management shall be fulfilled by the environment since the Smartcard Embedded Software is designed for a specific application context and uses the cryptographic functions provided by the TOE.

For the security functional requirements FCS_COP.1/TDES, FCS_COP.1/TDES_SCL, FCS_COP.1/AES, FCS_COP.1/AES_SCL, FCS_CKM.4/TDES, FCS_CKM.4/TDES_SCL, FCS_CKM.4/AES and FCS_CKM.4/AES_SCL the respective dependencies FCS_CKM.1 or [FDP_ITC.1 or FDP_ITC.2] have to be fulfilled by the environment. This means, that the environment should have a choice either to generate the symmetric keys (FCS_CKM.1) as defined in [3], section 10.1 or to import the keys ([FDP_ITC.1 or FDP_ITC.2]), as defined in [3], section 11.7.

For the security functional requirement FCS_COP.1/RSA-v1.02.013, FCS_COP.1/RSA-v2.07.003, FCS_COP.1/ECDSA-v1.02.013, FCS_COP.1/ECDSA-v2.07.003, FCS_COP.1/ECDH-v1.02.013 and FCS_COP.1/ECDH-v2.07.003 the respective dependencies FCS_CKM.4 have to be fulfilled by the environment. This means, that the environment shall provide the respective key destruction (FCS_CKM.4) as defined in [3], section 10.1. The TOE does already provide the respective key generation (FCS_CKM.1/EC-v1.02.013, FCS_CKM.1/EC-v2.07.003 and FCS_CKM.1/RSA-v2.07.003) as defined in 7.1.4.5. However, the environment has to either implement its own key generation (e.g. FCS_CKM.1) as defined in [3], section 10.1, or, instead, import the generated key into the TOE ([FDP_ITC.1 or FDP_ITC.2]), as defined in [3], section 11.7.

The cryptographic libraries SCL, RSA, EC, SHA-2 and the Toolbox library are delivery options. If one of the libraries RSA, EC and Toolbox or combination hereof are delivered, the Base Lib is automatically part of it. Therefore the TOE may come with free combinations of or even without these libraries. In the case of coming without one or any combination of the cryptographic libraries RSA, EC and SHA-2, the TOE does not provide the Additional Specific Security Functionality Rivest-Shamir-Adleman Cryptography (RSA) and/or Elliptic Curve Cryptography (EC) and/or SHA-2 and/or SCL based Advanced Encryption Standard (AES) and/or SCL based Triple Data Encryption Standard (TDES). The Toolbox and Base Library are no cryptographic libraries and provide no additional specific security functionality.

In case of a blocked Crypto@2304T the optionally delivered cryptographic libraries RSA and EC, as well as the supporting Toolbox and Base Libraries cannot be used in that TOE product. In case the SCP is blocked the optionally delivered cryptographic library SCL cannot be used and TOE does not provide the solely hardware based AES and TDES calculation as well. The SHA-2 library is computed in the CPUs and thus independent from the availability of the cryptographic coprocessors.

If the TOE is delivered without a specific cryptographic service, depending on the chosen delivery options, the operational environment does not have to fulfill the corresponding dependencies.

Comment 4

The dependencies FCS_CKM.1 and FMT_CKM.4 are not required for the SHA-2 algorithm, because the SHA-2 algorithm is a keyless operation. So the environment is not obligated to meet certain requirements for key management.

7.3.2 Rationale of the Assurance Requirements

The chosen assurance level EAL6 is augmentation with the requirements coming from ALC_FLR.1. In Table 19 the different assurance levels are shown as well as the augmentations. The augmentations are in compliance with the Protection Profile.

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

In order to provide a meaningful level of assurance and that the TOE provides an adequate level of defense against such high potential attacks, the evaluators have access to all information regarding the TOE including the TSF internals, the low level design and source code including the testing of the modular design. Additionally the mandatory technical document "Application of Attack Potential to Smartcards" [16] shall be taken as a basis for the vulnerability analysis of the TOE.

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

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

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

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 and FMT_LIM.2.

During the production phase (phase 3 and 4) or after the delivery to the customer (phase 5 or phase 6), the TOE provides the possibility to download, after a successful authentication process, a user specific encryption key and user code and data into the empty (erased) SOLID FLASH™ NVM area as specified by the associated control information of the Flash Loader software. This process is only possible after a successful authentication process. The integrity of the loaded data is checked with a signature process. The data to be loaded may be transferred optionally in encrypted form. After finishing the load operation, the Flash Loader can be permanently deactivated, so that no further load operation with the Flash Loader is possible. These procedures are defined as phase operation limitation.

The covered security functional requirement is FPT_LIM.2 “Limited availability”.

During operation within a phase the accesses to memories are granted by the MMU controlled access rights and related privilege level.

The covered security functional requirements are FDP_ACC.1, FDP_ACF.1 and FMT_MSA.1.

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.

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.

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.

Each operation phase is protected by means of authentication and encryption. The covered security functional requirements are FDP_ITT.1 and FPT_ITT.1.

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 buses, the 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 and by the memories SOLID FLASH™ NVM, RAM, CACHE and the bus are entirely encrypted. Note that the ROM contains the firmware only and no user data.

Therefore, no data in plain is handled anywhere on the TOE and thus also the two CPUs compute entirely masked. The symmetric cryptographic coprocessor is entirely masked as well.

The encryption covers the data processing policy and FDP_IFC.1 "Subset information flow control".

The covered security functional requirements are FPT_PHP.3, FDP_IFC.1, FPT_ITT.1 and FDP_ITT.1.

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 another component. The encryption of the memories is performed by the memory encryption and decryption unit MED providing protection against cryptographic analysis attacks. The few keys which have to be stored on the chip are protected against read out.

The covered security functional requirements are FPT_PHP.3, FDP_IFC.1, FPT_ITT.1, and FDP_ITT.1.

The CPU has no standard command set and discloses therefore no possibility for deeper analysis. The covered security functional requirement is FPT_PHP.3.

The entire design is kept in a non-standard way to aggravate attacks using standard analysis methods to an almost not practical condition. A proprietary CPU with a non-public bus protocol is implemented which makes analysis very complicate and time consuming.

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 processed data, protected by a bunch of other protecting means.

In the design a number of components are automatically synthesized and mixed up to disguise their physical boarders and to make an analysis more difficult.

A further protective design method implements special routing measure against probing.

The covered security functional requirements are FPT_PHP.3, FPT_ITT.1 and FDP_ITT.1.

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 and modified. In addition the correct privilege level is controlled by the MMU.

The covered security functional requirements are FPT_PHP.3, FPT_ITT.1 and FDP_ITT.1.

In contrast to the linear virtual address range the physical SOLID FLASH™ NVM pages are transparently and dynamically scrambled. These measures cause that the physical location of data is different from chip to chip. Even user software would always call the equal physical addresses.

An observation of the clock is used to prevent the TOE from single stepping. This is tested by the user mode security life control UMSLC.

The covered security functional requirements are FPT_PHP.3 and FPT_FLS.1.

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.

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

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, MMU and the bus system. Thus introduced failures are detected and certain errors are also automatically corrected (FDP_SDI.2).

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).

The covered security functional requirements are FRU_FLT.2, FPT_PHP.3, FDP_SDI.1 and FDP_SDI.2.

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 save write functionality covers FPT_FLS.1 “Failure with preservation of secure state” since if the programming was not successful, the old data are still present and valid, which ensures a secure state although a programming failure occurred. This action includes also FDP_SDI.1 “Stored data integrity monitoring” as the new data to be programmed are checked for integrity and correct programming before the page with the old data becomes the new physical page for the next new data.

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, FPT_PHP.3 and FDP_SDI.1.

The TOE is protected against fault and modifying attacks. The core provides the functionality of double-computing and 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 two CPUs computing on the same data is by this one of the most important security features of this platform. As the results of both CPUs are compared at the end, a fault induction of modifying attacks would have to be done on both CPUs at the correct place with the correct timing – despite all other countermeasures like dynamic masking, encryption and others. As the comparison and the register files are also protected by various measures successful manipulative attacks are seen as being not practical.

During start up, the STS performs various configurations and subsystem tests. After the STS has finished, the operating system or application can call the User Mode Security Life Control (UMSLC) test. The UMSLC checks the alarm lines and number of functions and sensors for correct operation.

This test can be released actively by the user software during normal chip operation at any time.

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 respective 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 (all iterations), FPT_FLS.1, FPT_PHP.3 and FPT_TST.2.

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 allow the user to check 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, FDP_IFC.1, FPT_ITT.1, FDP_ITT.1 and FPT_PHP.3.

The RMS provides the user also the testing of all security features enabled to generate an alarm. This security testing is called user mode security life control (UMSLC). As attempts to modify the security features will be detected from the test, the covered security functional requirement is FPT_TST.2.

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

The covered security functional requirements are FPT_FLS.1 and FPT_PHP.3.

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, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3 and FMT_SMF1.

The **SF_PMA** “Protection against Modifying Attacks” covers the security functional requirements FCS_CKM.4 (all iterations), 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_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 the privileged levels and gives the software the possibility to define different access rights. The address permissions of the privilege levels are controlled by the MMU. In case of an access violation the MMU will trigger a reset and then a trap service routine can react on the access violation. The policy of setting up the MMU and specifying the memory ranges, to a certain extend, for the privilege levels – with the exception of the IFX level - is defined from the user software (OS).

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, all memories present on the TOE are individually encrypted using individual keys assigned by complex key management. All data are protected by means of encryption or masking also during transportation via the busses. Induced errors are recognized by the Integrity Guard concept and lead to an alarm. 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, FDP_ITT.1, FPT_ITT.1, FDP_IFC.1 and FPT_FLS.1.

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_PHP.3, FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_FLS.1 and FMT_SMF.1.

8.5 SF_CS: Cryptographic Support

The TOE is equipped with several hardware accelerators and software modules to support the standard symmetric and asymmetric cryptographic operations. This security function is introduced to include the cryptographic operation in the scope of the evaluation as the cryptographic function respectively mathematic algorithm itself is not used from the TOE security policy. On the other hand these functions are of special interest for the use of the hardware as platform for the software. The components are a coprocessor supporting the DES and AES algorithms (alternatively a combination of a coprocessor and software, if the SCL is used) and a combination of a coprocessor and software modules to support RSA cryptography, ECDSA signature generation and verification, ECDH key agreement and EC public key calculation and public key testing.

Public

Note that the additional function of the EC library, ECC_ADD, providing the primitive elliptic curve operations, does not add specific security functionality and that the according user guidance abbreviates the Elliptic Curve cryptographic functions with ECC.

Note:

The cryptographic libraries SCL, RSA, EC, SHA-2 and the Toolbox library are delivery options. If one of the libraries RSA, EC and Toolbox or combination hereof are delivered, the Base Lib is automatically part of it. Therefore the TOE may come with free combinations of or even without these libraries. In the case of coming without one or any combination of the cryptographic libraries SCL, RSA, EC and/or SHA-2, the TOE does not provide the corresponding additional specific security functionality Rivest-Shamir-Adleman Cryptography (RSA) and/or Elliptic Curve Cryptography (EC) and/or SHA-2 and/or SCL based Advanced Encryption Standard (AES) and/or SCL based Triple Data Encryption Standard (TDES). The Toolbox and Base Library are no cryptographic libraries and provide no additional specific security functionality.

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 (neither solely hardware based nor SCL based). In case the Crypto@2304T is blocked, no RSA and EC computation supported by hardware is possible. The use of the SHA-2 library is also possible with both crypto coprocessors blocked. 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.

8.5.1 TDES

Hardware-Implemented TDES

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

National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Data Encryption Standard (DES), NIST Special Publication 800-67 [22], Revision 1.

The TOE implements the block cipher modes as specified in the SFR FCS_COP.1/TDES.

Please consider also the statement of chapter 7.1.4.1.

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

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

Software-Implemented TDES (SCL)

The SCL78-SCP-v3 symmetric crypto library supports the encryption and decryption in accordance with the specified cryptographic algorithm Triple Data Encryption Standard (TDES) with cryptographic key sizes of 112 bit and 168 bit meeting the standard:

National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Data Encryption Standard (DES), NIST Special Publication 800-67 [22], Revision 1.

The TOE implements the block cipher modes as specified in the SFR FCS_COP.1/TDES_SCL.

To implement FCS_CKM.4/TDES_SCL, SCL software performs reset triggering at the end of the kernel function (Des3Green_EnDecryption) by writing the “trigger reset” value 0xFFFF to the SCP_CTRL register (hardware). As a result, the key store register is overwritten with the reset value. The second step is a removal of the complete DES data object from RAM by overwriting it by random value.

Please consider also the statement of chapter 7.1.4.1.

Please note that the PCBC mode and the “*_*Sec1*”-functions of the SCL are not part of the evaluation.

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

8.5.2 AES

Hardware-Implemented 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:

U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), Advanced Encryption Standard (AES), FIPS PUB 197.

The TOE implements the block cipher modes as specified in the SFR FCS_COP.1/AES.

Please consider also the statement of chapter 7.1.4.1.

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

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

Software-Implemented AES (SCL)

The SCL AES complies with the standard:

AES Advanced Encryption Standard defined by “NIST FIPS PUB 197” and published in November 2001.

The TOE implements the block cipher modes as specified in the SFR FCS_COP.1/AES_SCL.

To implement FCS_CKM.4/AES_SCL, SCL software performs reset triggering at the end of the kernel function (Des3Green_EnDecryption) by writing the “trigger reset” value 0xFFFF to the SCP_CTRL register (hardware). As a result, the key store register is overwritten with the reset value. The second step is a removal of the complete AES data object from RAM by overwriting it by random value.

Please consider also the statement of chapter 7.1.4.1.

Please note that the PCBC mode and the “*_*Sec1*”-functions of the SCL are not part of the evaluation.

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

8.5.3 RSA

Encryption, Decryption, Signature Generation and Verification

The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm Rivest-Shamir-Adleman (RSA) and cryptographic key sizes 1976 - 4096 bit that meet the following standards:

FCS_COP.1/RSA is covered by:

Encryption:

1. According to section 5.1.1 RSAEP in PKCS [21]:

- *Supported for $n < 2^{4096 + 128}$*
- *5.1.1(1) not supported*

2. According to section 8.2.2 IFEP-RSA in IEEE [27]:

- *Supported for $n < 2^{4096 + 128}$*

Decryption (with or without CRT):

1. According to section 5.1.2 RSADP in PKCS [21] for u = 2, i.e., without any (r_i, d_i, t_i), i > 2

- *5.1.2(1) not supported*
- *5.1.2(2.a) not supported for $n < 2^{2048 + 64}$*
- *5.1.2(2.b) supported for $p \times q < 2^{4096 + 128}$*
- *5.1.2(2.b) (ii)&(v) not applicable due to u = 2*

2. According to section 8.2.3 IEEE [27]:

- *8.2.1(I) supported for $n < 2^{2048 + 64}$*
- *8.2.1(II) supported for $p \times q < 2^{4096 + 128}$*
- *8.2.1(III) not supported*

Signature Generation (with or without CRT):

1. According to section 5.2.1 RSASP1 in PKCS [21] for u = 2, i.e., without any (r_i, d_i, t_i), i >2

- *5.2.1(1) not supported*
- *5.2.1(2.a) supported for $n < 2^{2048 + 64}$*
- *5.2.1(2b) supported for $p \times q < 2^{4096 + 128}$*
- *5.2.1(2b) (ii)&(v) not applicable due to u = 2*

2. According to section 8.2.4 IFSP-RSA1 in IEEE [27]:

- *8.2.1(I) supported for $n < 2^{2048 + 64}$*
- *8.2.1(II) supported for $p \times q < 2^{4096 + 128}$*
- *8.2.1(III) not supported*

Signature Verification:

1. According to section 5.2.2 RSAVP1 in PKCS [21]:

supported for $n < 2^{4096 +128}$

- *5.2.2(1) not supported*

2. According to section 8.2.5 IEEE [27]:

- *Supported for $n < 2^{4096 +128}$*
- *8.2.5(1) not supported*

Please consider also the statement of chapter 7.1.4.1.

The covered security functional requirement is FCS_COP.1/RSA.

8.5.3.1 Asymmetric Key Generation

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm RSA specified in PKCS [21] and specified cryptographic key sizes of 1976 – 4096 bit that meet the following standard: FCS_CKM.1/RSA is covered by:

1. According to section 3.1 and 3.2 in PKCS [21]:

for u=2, i.e., without any (r_i, d_i, t_i), $i > 2$

- *3.1 supported for $n < 2^{4096 + 128}$*
- *3.2(1) supported for $n< 2^{2048 + 64}$*
- *3.2(2) supported for $p \times q < 2^{4096 + 128}$*

2. According to section 8.1.3.1 in IEEE [27]:

- *8.1.3.1(1) supported for $n < 2^{2048 + 64}$*
- *8.1.3.1(2) supported for $p \times q < 2^{4096 + 128}$*
- *8.1.3.1(3) supported for $p \times q < 2^{2048 + 64}$*

Note:

For easy integration of RSA functions into the user’s operating system and/or application, the library contains single cryptographic functions respectively primitives which are compliant to the standard. The primitives are referenced above. Therefore, the library supports the user to develop an application representing the standard if required.

Please consider also the statement of chapter 7.1.4.1.

The covered security functional requirement is FCS_CKM.1/RSA.

8.5.4 Elliptic Curves EC

The certification covers the standard NIST [17] and Brainpool [18] Elliptic Curves with key lengths of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits, due to national AIS32 regulations by the BSI. Note that there are further uncounted side channel secure curve types, which the user can optionally add in the composition certification process.

8.5.4.1 Signature Generation and Verification

The TSF shall perform signature generation and signature verification in accordance with a specified cryptographic algorithm ECDSA and cryptographic key sizes of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits that meet the following standard:

Signature Generation:

1. According to section 7.3 in ANSI X9.62 - 2005
Not implemented are steps d) and e) thereof.
The output of step e) has to be provided as input to our function by the caller.
Deviation of steps c) and f):
The jumps to step a) were substituted by a return of the function with an error code, the jumps are emulated by another call to our function.

2. According to sections 6.2 (6.2.2. + 6.2.3) in ISO/IEC 15946-2:2002
Not implemented is section 6.2.1:
The output of 5.4.2 has to be provided by the caller as input to the function.

Signature Verification:

1. *According to section 7.4.1 in ANSI X9.62–2005*
Not implemented are steps b) and c) thereof.
The output of step c) has to be provided as input to our function by the caller.
Deviation of step d):
Beside noted calculation, our algorithm adds a random multiple of BasepointerOrder n to the calculated values u1 and u2.

2. According to sections 6.4 (6.4.1. + 6.4.3 + 6.4.4) in ISO/IEC 15946-2:2002
Not implemented is section 6.4.2:
The output of 5.4.2 has to be provided by the caller as input to the function.

8.5.4.2 Asymmetric Key Generation

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Elliptic Curve EC specified in ANSI X9.62-2005 and ISO/IEC 15946-1:2002 and specified cryptographic key sizes of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits that meet the following standards:

ECDSA Key Generation:

1. According to the appendix A4.3 in ANSI X9.62-2005
the cofactor h is not supported.
2. According to section 6.1 (not 6.1.1) in ISO/IEC 15946-1:2002

8.5.4.3 Asymmetric Key Agreement

The TSF shall perform elliptic curve Diffie-Hellman key agreement in accordance with a specified cryptographic algorithm ECDH and cryptographic key sizes of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits that meet the following standards:

1. According to section 5.4.1 in ANSI X9.63 -2001
Unlike section 5.4.1.3 our implementation not only returns the
x-coordinate of the shared secret, but rather the x-coordinate and
y-coordinate.
2. According to sections 8.4.2.1, 8.4.2.2, 8.4.2.3, and 8.4.2.4 in
ISO/IEC 15946-3:2002:
The function enables the operations described in the four sections.

Note:

For easy integration of EC functions into the user's operating system and/or application, the library contains single cryptographic functions respectively primitives which are compliant to the standard. The primitives are referenced above. Therefore, the library supports the user to develop an application representing the standard if required.

The covered security functional requirements are FCS_COP.1/ECDSA, FCS_CKM.1/EC and FCS_COP.1/ECDH.

8.5.5 SHA-2

The TOE comes optionally with the SHA-2 library for hash value calculation. Regarding the SHA-2 library it has to be noted that the secure hash-algorithm SHA-2 is intended to be used for signature generation, verification and generic data integrity checks. The use for keyed hash operations like HMAC or similar security critical operations involving keys, is not subject of this TOE and requires specific security improvements and DPA analysis including the operating system, which is not part of this TOE. Further essential information about the usage is given in the confidential user guidance [11].

Nevertheless, following is valid:

The TSF shall perform hash-value calculation of user chosen data in accordance with a specified cryptographic algorithm SHA-2 and with cryptographic key sizes of none that meet the following standards:

U.S. Department of Commerce / National Institute of Standards and Technology, Secure Hash Standard (SHS), FIPS PUB 180-4, 2012-March, section 6.2 SHA-256 and section 6.4 SHA-512.

The covered security functional requirement is FCS_COP.1/SHA.

8.5.6 Toolbox Library

The toolbox provides the following basic long integer arithmetic and modular functions in software, supported by the cryptographic coprocessor: Addition, subtraction, division, multiplication, comparison, reduction, modular addition, modular subtraction, modular multiplication, modular inversion and modular exponentiation. No security relevant policy, mechanism or function is supported. The toolbox library is deemed for software developers as support for simplified implementation of long integer and modular arithmetic operations.

The toolbox does not cover security functional requirements.

8.5.7 Base Library

The Base Library provides the low level interface to the asymmetric cryptographic coprocessor. The base library does not provide any security functionality, implements no security mechanism, and does not provide additional specific security functionality. However the Base library is necessary in order to use the RSA, EC or Toolbox library.

The Base Library does not cover security functional requirements on its own.

8.5.8 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 (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 or TRNG implements also self-testing features. The PTRNG or TRNG meets the requirements of the functionality class PTG2 of the AIS31 [5].

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

8.5.9 Summary of SF_CS: Cryptographic Support

The **SF_CS** "Cryptographic Support" covers the security functional requirements FCS_COP.1/TDES, FCS_COP.1/TDES_SCL, FCS_CKM.4/TDES, FCS_CKM.4/TDES_SCL, FCS_COP.1/AES, FCS_COP.1/AES_SCL, FCS_CKM.4/AES, FCS_CKM.4/AES_SCL, FCS_COP.1/RSA, FCS_COP.1/ECDSA, FCS_CKM.1/EC, FCS_COP.1/ECDH, FCS_COP.1/SHA, FPT_PHP.3, FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_TST.2, FPT_FLS.1 and FCS_RNG.1.

Note:

The cryptographic libraries SCL, RSA, EC, SHA-2 and the Toolbox library are delivery options. If one of the libraries RSA, EC and Toolbox or combination hereof are delivered, the Base Lib is automatically part of it. Therefore the TOE may come with free combinations of or even without these libraries. In the case of coming without one or any combination of the cryptographic libraries SCL, RSA, EC and SHA-2, the TOE does not provide the corresponding additional specific security functionality Rivest-Shamir-Adleman Cryptography (RSA) and/or Elliptic Curve Cryptography (EC) and/or SHA-2 and/or SCL based Triple Data Encryption Standard (TDES) and/or SCL based Advanced Encryption Standard (AES). The Toolbox and Base Library are no cryptographic libraries and provide no additional specific security functionality.

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 TDES computation supported by hardware is possible (neither solely hardware based nor SCL based). In case the Crypto@2304T is blocked, no RSA and EC computation supported by hardware is possible. The use of the SHA-2 library is also possible with both crypto coprocessors blocked. 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.

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 sections the sections above. The results are shown in Table 22. 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 22: 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_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_COP.1/TDES_SCL					X

Security Functional Requirement	SF_DPM	SF_PS	SF_PMA	SF_PLA	SF_CS
FCS_CKM.4/TDES			X		X
FCS_CKM.4/TDES_SCL			X		X
FCS_COP.1/AES					X
FCS_COP.1/AES_SCL					X
FCS_CKM.4/AES			X		X
FCS_CKM.4/AES_SCL			X		X
FCS_COP.1/RSA-v1.02.013					X
FCS_COP.1/RSA-v2.07.003					X
FCS_CKM.1/RSA-v2.07.003					X
FCS_COP.1/ECDSA-v1.02.013					X
FCS_COP.1/ECDSA-v2.07.003					X
FCS_COP.1/ECDH-v1.02.013					X
FCS_COP.1/ECDH-v2.07.003					X
FCS_COP.1/SHA					X
FCS_CKM.1/EC-v1.02.013					X
FCS_CKM.1/EC-v2.07.003					X

8.7 Security Requirements are Internally Consistent

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

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

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.

The requirement FDP_SDI.2.1 allows detection of integrity errors of data stored in memory. FDP_SDI.2.2 in addition allows correction of one bit errors or taking further action. Both meet the security objective O.Malfunction.

The requirements FRU_FLT.2, FPT_FLS.1, and FDP_ACC.1 which also meet this objective are independent from FDP_SDI.2 since they deal with the observation of the correct operation of the TOE and not with the memory content directly.

9 Referenced Literature

Ref	Version	As off	Title
[1]	1.0	2007-06-15	Security IC Platform Protection Profile PP0035
[2]	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
[3]	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
[4]	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
[5]	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
[6]	Rev. 1.7.1	2015-09-21	M7892 SOLID FLASH™ Controller for Security Applications, 16-bit Security Controller Family, 90nm Technology, Hardware Reference Manual
[7]		2015-04-01	SLx 70 Family Production and Personalization User's Manual
[8]	v9.7	2017-09-14	16-bit Controller Family, SLE 70, Programmer's Reference Manual
[9]	v1.02.013	2017-06-20	SLE70 Asymmetric Crypto Library Crypto@2304T, RSA / EC / Toolbox, User Interface, Update 2017-06-20
[10]	v2.02.012	2017-05-02	SCL78 Symmetric Crypto Library for SCP v3, DES / AES, 16-bit Security Controller, User Interface
[11]		2009-11-06	Chipcard and Security iCs, SLx70 Family, Secure Hash Algorithm SHA-2, (SHA 256/224, SHA 512/384) (optional)
[12]		2010-03-23	SLE70 Crypto@2304T User Manual
[13]	1.1	2013-09-24	AMM Advanced Mode for Mifare-Compatible Technology, Addendum to M7892_HRM_Addendum_AMM
[14]		2017-06-28	M7892 Security Guidelines
[15]	Rev.4.1	2017-06-21	M7892 Errata Sheet
[16]	2.9	2013-01	Application of Attack Potential to Smartcard, mandatory technical document, CCDB-2013-05-002, http://www.commoncriteriaportal.org
[17]		2009-06	NIST: FIPS publication 186-3: Digital Signature Standard (DSS), June 2009
[18]	RFC 5639	2010-03	IETF: RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010, http://www.ietf.org/rfc/rfc5639.txt
[19]	180-4	2015-08	Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8900, Federal Information Processing Standards Publication, Secure Hash Standard (SHS)
[20]	X.9.63	2001-11-20	American National Standard for Financial Services X9.63-2001, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, American National Standards Institute
[21]	ISO/IEC 15946-3	2002	ISO/IEC 15946-3:2002 Information Technology – Security Techniques – Cryptographic techniques based on elliptic curves – part 3: Key Establishment
[22]	SP 800-67 Rev. 1	2012-01	National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce, NIST Special Publication 800-67

Ref	Version	As off	Title
[23]	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
[24]	PKCS, RFC 3447, v2.1	2002-06-14	PKCS #1: RSA Cryptography Standard, RSA Laboratories
[25]	X.9.62	2005-11-16	American National Standard for Financial Services ANS X9.62-2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standards Institute
[26]	ISO/IEC 15946-2	2002	ISO/IEC 15946-2:2002 Information Technology – Security Techniques – Cryptographic techniques based on elliptic curves – part 2: Digital Signatures
[27]	I	2009-08-14	Act on the Federal Office for Information Security (BSI-Gesetz - BSIG), Bundesgesetzblatt I p. 2821.
[28]	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)
[29]	ISO/IEC 10118	2004	ISO/IEC 10118-3:2004, Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash functions (for AES)
[30]	ISO/IEC 18033	2005	ISO/IEC 18033-3:2004, Information technology – Security techniques – Encryption algorithms– Part 3: Block ciphers [18033] (for AES)
[31]	PUB 140-2	2002-12-03	National Institute of Standards and Technology, “*Security Requirements for Cryptographic Modules*”, Federal Information Processing Standards Publication (FIPS) 140-2 , 2002-12-03
[32]	ISO/IEC 15946-1	2002	ISO/IEC 15946-1:2002 Information Technology - Security Techniques - Cryptographic techniques based on elliptic curves - part 1: General
[33]	V3.1 Rev 4	2012-09	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, CCMB-2012-09-004
[34]	ISO/IEC 97971: 2011	2011-03-01	Information technology – Security techniques - Message Authentication Codes (MACs) Part 1 Mechanisms using block cipher
[35]	V2.07.003	2017-05-15	SLE70 Asymmetric Crypto Library for Crypto@2304T, RSA / ECC / Toolbox, User Interface, Infineon Technologies, 2017-05-15, SLE70-CryptoLibrary-UserInterface_v2.07.003.pdf
[36]	ISO / IEC 14888-3	2006, published 2009-02-15	INTERNATIONAL STANDARD ISO/IEC 14888-3:2006, TECHNICAL CORRIGENDUM 2, Published 2009-02-15, Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms
[37]	IEEE 1363	2000-01-30 (approved)	IEEE Standard Specification for Public Key Cryptography, IEEE Standards Board. The standard covers specification for public key cryptography including mathematical primitives for secret value deviation, public key encryption and digital signatures and cryptographic schemes based on those primitives.
[38]	ISO/IEC 11770-3	2008, published 2009-09-15	INTERNATIONAL STANDARD ISO/IEC 11770-3:2008, TECHNICAL CORRIGENDUM 1, Published 2009-09-15, Information technology-Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques
[39]	3.2	2017-11-09	Confidential Secure Target for M7892 B11

10 Appendix

In the following the hash signatures of the optional software libraries are listed. Several hash algorithms are used for convenience.

RSA, EC, Toolbox, Base Version v1.02.013:

Cl70-LIB-base-XSMALL-HUGE.lib:

MD5=d080392bc14a65de9094d846498f28a3

SHA1=4149318953b22876c6d9f712e084f00dccaac88f

SHA256=c08bf0778baf3a25123e1ff45590eeec6bff29cb38ede2a07a377f968d5eeade

Cl70-LIB-2k-XSMALL-HUGE.lib:

MD5=e1829fa50cbd46f912e40528e92e77d4

SHA1=41a4c013fe08cbcf4917753076d8c035657040a0

SHA256=afe2dc4b3ecebbd67dab8add2581f3ceb4f6268d5f6c0091f7d975afbbec86ca

Cl70-LIB-4k-XSMALL-HUGE.lib:

MD5=3c2ac3030c2abbc9e6d32b46c244f59b

SHA1=0867b74168c2b228a12c2835de92262d9536bdde

SHA256=11736a910bdc9e8a2d74b56db60d2002ff8bd9ba49be8c8fc08d744128ac6e3b

Cl70-LIB-ecc-XSMALL-HUGE.lib:

MD5=9ccf23232e16645448323670e8fa3171

SHA1=315952fc79e4e711e6f95e2b9d547a5c91d88d1c

SHA256=69ad0d5bfaf2308c24d19ee8824d61952a73c273dd57ee19612dace6ba92e772

Cl70-LIB-toolbox-XSMALL-HUGE.lib:

MD5=4c577bcf9853c8c030b84ebe19d22b8d

SHA1=4c12dc67dad4bbe88c4b23c43a275b3ad3be71f3

SHA256=e6de94b27ffce43b8a023c04ceb86795585617b4cac8e7a53a78cf273b1fe8fc

SHA-2 Library Version 1.01:

SHA-2 values computed from: SLE70-SHA2-Lib_RE_1v01_2009-06-29.LIB

MD5=70d2df490185b419fb820d597d82d117

SHA1= df15ff79b5f5ab70bbad0ee031953e1877cabd47

SHA256=765fc5d47cf8274833476406b24010a56ebcfd4b0972704ddd27e2d3e3e086f8

SCL Library Version v2.02.012:

Scl78-SCP-v3-LIB-cipher-XSMALL-HUGE.lib:

MD5=65608681520d05588a73d9387fd2d71c

SHA1=1bff8e54aaffd7f4c7b8a0a9e4151bfe7d3ed3a0

SHA256=13f69d8814845f00ebd4f4ebfa737ebc229c87fef376a415f274e40052d60b14

Scl78-SCP-v3-LIB-des-XSMALL-HUGE.lib:

MD5=f1d05ef1cd33dc077c09bc1709a4fa69

SHA1=42b663aef9e5ad4c91f1793f44f8f455cd1c1d58

SHA256=12a153d195bd13f9005c6f0bf9b4f4745a5dbfafc78923a8e678d1f2b7374979

Scl78-SCP-v3-LIB-aes-XSMALL-HUGE.lib:

MD5=c4b7480a220f6dc1f11d96c9467f0837

SHA1=14270582aee21460286445a51625db5419a00d24

SHA256=e35b06a570b7468b3a337a442a31c968b106cf700eead1a2b2f1cf3cd1385c27

11 List of Abbreviations

AES	Advanced Encryption Standard
AIS31	“Anwendungshinweise und Interpretationen zu ITSEC und CC Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren”
API	Application Programming Interface
BPU	Bill Per Use
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. Sometimes also referred as Crypto2304T
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 (EEPROM) a Non Volatile Memory
EMA	Electro magnetic analysis
FL	Flash Loader
HW	Hardware
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	Object
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
SAM	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
SO	Security objective
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
UM	User Mode (STS)
UmSLC	User mode Security Life Control
WDT	Watch Dog Timer
XRAM	eXtended Random Access Memory
TDES	Triple DES Encryption Standard

12 Glossary

Application Program/Data	Software which implements the actual TOE functionality provided for the user or the data required for that purpose
Bill-Per-Use	Bill-Per-Use concept allowing the user to configure the chips
Central Processing Unit	Logic circuitry for digital information processing
Chip	Integrated Circuit]
Chip Identification Data	Data stored in the SOLID FLASH™ NVM containing the chip type, lot number (including the production site), die position on wafer and production week and data stored in the ROM containing the STS version number
Chip Identification Mode	Operational status phase of the TOE, in which actions for identifying the individual chip by transmitting the Chip Identification Data take place
Controller	IC with integrated memory, CPU and peripheral devices
Crypto@2304T	Cryptographic coprocessor for asymmetric cryptographic operations (RSA, Elliptic Curves). Sometimes also referred as Crypto2304T.
Cyclic Redundancy Check	Process for calculating checksums for error detection
Electrically Erasable and Programmable Read Only Memory (SOLID FLASH™ NVM)	Non-volatile memory permitting electrical read and write operations
End User	Person in contact with a TOE who makes use of its operational capability
Firmware	Is software essential to put the chip into operation. The firmware is located in the ROM and parts of it in the SOLID FLASH™ NVM
Flash Loader	Software enabling to download software after delivery
Hardware	Physically present part of a functional system (item)
Integrated Circuit	Component comprising several electronic circuits implemented in a highly miniaturized device using semiconductor technology
Security Target	Description of the intended state for countering threats
Mechanism	Logic or algorithm which implements a specific security function in hardware or software
Memory Encryption and Decryption	Module for encoding/decoding data transfer between CPU and memory
Memory	Hardware part containing digital information (binary data)
Microprocessor	CPU with peripherals
Object	Physical or non-physical part of a system which contains information and is acted upon by subjects
Operating System	Software which implements the basic TOE actions necessary to run the user application
Programmable Read Only Memory	Non-volatile memory which can be written once and then only permits read operations
Random Access Memory	Volatile memory which permits write and read operations
Random Number Generator	Hardware part for generating random numbers

Read Only Memory	Non-volatile memory which permits read operations only
Resource Management System	Part of the firmware containing SOLID FLASH™ NVM programming routines, AIS31 testbench etc.
SCP	Is the 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
Smart Card	Is a 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

www.infineon.com

Published by Infineon Technologies AG