Public

Security Target Lite Lite

M5073 G11

Common Criteria CCv3.1 EAL6 augmented (EAL6+)

Resistance to attackers with HIGH attack potential

INTEGRITY GUARD SOLID FLASH™

Document version 1.0 as of 2017-09-27

Dr. Oleg Rudakov

Edition 2017-09-27

Published by Infineon Technologies AG,

81726 Munich, Germany.

Legal Disclaimer

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics. With respect to any examples or hints given herein, any typical values stated herein and/or any information regarding the application of the device, Infineon Technologies AG hereby disclaims any and all warranties and liabilities of any kind, including without limitation, warranties of non-infringement of intellectual property rights of any third party.

Information

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

Warnings

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

Infineon Technologies AG components may be used in life-support devices or systems only with the express written approval of Infineon Technologies AG, if a failure of such components can reasonably be expected to cause the failure of that life-support device or system or to affect the safety or effectiveness of that device or system. Life support devices or

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.

Public

Revision History

Major changes since previous revision		
Date	**Version**	**Change Description**
2017-09-27	1.0	Initial Version

Table of Contents

Public

1 Security Target Introduction (ASE_INT)

1.1 Security Target and Target of Evaluation Reference

The title of this document is Security Target Lite M5073 G11 Common Criteria CCv3.1 EAL6 augmented (EAL6+).

This document comprises the Infineon Technologies AG Security Controller (Integrated Circuit IC) M5073 G11 with specific IC dedicated firmware and optional software:

- RSA v2.03.008 or v2.07.003
- EC v2.03.008 or v2.07.003
- Toolbox v2.03.008 or v2.07.003
- SHA-2 v1.01
- Symmetric Crypto Library v2.02.010.

The target of evaluation (TOE) M5073 G11 is described in the following.

The reference to the belonging confidential Security Target is given in chapter 9.

The Target of Evaluation (TOE) is the Infineon Security Controller M5073 G11 with optional RSA2048/4096 v2.03.008 or v2.07.003, EC v2.03.008 or v2.07.003, SHA-2 v1.01 and Toolbox v2.03.008 or v2.07.003 libraries, symmetric crypto library v2.02.010, as well as with specific IC dedicated firmware, including the Flash Loader enhanced by the Mutual Authentication Extension (MAE).

The version of ECC, RSA and Toolbox libraries cannot be chosen independently. The libraries have to be of one version.

The design step of this TOE is G11.

The Security Target is based on the PP number 0084 “Security IC Platform Protection Profile with Augmentation Packages” [11] as publicly available for download at https://www.bsi.bund.de and certified under BSI-CC-PP-0084-2014. MAE and Flash Loader are regarded by the definition of “loader package 1+” according to “PP0084: Interpretations” [35].

The Protection Profile and the Security Target are built in compliance with Common Criteria v3.1. The Protection Profile is abbreviated with “PP” in the following.

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

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

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

Public

Table 1: Identification

Object	Version	Date	Registration
Security Target	1.0	2017-09-27	Security Target M5073 G11 Common Criteria CCv3.1 EAL6 augmented (EAL6+)
Target of Evaluation			M5073 G11 With FW-Identifier 78.023.01.2 MAE: 8.00.006 And following optional SW libraries: RSA2048 v2.03.008 or v2.07.003 RSA4096 v2.03.008 or v2.07.003 EC v2.03.008 or v2.07.003 SHA-2 v1.01 Base[1] v2.03.008 or v2.07.003 Toolbox v2.03.008 or v2.07.003 SCL v2.02.010 and belonging User Guidance documentation.
Protection Profile (PP)	1.0	2014-01-13	Security IC Platform Protection Profile with Augmentation Packages BSI-CC-PP-0084-2014
Common Criteria	3.1 Revision 5	2017-04	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCMB-2017-04-001 Part 2: Security functional requirements CCMB-2017-04-002 Part 3: Security Assurance Components CCMB-2017-04-003
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.			

[1] Please note that the Base Library cannot be ordered. However this library is part of the delivery if the RSA2048, the RSA4096, the EC or the Toolbox library is ordered.

Public

The user can identify the TOE and its configuration using the Non-ISO ATR in combination with firmware functions. The TOE answers the Non-ISO ATR with the Generic Chip Identification Mode (GCIM). The GCIM outputs a chip identifier byte, design step, firmware identifier version and further configuration information. The identification data and configuration details are described in the confidential Security Target [9] and in the Family Hardware Reference Manual HRM [1].

Furthermore, the MAE can be identified utilising its version, as described in the Production and personalization Mutual Authentication Extension [36]. The version is part of the "basic chip information" provided by the command FLASH_GET_CHIP_STATUS.

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 M5073 G11. All product derivatives are identically from module design, layout and footprint, but are made different in their possibilities to connect to different types of antennas or to a contact based interface only. Therefore, the TOE is represented and made out of different mask sets.

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

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

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 [1]. An overview upon the different mask sets is given in the confidential Security Target [9].

The M5073 G11 allows for a maximum of configuration possibilities defined by the customer order or his blocking following the market needs. For example, a M5073 G11 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 and user ROM size. And more, the user has the free choice, whether he needs the symmetric coprocessor SCP, or the asymmetric coprocessor Crypto@2304T, or both, or none of them. In addition, the user decides, whether the TOE comes with a free combination of software libraries or without any. However, the version of ECC, RSA and Toolbox libraries cannot be chosen independently. If selected the libraries have to be of one version. And, to be even

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

more flexible, various interface options can be chosen as well. To sum up the major selections, the user defines by his order:

- The available memory sizes of the SOLID FLASH™ NVM and RAM.
- The availability of the cryptographic coprocessors.
- The availability of the optional cryptographic libraries.
- The availability of Mutual Authentication Extension (MAE) and 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.

BPU enables our customers to block the chip on demand into the final configuration at his own premises, without further delivery or involving support by Infineon Technology. Further information is given in the confidential Security Target [9].

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

The Flash Loader BPU software part is only available on the products which have been ordered with the BPU option. In all other cases this software is disabled on the product. If a product is ordered without Flash Loader, also the Flash Loader BPU software part is disabled and the BPU configuration changes are blocked in the IFX-configuration, which additionally renders the BPU functionality unusable. Various delivery combinations are given and for example, a product can come with a fix configuration and with Flash Loader, to enable the user to download software, but without BPU option. Following cases can occur:

- Order in fixed configuration, without activatable MAE and Flash Loader feature:
  no download of user software and no blocking possibility after delivery

Public

- Order in fixed configuration with activatable MAE[1] and Flash Loader but without BPU option: download of user software but no blocking possibility after delivery
- Order with activatable MAE and Flash Loader feature and Bill-per-Use option in starting configuration: final chip configuration by the user and download of user software

In case a customer decides to order the TOE with activatable MAE and Flash Loader, he has to make sure that the Flash Loader is protected against misuse. This explicitly includes the delivery process from Infineon to the customer. In addition, the Flash Loader has to be used in an MSSR-audited environment. Furthermore, the Flash Loader (and MAE) has to be deactivated permanently before chips are delivered to the end-customer. These aspects are not within the scope of this evaluation but have to be considered for a composite TOE which is based on the M5073 G11.

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 this 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 are no user data in the ROM.	After successful external authentication using MAE, the Flash Loader can be activated by the user or subcontractor to download his software in the SOLID FLASH™ NVM – until the Flash Loader is finally permanently 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 are no user data in the ROM.	The Flash Loader is permanently deactivated (and MAE is not installed).

[1] „Activatable MAE“ means either that MAE is installed and will be active after power-up or reset of the TOE or that MAE can be (re-)installed and activated via the Flash Loader.

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 are no user data in the ROM.	MAE and Flash Loader are deactivated afterwards, but can be 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.
4	The user provides the software for implementation into the ROM mask.	The Flash Loader is permanently deactivated (and MAE is not installed).
5	The user provides the software for implementation into the ROM mask.	MAE and Flash Loader are deactivated, but can be activated or reactivated by the user or subcontractor to download his software in the Infineon® SOLID FLASH™ memory. Precondition is that the user has provided an own reactivation procedure in software prior chip production to Infineon Technologies AG.
6	The user provides the software for implementation into the ROM mask and provides software for the download into the SOLID FLASH™ NVM to Infineon Technologies AG.	The Flash Loader is permanently deactivated (and MAE is not installed).
7	The user provides the software for implementation into the ROM mask and provides software for the download into the SOLID FLASH™ NVM to Infineon Technologies AG.	MAE and Flash Loader are deactivated afterwards, but can be reactivated by the user or subcontractor to download his software in the Infineon® SOLID FLASH™ memory. Precondition is that the user has provided an own reactivation procedure in software prior chip production to Infineon Technologies AG.

For the cases with activatable MAE and Flash Loader and whenever the user has finalized his software 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 locking is the final step and 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. In locked state it is also impossible to re-install/activate the MAE (as this would need an active Flash Loader).

Public

Note that whenever a TOE comes with a permanently deactivated Flash Loader, the BPU feature is not possible as well. On the other hand, an ordered activatable Flash Loader can come without the BPU feature. The availability of the BPU feature depends on the user order but is only given on products with activatable Flash Loader.

The following listing contains the memory size ranges and other blocking options, focusing on the maximum respectively minimum user available limitations. Within those limitations the TOE configurations can vary under only one identical IC-hardware. It is regardless whether the configurations are set by Infineon or within further limitations by the user. All configurations the TOE is made off and all thereof resulting derivatives have no impact on security and are covered by the certificate.

Wherever user blocking is stated in the table below, the user can block the chip within the therein defined limitations, but only if the product was ordered with the BPU option.

The below given configuration possibilities are valid unchanged throughout the mentioned different mask sets. Wherever user blocking is stated below, the user can block the chip within the defined limitations, but only if the product was ordered with the user configuration capability.

The following table provides an excerpt of possible configurations:

Table 3: Configuration ranges and blocking options for the user

Module / Feature (User view)	Max-Value (User view)	Min-Value (User view)	User Blocking	User Blocking Step
Memories				
SOLID FLASH™ NVM	628 KByte	0 KByte	Yes	1 KByte
ROM	444 KByte	0 KByte	By order only	n.a.
RAM for the user	12 KByte	1 KByte	Yes	1 KByte
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
Inter Integrated Circuit I2C	Available	Not available	Yes	On/off
RFI – ISO 14443 generally	Available	Not available	Yes	On/off

Public

Module / Feature (User view)	Max-Value (User view)	Min-Value (User view)	User Blocking	User Blocking Step
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
Software controlled Input Output (SWIO)	Available	Available	No	No
Mifare hardware support for card mode	Available	Not available	By order only	None

There are further communication modes and blocking options available which are outlined in the confidential Security Target [9] and the confidential User Guidance.

All possible TOE configurations equal and/or within the physical specified ranges as outlined in the confidential Security Target [9] and in the hardware reference manual HRM [1] are covered by the certificate.

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 HRM [1]. These predefined products come with the most requested configurations and allow to produce volumes on stock in order to simplify logistic processes.

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

Note that the TOE outputs the Generic Chip Identification data enabling the user together with the user guidance for a clear interpretation and identification of the TOE. More information is given in the confidential Security Target [9].

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

Public

The firmware parts are the RMS library, the Service Algorithm Minimal (SA), the STS firmware for test purpose (see chapter 2.2.2), providing some functionality via an API to the Smartcard Embedded Software, the MAE and the Flash Loader for downloading user software to the SOLID FLASH™ NVM and the Mifare compatible software interface. The entire firmware is located in the ROM and the belonging patches are stored in the SOLID FLASH™ NVM.

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

The software parts are differentiated into the cryptographic libraries RSA[1], EC[2], SHA-2[3], symmetric cryptographic library (SCL) and the supporting libraries Toolbox and Base. RSA, EC, SHA-2, Toolbox and SCL provide certain functionality via an API to the Smartcard Embedded Software. The Base Library does not provide a dedicated functionality on its own and is mainly used internally by the RSA, EC and Toolbox libraries. If none of the libraries RSA, EC and Toolbox is delivered, also the Base Library is not on board.

The TOE can be delivered including – in free combinations –the functionality of the cryptographic libraries SCL, EC, RSA, SHA-2 and the supporting Toolbox library. However, the version of ECC, RSA and Toolbox libraries cannot be chosen independently. If selected the libraries have to be of one version. If RSA or EC or Toolbox is delivered, automatically the Base Library is part of the shipment too.

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 Rivest-Shamir-Adleman (RSA) and/ or EC and/or SHA-2 and/or SCL based Advanced Encryption Standard (AES) and 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.

The Base Library provides the low level interface to the asymmetric cryptographic coprocessor for the RSA, EC and Toolbox libraries. The Base Library does not provide any dedicated security functionality on its own.

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.

[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

Public

The SCL, RSA, EC, SHA-2 and Toolbox libraries can be loaded, together with the Smartcard Embedded software, into the SOLID FLASH™ NVM. This holds also for the Base Library, if the RSA, EC or Toolbox or combinations hereof is/are part of the shipment.

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

1.2 Target of Evaluation overview

The TOE comprises the Infineon Technologies AG Dual Interface Security Controller M5073 G11 with specific IC dedicated software and optional SCL, RSA, EC, SHA-2, Toolbox and Base library.

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

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

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

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

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

Contact based interfaces

- ISO 7816

  This is the ISO defined standard contact-based communication protocol, using the pads.

- Inter Integrated Circuit (I2C)

  The Inter-Integrated Circuit (I2C, also IIC) module is able to be connected as slave to an external multi-master-

serial-bus-system used to connect the TOE to an external master, using the IIC protocol. The master can also be a multi master IIC system. The IIC protocol software is not part of the TOE.

- There are further communication modes which are outlined in the confidential Security Target [9].

Contactless interfaces

- ISO 14443 Type A and Type B

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

- ISO/IEC 18092 passive mode

  This is an ISO defined proximity contactless protocol using an external antenna and the TOE implemented analogue and digital radio frequency interface.

- Mifare compatible software Interface

  This is a proprietary proximity contactless protocol using an external antenna and the TOE implemented analogue and digital radio frequency interface, as well as the memory part reserved for Mifare use.

- And various further communication modes

All interfaces and protocols can be made available sequentially. How the interfaces are used or combined depends exclusively on the user software.

Further communication modes, details and an overview about their combinations are outlined in the confidential Security Target [9].

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

The RMS library providing some functionality via an API to the Smartcard Embedded Software contains for example SOLID FLASH™ NVM service routines. The Service Algorithm Minimal (SAM) provides functionality for the tearing-safe write into the SOLID FLASH™ NVM. The STS firmware is used for test purposes during start-up and the MAE and Flash Loader allow for mutual authentication with the TOE and secure downloading of 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.

Public

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 [15]. It is used for provision of random number generation as a security service to the user and for internal purposes. The produced genuine random numbers can be used directly or as seed for the Deterministic Random Number Generator (DRNG), formerly named as Pseudo Random Number Generator (PRNG). The DRNG respectively PRNG is not in the scope of the evaluation. The TRNG respectively PTRNG is specially designed for smart cards, but can also be used in any other application where excellent physical random data are required.

The two cryptographic coprocessors serve the need of modern cryptography: The symmetric coprocessor (SCP) combines both AES and Triple-DES with dual-key or triple-key hardware acceleration. The Asymmetric Crypto Coprocessor, called Crypto@2304T performs RSA-2048 bit (4096-bit with CRT) and Elliptic Curve (EC) cryptography.

The software part of the TOE consists of the cryptographic libraries SCL, RSA, EC and SHA-2 and the supporting libraries Toolbox and Base. The Base library is used internally by the RSA, EC and Toolbox library and provides the low-level interface to the asymmetric cryptographic coprocessor. Thus if one of the aforementioned libraries is ordered, the Base library will be included in the delivery automatically. 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 generation of RSA Key Pairs, the 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 bit.
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 ECC Add and ECC Double. EC curves over prime field Fp, as well as over GF(2^n) finite field are supported too. Note that the according user guidance documentation uses the abbreviation ECC for the Elliptic Curve cryptographic functions. 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 bit, due to national AIS32 regulations by the BSI. Numerous other curve types, being also secure in terms of side channel attacks on this TOE, exist, which the user optionally can add in the composition certification process.

[1] BSI Bundesamt für Sicherheit in der Informationstechnik – Federal Office for Information Security

Public

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. 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 [5].

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 asymmetric 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 the symmetric coprocessor. The SCL implements 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. The public API of the SCL is described in [33]. Please note that the single DES operation, the PCBC block cipher mode, the “CipAlg_*_Sec1”-functions and the additional blocker cipher modes, which may be implemented by the generic BCM extension concept are not 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. The TOE can 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 and which has proven its resistance against attackers with high attack potential. This TOE utilizes digital security features to include customer friendly security, combined with a robust design overcoming the disadvantages on analogue protection technologies. The TOE provides full on-chip encryption of the data path, covering the core including the ALUs of the CPUs, busses, memories and cryptographic coprocessors leaving no plaintext on the chip. Therefore the attractiveness for attackers is extremely reduced as encrypted signals are of no use for the attacker – neither for manipulation nor for eavesdropping.
In addition, the TOE is equipped with a comprehensive error detection capability for the complete data path. The dual CPU approach allows error detection even while processing. A comparator detects whether a calculation was performed without errors. This approach does not leave any parts of the core circuitry unprotected. The concept allows that the

relevant attack scenarios are detected, whereas other conditions that would not lead to an error would mainly be ignored. That renders the TOE robust against environmental influences.

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

In this security target 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 PP [11] 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 common standard defined in the Common Criteria documents [12], [13], [14] and in the PP [11].

2 Target of Evaluation Description

The TOE description helps to understand the specific security environment and the security policy. In this context the assets, threats, security objectives and security functional requirements can be employed. The following is a more detailed description of the TOE than in the Security IC Platform Protection Profile PP [11] as it belongs to the specific TOE.

The Security IC Platform Protection Profile is in general often abbreviated with 'PP' and its version number.

2.1 TOE Definition

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

This TOE is intended to be used in smart cards and any other form factor for particularly applications requiring highest levels of security and for its previous use as developing platform for smart card operating systems according to the lifecycle model from Protection Profile the PP [11].

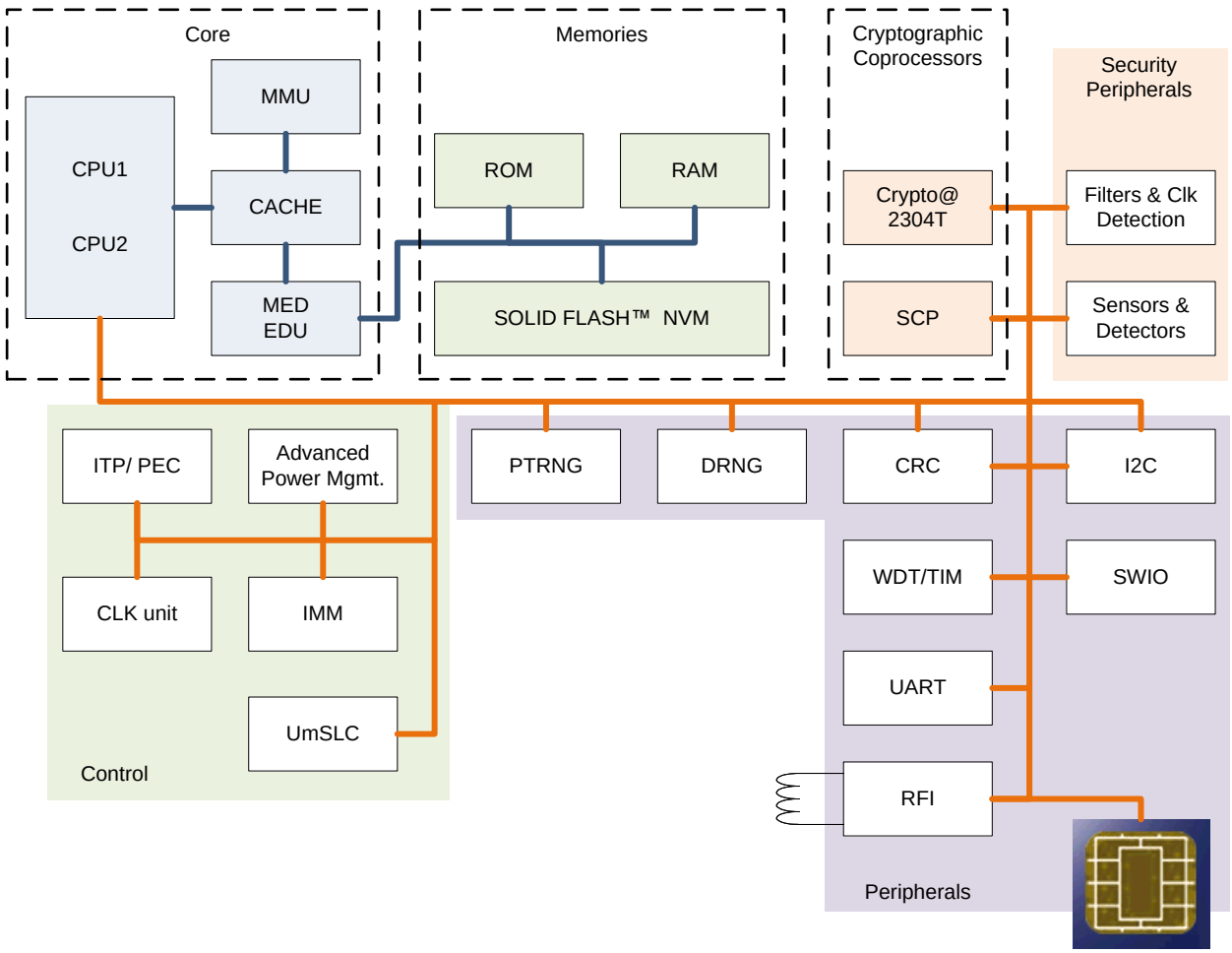
The term Smartcard Embedded Software is used in the following for all operating systems and applications stored and executed on the TOE. The TOE is the platform for the Smartcard Embedded Software. The Smartcard Embedded Software itself is not part of the TOE.

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

Public

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

Figure 1: Simplified block diagram of the TOE



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

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

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

Public

The CPU accesses the memory via the integrated Memory Encryption and Decryption unit (MED), which transfers 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 1-Bit-errors are also corrected (ECC). The TOE uses also Special Function Registers SFR. These SFR registers are used for general purposes and chip configuration. These registers are located in the SOLID FLASH™ NVM as configuration area page.

The non-volatile ROM contains the firmware parts and, if desired by the user, also user software. If this is the case, the user must provide his software package for the ROM prior production, as the software is processed as a hardware mask during chip production and implementation of the ROM. The firmware part STS of the ROM is accessible for Infineon only. 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 Crypto@2304T for calculation of asymmetric algorithms like RSA and Elliptic Curve (EC) and the Symmetric Cryptographic Processor (SCP) for dual-key or triple-key triple-DES and AES calculations. These coprocessors are especially designed for smart card applications with respect to the security and power consumption, but can of course be used in any other application of form factor where suitable. The SCP module computes the complete DES algorithm within a few clock cycles and is especially designed to counter attacks like DPA, EMA and DFA.

Note that this TOE can come with both crypto coprocessors accessible, or with a blocked SCP or with a blocked Crypto@2304T, or with both crypto coprocessors blocked. The blocking depends on the customer demands prior to the production of the hardware. No accessibility of the deselected cryptographic coprocessors is without impact on any other

security policy of the TOE; 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 Clock unit, the Advanced Power Management, the Interface Management Module and the UmSLC, which is the abbreviation for User Mode Security Life Control. The UmSLC enables for checking the proper functions of modules and subsystems and checks the correct operation of the TOE.

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

The peripherals block is constituted out of PTRNG, DRNG, CRC, Timer & WDT, the RFI, I2C, SWIO and the UART. The modules are briefly described in the following:

The TRNG respectively PTRNG is specially designed for smart cards, but can also be used in any other application where excellent physical random data is required. The TRNG respectively PTRNG 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 [1].

Public

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

Contact-based interfaces

- ISO 7816
  The ISO defined standard contact-based communication protocol, using the pads.
- Inter Integrated Circuit (I2C)
  The Inter-Integrated Circuit (I2C, also IIC) module is able to be connected as slave to an external multi-master-serial-bus-system used to connect the TOE to an external master, using the IIC protocol. The master can also be a multi master IIC system. The IIC protocol software is not part of the TOE.
- And further communication modes which are outlined in the confidential Security Target [9].

Contactless interfaces

- ISO 14443 Type A and Type B
  The ISO defined proximity contactless protocols using an external antenna and the TOE implemented analogue and digital radio frequency interface.
- ISO/IEC 18092 passive mode
  The ISO defined proximity contactless protocol using an external antenna and the TOE implemented analogue and digital radio frequency interface.
- Mifare compatible software interface
  This is a proprietary proximity contactless protocol using an external antenna and the TOE implemented analogue and digital radio frequency interface, as well as the memory part reserved for Mifare use.
- And various further communication modes

All interfaces and protocols can be made available sequentially. How the interfaces are used or combined depends exclusively on the user software.

Further communication modes, details and an overview about their possible parallel usage are outlined in the confidential Security Target [9].

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

The individual combinations of the interface options are depicted in the confidential Security Target [9].

Public

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 each 1 up to 4 Kbyte 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 bus system comprises two separate bus entities: a memory bus supporting communication between the core and the memories and a peripheral bus for high-speed 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 (SA) 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 SA functions are grouped together in a common privilege level. These privilege levels are protected by a hardwired Memory Management Unit (MMU) setting.
The optional MAE software is stored in the SOLID FLASH™ NVM. The user software can be implemented in various options depending on the user's choice as described in chapter 1.1. Thereby the user software, or parts of it, can be downloaded into the SOLID FLASH™ NVM, either during production of the TOE or at customer 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. Once the user software has been downloaded onto the TOE, any MAE software that was on the TOE is no longer available (yet it might be re-installed and activated if the Flash Loader is not locked yet and if an activated user software has implemented functionality to re-activate the Flash Loader).

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. 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 [5].

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 Base Library provides the low level interface to the asymmetric cryptographic coprocessor for the RSA, EC and Toolbox libraries. The Base Library does not provide any dedicated security functionality on its own.

Public

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 generation of RSA Key Pairs, the 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 bit. 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 ECC Add and ECC Double. EC curves over prime field Fp, as well as over GF(2^n) finite field are supported too. Note that in the according user guidance the Elliptic Curve cryptographic functions are abbreviated using ECC.
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 bit, due to national AIS32 regulations by the BSI. Numerous other curve types, being also secure in terms of side channel attacks on this TOE, exist, which the user optionally can add in the composition certification process.

Note that this TOE can come with both cryptographic coprocessors accessible, with a blocked SCP, 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. The TOE can be delivered without a specific 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 and/or SCL-based Advanced Encryption Standard and/or SCL-based Triple Data Encryption Standard (TDES).

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 bit, 192 bit, 256 bit. 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 bit (plus 8 parity bits) as well as 112 bit and 168 bit, respectively. Please note that the single DES operation, the PCBC block cipher mode, the "*_Sec1"-functions and the additional block cipher modes, which may be implemented by the generic BCM extension concept of the SCL, are not part of this evaluation.

[1] BSI Bundesamt für Sicherheit in der Informationstechnik – Federal Office for Information Security

Public

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

Therefore, this TOE includes:

- The silicon die, respectively the Integrated Circuit (IC) respectively the hardware of this TOE, in several versions. The versions differ from each other by the interface capabilities: The IC comes with a variety of interface capacitances, enabling connections to a variety of external antennas, or to be operated contact-based only.
- The TOE is also delivered in various configurations, achieved by means of blocking by the customer and/or depending on the customer order.
- All configurations and resulting derivatives generated out of the mask sets described as above.
- The according equal firmware on all derivatives, and with or without
- Optional equal software in various combinations as ordered for all TOE derivatives.
- All configurations of any individual TOE product.
- 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 differentiated by the GCIM data and the configuration information output, are manufactured by Infineon Technologies AG. In the following descriptions, the term “manufacturer” stands short for Infineon Technologies AG, the manufacturer of the TOE.

Public

New configurations can occur at any time depending on the user blocking or by different configurations applied by the manufacturer. 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.

The various blocking options, as well as the means used for the blocking, are done during the manufacturing process or at user premises. Entirely all means of blocking and the, for the blocking involved firmware respectively software parts, used at Infineon and/or the user premises, are 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
- The piece of software running at user premises and collecting the BPU receipts coming from the TOE. This BPU software part is the commercially deemed part of the BPU software, not running on the TOE, but allowing refunding the customer, based on the collected user blocking information. The receipt from each blocked TOE is collected by this software – chip by chip.

2.2.1 Hardware of the TOE

The hardware part of the TOE as defined in the Protection Profile PP [11] is comprised of:

Core System

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

CACHE with Post Failure Detection

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

Memory Management Unit (MMU)

Memories

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

Read-Only Memory (ROM)

Random Access Memory (RAM)

Public

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)

Inter-integrated Circuit (I2C)

Software controlled Input Output (SWIO)

Control

Advanced Power Management

CLK Unit

Interrupt and Peripheral Event Channel Controller (ITP and PEC)

Interface Management Module (IMM)

User mode Security Life Control (UmSLC)

Coprocessors

Crypto@2304T for asymmetric algorithms like RSA and EC (optionally blocked)

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

Security Peripherals

Filters and Clk Detection

Sensors and Detectors

Buses

Memory Bus

Peripheral Bus

2.2.2 Firmware and Software of the TOE

The entire firmware of the TOE consists of different parts:

Public

One part comprises the RMS and SA routines used for providing the chip resource management interface for the user. The routines are used for tearing-safe handling of the SOLID FLASH™ NVM, user testing of the security functions and error correction (Resource Management System, IC Dedicated Support Software in PP [11]). These routines are stored in a reserved area of the IFX ROM, while belonging patches (if any) are located in the SOLID FLASH™ NVM. If required also user software can be stored in the ROM.

The second part is the STS, consisting of test and initialization routines (Self-Test Software, IC Dedicated Test Software in PP [11]). The STS routines are stored in the ROM and the belonging patch is located in the access protected SOLID FLASH™ NVM area. The STS is not accessible for the user software.

The third part is MAE and Flash Loader. This piece of software enables the secure download of the user software or parts of it to the SOLID FLASH™ NVM. The Flash Loader routines are stored in the especially protected test ROM but parts of it are also stored in the SOLID FLASH™ NVM. The MAE routines are stored in the SOLID FLASH™ NVM (if the Flash Loader is already permanently deactivated during delivery, MAE software is not present in the TOE and cannot be (re-)installed either). Depending on the order, the Flash Loader comes with the BPU-software enabling for TOE configuration at user premises. After completion of the download and/or final configuration of the TOE, and prior delivery to the end user, the user is obligated to lock the Flash Loader. Locking is the permanent deactivation of the Flash Loader meaning that if once locked it can no more be reactivated and used. Note that the Flash Loader routines are always present, but are deactivated in case of the derivatives ordered without the software download option. Thus the user interface is identically in both cases – with and without Flash Loader on board – and consequently the related interface routines can be called in each of the derivatives.

The fourth part is the Mifare compatible software interface routines. Note that these routines are always present, but deactivated, in case of the derivatives comes without RF interface. Thus the user software interface is identical in both cases and consequently the related Mifare compatible interface routines can be called in each of the derivatives. In case the related interface routines are called in derivatives without this option, 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 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 but implements also countermeasures against all known weaknesses of the SCP v3 (e.g. dummy calculations and block repetitions). The SCL supports the ECB, CBC, CTR CFB and PCBC block cipher modes. Please note that the PCBC mode, the single DES operation, the “*_Sec1”-functions and the additional block cipher modes, which may be implemented using the generic BCM extension concept of the SCL, are not covered by the evaluation.

Public

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 generation of RSA Key Pairs, 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 bit to 4096 bit. 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 lengths from 1976 bit to 2048 bit, and the RSA CRT[1] operations with key lengths from 1976 bit to 4096 bit.

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 a 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. Note that the according user guidance abbreviates the Elliptic Curve cryptographic functions with ECC.
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 bit, due to national AIS32 regulations by the BSI. Numerous other curve types, being also secure in terms of side channel attacks on this TOE, exist, which the user optionally can add in the composition certification process.

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. 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 [5].

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.

[1] CRT: Chinese Remainder Theorem

Public

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.

Note:
The cryptographic libraries SCL, RSA, EC and SHA-2 are delivery options. Therefore the TOE may come with free combinations of or without these libraries. However, the version of ECC, RSA and Toolbox libraries cannot be chosen independently. If selected the libraries have to be of one version. In the case of coming without one or any combination of these libraries 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.

2.2.3 Interfaces of the TOE

- The physical interface of the TOE to the external environment is the entire surface of the IC.
- The electrical interface of the TOE to the external environment is constituted by the pads of the chip, particularly the contacted RES, I/O, CLK lines and supply lines VCC and GND, as well as by the contactless RF interface. The contact-based communication is according to ISO 7816/ETSI/EMV.

  A further electrical interface is constituted by the L_a and L_b pads used for the antenna connection. More information is given in the confidential Security Target [9].
- The RF interface (radio frequency power and signal interface) enables contactless communication between a PICC (proximity integration chip card, PICC) and a PCD reader/writer (proximity coupling device, PCD). Power supply is received and data are received or transmitted by an antenna which consists of a coil with a few turns directly connected to the IC. Depending on customer orders the contactless interface options are set by means of blocking either at Infineon premises or at the premises of the user.
- The data-oriented I/O interface to the TOE is formed by the I/O pad and by the various RF options.
- The interface to the firmware is constituted by special registers used for hardware configuration and control (Special Function Registers, SFR).
- The interface of the TOE to the operating system is constituted on one hand by the RMS routine calls and on the other by the instruction set of the TOE.
- The interface of the TOE to the test routines is formed by the STS test routine call, i.e. entry to test mode (STS-TM entry).
- 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 Toolbox is defined from the Toolbox library interface
- The interface to the SHA-2 calculation is defined from the SHA-2 library interface.
- The interface to the symmetric crypto-operations DES/TDES/AES is defined from the SCL library interface.

Public

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

2.2.4 Guidance documentation

The guidance documentation consists of the listing given in the chapter 1.1. The exact versions of these documents are also given there, as well as the document number referenced here. The documents provide guidance as follows:

- The Hardware Reference Manual HRM [1] is the user data book of the TOE and contains the relevant module, function and feature description.
- The Family Production and Personalization User Manual PPUM [2] contains detailed information about the usage of the Flash Loader.
- The Production and Personalization Mutual Authentication Extension User Manual [36] contains detailed information about the usage of the Mutual Authentication Extension.
- The document Family Programmers Reference Manual PRM [3] describes the usage and interface of the Resource Management System RMS.
- The documents [4] and [37] Asymmetric Cryptographic Library Crypto@2304T contains all interfaces of the RSA, EC and Toolbox library and are only delivered to the user in case the RSA library and/or the EC library is/are part of the delivered TOE.
- The document Secure Hash Algorithm (SHA-2) [5] 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. The security guidelines contain all hints and recommendations for a secure programming of the TOE.
- The document Crypto@2304T User Manual [6] describes the architecture of cryptographic coprocessor on register level. It also provides a functional description of the register architecture, instruction set and gives programming guidance.
- The document Security Guidelines User Manual [7] represents the User Manual for the software programmers.
- The document Errata sheet [8] contains the description of all interfaces of the software to the hardware relevant for programming the TOE. The SLE70 Family Errata Sheet can be changed during the life cycle of the TOE. This is reported in a monthly updated list provided from Infineon Technologies AG to the user.
- The document Advanced Mode for Mifare Technology (AMM) [10] describes how to apply this type of communication. This documentation is provisioned to the user if the AMM option has been ordered and is an addendum to the Hardware Reference Manual HRM [1].
- The document SCL78 Symmetric Crypto Library for SCPv3 DES/AES [33] contains the description of the user interface, general concepts and important security guidelines for software designers.

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.

Public

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 audited as compliant to the Common Criteria scheme.

The delivery can therefore be at the end of phase 3 or at the end of phase 4 which can also include pre-personalization steps according to PP [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 MAE and 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 (and MAE). Note that it depends on the procurement order, whether the MAE and Flash Loader program is present or not.

More information on the forms of delivery of the TOE components is given in the confidential Security Target [9].

2.2.6 Production Sites

The TOE may be handled in different production sites but the silicon of this TOE is produced in one dedicated production site only. To distinguish the different production sites of various products in the field, this production site is coded into the Generic Chip Ident Mode (GCIM) data. The exact coding of the generic chip identification data is given in the confidential Security Target [9].

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 [12], part 2 [13] and part 3 [14].

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 [11].

The Security IC Platform Protection Profile PP [11] with Augmentation Packages is registered and certified by the Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference:

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

The Protection Profile [11] requires the **strict conformance** for the ST claiming conformance to this PP. This is mentioned in section 2.2 of [11].

3.3 Package Claim

This Security Target claims conformance to the following packages from the Security IC Protection Profile with Augmentation Packages [11] and “PP0084: Interpretations” [35] depending on the TOE configuration:

In case the optional Flash loader with MAE functionality is available as well, the ST is

- “Package 1: Loader dedicated for usage in secured environment only” augmented. In this case, the augmentation refers to the Package 1+ as defined in “PP0084: Interpretations” [35] and
- “Authentication of the Security IC” conformant; see [11] section 7.2. Please note that the functionality related to this package is only available as long as the Flash Loader is not permanently blocked.

Note:

This package is optional and fulfilled only by TOE products coming with MAE enhanced Flash Loader. Furthermore, it should be noted that in contrast to the functional package introduced in the PP [11], the availability of the authentication mechanism is not given after locking the Flash Loader. The intended use case of the authentication is to prevent a customer from flashing user data on a non-genuine TOE. No authentication mechanism can be provided after the MAE enhanced Flash Loader is locked.

After locking of the MAE enhanced Flash Loader, the related threats and objectives for the operational environment and

Public

SFRs related to the TOE authentication are regarded as not applicable, due to the fact that it is out of scope of the intended use-case and the authentication functionality is no longer available.

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

- "TDES" augmented; see [11], Section 7.4.1 and
- "AES" conformant; see [11], Section 7.4.2.

Depending on the availability of the optional SCL, the ST is

- "TDES" augmented; see [11], Section 7.4.1 and
- "AES" augmented; see [11], Section 7.4.2.

Furthermore, depending on the availability of the optional SHA-2 library the ST is

- "Hash Functions" conformant; see [11], Section 7.4.3.

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

Furthermore the Security Target is EAL6 augmented (EAL6+) with the component ALC_FLR.1.

The augmentation goes beyond the PP [11] and is achieved – with regard to CCv3.1 Part 3: Security assurance components – as follows:

Table 4 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 [11].

The Protection Profile requires **strict conformance** for the ST claiming conformance to this PP [11]. This is mentioned in chapter 2.2 of [11].

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.

Public

- The IC Dedicated Test Software.
- The IC Dedicated Support Software.
- The associated user's guidance documentation.

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

3.4.1 Security Problem Definition:

Following the PP [11], the security problem definition of this Security Target is enhanced by adding:

- Additional threat (for details refer to chapter 4.1.2).
- Additional organization security policy (for details refer to chapter 4.2.1).
- And additional augmented assumption (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 [11], as the Protection Profile [11] 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 Objective

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 and 5.2). These modifications are necessary due to the additional security functionalities, one coming from the cryptographic libraries (O.Add-Functions), the memory access control (O.Mem-Access) and the MAE and Flash Loader functionality (O.Ctrl_Auth_Loader/Package1+, O.Prot_TSF_Confidentiality).

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.

Furthermore, this Security Target contains an additional security objective for the operational environment due to the MAE and Flash Loader functionality (OE.Loader_Usage/Package1+). The Security Target is still conformant to the PP [12], as the additional security objective for the operational environment neither mitigates a threat meant to be addresseed by a security objective from the TOE in the PP [12], nor fulfils an OSP meant to be addressed by security objectives for the TOE in the PP [12].

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 [11].

Public

The Security Target augments the required assurance package EAL4+ augmented with AVA_VAN.5 and ALC_DVS.2 of the PP [11] to EAL6+ augmented with ALC_FLR.1. Thus the Security Target contains all assurance requirements, respectively hierarchically higher assurance requirements, of the PP [11].

All security functional requirements defined in the PP [11] are included and completely defined in this ST. The augmented security functional requirements are listed in Table 20.

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

- FPT_TST.2 “Subset TOE security testing“ (Requirement from [11])

All assignments and selections of the security functional requirements are either done in the PP [11] or in this Security Target (please refer to section 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 [11] according to “Anwendungshinweise und Interpretationen zum Schema (AIS)” respectively “Functionality classes and evaluation methodology for physical random number generators”, AIS31 [15].

4 Security Problem Definition (ASE_SPD)

The content of the PP [11] applies to this chapter completely.

4.1 Threats

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

The threats to security are defined and described in PP [11] section 3.2.

Table 5: Threats according to PP [11]

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 Loader Package Functionality

The following two threats are taken from the optional “loader package 1+”, as defined in PP interpretation [35] section 2.

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

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

Public

"Loader package 1+", as defined in the PP interpretation [35] requires that the the TOE shall avert the threat "Masquerade the TOE (T.Masquerade_TOE)" as specified below (this threat is taken from Package "Authentication of the Security IC" as defined in PP [11]):

T.Masquerade_TOE	Masquerade the TOE An attacker may threaten the property being a genuine TOE by producing an IC which is not a genuine TOE but wrongly identifying itself as genuine TOE sample.

Table 6: Additional optional threats according to PP [11] and PP interpretation [35]

T.Masquerade_TOE	Masquerade the TOE
T.Open_Samples_Diffusion	Diffusion of open samples

Note:
The threats T.Open_Samples_Diffusion and T.Masquerade_TOE apply only to TOE products coming with activatable MAE and Flash Loader for software or data download by the user. In other cases MAE and Flash Loader are permanently deactivated and the user software or data download is completed. Depending on the capabilities of the user software these threats may then reoccur as subject of the composite TOE.

4.1.2 Additional Threat due to TOE specific Functionality

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

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

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

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

Table 7: Additional threat due to TOE specific functions and augmentations

T.Mem-Access	Memory Access Violation

4.1.3 Assets Regarding the Threats

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

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

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

SC4 is covered by an additional security service provided by this TOE which is the availability of random numbers. These random numbers are generated either by a physical true random number (PTRNG) or a deterministic random number (DRNG) generator or by both, if the true random number output is used as source for the seed input of the deterministic random number generator. Note that the generation of random numbers is a requirement of the PP [11].

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

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

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

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

Public

- photomasks and products in any form

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

For details see PP [11] 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 as defined in PP [11] section 3.3 and stated below covers this aspect.

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

Table 8: Organizational Security Policy according to PP [11]

P.Process-TOE	Identification during TOE Development and Production

Due to the augmentations of PP [11] and the chosen packages additional policies are introduced and described in the next chapter."

4.2.1 Augmented Organizational Security Policy

Due to the augmentations of the PP [11] and the chosen packages additional policies are introduced.

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

The following Organizational Security Policies are derived from the packages of the PP [11]:

The IC Developer / Manufacturer must apply the organizational security policy "Cryptographic services of the TOE (P.Crypto-Service)" ([PP, 7.4]) as specified below:

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

Note:

This TOE can come with both cryptographic coprocessors accessible, or with a blocked SCP or with a blocked Crypto@2304T, or with both cryptographic coprocessors blocked. The blocking depends on the customer demands prior to the production of the hardware. In case the SCP is blocked, no AES and DES computations supported by hardware (neither solely hardware-based nor SCL-based) are possible. Furthermore the cryptographic libraries SCL and SHA-2 are delivery options. In case that the SCL is not delivered, the TOE does not provide the additional SCL-based crypto service AES and TDES. However the solely hardware-based alternative can still be used, if the SCP is available. In case the SHA-2 library is not delivered, the TOE does not provide the additional SHA-2 computations. The use of the SHA-2 library is however possible if both cryptographic 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 IC Developer / Manufacturer must apply the organizational security policy “Limiting and Blocking the Loader Functionality (P.Lim_Block_Loader)” ([PP, 7.3.1]) as specified below:

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

Note:

This policy does apply only if the TOE is delivered with activatable MAE and Flash Loader.

Table 9: Organizational Security Policies according the packages of the PP [11]

P.Crypto-Service	Cryptographic services of the TOE
P.Lim_Block_Loader	Limiting and Blocking the Loader Functionality

Due to the augmentations of the PP [11] the following additional Organizational Security Policy is introduced.

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: • Rivest-Shamir-Adleman Cryptography (RSA) • Elliptic Curve Cryptography (EC)

Note:

This TOE can come with both cryptographic coprocessors accessible, or with a blocked SCP or with a blocked Crypto@2304T, or with both cryptographic coprocessors blocked. The blocking depends on the customer demands prior to the production of the hardware. In case the Crypto@2304T is blocked no RSA or EC computations supported by hardware are possible. Furthermore the cryptographic libraries RSA, EC, 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 both of the cryptographic libraries RSA and EC, the TOE does not provide the Additional Specific Security Functionality Rivest-Shamir-Adleman Cryptography (RSA) and/or Elliptic Curve Cryptography (EC). The Toolbox library is no cryptographic library and provides no additional specific security functionality. If RSA, EC or Toolbox libraries are part of the shipment, the Base Library is automatically included. The Base Library does not provide additional specific functionality.

Table 10: Additional OSP due to TOE specific functions and augmentations

P.Add-Functions	Additional Specific Security Functionality

4.3 Assumptions

The TOE assumptions on the operational environment are defined and described in PP [11] section 3.4.

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

A.Process-Sec-IC	Protection during Packaging, Finishing and Personalization It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

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

Table 11: Assumptions according to PP [11]

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

Public

4.3.1 Augmented Assumptions

Due to the support of cipher schemas an additional assumption needs to be made compared to the PP [11].

Usage of Key-dependent Functions

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

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

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

Table 12: Additional Assumption due to TOE specific functions and augmentations

A.Key-Function	Usage of Key dependent Functions

5 Security Objectives (ASE_OBJ)

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

5.1 Security objectives for the TOE

The security objectives of the TOE are defined and described in PP [11] sections 4.1, 7.3.1, 7.4.1, 7.4.2 and 7.4.3.

Table 13: Objectives for the TOE according to PP [11]

O.Phys-Manipulation	Protection against Physical Manipulation
O.Phys-Probing	Protection against Physical Probing
O.Malfunction	Protection against Malfunction
O.Leak-Inherent	Protection against Inherent Information Leakage
O.Leak-Forced	Protection against Forced Information Leakage
O.Abuse-Func	Protection against Abuse of Functionality
O.Identification	TOE Identification
O.RND	Random Numbers
O.Cap_Avail_Loader	Capability and availability of the Loader (Valid only for TOE derivatives delivered with activatable MAE and Flash Loader)
O.TDES	Cryptographic service Triple-DES
O.AES	Cryptographic service AES
O.SHA	Cryptographic service Hash function
O.Authentication	Authentication to external entities

Public

Note:

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

O.SHA only applies if the TOE is ordered with the optional SHA-2 library.

O.Cap_Avail_Loader and O.Authentication only apply only to TOE products coming with activatable MAE and Flash Loader for software or data download by the user. In other cases MAE and Flash Loader are permanently deactivated and the user software or data download is completed. Depending on the capabilities of the user software these objectives may then reoccur as subject of the composite TOE. Furthermore, it should be noted that in contrast to the functional package introduced in the PP [12], the availability of the authentication mechanism is not given after locking the Flash Loader. The intended use case of the authentication is to prevent a customer from flashing user data on a non-genuine TOE. No authentication mechanism can be provided after the MAE enhanced Flash Loader is locked. After locking of the MAE enhanced Flash Loader, the objective O.Authentication related to the TOE authentication is regarded as not applicable, due to the fact that it is out of scope of the intended use-case and the authentication functionality is no longer available.

The following two security objectives for the TOE are taken from the optional “loader package 1+”, as defined in PP interpretation [35] section 3.

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

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

The TOE shall meet “Access control and authenticity for the Loader (O.Ctrl_Auth_Loader/Package1+)” as specified below:

O.Ctrl_Auth_Loader/Package1+	Access control and authenticity for the Loader The TSF provides communication channel with authorized user, supports authentication of the user data to be loaded and access control for usage of the Loader functionality.

Table 14: Additional objectives for the TOE according to PP interpretation [35]

O.Prot_TSF_Confidentiality	Protection of the confidentiality of the TSF
O.Ctrl_Auth_Loader/Package1+	Access control and authenticity for the Loader

Note:

The objectives O.Prot_TSF_Confidentiality and O.Ctrl_Auth_Loader/Package1+ apply only to TOE products coming with activatable MAE and Flash Loader for software or data download by the user. In other cases MAE and Flash Loader are permanently deactivated and the user software or data download is completed. Depending on the capabilities of the user software these objectives may then reoccur as subject of the composite TOE.

Public

The objectives O.TDES and O.AES apply only to TOEs coming with accessible symmetric cryptographic coprocessor (SCP). The objective O.SHA only applies, if the optional SHA-2 library is ordered. The use of the SHA-2 library is also possible if both cryptographic coprocessors are blocked.

The TOE provides the following additional Security Objectives compared to the PP [11].

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: • Rivest-Shamir-Adleman Cryptography (RSA) • Elliptic Curve Cryptography (EC)

Note:

The cryptographic libraries RSA, EC 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 both of the cryptographic libraries RSA and EC the TOE does not provide the Additional Specific Security Functionality Rivest-Shamir-Adleman Cryptography (RSA) and/or Elliptic Curve Cryptography (EC). The Toolbox and Base Library are no cryptographic libraries and provide no additional specific security functionality.

Note:

This TOE can come with both cryptographic coprocessors accessible, or with a blocked SCP or with a blocked Crypto@2304T, or with both cryptographic coprocessors blocked. The blocking depends on the customer demands prior to the production of the hardware. In case the Crypto@2304T is blocked, no RSA and EC computation supported by hardware is possible. No accessibility of the deselected cryptographic coprocessors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic coprocessors.

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 15: Additional Security 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 are defined in PP [11] section 4.2 and 4.3.

The operational environment of the TOE shall provide "Limitation of capability and blocking the Loader (OE.Lim_Block_Loader)" as specified below (this objective is taken from PP [11], Package "Loader", Package 1):

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

The operational environment of the TOE shall provide "Secure usage of the Loader (OE.Loader_Usage/Package1+)" as specified below (this objective is taken from PP interpretation [35], "loader package 1+" definition):

OE.Loader_Usage/Package1+	Secure usage of the Loader The authorized user must fulfil the access conditions required by the Loader.

The operational environment of the TOE shall provide "External entities authenticating of the TOE (OE.TOE_Auth)" as specified below (this objective is taken from PP [11], Package "Authentication of the Security IC"):

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

Note:

The objectives OE.Lim_Block_Loader, OE.Loader_Usage/Package1+ and OE.TOE_Auth for the development and operation environment apply only to TOE products coming with activatable MAE and Flash Loader for software or data download by the user. In other cases MAE and Flash Loader are permanently deactivated and the user software or data download is completed. Depending on the capabilities of the user software this objective may then reoccur as subject of the composite TOE.

In case a customer decides to use MAE and Flash Loader, this has to be done in an MSSR-audited environment. This has to be considered in a composite evaluation.

The table below lists the security objectives for the operational and development environment.

Table 16: Security objectives for the environment according to PP [11]

Phase 1	OE.Resp-Appl	Treatment of User data of the Composite TOE
Phase 5 – 6 optional Phase 4	OE.Process-Sec-IC	Protection during composite product manufacturing
Phase 5 – 6 optional Phase 4	OE.Lim_Block_Loader	Limitation of capability and blocking the loader (Valid only for TOE derivatives delivered with activatable MAE and Flash Loader.)
Phase 5 – 6 optional Phase 4	OE.TOE_Auth	External entities authenticating of the TOE (Valid only for TOE derivatives delivered with activatable MAE and Flash Loader.)

Table 17: Security objectives for the environment according to PP interpretation [35]

Phase 5 – 6 optional Phase 4	OE.Loader_Usage/ Package1+	Secure usage of the Loader (Valid only for TOE derivatives delivered with activatable MAE and Flash Loader. Covers the usage part (not the secure communication) of OE.Loader_Usage as defined in Package “Loader”, Package 2 from PP [11].)

5.2.1 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.

5.2.2 Clarification of “Treatment of user data of the composite TOE (OE.Resp-Appl)”

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

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

Regarding the memory, software and firmware protection and the SFR and peripheral access rights handling these objectives of the environment have to be clarified. The treatment of user data of the Composite TOE is also required when a multi-application operating system is implemented as a part of the Smartcard Embedded Software on the TOE. In

this case the multi-application operating system should not disclose security relevant user data of one application to another application when it is processed or stored on the TOE.

5.3 Security Objectives Rationale

The security objectives rationale of the TOE are defined and described in PP [11] section 4.4. For the additional objectives of this ST a rationale is provided below.

Table 18: Security Objective Rationale

Assumption, Threat or Organizational Security Policy	Security Objective
P.Add-Functions	O.Add-Functions
A.Key-Function	OE.Resp-Appl
T.Mem-Access	O.Mem-Access
P.Crypto-Service	O.TDES
	O.AES
	O.SHA
P.Lim_Block_Loader	O.Cap_Avail_Loader
	OE.Lim_Block_Loader
T.Open_Samples_Diffusion	O.Prot_TSF_Confidentiality
	O.Ctrl_Auth_Loader/Package1+
	OE.Loader_Usage/Package1+
T.Masquerade_TOE	O.Authentication
	OE.TOE_Auth

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; thus 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 of the composite TOE or TSF data) in general. User data of the composite TOE are also processed by the specific security functionality required by P.Add-Functions.

Public

Compared to the PP [11] a further clarification has been made for the security objective “Treatment of user data of the Composite TOE (OE.Resp-Appl)”: By definition cipher or plain text data and cryptographic keys are user data of the Composite TOE. So, the Smartcard Embedded Software will protect such data if required and use keys and functions appropriately in order to ensure the strength of cryptographic operation. The user has appropriate means to generate a key in a safe environment and import it to the TOE. Quality and confidentiality must be maintained for keys that are imported and/or derived from other keys. This implies that appropriate key management has to be realized in the environment. That is expressed by the assumption A.Key-Function which is covered from OE.Resp-Appl. 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 [11] an enhancement regarding memory area protection has been established. The clear definition of privilege levels for operated software establishes the clear separation of different restricted memory areas for running the firmware, downloading and/or running the operating system and to establish a clear separation between different applications. Nevertheless, it is also possible to define a shared memory section where separated applications may exchange defined data. The privilege levels clearly define by using a hierarchical model the access right from one level to the other. These measures ensure that the threat T.Mem-Access is clearly covered by the security objective O.Mem-Access.

The PP [11] chapter 7.3.1 considers the life cycle phases of the TOE also with the organizational policy P.Lim_Block_Loader as the TOE must be protected against download of hazardous software before the user downloads his software and also after the user has completed his download. This is formalized with the objective O.Cap_Avail_Loader requiring limited capability of the Loader functionality and irreversible termination of the Loader. Both requirements are fulfilled by the Flash Loader due the strong authentication means enabling only the allowed user for the download and due to final locking command to be applied by the user before delivery. As a consequence the operational environment objective OE.Lim_Block_Loader obligates the composite manufacturer to protect the Loader functionality against misuse, limit the capability of the Loader and deactivate irreversibly the Loader after intended usage MAE and Flash Loader provide the required functionality to be applied by the composite manufacturer for covering all the aforementioned objectives.

If the TOE is delivered to the user with MAE and Flash Loader still activatable, according to PP interpretation [35] chapter 3 additionally the threats T.Open_Samples_Diffusion and T.Masquerade_TOE apply. To counter these, according to PP interpretation [35] security objectives for the TOE O.Prot_TSF_Confidentiality and O.Ctrl_Auth_Loader/Package1+ and the security objective for the environment OE.Loader_Usage/Package1+ shall be met. Furthermore, T.Masquerade_TOE implies inclusion of the PP Package “Authentication of the Security IC” containing the additional security objective for the TOE O.Authentication and for the environment OE.TOE_Auth. O.Prot_TSF_Confidentiality, O.Ctrl_Auth_Loader/Package1+ and OE.Loader_Usage/Package1+ counter threat T.Open_Samples_Diffusion by ensuring that no confidential information about the TSF can be disclosed by an attacker, by requesting access control and authenticity for the Loader and by requesting the user to fulfil the Loader access conditions. O.Authentication and OE.TOE_Auth in combination are suitable

to counter threat T.Masquerade_TOE by requesting means of the TOE authenticating itself against the environment, and means of the environment to support such authentication of the TOE.

O.Cap_Avail_Loader, OE.Lim_Block_Loader and P.Lim_Block_Loader as discussed in PP [11] chapter 7.3.1 as well as O.Prot_TSF_Confidentiality, O.Ctrl_Auth_Loader/Package1+ and OE.Loader_Usage/Package1+ as defined in PP interpretation [35] chapter 3 apply only to TOE products at the life cycle phase delivery, if these products come with activatable MAE and Flash Loader for software or data download by the user. In other cases MAE and Flash Loader are permanently deactivated and the user software or data download is completed. Depending on the capabilities of the user software these objectives may then reoccur as subject of the composite TOE. However, it should be noted that in contrast to the functional package introduced in the PP [12], the availability of the authentication mechanism is not given after locking the Flash Loader. The intended use case of the authentication is to prevent a customer from flashing user data on a non-genuine TOE. No authentication mechanism can be provided after the MAE enhanced Flash Loader is locked. After locking of the MAE enhanced Flash Loader, the related threats and objectives for the operational environment and SFRs related to the TOE authentication are regarded as not applicable, due to the fact that it is out of scope of the intended use-case and the authentication functionality is no longer available.

The PP [11] includes the organizational security policy P.Crypto-Service Cryptographic services of the TOE in a different extend as it formalizes the objectives O.TDES, O.AES and O.SHA.

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

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

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

For the objective O.SHA a concrete standard reference with an algorithm selection is given the implementation must follow. The implementation complies to the given security functional requirements and the objective O.SHA is met.

The justification of the additional policy and the additional assumption show that they do not contradict to the rationale already given in the PP [11] for the assumptions, policy and threats defined there.

6 Extended Component Definition (ASE_ECD)

The following extended components are defined and described for the TOE:

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

The extended components FCS_RNG, FMT_LIM, FAU_SAS, FIA_API and FDP_SDC are defined and described in PP [12] section 5 and 7.2.2. 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.

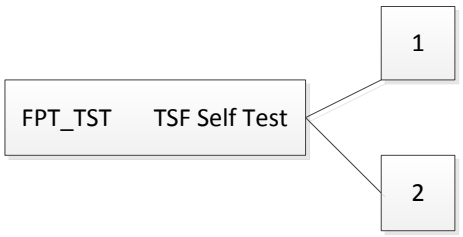
Public

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

6.3 TSF self-test (FPT_TST)

Family Behavior The Family Behavior is defined in [13] section 15.14 (442, 443).

Component leveling



FPT_TST.1: The component FPT_TST.1 is defined in [13] section 15.14 (444, 445, 446).

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

Management: FPT_TST.2

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

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

Audit: FPT_TST.2

There are no auditable events foreseen.

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

7 Security Requirements (ASE_REQ)

For this section, section 6 of the PP [11] 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 [11] section 6.1, 7.2, 7.3.1, 7.4 and in the following description.

Following table provides an overview of the functional security requirements of the TOE, defined in the in PP [11] section 6.1, 7.2, 7.3.1 and 7.4. In the last column it is marked if the requirement is refined. The refinements are also valid for this ST.

Table 19: Security Functional Requirements defined in PP [11]

Security Functional Requirement		Refined y/n or Defined in PP [11]
FRU_FLT.2	“Limited fault tolerance“	Yes
FPT_FLS.1	“Failure with preservation of secure state”	Yes
FMT_LIM.1	“Limited capabilities”	Defined
FMT_LIM.2	“Limited availability”	Defined
FAU_SAS.1	“Audit storage”	Defined
FDP_SDC.1	“Stored data confidentiality”	Defined
FDP_SDI.2	“Stored data integrity monitoring and action”	No
FPT_PHP.3	“Resistance to physical attack”	Yes
FDP_ITT.1	“Basic internal transfer protection”	Yes
FPT_ITT.1	“Basic internal TSF data transfer protection	Yes
FDP_IFC.1	“Subset information flow control”	No
FCS_RNG.1	“Random number generation”	Defined
FMT_LIM.1/Loader	“Limited Capabilities – Loader”	Defined
FMT_LIM.2/Loader	“Limited Availability – Loader”	Defined
FIA_API.1	“Authentication Proof of Identity”	Defined
FCS_COP.1/TDES	“Cryptographic operation – TDES”	No
FCS_CKM.4/TDES	“Cryptographic key destruction – TDES”	No
FCS_COP.1/AES	“Cryptographic operation – AES”	No
FCS_CKM.4/AES	“Cryptographic key destruction – AES”	No

Security Functional Requirement		Refined y/n or Defined in PP [11]
FCS_COP.1/SHA	“Cryptographic operation –SHA”	No

The following table provides an overview about the augmented security functional requirements, which are added to the TOE and are defined in this ST. All requirements are taken from Common Criteria Part 2 [13], with the exception of the requirement FPT_TST.2, which is defined in this ST completely.

Table 20: 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 initialisation”
FMT_SMF.1	“Specification of Management functions”
FDP_SDI.1	“Stored data integrity monitoring”
FCS_COP.1/RSA	“Cryptographic Operation – RSA”
FCS_CKM.1/RSA	“Cryptographic key management – RSA”
FCS_COP.1/ECDSA	“Cryptographic Operation – ECDSA”
FCS_CKM.1/EC	“Cryptographic key management – EC”
FCS_COP.1/ECDH	“Cryptographic Operation – ECDH”
FCS_COP.1/AES_SCL	“Cryptographic operation – AES _SCL”
FCS_CKM.4/AES_SCL	“Cryptographic key destruction – AES_ SCL”
FCS_COP.1/TDES_SCL	“Cryptographic operation – TDES _SCL”
FCS_CKM.4/TDES_SCL	“Cryptographic key destruction – TDES_SCL”
FDP_ACF.1/Loader	“Security attribute based access control – Loader”
FDP_ACC.1/Loader	“Subset access control – Loader”

Note:

The security functional components FMT_LIM.1/Loader, FMT_LIM.2/Loader, FDP_ACC.1/Loader, FDP_ACF.1/Loader and FIA_API.1 listed in the tables above are included to comply with “loader package 1+” as defined in PP interpretation [35] (FMT_LIM.1/Loader and FMT_LIM.2/Loader are defined by PP [12] Package “Loader”, Package 1, whereas FDP_ACC.1/Loader and FDP_ACF.1/Loader are a part of the security functional components as defined in PP [12] Package

Public

"Loader", Package 2. However, as a partial package claim is not permissalbe, they are treated as augmented security functional requirements compared to the PP. Finally FIA_API.1 is defined by PP [12] Package "Authentication of the Security IC").

All assignments and selections of the security functional requirements of the TOE are done in PP [11] and in the following description.

7.1.1 Extended Components FCS_RNG.1 and FAU_SAS.1

7.1.1.1 FCS_RNG

To define the IT security functional requirements of the TOE an additional family (FCS_RNG) of the Class FCS (cryptographic support) is defined in the PP [11]. This family describes the functional requirements for random number generation used for cryptographic purposes.

Please note that the national regulation are outlined in PP [11] chapter 7.5.1 and in AIS31 [15]. These regulations apply for this TOE.

The functional requirement FCS_RNG.1 is defined in the Protection Profile [11] and is completed in this ST according to "AIS31 Anwendungshinweise und Interpretationen zum Schema (AIS)" respectively in English language "A proposal for: Functionality classes for random number generators" [15] as follows.

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 [15]
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 [15] does not distinguish the internal random numbers from output sequences of an ideal RNG.*
	PTG.2.7	*The average Shannon entropy per internal random bit exceeds 0.997.*

Note:
The physical random number generator implements total failure testing of the random source data and a continuous random number generator test according to:
National Institute of Standards and Technology, Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication (FIPS) 140-2 [34], 2002-12-03, chapter 4.9.2.

7.1.1.2 FAU_SAS

The PP [11] defines additional security functional requirements with the family FAU_SAS of the class FAU (Security Audit). This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

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

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

7.1.2 Subset of TOE security 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.

Public

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

FPT_TST.2	Subset TOE security testing
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.2.1	The TSF shall run a suite *of self tests at the request of the authorized user to demonstrate the correct operation of the alarm lines and/or following environmental sensor mechanisms:* *More information is given in the confidential Security Target [9].*

7.1.3 Memory Access Control

Usage of multiple applications in one Smartcard often requires code and data separation in order to prevent that one application can access code and/or data of another application. For this reason the TOE provides Area based Memory Access Control. The underlying memory management unit (MMU) is documented in section 4 in the hardware reference manual HRM [1].

The security service being provided is described in the Security Function Policy (SFP) **Memory Access Control Policy**. The security functional requirement **"Subset access control (FDP_ACC.1)"** requires that this policy is in place and defines the scope were it applies. The security functional requirement **"Security attribute based access control (FDP_ACF.1)"** defines security attribute usage and characteristics of policies. It describes the rules for the function that implements the Security Function Policy (SFP) as identified in FDP_ACC.1. The decision whether an access is permitted or not is taken based upon attributes allocated to the software. The Smartcard Embedded Software defines the attributes and memory areas. The corresponding permission control information is evaluated "on-the-fly" by the hardware so that access is granted/effective or denied/inoperable.

The security functional requirement **"Static attribute initialisation (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.

Public

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. The access rights are controlled by the MMU and related to the privilege level. More details are given in the confidential Security Target [9].

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*.

Public

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 initialisation
FDP_ACF.1.1	The TSF shall enforce the *Memory Access Control Policy* to objects based on the following: *Subject*: *- Software running at the IFX, OS1 and OS2 privilege levels required to securely operate the chip. This includes also privilege levels running interrupt routines.* *- Software running at the privilege levels containing the application software* *Object*: *- Data including code stored in memories* *Attributes*: *- The memory area where the access is performed to and/or* *- The operation to be performed*.
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *evaluate the corresponding permission control information of the relevant memory range before, during or after the access so that accesses to be denied cannot be utilized by the subject attempting to perform the operation*.
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none*.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the *following additional rules: none*.

Public

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

FMT_MSA.3	**Static attribute initialisation**
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the *Memory Access Control Policy* to provide *well defined*[1] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow *any subject, provided that the Memory Access Control Policy is enforced and the necessary access is therefore allowed*[2]*,* to specify alternative initial values to override the default values when an object or information is created.

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

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

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

FMT_SMF.1	**Specification of management functions**
Hierarchical to:	No other components
Dependencies:	No dependencies
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions*: access the configuration registers of the MMU*.

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

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

Public

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)
- Triple Data Encryption Standard (TDES)
- Elliptic Curve Cryptography (EC)
- Rivest-Shamir-Adleman (RSA)[1]
- 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 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. 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.

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 additional specific security functionality

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

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).

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 [32] Section 9, Para.4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bit can no longer be regarded as secure without considering the application context. Therefore, for these functions it shall be checked whether the related cryptographic operations are appropriate for the intended system. Some further hints and guidelines can be derived from the "Technische Richtlinie BSI TR-02102-1", www.bsi.bund.de.

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

Table 21: Cryptographic TOE functionality

Cryptographic Mechanism	Standard of Implementation	Key Size in bit	Security Level above 100 bit
Triple DES	[19]	|k| = 112	No
	proprietary	|k| = 112 Recrypt and BLD Mode	No
	[19], [20]	|k| = 112 in operating modes EBC, CBC, CFB, CTR	No
	[19]	|k| = 168	Yes
	[19], [20]	|k| = 168 in operating modes CBC, CFB, CTR	Yes
	[19], [20]	|k| = 168 in operating mode ECB	No
	proprietary	|k| = 168 Recrypt and BLD Mode	No
AES	[30]	|k| = 128, 192, 256	Yes
	[20], [30]	|k| = 128, 192, 256 in operating modes CBC, CFB, CTR	Yes
	[20], [30]	|k| = 128, 192, 256 in operating mode ECB	No
Physical True RNG PTG.2	[15]	N/A	N/A

Cryptographic Mechanism	Standard of Implementation	Key Size in bit	Security Level above 100 bit
SHA-2 256 and SHA-2 512	[24]	None	None (keyless operation)
RSA encryption / decryption / signature generation / verification (only modular exponentiation part)	[21], [27]	Modulus length = 1976 – 4096	Yes
ECDH	[17], [18], [23], [26], [27]	Key sizes corresponding to the used elliptic curves P-{256, 384, 521}, K-409, B-{283, 409} [17], brainpoolP{256,320,384,512}r1, brainpoolP{256,320,384,512}t1 [18]	Yes
ECDH	[17], [18], [23], [26], [27]	Key sizes corresponding to the used elliptic curves P-{192, 224}, K-{163, 233}, B-233 [17] and brainpoolP{160, 192, 224}r1, brainpoolP{160, 192, 224}t1 [18]	No
ECDSA key generation	[17], [18], [22], [25], [27]	Key sizes corresponding to the used elliptic curves P-{256, 384, 521}, K-409, B-{283, 409} [17], brainpoolP{256,320,384,512}r1, brainpoolP{256,320,384,512}t1 [18]	Yes
ECDSA key generation	[17], [18], [22], [25], [27]	Key sizes corresponding to the used elliptic curves P-{192, 224}, K-{163, 233}, B-233 [17] and brainpoolP{160, 192, 224}r1, brainpoolP{160, 192, 224}t1 [18]	No
ECDSA signature generation / verification	[17], [18], [22], [25], [27]	Key sizes corresponding to the used elliptic curves P-{256, 384, 521}, K-409, B-{283, 409} [17], brainpoolP{256,320,384,512}r1, brainpoolP{256,320,384,512}t1 [18])	Yes
ECDSA signature generation / verification	[17], [18], [22], [25], [27]	Key sizes corresponding to the used elliptic curves P-{192, 224}, K-{163, 233}, B-233 [17] and brainpoolP{160, 192, 224}r1, brainpoolP{160, 192, 224}t1 [18]	No

Public

7.1.4.2 Triple-DES Operation

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

FCS_COP.1/TDES	Cryptographic operation – TDES
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/TDES	The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm TDES in the *Electronic Codebook Mode (ECB), in the Cipher Block Chaining Mode (CBC), in the Blinding Feedback Mode (BLD), and in the Recrypt Mode* and cryptographic key sizes of *112 bit and 168* bit that meet the following standards: • *TDES:* *National Institute of Standards and Technology (NIST) SP 800-67 Rev. 1 [19]* • *ECB, CBC:* *National Institute of Standards and Technology (NIST) SP 800-38A [20]* • *Recrypt and BLD Mode:* *Proprietary, description given in the hardware reference manual HRM [1]*

Note:

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

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

Note:

This SFR applies to the solely hardware-based TDES and is not applicable if the TOE is delivered with a blocked SCP. The key destruction can be done by overwriting the key register interfaces or by software reset of the SCP which provides immediate zeroing of all SCP key registers.

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 generation] 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 *TDES in the Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB) and Counter (CTR) Modes* and with cryptographic key sizes of *112 bit and 168 bit* that meet the following standards: • *TDES:* *National Institute of Standards and Technology (NIST) SP 800-67 Rev. 1 [19]* • *ECB, CBC, CFB, CTR:* *National Institute of Standards and Technology (NIST) SP 800-38A [20]*

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 SCP or without SCL. Please consider the statement of chapter 7.1.4.1.

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.4.1/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 requirements “Cryptographic operation (FCS_COP.1)” and “Cryptographic key destruction (FCS_CKM.4)” as specified below.

FCS_COP.1/AES	Cryptographic operation – AES
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/AES	The TSF shall perform decryption and encryption in accordance with a specified cryptographic algorithm AES in *ECB mode and CBC mode* and cryptographic key sizes of *128 bit, 192 bit and 256 bit* that meet the following standards: • *National Institute of Standards and Technology (NIST) SP 800-38A [20]* • *FIPS 197 [30]*

Note:

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

FCS_CKM.4/AES	Cryptographic key destruction – AES
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_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 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 *decryption and encryption* 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, 192 bit and 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 [30]* • *Block Cipher Modes: ECB, CBC, CTR, CFB* *National Institute of Standards and Technology (NIST) SP 800-38A [20]*

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. Please consider the statement of chapter 7.1.4.1.

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_CKM4.1/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.

FCS_COP.1/RSA	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	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:

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*

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.

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	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	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.

Public

7.1.4.6 General Preface regarding Elliptic Curve Cryptography

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 bit, due to national AIS32 regulations by the BSI. Numerous other curve types, being also secure in terms of side channel attacks on this TOE, exist, which the user optionally can add in the composition certification process.

All curves are based on finite field GF(p) with size $p \in \lfloor 2^{41-1};\ 2^{521} \rfloor$ as well as curves based on a finite field GF(2^n) with size $n \in [41-1; 521]$ are supported.

7.1.4.7 Elliptic Curve DSA (ECDSA) Signature Generation and Verification

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

FCS_COP.1/ECDSA	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	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 [22]:*
   - *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 [25]:*
   - *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 [27]:*
   - *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 [22]:*
   - *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 [25]:*
   - *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 [27].*

Note:

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

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)”

FCS_CKM.1/EC	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	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 [22]: 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 [25]* 3. *According to appendix A.16.9 An algorithm for generating EC keys in IEEE Std. 1363-2000 [27]*

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. The following statements hold true for both cryptographic library versions.

FCS_COP.1/ECDH	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	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 [23]* *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 [26] the function enables the operations described in appendix D.6* *3. According to section 7.2.1 ECSVHDP-DP in IEEE Std. 1363:2000 [27]* *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 bit, due to national AIS32 regulations by the BSI. Numerous other curve types, being also secure in terms of side channel attacks on this TOE, exist, which the user optionally can 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.

Public

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 hashing in accordance with a specified cryptographic algorithm *SHA-256 and SHA-512* and cryptographic key sizes *none* that meet the following FIPS: *U.S. Department of Commerce / National Institute of Standards and Technology, Secure Hash Standard (SHS), FIPS 180-4 [24], section 6.2 SHA-256 and section 6.4 SHA-512.*

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 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. 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 [5].

7.1.5 Data Integrity

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

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

Public

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

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

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

FDP_SDC.1	Stored data confidentiality
Hierarchical to:	No other components
Dependencies:	No dependencies
FDP_SDC.1	The TSF shall ensure the confidentiality of the information of the user data while it is stored in the *RAM, ROM, Cache and SOLID FLASH™ NVM.*

7.1.6 Support of MAE and Flash Loader

MAE and Flash Loader together shall fulfil the requirements concerning the generic “Loader” definition as expressed in PP [11] and PP interpretation [35]. The usage of MAE and Flash Loader is only allowed in a secured environment during the production phase.

The TOE shall grant the access to the loader functionality of the MAE enhanced Flash loader only after successful the mutual authentication. Otherwise, access to the Flash loader functions is denied.

Authorised users are allowed to download and program signed Flash images to the Flash memory of the TOE. Furthermore, the Flash loader can be locked permanently. After locking the loader, any access to the Flash loader functionality shall be denied.

Public

The TOE shall meet the requirement "Limited capabilities – Loader (FMT_LIM.1/Loader)" as specified below (this requirement is taken from "Package 1: Loader dedicated for usage in secured environment only" as defined in PP [11] section 7.3.1):

FMT_LIM.1/Loader	Limited capabilities – Loader
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability.
FMT_LIM.1.1/Loader	The TSF shall be designed and implemented in a manner that limits its capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: Deploying Loader functionality after permanent deactivation does not allow stored user data to be disclosed or manipulated by unauthorized user.

The TOE shall meet the requirement "Limited availability – Loader (FMT_LIM.2/Loader)" as specified below (this requirement is taken from Package "Loader", Package 1 as defined in PP [11] section 7.3.1):

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

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

FDP_ACC.1/Loader	Subset access control – Loader
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control.
FDP_ACC.1.1/Loader	The TSF shall enforce the Loader SFP on 1. the subjects *Authenticated User with the necessary access rights*, 2. the objects *Flash memory*, 3. the operation deployment of Loader

Public

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

FDP_ACF.1/Loader	Security attribute based access control – Loader
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/Loader	The TSF shall enforce the Loader SFP to objects based on the following: (1) the subjects *authenticated Users with the necessary access rights* with security attributes: *none* (2) the objects *Flash memory* with security attributes: *Flash Image with Signature*.
FDP_ACF.1.2/Loader	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *The Authenticated User with the necessary access rights is allowed to Download and Program a Flash Image that is presented with a correct Signature to the Flash memory*..
FDP_ACF.1.3/Loader	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*.
FDP_ACF.1.4/Loader	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *See definition of SFR FMT_LIM.2/Loader*.

The TOE shall meet the requirement “Authentication Proof of Identity (FIA_API.1)” as specified below (this requirement is taken from Package “Authentication of the Security IC” as defined in PP [11] section 7.2):

FIA_API.1	Authentication Proof of Identity
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide the *authentication mechanism of MAE* to prove the identity of the *TOE* to an external entity.

Note:

The security functional requirements FMT_LIM.1/Loader, FMT_LIM.2/Loader, FDP_ACC.1/Loader, FDP_ACF.1/Loader and FIA_API.1 apply only to TOE products coming with activatable MAE and Flash Loader for software or data download by the user. In other cases MAE and Flash Loader are permanently deactivated and the user software or data download is completed. Depending on the capabilities of the user software these security functional requirements may then reoccur as subject of the composite TOE.

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 [11] is expressed with bold letters.

Table 22: Assurance Components

Aspect	Acronym	Description	Refinement
Development	ADV_ARC.1	Security Architecture Description	In PP [11]
	ADV_FSP.5	**Complete semi-formal functional specification with additional error information**	in ST
	ADV_IMP.2	**Complete mapping of the implementation representation of the TSF**	in ST
	ADV_INT.3	**Minimally complex internals**	
	ADV_TDS.5	**Complete semi-formal modular design**	
	ADV_SPM.1	**Formal TOE security policy model**	
Guidance Documents	AGD_OPE.1	Operational user guidance	in PP [11]
	AGD_PRE.1	Preparative procedures	in PP [11]
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 [11]
	ALC_DVS.2	Sufficiency of security measures	in PP [11]
	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	

Public

Aspect	Acronym	Description	Refinement
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 [11]

7.2.1 Refinements

Some refinements are taken unchanged from the PP [11]. 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 [11] have to be discussed here in the Security Target, as the assurance level is increased. The refinements from the PP [11] are included in the chosen assurance level EAL 6 augmented with ALC_FLR.1.

7.2.1.1 Development (ADV)

ADV_IMP Implementation Representation:

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

The covered higher assurance component ADV_IMP.2 requires a complete and not curtailed mapping of the implementation representation of the TSF, and the mapping of the design description to the entire implementation representation. In addition, the correspondence of design description and the implementation representation shall be demonstrated. The ADV_IMP.1 aspect and refinement remains therefore valid. The enhancement underlines the refinement in the PP [11] and by that the entirely complete design i.e. not curtailed representation with according mapping was provided, demonstrated and reviewed.

ADV_FSP Functional Specification:

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

These aspects from ADV_FSP.5 are independent from the ADV_FSP.4 refinements from the PP [11] but constitute an enhancement of it. By that the aspects of ADV_FSP.4 and its refinement in the PP [11] apply also here. The assurance and evidence was provided accordingly.

Public

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 component ALC_CMS.5 is therefore an enhancement to ACL_CMS.4 and the package with its refinement in the PP [11] remains valid. The assurance and evidence was provided accordingly.

ALC_CMC Configuration Management Capabilities:

The PP refinement from the assurance component 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 assurance component ALC_CMC.5 Advanced 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 ACL_CMC.4 and therefore the aspects and ACL_CMC.4 refinements in the PP [11] remain valid. The assurance and evidence was provided.

7.2.1.3 Tests (ATE)

ATE_COV Test Coverage:

The PP refined assurance component 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 [11].

Public

This assurance component ATE_COV.2 has been enhanced to ATE_COV.3 to cover the rigorous analysis of coverage. This requires the presence of evidence that exhaustive testing on rigorous entirely all interfaces as documented in the functional specification was conducted. By that ATE_COV.2 and refinements as given in the PP [11] are enhanced by ATE_COV.3 and remain as well. The TSFIs were completely tested according to ATE_COV.3 and the assurance and evidence was provided.

7.2.2 ADV_SPM Formal Security Policy Model

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

ADV_SPM.1	Formal TOE security policy model
Hierarchical to:	No other components
Dependencies:	ADV_FSP.4 Complete function description
ADV_SPM.1.1D	The developer shall provide a formal security policy model for the
	Memory Access Control Policy and the corresponding SFRs • *FDP_ACC.1 Subset Access Control* • *FDP_ACF.1 Security attribute based access control* • *FMT_MSA.1 Management of Security Attributes* • *FMT_MSA.3 Static Attribute Initialisation.*
	Support of MAE and Flash Loader • *FMT_LIM.1/Loader Limited capabilities – Loader* • *FMT_LIM.2/Loader Limited availability – Loader* • *FDP_ACF.1/Loader Subset Access Control – Loader* • *FDP_ACC.1/Loader Security attribute based access control – Loader* • *FIA_API.1 Authentication Proof of Identity*
	Moreover, the following SFRs shall be addressed by the formal security policy model: • *FDP_SDI.1 Stored data integrity monitoring* • *FDP_SDI.2 Stored data integrity monitoring and action* • *FDP_SDC.1 Stored data confidentiality* • *FDP_ITT.1 Basic Internal Transfer Protection* • *FDP_IFC.1 Information Flow Control* • *FPT_ITT.1 Basic internal TSF data transfer protection* • *FPT_PHP.3 Resistance to physical attack*

	• *FPT_FLS.1 Failure with preservation of secure state* • *FRU_FLT.2 Limited fault tolerance* • *FMT_LIM.1 Limited capabilities* • *FMT_LIM.2 Limited availability* • *FAU_SAS.1 Audit storage* • *FMT_SMF.1 Specification of Management Functions*
ADV_SPM.1.2D	For each policy covered by the formal security policy model, the model shall identify the relevant portions of the statement of SFRs that make up that policy.
ADV_SPM.1.3D	The developer shall provide a formal proof of correspondence between the model and any formal functional specification.
ADV_SPM.1.4D	The developer shall provide a demonstration of correspondence between the model and the functional specification.

7.3 Security Requirements Rationale

7.3.1 Rationale for the Security Functional Requirements

The rationale for the security functional requirements is given in the PP [11] chapter 6.3.1 with a mapping of the SFRs to their objectives. The SFRs and rationale for the loader are given in PP [11] chapter 7.3.1 and the rationale for the cryptographic services is given in chapter 7.4.

The additional introduced SFRs are discussed below:

Table 23: Rationale for additional SFRs in the ST

Objective	TOE Security Functional Requirements
O.Add-Functions	FCS_COP.1/RSA „Cryptographic operation – RSA“ FCS_COP.1/ECDSA „Cryptographic operation – ECDSA“ FCS_COP.1/ECDH „Cryptographic operation – ECDH“ FCS_CKM.1/RSA „Cryptographic key generation – RSA“ FCS_CKM.1/EC „Cryptographic key generation – EC“
O.TDES	FCS_COP.1/TDES_SCL “Cryptographic operation – TDES_SCL” FCS_CKM.4/TDES_SCL “Cryptographic key destruction – TDES_SCL”
O.AES	FCS_COP.1/AES_SCL “Cryptographic operation – AES_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“

Public

Objective	TOE Security Functional Requirements
O.Mem-Access	FDP_ACC.1 “Subset access control” FDP_ACF.1 “Security attribute based access control” FMT_MSA.3 “Static attribute initialisation” FMT_MSA.1 “Management of security attributes” FMT_SMF.1 “Specification of Management Functions”
O.Prot_TSF_Confidentiality	FDP_ACC.1/Loader “Subset access control – Loader” FDP_ACF.1/Loader “Security attribute based access control – Loader”
O.Ctrl_Auth_Loader/Package1+	FDP_ACC.1/Loader “Subset access control – Loader” FDP_ACF.1/Loader “Security attribute based access control – Loader”

The table above gives an overview, how the security functional requirements are combined to meet the security objectives. The justification related to the security objective “Additional Specific Security Functionality (O.Add-Functions)” is as follows:

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. FCS_CKM.1/RSA supports the generation of RSA keys, 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, FCS_CKM.1/RSA, and FCS_CKM.1/EC are suitable to meet the security objective.

The justification related to the security objective “Cryptographic service AES (O.AES)” is as follows:

The rationale provided in section 7.4.2 of the PP [11] applies to this objective for the solely hardware based AES. Furthermore, the SCL-SFRs FCS_COP.1/AES_SCL and FCS_CKM.4/AES_SCL are suitable to meet this security objective, as they formalize the cryptographic service introduced by O.AES. Section 7.4 of the PP [11] explicitly mentions that the cryptographic algrotithm may be a more complex combination of hardware and software.

The justification related to the security objective “Cryptographic service Triple-DES (O.TDES)” is as follows:

The rationale provided in section 7.4.1 of the PP [11] applies to this objective for the solely hardware based TDES. Furthermore, the SCL-SFRs FCS_COP.1/TDES_SCL and FCS_CKM.4/TDES_SCL are suitable to meet this security objective, as they formalize the cryptographic service introduced by O.TDES. Section 7.4 of the PP [11] explicitily mentions that the cryptographic algorithm may be a more complex combination of hardware and software.

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

Public

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 Composite TOE accordingly (OE.Resp-Appl). For further details on the dependencies, which have to be achieved by the operational environment, please refer to section 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 TDES and AES are provided by the environment. Keys for RSA and EC algorithms can be provided either by the TOE or the environment.

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

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

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

The security functional requirement FPT_TST.2 will detect attempts to conduce a physical manipulation on the monitoring functions of the TOE. The objective of FPT_TST.2 is O.Phys-Manipulation. The physical manipulation will be tried to overcome security enforcing functions.

Public

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. The ECC mechanism protects the TOE from the use of corrupt data. The security reset performs an action to prevent the TOE to operate with manipulated data. Therefore FDP_SDI.2 is suitable to meet the security objective O.Phys-Manipulation.

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

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

The justification of the security objective and the additional requirements show that they do not contradict to the rationale already given in the PP for the assumptions, policy and threats defined there. Moreover, these additional security functional requirements cover the requirements by CC [13] user data protection of chapter 11 which are not refined by the PP [11].

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 justification related to the security objective “Capabillity and availability of the Loader (O.Cap_Avail_Loader)” is as follows:

The objective O.Cap_Avail_Loader requires limited capabilities of the Loader functionality and irreversible termination of the Loader. First, this is covered by the functional requirement FMT_LIM.1/Loader, which implements protection against data manipulation and disclosure by unauthorized users after permanent deactivation of the Flash Loader. Second, the functional requirement FMT_LIM.2/Loader limits the Flash Loader availability after the download has been finished by the user. The Flash Loader provides a final locking command, which permanently deactivates the Flash Loader availability. This command execution must be applied after user has finalized his download. As the functional requirements are met by the Flash Loader the objective is covered.

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

Public

The objective O.Prot_TSF_Confidentiality requests that the TOE must be protected against disclosure of confidential operations by the use of dedicated code loaded on open samples. This is covered by FDP_ACC.1/Loader and FDP_ACF.1/Loader defining an access control policy that restricts code loading to authorized users and only authentic (i.e. signed) code.

The justification related to the security objective "Access control and authenticity of the Loader (O.Ctrl_Auth_Loader/Package1+)" is as follows:

The objective O.Ctrl_Auth_Loader/Package1+ requests that the loader functionality can only be used by an authorized user, that only authentic data can be loaded and that an access control shall be in place to control the usage of the loader. This is covered by FDP_ACC.1/Loader and FDP_ACF.1/Loader defining a corresponding access control policy: only authenticated users can download a Flash Image, and only Flash Images presented with a correct Flash Image Signature are accepted for download.

The justification related to the security objective "Authentication to external entities (O.Authentication)" is as follows:

The objective O.Authentication requests that the TOE provides a means to authenticate itself against the environment, to prevent masquerading of the TOE. This is directly covered by FIA_API.1 requiring such an authentication capability of the TOE.

The above named objective O.Cap_Avail_Loader O.Prot_TSF_Confidentiality, O.Ctrl_Auth_Loader/Package1+ and O.Authentication, as well as the corresponding the security functional requirements apply only to TOE products coming with activatable MAE and Flash Loader for software or data download by the user. In other cases MAE and Flash Loader are permanently deactivated and the user software or data download is completed. Depending on the capabilities of the user software these security functional requirements may then reoccur as subject of the composite TOE.

The presence of true random numbers is the security goal 4 (SG4) which is formalized in the objective O.RND Random Numbers. This objective must be covered by fulfillment of the security functional requirement FCS_RNG. This is defined in the PP [11] chapter 5.1. The requirement implements a quality metric, which is defined by national regulations. The implemented random number generation fulfills the definitions of ASI31 [14] in the quality classes as outlined in chapter 7.1.1.1. Therefore the SFR FCS_RNG and the objective O.RND are covered.

The additional SFRs (FCS_COP.1/TDES_SCL, FCS_COP.1/AES_SCL, FCS_CKM.4/TDES_SCL and FCS_CKM.4/AES_SCL), introduced due to the optional symmetric cryptographic library (SCL), only apply if the TOE is delivered with the optional library SCL. In order to use the SCL, the SCP has to be available

7.3.1.1 Dependencies of Security Functional Requirements

The dependence of security functional requirements are defined and described in PP [11] section 6.3.2 for the following security functional requirements:

FDP_ITT.1	FDP_IFC.1	FPT_ITT.1	FPT_PHP.3	FPT_FLS.1
FRU_FLT.2	FMT_LIM.1	FMT_LIM.2	FCS_RNG.1	FAU_SAS.1
FDP_SDI.2	FDP_SDC.1			

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

Table 24: Dependencies for the additional Security Functional Requirements

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FCS_COP.1/RSA	FCS_CKM.4	Yes, see comment 2
	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM1]	Yes, FCS_CKM.1/RSA.
FCS_CKM.1/RSA	[FCS_CKM.2 or FCS_COP.1]	Yes, FCS_COP.1/RSA
	FCS_CKM.4	Yes, see comment 2
FCS_COP.1/ECDSA	FCS_CKM.4	Yes, see comment 2
	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM1]	Yes, FCS_CKM.1/EC.
FCS_CKM.1/EC	[FCS_CKM.2 or FCS_COP.1]	Yes, FCS_COP.1/ECDSA and FCS_COP.1/ECDH
	FCS_CKM.4	Yes, see comment 2
FCS_COP.1/ECDH	FCS_CKM.4	Yes, see comment 2
	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM1]	Yes, FCS_CKM.1/EC.
FCS_COP.1/SHA	No dependencies, see comment 3	N/A, see comment 3
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 2
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 2
FCS_CKM.4/TDES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, see comment 2
FCS_CKM.4/TDES_SCL	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, see comment 2
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 2
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 2
FCS_CKM.4/AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, see comment 2
FCS_CKM.4/AES_SCL	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, see comment 2
FPT_TST.2	No dependencies	N/A

Public

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FDP_ACC.1	FDP_ACF.1	Yes, FDP_ACF.1
FDP_ACF.1	FMT_MSA.3	Yes, FMT_MSA.3
	FDP_ACC.1	Yes, FDP_ACC.1
FMT_MSA.3	FMT_MSA.1	Yes, FMT_MSA.1
	FMT_SMR.1	Not required, see comment 1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	Yes, FDP_ACC.1
	FMT_SMR.1	Not required, see comment 1
	FMT_SMF.1	Yes
FMT_SMF.1	None	N/A
FDP_SDI.1	None	N/A
FMT_LIM.1/Loader	FMT_LIM.2/Loader	Yes
FMT_LIM.2/Loader	FMT_LIM.1/Loader	Yes
FDP_ACC.1/Loader	FDP_ACF.1/Loader	Yes
FDP_ACF.1/Loader	FDP_ACC.1/Loader	Yes
	FMT_MSA.3	Not required, see comment 4
FIA_API.1	None	N/A

Comment 1:

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

Comment 2:

These requirements all address the appropriate management of cryptographic keys used by the specified cryptographic function and are not part of the PP [11]. 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

Public

[FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2] have to be fulfilled by the environment. This means, that the environment shall generate the symmetric keys (FCS_CKM.1) as defined in [13], section 10.1 or shall import the keys ([FDP_ITC.1 or FDP_ITC.2]) as defined in [13], section 11.7.

For the security functional requirement FCS_COP.1/RSA, FCS_COP.1/ECDSA and FCS_COP.1/ECDH the respective dependencie FCS_CKM.4 has to be fulfilled by the environment. This means, that the environment shall provide the respective key destruction (FCS_CKM.4) as defined in [13], section 10.1.

The TOE does already provide the respective key generation (FCS_CKM.1/EC and FCS_CKM.1/RSA) as defined in7.1.4.5 and 7.1.4.8, however alternatively the environment can implement its own key generation (FCS_CKM.1) as defined in [13], section 10.1 or import keys into the TOE ([FDP_ITC.1 or FDP_ITC.2]), as defined in [13], 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 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).

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 fulfil the corresponding dependencies.

Comment 3

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. Thus the environment is not obligated to meet certain requirements for key management.

Comment 4:

The Loader SFP does not allow to create objects, whose security attributes would have to be initialized. For the security attributes neither default values are provided, nor is it possible to specify alternative initial values for the security attributes during creation of objects or information. Therefore the dependency FMT_MSA.3 is not required.

7.3.2 Rationale of the Assurance Requirements

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

Public

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 [14].

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
- SF_MAE Mutual Authentication Extension

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

8.1 SF_DPM: Device Phase Management

The life cycle of the TOE is split-up in several phases. Chip development and production (phase 2, 3, 4) and final use (phase 4-7) is a rough split-up from TOE point of view. These phases are implemented in the TOE as test mode (phase 3) and user mode (phase 4-7).

In addition, a chip identification mode exists which is active in all phases. The chip identification data (O.Identification) is stored in a not changeable configuration page area and non-volatile memory. In the same area further TOE configuration data is stored. In addition, user initialization data can be stored in the non-volatile memory during the production phase as well. During this first data programming, the TOE is still in the secure environment and in Test Mode.
The covered security functional requirement is FAU_SAS.1 “Audit storage”.
During start-up of the TOE the decision for one of the various operation modes is taken dependent on phase identifiers. The decision of accessing a certain mode is defined as phase entry protection. The phases follow also a defined and protected sequence. The sequence of the phases is protected by means of authentication.
The covered security functional requirements are FMT_LIM.1 ”Limited Capabilities” and FMT_LIM.2 “Limited availability”.
During the production phase (phase 3 and 4) or after the delivery to the user (phase 5 or phase 6), the TOE provides the possibility to download, after a successful authentication process, a user specific encryption key, user code and data into the empty (erased) SOLID FLASH™ NVM area as specified by the associated control information of the Flash Loader software.
In case the user has ordered TOE derivatives without Flash Loader, the software download by the user (phase 5 or phase 6) is permanently deactivated and all user data of the Composite TOE is already stored on the TOE at Infineon premises. In both cases the integrity of the loaded data is checked with a checksum process after the download is completed. 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. If the TOE has been finalized by the user (phase 5 or phase 5) the user is

obligated to lock the Flash Loader which results in a permanent disabling of the Flash Loader. A later reactivation possibility, i.e. after delivery to the end user, is after locking no more given.

The covered security functional requirement are FDP_ACC.1/Loader, FDP_ACF.1/Loader “Security attribute based access control – Loader”, FPT_LIM.1./Loader “Limited capabilities – Loader” and FPT_LIM.2/Loader “Limited availability – Loader”.

The above named functional requirements FPT_LIM.1./Loader “Limited capabilities – Loader” and FPT_LIM.2/Loader “Limited availability – Loader” apply only to TOE products coming with activatable MAE and Flash Loader for software or data download by the user. In other cases MAE and Flash Loader are permanently deactivated and the user software or data download is completed. Depending on the capabilities of the user software these security functional requirements may then reoccur as subject of the composite TOE.

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

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

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

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

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

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

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

8.2 SF_PS: Protection against Snooping

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

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

Public

Data are transferred, handled and computed only encrypted or masked anywhere on the TOE, and also the dual CPU computes entirely masked. Further protection means are described in the confidential Security Target [9].

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

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

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

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

The entire design is kept in a non-standard way to complicate attacks using standard analysis methods to an almost not practical condition. A proprietary CPU implementation with a non-public bus protocol is used which renders analysis very complicated and time consuming. Besides the proprietary structures also the internal timing behavior is proprietary and by this aggravating significantly the analysis in addition. Important parts of the chip are especially designed to counter leakage or side channel attacks like DPA/SPA or EMA/DEMA. Therefore, even the physical data gaining is difficult to perform, since timing and current consumption is almost independent of the dynamically encrypted, respectively masked and/or randomized data.

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

A further protective design method used is secure wiring. All security critical wires have been identified and protected by special routing measures against probing. Additionally, artificial shield lines are implemented and mixed up with normal signal lines required for chip operation, which renders probing attacks with high feasibility to not practical. This provides the so called intelligent implicit active shielding “I^2-shield”.

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

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

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

In contrast to the linear virtual address range the physical SOLID FLASH™ NVM pages are transparently and dynamically scrambled on every page modification. This scrambling is entirely independent from the user software and the MMU. Further information is given in the confidential Security Target [9].

An extra mechanism is implemented to prevent the TOE from single stepping. This mechanism is also subject of on-chip testing.

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

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

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

8.3 SF_PMA: Protection against Modifying Attacks

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

The TOE is equipped with an error detection code (EDC) which covers the memory system of RAM, ROM and SOLID FLASH™ NVM and includes also the MED and MMU. Thus introduced failures can be detected and the appropriate action is taken. In terms of single bit errors in the SOLID FLASH™ NVM, the errors are also automatically corrected. This contributes to FDP_SDI.2 “Stored data integrity monitoring and action” and FRU_FLT.2 “Limited fault tolerance”. In order to prevent accidental bit faults during production in the ROM, over the data stored in ROM an EDC value is calculated (FDP_SDI.1 “Stored data integrity monitoring”).

The error detection and partly correction means protect against physical and provide the appropriate reaction in terms of induced errors and faults. The covered security functional requirements are FRU_FLT.2 “Limited fault tolerance”, FPT_PHP.3 “Resistance to physical attack”, FDP_SDI.1 “Stored data integrity monitoring” and FDP_SDI.2 “Stored data integrity monitoring and action”.

If a user tears the card resulting in a power off situation during a SOLID FLASH™ NVM programming operation or if other perturbation is applied, no data or content loss occurs and the TOE restarts power on. The SOLID FLASH™ NVM tearing-safe write functionality covers FPT_FLS.1 “Failure with preservation of secure state”. The implemented means includes FDP_SDI.1 “Stored data integrity monitoring”. More information is given in the confidential Security Target [9

Public

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

The above mentioned error management in the memories and the tearing protection of the SOLID FLASH™ NVM contribute also to the security functional requirement FRU_FLT.2 “Limited fault tolerance” as induced faults are detected with high probability and the correct operation is continued by taking the appropriate action.
The TOE is protected against fault and modifying attacks. The core provides the functionality of double-computing and e.g. result comparison of all tasks to detect incorrect calculations. The detection of an incorrect calculation is stored and the TOE enters a defined secure state which causes the chip internal reset process.

The implementation of the dual CPU computing on the same data is by this one of the most important security features of this platform. As also the results of both CPU parts are compared at the end, a fault induction of modifying attacks would have to be done on both CPU parts. More information is given in the confidential Security Target [9].

During start up, the STS performs various configurations and subsystem tests. After the STS has finished, the operating system or application can call on chip testing feature. The testing feature checks the variety of alarm sources and security features for correct operation as given in the HRM [1]. This test can also be released actively by the user software during normal chip operation by calling an RMS function. As attempts to modify the security features will be detected by the test, the covered security functional requirement is FPT_TST.2 “Subset TOE security testing“.

In the case that a physical manipulation or a physical probing attack is detected, the processing of the TOE is immediately stopped and the TOE enters a secure state called security reset. By release of a security reset all logic and memory of the coprocessors (SCP and Crypto) immediately reset with their respectful reset values. The stored keys are overwritten with the default reset values and memory data structures are overwritten with random values. The covered security functional requirements are FCS_CKM.4 “Cryptographic key destruction” (all iterations), FPT_FLS.1 “Failure with preservation of secure state”, FPT_PHP.3 “Resistance to physical attack“ and FPT_TST.2 “Subset TOE security testing“.
As physical effects or manipulative attacks may also address the program flow of the user software, a watchdog timer and a check point register are implemented. These features enable the user for checking the correct processing time and the integrity of the program flow of the user software.
Another measure against modifying and perturbation respectively differential fault attacks (DFA) is the implementation of backward calculation in the SCP. By this induced errors are discovered.
The covered security functional requirements are FPT_FLS.1 “Failure with preservation of secure state”, FDP_IFC.1 “Subset information flow control”, FPT_ITT.1 “Basic internal TSF data transfer protection”, FDP_ITT.1 “Basic internal transfer protection”and FPT_PHP.3 “Resistance to physical attack”.
All communication via the busses is in addition protected by a monitored hardware handshake. If the handshake was not successful an alarm can be generated.

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

The virtual memory system and privilege level model are enforced by the MMU. This controls the access rights throughout the TOE. There is a clear differentiation within the privilege levels defined. The covered security functional requirements are FDP_ACC.1 “Subset access control”, FDP_ACF.1 “Security attribute based access control”, FMT_MSA.1 “Management of security attributes”, FMT_MSA.3 “Static attribute initialisation” and FMT_SMF1 “Specification of Management Functions”.

The **SF_PMA** “Protection against Modifying Attacks” covers the security functional requirements FCS_CKM.4 (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_SDC.1, FDP_SDI.1, FDP_SDI.2 and FPT_FLS.1.

8.4 SF_PLA: Protection against Logical Attacks

The memory access control of the TOE uses a memory management unit (MMU) to control the access to the available physical memory by using virtual memory addresses and to segregate the code and data to a privilege level model. The MMU controls the address permissions of up seven privileged levels and gives the software the possibility to define different access rights for the privileged levels 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 initialisation”, FMT_MSA.1 “Management of security attributes” and FMT_SMF.1 “Specification of Management functions”.

The TOE provides the possibility to protect the property rights of user code and data by the encryption of the SOLID FLASH™ NVM areas with a specific key defined by the user. Due to this key management FDP_ACF.1 is fulfilled. In addition, each memory present on the TOE is encrypted using either mask specific or chip individual or even session depending keys, assigned by a complex key management. Induced errors are recognized by the Integrity Guard concept and lead to an alarm with high feasibility. In case of security critical errors a security alarm is generated and the TOE ends up in a secure state. The covered security functional requirements are FPT_PHP.3 “Resistance to physical attack”, FDP_ITT.1 “Basic internal transfer protection”, FPT_ITT.1 “Basic internal TSF data transfer protection”, FDP_IFC.1 “Subset information flow control” and FPT_FLS.1 “Failure with preservation of secure state”.

Beside the access protection and key management, also the use of illegal operation code is detected and will release a security reset. The covered security functional requirements FDP_ITT.1 “Basic internal transfer protection” and FPT_FLS.1 “Failure with preservation of secure state”.

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

8.5 SF_CS: Cryptographic Support

The TOE is equipped with 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, RSA key generation, ECDSA signature generation and verification, ECDH key agreement and EC public key calculation and public key testing.

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 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.

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 Triple DES

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), SP 800-67 [19].

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

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

Public

- Recrypt Mode.

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

National Institute of Standards and Technology (NIST), SP 800-38A [20].

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

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

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

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

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 [19], Revision 1.

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

- Electronic Code-Book (ECB),
- Cipher Block Chaining (CBC),
- Cipher Feedback (CFB),
- Counter (CTR),

defined by “NIST FIPS PUB 800-38” [20] and published in December 2001.

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

Please consider also the statement of chapter 7.1.4.1. Furthermore, this security feature is optional and is only provided if the TOE is ordered with accessible SCP and SCL.

Please note that the PCBC mode, the “*_Sec1”-functions, the single DES operation, as well as the additional Block Cipher Modes, which may be implemented by the generic BCM extension concept 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.

Public

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) with the blocker cipher modes ECB and CBC and cryptographic key sizes of 128 bit or 192 bit or 256 bit that meet the standards:

- National Institute of Standards and Technology (NIST) SP 800-38A [20]
- FIPS 197 [30]

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.

Please consider also the statement of chapter 7.1.4.1.

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

Software-Implemented AES

The SCL AES supports the encryption and decryption in accordance with the specified cryptographic algorithm Advanced Encryption Standard (AES) with the blocker cipher modes ECB, CBC, CTR and CFB and cryptographic key sizes of 128 bit or 192 bit or 256 bit that meet the standards:

- National Institute of Standards and Technology (NIST) SP 800-38A [20]
- FIPS 197 [30]

The TOE implements the following alternative block cipher modes for the user: the ECB, CBC, CTR and CFB block cipher modes, defined by “NIST FIPS PUB 800-38” [20] and published in December 2001.

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

Please consider also the statement of chapter 7.1.4.1. Furthermore, this security feature is optional and is only provided if the TOE is ordered with accessible SCP and SCL.

Please note that the PCBC mode, the “*_Sec1”-functions, the single DES operation, as well as the additional Block Cipher Modes, which may be implemented by the generic BCM extension concept 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

8.5.3.1 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 × 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 × 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 × 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 × 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]:*

Public

- *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.

8.5.3.2 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 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:

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 bit, due to national AIS32 regulations by the BSI. Note that numerous other side channel attack resistant curve types exist, which the user optionally can add in the composition certification process.

All curves are based on finite field GF(p) with size p ∈ $[2^{41-1};\ 2^{521}]$ as well as curves based on a finite field GF(2^n) with size $n \in [41-1; 521]$ are supported.

Public

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 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 and 521 bit that meet the following standard:

FCS_COP.1/ECDSA is covered by:

ECDSA Signature Generation:

1. *According to section "7.3 Signing Process" in ANSI X9.62 – 2005 [22]:*
   - *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 [25]:*
   - *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 [27]:*
   - *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 [22]:*
   - *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 [25]:*
   - *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 [27].*

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

8.5.4.2 Asymmetric Key Generation

The TSF shall generate cryptographic keys in accordance with a specific cryptographic key generation algorithm Elliptic Curve EC specified in ANSI X9.62-2005 [22], ISO/IEC 14888-3 [25] and IEEE Std. 1363-2000 [27] and specified cryptographic key sizes 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bit that meet the following standard:

FCS_CKM.1/EC is covered by:

ECDSA *Key Generation:*

1. According to the appendix A4.3 Elliptic Curve Key Pair Generation in ANSI X9.62 [22]: 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 [25]

3. According to appendix A.16.9 An algorithm for generating EC keys in IEEE Std. 1363-2000 [27]

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

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 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bit that meet the following standard:

FCS_COP.1/ECDH is covered by:

1. According to section 5.4.1 Standard Diffie-Hellman Primitive in ANSI X9.63 [23]
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 [26]
the function enables the operations described in appendix D.6

3. According to section 7.2.1 ECSVHDP-DP in IEEE Std. 1363:2000 [27]
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:

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 requirement is 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 [5].

Nevertheless, following is valid:

The TSF shall perform hash-value calculation of user chosen data in accordance with specified cryptographic algorithm SHA-2 (using no cryptographic key) that meets the following standards:

U.S. Department of Commerce / National Institute of Standards and Technology, Secure Hash Standard (SHS), FIPS PUB 180-4 [24], 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 SCL

The SCL78-SCP-v3 symmetric crypto library is delivered as a binary code and is in this way available for the user software. The API of the SCL includes security functions:

“Cipher_*”	for operations with cipher’s software object
“BCM_* ”	for Block Cipher Mode operations
“CipAlg_AES*_SEC2”	for AES-calculations on Cipher Block
“CipAlg_DES*_SEC2”	for DES/TDES calculations on Cipher Block

For details on the provided security functionality of the SCL please refer to the “software implementation” section of the chapters 8.5.1 and 8.5.2.

8.5.7 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.

Public

The Toolbox does not cover security functional requirements.

8.5.8 Base Library

The Base Library provides the low level interface to the asymmetric cryptographic coprocessor and has no user available interface. The Base Library does not provide any security functionality, implements no security mechanism, and does not provide additional specific security functionality.

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 Base Library does not cover security functional requirements and has no user interface.

8.5.9 PTRNG respectively TRNG

Random data is essential for cryptography as well as for security mechanisms. The TOE is equipped with a physical True Random Number Generator (PTRNG respectively TRNG, FCS_RNG.1). The random data can be used from the Smartcard Embedded Software and is also used from the security features of the TOE, like masking. The PTRNG respectively TRNG implements also self-testing features. The PTRNG respectively TRNG is compliant to the requirements of the functionality class PTG.2 of AIS31, please refer to [15].

The PTRNG covers the security functional requirements FCS_RNG.1, FPT_PHP.3, FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_TST.2 and FPT_FLS.1.

8.5.10 Summary of SF_CS: Cryptographic Support

The **SF_CS** “Cryptographic Support” covers the security functional requirements FCS_COP.1/TDES, FCS_CKM.4/TDES, FCS_COP.1/TDES_SCL, FCS_CKM.4/TDES_SCL, FCS_COP.1/AES, FCS_CKM.4/AES, FCS_COP.1/AES_SCL, FCS_CKM.4/AES_SCL, FCS_COP.1/RSA, FCS_CKM.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.

Public

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 SF_MAE: Mutual Authentication Extension

SF_MAE is an optional security feature, which is only available if the TOE comes with activatable MAE (and Flash Loader). In that case SF_MAE provides a mutual authentication between production equipment and the TOE according to ISO 9798-2 [38], section 6.2.2, “Mechanism 4 — Three pass authentication”. Only if the production equipment was successfully authenticated by an external authenticate command, the Flash Loader is activated to download software to the TOE’s Non Volatile Memory.

Furthermore, SF_MAE contains an internal authenticate command by which the authenticity of a copy of the TOE can be verified.

Once the Flash Loader is permanently deactivated, also SF_MAE is not available anymore.

SF_MAE covers security functional components FDP_ACC.1/Loader “Subset access control – Loader”, FDP_ACF.1/Loader “Security attribute based access control – Loader” and FIA_API.1 “Authentication Proof of Identity”.

8.7 Assignment of Security Functional Requirements to TOE’s Security Functionality

The justification and overview of the mapping between security functional requirements (SFR) and the TOE’s security functionality (SF) is given in sections the sections above. The results are shown in the table below. The security functional requirements are addressed by at least one relating security feature.

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

Table 25: Mapping of SFR and SF

Security Functional Requirement	SF_DPM	SF_PS	SF_PMA	SF_PLA	SF_CS	SF_MAE
FAU_SAS.1	X					
FMT_LIM.1	X					

Security Functional Requirement	SF_DPM	SF_PS	SF_PMA	SF_PLA	SF_CS	SF_MAE
FMT_LIM.2	X					
FMT_LIM.1/Loader	X					
FMT_LIM.2/Loader	X					
FDP_ACC.1	X		X	X		
FDP_ACF.1	X		X	X		
FDP_ACC.1/Loader	X					X
FDP_ACF.1/Loader	X					X
FIA_API.1						X
FPT_PHP.3	X	X	X	X	X	
FDP_ITT.1	X	X	X	X	X	
FDP_SDC.1		X	X			
FDP_SDI.1			X			
FDP_SDI.2			X			
FDP_IFC.1		X	X	X	X	
FMT_MSA.1	X		X	X		
FMT_MSA.3	X		X	X		
FMT_SMF.1	X		X	X		
FRU_FLT.2			X			
FPT_ITT.1	X	X	X	X	X	
FPT_TST.2			X		X	
FPT_FLS.1		X	X	X	X	
FCS_RNG.1					X	
FCS_COP.1/TDES					X	
FCS_CKM.4/TDES			X		X	
FCS_COP.1/AES					X	
FCS_CKM.4/AES			X		X	
FCS_COP.1/TDES_SCL					X	

Security Functional Requirement	SF_DPM	SF_PS	SF_PMA	SF_PLA	SF_CS	SF_MAE
FCS_CKM.4/TDES_SCL			X		X	
FCS_COP.1/AES_SCL					X	
FCS_CKM.4/AES_SCL			X		X	
FCS_COP.1/RSA					X	
FCS_CKM.1/RSA					X	
FCS_COP.1/ECDSA					X	
FCS_COP.1/ECDH					X	
FCS_CKM.1/EC					X	
FCS_COP.1/SHA					X	

8.8 Security Requirements are internally consistent

For this chapter the PP [11] section 6.3.4 can be applied completely.

In addition to the discussion in section 6.3 of PP [11] 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

Public

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 Literature

Ref	Version	As of	Title
[1]	1.1	2015-05-22	M5073 SOLID FLASH™ Controller for Security Applications 16-bit Security Controller Family Hardware Reference Manual
[2]		2015-04-01	SLx 70 Family Production and Personalization User's Manual
[3]	v9.6	2017-07-04	16-bit Controller Family SLE 70 Programmer's Reference Manual
[4]	v2.07.003	2017-05-15	CL70 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox User Interface
[5]		2009-11-06	Chip Card and Security iCs SLx70 Family Secure Hash Algorithm SHA-2 (SHA 256/224, SHA 512/384) (optional)
[6]		2010-03-23	Crypto@2304T User Manual
[7]		2017-08-03	16-bit Security Controller - M5073 Security Guidelines
[8]	3.1	2016-06-21	M5073 SOLID FLASH™ Controller for Security Applications Errata Sheet
[9]	1.7	2017-09-27	Confidential Security Target for this TOE
[10]	1.0	2014-11-04	AMM Advanced Mode for Mifare-Compatible Technology Addendum to M5073 Hardware Reference Manual
[11]	1.0	2014-01-13	Security IC Platform Protection Profile PP-0084 “Security IC Platform Protection Profile with Augmentation Packages”, BSI-CC-PP-0084-2014, available at https://www.bsi.bund.de
[12]	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
[13]	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
[14]	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
[15]	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
[16]	2.9	2013-01	Application of Attack Potential to Smartcard, mandatory technical document, CCDB-2013-05-002, http://www.commoncriteriaportal.org
[17]	FIPS PUB 186-4	2013-09-05	Federal Information Processing Standards Publication, FIPS PUB 186-4, Digital Signature Standard (DSS), U.S. Department of Commerce, National Institute of Standards and Technology (NIST)
[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]	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
[20]	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)

Ref	Version	As of	Title
[21]	PKCS, RFC 3447, v2.1	2002-06-14	PKCS #1: RSA Cryptography Standard, RSA Laboratories
[22]	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
[23]	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
[24]	FIPS PUB 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)
[25]	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
[26]	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
[27]	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.
[30]	FIPS PUB 197	2001-11-26	U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), Advanced Encryption Standard (AES), FIPS PUB 197
[32]	I	2009-08-14	Act on the Federal Office for Information Security (BSI-Gesetz - BSIG), Bundesgesetzblatt I p. 2821.
[33]	v2.02.010	2016-10-14	SCL78 Symmetric Crypto Library for SCPv3 DES / AES User Interface
[34]	FIPS 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
[35]	v3	2016-06-01	Secrétariat général de la défense et de la sécurité nationale, Agence nationale de la sécurité des systèmes d'information, PP0084: Interpretations, Reference PP0084.03
[36]	1.2	2017-07-26	Production and personalization Mutual Authentication Extension for teh SLx 70 family in 90nm
[37]	v2.03.008	2017-05-10	SLE70 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox User Interface
[38]	ISO/IEC 9798-2	2008-12	ISO 9798-2:2008 Information technology -- Security techniques -- Entity authentication -- Part 2: Mechanisms using symmetric encipherment algorithms; Third edition 2008-12-15

10 Appendix

Following tables document the hash signatures of the respective optional software and the separate firmware components. For convenience purpose several hash algorithms were used.

Table 26: References of Hash Values of the optional Cryptographic Libraries

RSA, EC, Toolbox, Base v2.03.008

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

MD5=00503528859c293140fe231265c1cdba

SHA1=7723660ac9222527f429c94ce015dac1ab2a2ffb

SHA256=77d5f9f0d03e38d7c0d0a3b33a9ae6bf2192748573e01fcad29a418998dad724

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

MD5=b189b6ecb0435c91797e8b9bdce7edd8

SHA1=b94a7a3a4af019febeb3236fff54f1bc36af2c8b

SHA256=aaec91f8b273efd3a7510be5cf2e2d825e01be9e2d9caf7c5dc595bd79c4b870

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

MD5=4820f7af7ead4b76b53ec9498505c715

SHA1=d1c8df9a2b9b29ae7395a3ab0bf13a965a0957d2

SHA256=eba3ba1c33cf91880ee6c838674cda16f1eec7f536c55034217a6f958874c130

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

MD5=0d18984da350fae0b08099fa8ce60541

SHA1=3d2dc9c74f992f18883ae3b1f498b9dac460f309

SHA256=6ec924a46a729df061826f45abb1fd8a9f3aeb54e745be5e7ca69e665dc6f944

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

Public

MD5=eda224cea852510b37dea323719362d8

SHA1=1d861a3b26a8000b80e727b8c98fd6a1172ece91

SHA256=b03c32463922bb2d4312bf8c62e747cd48f0752dbea90129042fdefac36bf092

MAE V8.00.006

MD5=DBA314EB768CD4E68A694C67B1EFBBBD

SHA1=190DB81AF952351097939FCB93BFBC0CD3063347

SHA256=71B5490B18046DB5B553CEC9D828378BBB8855F75164990AA7BA7DAACA5A8C66

RSA, EC, Toolbox, Base v2.07.003

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

MD5=36d8c2e204caa609acedb4df585263b9

SHA1=23b30bb98f5e81b0f9527960b8d19e6ae97bf586

SHA256=49fdd52525e455cddf92e88057f6698e8bffc1519f6b95a0f720dd082ea625e8

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

MD5=74e91c3c5f9fcfa155fd2fb10398fe7d

SHA1=cebbad8684b9fa7356a3e788cd24e390cc1755f0

SHA256=0d01e09e85a8e56406eb41870d03772731c502cd5f899cb76cd2f6c588d92ae6

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

MD5=26c597e6c2bef1eaf7afacab211acfcf

SHA1=7cf440ae4048b2ac0679db3861cbd8240b4362a5

SHA256=003ae92c0b756b28edb60b04ce5f619db3309a177ddafb376d314fa499e9249a

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

MD5=f9f3d6a030473129f8ef229f93bea92c

SHA1=7ea6b473aec909320e5776f62464849f879a56ac

SHA256=1e664e24081d4cc4f19247f62c6295960cf240ce2c85bf74aadb8c7c88d33f0d

Public

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

MD5=8ba54e63d862d05b023d5f78bfb5540c

SHA1=2914692a09b0ab9e650219a6fc1f525b82ddd6d4

SHA256=887f231345428a4c0c94a58dff60d3a3af075b959f55d730d83299e3a4d8deec

SHA-2 Library Version v1.01

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

MD5=70d2df490185b419fb820d597d82d117

SHA1= df15ff79b5f5ab70bbad0ee031953e1877cabd47

SHA256=765fc5d47cf8274833476406b24010a56ebcfd4b0972704ddd27e2d3e3e086f8

SCL Library Version v2.02.010

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

MD5=fda1638129910ae1b67e0eafe46856ff

SHA1=745411582d5f1af4b6f1771e921b1935d57b82a6

SHA256=b758150725a310d4269de566426a70e7114d6af13a25ff712e16144ba1a9b5e4

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

MD5=71400373a23db40fe94424ed2e7bbe04

SHA1=f4c1f11055166000238ef23b4e4841051d1f4983

SHA256=beacd54f096f9967b9223764c6e09189ab743b2009956df187c5dbe8e2ef4d1d

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

MD5=964432c8339a8e3432a5a52a6888e1f8

SHA1=5f104d9ea356d29622d46fb7c0fdecde595a0b7d

SHA256=592c1c0fe7d4dfa5b68b09c6092542cbe3a07bb6fb2c0029b44a8bc4b0bcca48

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
CRT	Chinese Reminder Theorem
DES	Data Encryption Standard
DPA	Differential Power Analysis
DFA	Differential Failure Analysis
DTRNG	Deterministic Random Number Generator
EC	Elliptic Curve Cryptography
ECC	Error Correction Code and Elliptic Curve Cryptography depending on the context
EDC	Error Detection Code
EDU	Error Detection Unit
SOLID FLASH™ NVM	Electrically Erasable and Programmable Read Only Memory
EMA	Electromagnetic analysis
Flash	Infineon® SOLID FLASH™ Memory
IC	Integrated Circuit
ICO	Internal Clock Oscillator
ID	Identification
IMM	Interface Management Module
ITP	Interrupt and Peripheral Event Channel Controller
I/O	Input/Output

Public

IRAM	Internal Random Access Memory
ITSEC	Information Technology Security Evaluation Criteria
M	Mechanism
MED	Memory Encryption and Decryption
MMU	Memory Management Unit
NVM	Non Volatile Memory
O	Objective (for the TOE)
OE	Objective (for the environment)
OS	Operating system
PEC	Peripheral Event Channel
PRNG	Pseudo Random Number Generator
PROM	Programmable Read Only Memory
PTRNG	Physical Random Number Generator
RAM	Random Access Memory
RFI	Radio Frequency Interface
RMS	Resource Management System
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rives-Shamir-Adleman Algorithm
SA	Service Algorithm Minimal
SCL	Symmetric Cryptographic Library
SCP	Symmetric Cryptographic Processor
SF	Security Feature
SFR	Special Function Register, as well as Security Functional Requirement
	The specific meaning is given in the context
SPA	Simple power analysis
STS	Self-Test Software
SW	Software
SWIO	Software controlled Input Output
T	Threat
TM	Test Mode (STS)
TOE	Target of Evaluation

Public

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)
Cyclic Redundancy Check	Process for calculating checksums for error detection
EEPROM or NVM or SOLID FLASH™ NVM	Electrically Erasable and Programmable Read Only Memory, the Non-Volatile Memory (NVM) permitting electrical read and write operations
End User	Person in contact with a TOE who makes use of its operational capability
Firmware	Is software essential to put the chip into operation and provides specific routines for the user software. The firmware is located in the ROM and parts of it in the SOLID FLASH™ NVM
Flash Loader	Software enabling to download software after delivery
Hardware	Physically present part of a functional system (item)
Integrated Circuit	Component comprising several electronic circuits implemented in a highly miniaturized device using semiconductor technology
Internal Random Access Memory	RAM integrated in the CPU
Mechanism	Logic or algorithm which implements a specific security function in hardware or software
Memory Encryption and Decryption	Method of encoding/decoding data transfer between CPU and memory
Memory	Hardware part containing digital information (binary data)
Microprocessor	CPU with peripherals

Public

Mutual Authentication Extension	Implementation allowing to mutually authenticate production equipment and the TOE
Object	Physical or non-physical part of a system which contains information and is acted upon by subjects
Operating System	Software which implements the basic TOE actions necessary to run the user application
Programmable Read Only Memory	Non-volatile memory which can be written once and then only permits read operations
Random Access Memory	Volatile memory which permits write and read operations
Random Number Generator	Hardware part for generating random numbers
Read Only Memory	Non-volatile memory which permits read operations only
Resource Management System	Part of the firmware containing SOLID FLASH™ NVM programming routines, AIS31 test bench etc.
SCP	Symmetric cryptographic coprocessor for symmetric cryptographic operations (TDES, AES).
Self-Test Software	Part of the firmware with routines for controlling the operating state and testing the TOE hardware
Security Function	Part(s) of the TOE used to implement part(s) of the security objectives
Security Target	Description of the intended state for countering threats
Smart Card	Plastic card in credit card format with built-in chip. Other form factors are also possible, i.e. if integrated into mobile devices
Software	Information (non-physical part of the system) which is required to implement functionality in conjunction with the hardware (program code)
Subject	Entity, generally in the form of a person, who performs actions
Target of Evaluation	Product or system which is being subjected to an evaluation
Test Mode	Operational status phase of the TOE in which actions to test the TOE hardware take place
Threat	Action or event that might prejudice security
User Mode	Operational status phase of the TOE in which actions intended for the user takes place

w w w . i n f i n e o n . c o m

Published by Infineon Technologies AG