Public Security Target

Common Criteria v3.1 – EAL6 augmented / EAL6+

IFX_CCI_000007h
IFX_CCI_000009h
IFX_CCI_00000Ah
IFX_CCI_00000Bh
IFX_CCI_000016h
IFX_CCI_000017h
IFX_CCI_000018h

G13

Resistance to attackers with HIGH attack potential

Author: Hans-Ulrich Buchmüller

Revision: 0.4

Table of Contents

1 Security Target Introduction (ASE_INT)

1.1 Security Target and Target of Evaluation Reference

The title of this document is Public Security Target, covering one hardware platform with following Common Criteria Identifiers (CCI)

- IFX_CCI_000007h
- IFX_CCI_000009h
- IFX_CCI_00000Ah
- IFX_CCI_00000Bh
- IFX_CCI_000016h
- IFX_CCI_000017h
- IFX_CCI_000018h

including optional software libraries and dedicated firmware as stated below.

In order to ease the readability of this document the bunch of Common Criteria Identifiers as listed above is shortened and simply expressed with TOE (Target of Evaluation).

This document is formed according to Common Criteria CCv3.1 EAL6 augmented (EAL6+) and comprises the Infineon Technologies AG Security Controller (Integrated Circuit IC) with the above listed Common Criteria Identifiers and with specific IC dedicated firmware and optional software.

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

This confidential Security Target has the revision 0.4 and is dated 2017-08-16.

The Target of Evaluation (TOE) is one Infineon Security Controller represented by the CCIs as listed above and with following optional available software packages:

- RSA2048/4096 v2.06.003,
- EC v2.06.003,
- Toolbox v2.06.003 libraries
- Hardware Support Library (HSL) v01.22.4346

and with specific IC dedicated software (firmware).

The design step of this TOE is G13.

The Security Target is based on the Protection Profile PP-0084 "Security IC Platform Protection Profile with Augmentation Packages" [9] as publicly available for download at https://www.bsi.bund.de and certified under BSI-CC-PP-0084-2014.
The Protection Profile and the Security Target are built in compliance with Common Criteria v3.1.

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

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

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

Table 1 Identification

	Version	Date	Registration
Security Target	0.4	2017-08-16	Covering the CCIs as listed below:
Target of Evaluation			• IFX_CCI_000007h • IFX_CCI_000009h • IFX_CCI_00000Ah • IFX_CCI_00000Bh • IFX_CCI_000016h • IFX_CCI_000017h • IFX_CCI_000018h In the Design Step G13 With FW-Identifier 80.101.07.0 or alternatively with FW-Identifier 80.101.07.1 And following optional SW - libraries: RSA2048 v2.06.003 RSA4096 v2.06.003 EC v2.06.003 Toolbox v2.06.003 HSL v01.22.4346 with belonging user guidance documentation
Protection Profile	1.0	2014-01-13	Security IC Platform Protection Profile with Augmentation Packages BSI-CC-PP-0084-2014
Common Criteria	3.1 Revision 4	2012-September	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCMB-2012-09-001 Part 2: Security functional requirements CCMB-2012-09-002 Part 3: Security Assurance Components CCMB-2012-09-003
User Guidance Documentation Set 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 in this chapter listed set of user guidance documents belongs to the TOE.			

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

The TOE can be identified with the Generic Chip Identification Mode (GCIM). The TOE hardware platform is identified by defined bytes of the GCIM as given in the HRM [1]:

The unique hexadecimal values as stated in the title are:

- IFX_CCI_000007h
- IFX_CCI_000009h
- IFX_CCI_00000Ah
- IFX_CCI_00000Bh
- IFX_CCI_000016h
- IFX_CCI_000017h
- IFX_CCI_000018h

These bytes clearly identify the hardware platform, or, in other words, the therein possible values for the TOE (without prefix IFX_CCI_) represent the equal hardware platform of this TOE. This means that the hardware entirely equals throughout all derivatives and that the differences are achieved by configuration and blocking means only. These values are unique for this hardware platform. This means that these values will not be used in any other platform or product.
The interpretation of the output GCIM data is clearly explained in the user guidance, Hardware Reference Manual HRM [1].
To each of the uncounted possible TOE derivatives an individual clear value is assigned, which is part of the data output of the Generic Chip Identification Mode (GCIM). This number represents the clear derivative number with an individually assigned configuration. By that each single TOE derivative can be clearly identified and differentiated from others by the GCIM output. The interpretation of the output GCIM data is clearly explained in the user guidance, Hardware Reference Manual HRM [1].
The differences between the derivatives are achieved by blocking only and have no impact on the TOEs security policies and related functions. Details are explained in the user guidance hardware reference manual HRM [1]. All product derivatives are identically from module design, layout and footprint.
The TOE product allows for a maximum of configuration possibilities defined by the customer order following the market needs. For example, a TOE product can come in one project with the fully available SOLID FLASH™ NVM[1] or in another project with any other SOLID FLASH™ NVM -size below the physical implementation size, or with a different RAM size. And more, the user has the free choice, whether he needs the symmetric cryptographic co-processor SCP, or the asymmetric cryptographic co-processor Crypto2304T, or both, or none of them. In addition, the user decides, whether the TOE comes with a free combination of software libraries or without any. And, to be even more flexible, various interface options can be chosen as well. To sum up the major selections, the user defines by his order:

- the available memory sizes of the SOLID FLASH™ NVM and RAM
- the availability of the cryptographic coprocessors
- the availability and free combinations of the cryptographic libraries
- the availability of the Flash Loader
- the availability of the HSL
- the availability of various contact based interface options
- the possibility to tailor the product by blocking on his own premises (BPU)

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

[1] SOLID FLASH™ is an Infineon Trade Mark and stands for the Infineon Flash NVM. The abbreviation NVM is short for Non Volatile Memory. The information remains stored even the power has been removed.

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.
The realization of it requires the presence of the Flash Loader software, enhanced with the BPU blocking software part. The presence of the BPU ability defines the customer with his order.
More information is given in the confidential Security Target [8].

If the user decides to use the Flash Loader, regardless whether it is ordered with or without BPU, an additional process option can be ordered which results in an additional status of the Flash Loader. This process is called PIN-Letter and enables for simplified logistics and thereby for faster delivery of the ordered TOE products to the user. The PIN-Letter feature enabling for the PIN-Letter process is an implemented part of the Flash Loader. The resulting logistical acceleration is possible since the PIN-Letter enables for delivery of not user-specific configured, not flashed and not personalized TOE products to the user warehouse.
By delivery the user warehouse gets filled and depending on market demands the user can immediate apply the authentication means of the PIN-letter. If passing, the TOE products become user specific configured and the Flash Loader can be used for this specific user in a second step. More information is given in the confidential Security Target [8].

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

Table 2 Options to implement user software at Infineon production premises

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

For the cases with active Flash Loader on board and whenever the user has finalized his SW-download, respectively the TOE is in the final state and about to be delivered to the end-user, the user is obligated to lock the Flash Loader. This 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.
Note that whenever a TOE comes without active Flash Loader, BPU and PIN-Letter process are not possible.

All in all various delivery combinations are given and for example, a product can come with a fix configuration and with Flash Loader, to enable the user to download software, but without BPU option and with PIN-Letter. The following cases can occur:

Table 3 Options with Flash Loader, BPU and PIN-Letter

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

More information about the possible configuration options is given in the confidential Security Target [8].

Within those limitations the TOE configurations can vary under only one identical IC-hardware, 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.
Note that this TOE has no user available ROM. The user software and data are entirely located in a dedicated and protected part of the SOLID FLASH™ NVM. The long life storage endurance together with the means for error detection and correction serves for excellent reliability and endurance.
In addition to the above listed flexible ranges, the user guidance contains a number of predefined configurations for those customers not making use of the BPU option. All of these configurations belong to the TOE as well and are of course made of the equal hardware and are inside the above declared ranges.
Today's predefined configurations of the TOE are listed in the hardware reference manual HRM [1] and is completed with the list of identification data of the derivatives. 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.

This TOE provides dedicated identification means and outputs the platform identifier, the design step and further configuration information. The hardware reference manual HRM [1] is part of the user guidance and enables for the clear interpretation of the read out
These output data enable the user for clear identification of the TOE and therewith for examination of the validity of the certificate.
In addition, a dedicated RMS function allows reading out the present configuration in detail. The output RMS data together with the hardware reference manual HRM [1] enables for clear identification of a product and its configuration. All these steps for gathering identification and detailed configuration information can be done by the user himself, without involving Infineon Technologies AG.
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.
The firmware consists of:

- the Boot Software (BOS) firmware conducting configuration and testing task (see chapter 2.2.2) at start-up of the TOE
- the Resource Management System (RMS) library providing essential basis functions for the management of the RAM, the branch table, the Memory Management Unit (MMU) and other resources
- the optional Flash Loader enabling for the download of user software to the SOLID FLASH™ NVM and required for the optional Bill per Use (BPU) feature and the PIN-letter feature

The BOS functions are implemented in a separated Test-ROM also being part of the TOE but not available for the user.
The firmware comes with two alternative Firmware-Identifiers. The second and new Firmware-Identifier does not change anything on the TOE except the version number of the Firmware-Identifier. I.e. the entire firmware on the TOE equals entirely for the two Firmware-Identifiers so that it is from user perspective regardless which Firmware-Identifier is chosen. The effective change is on Infineon Technologies production testing only which results by an automatism in this version increase.
The optional software parts are differentiated into the cryptographic libraries RSA[1], EC[2] and the supporting libraries Toolbox and HSL.

[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.

RSA, EC and Toolbox provide certain functionality via an API to the Smartcard Embedded Software. The private parts of the cryptographic libraries are only used internally and have no user interface. If neither the RSA- nor the EC library is delivered, also the belonging private parts are not on board. The Toolbox library does not have private library parts.
The TOE can be delivered including - in free combinations - or not including any of the functionality of the cryptographic libraries EC and RSA. This holds also for the HSL and the Toolbox library.
If the user decides not to use one or all of the cryptographic library(s), the specific library(s) is (are) not delivered to the user and the accompanying "Additional Specific Security Functionality (O.Add-Functions)" Rivest-Shamir-Adleman (RSA) and/ or EC is/are not provided by the TOE.

The RSA, EC and Toolbox libraries can be loaded, together with the Smartcard Embedded software, into the SOLID FLASH™ NVM.

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 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.

Beside the inclusion and support of cryptographic libraries this TOE comes with the optional Hardware Support Library (HSL) significantly simplifying the management of the SOLID FLASH™ NVM functionality. The HSL constitutes an application interface (API) accessing the HSM state machine and abstracting low level properties like special function registers and settings of specific hardware features. In short the HSL provides a user friendly also use case oriented interface considering endurance, reliability and performance. In certain configurations the HSL provides also functions implementing tearing safe behaviour of the SOLID FLASH™ NVM. If used the user has no need to care about cases where the TOE is suddenly cut off the power supply even during managing the SOLID FLASH™ NVM.
Anyhow, the HSL remains as an optional library as even sudden power off situations does never lead to exploitable conditions of the TOE. In the worse the TOE ends operation in case of a faulty programmed SOLID FLASH™ NVM location.
All other Smartcard Embedded Software does not belong to the TOE and is not subject of the evaluation.

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.

1.2 Target of Evaluation overview

The TOE comprises the Infineon Technologies Security Controller TOE with specific IC dedicated software and optional RSA, EC and Toolbox libraries.
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.
This TOE is intended to be used in any application and device requiring the highest level of security, for example as secure element in various devices with various form factors.
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 double 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 upper layers, finally providing the so called intelligent implicit active shielding "I²-shield". This provides physical protection against probing and forcing.
This TOE provides several also freely user programmable contact based interface options for various applications and markets. Due to the interface flexibility the product can be used in almost any application, within any device and almost any form factor.
Again these communication and application independency capabilities enable the usage to almost everywhere, where highly secure applications are in use and of course in any other application as well. This TOE is deemed for governmental, corporate, transport and payment markets, or wherever a secure root of trust is required. Various types of applications can use this TOE, for example in closed loop logical access controls, physical access controls, secure internet access control and internet authentication, or as multi-application token or simply as encrypted storage.

This controller is able to communicate contact based using following communication protocols respectively methods:

- ISO/IEC 7816-3 card
  This is the ISO/IEC defined standard contact based communication protocol, using the UART and the belonging pads.
- Inter Integrated Circuit Interface (I2C)
  The Inter-Integrated Circuit (IIC) module is able to be connected to an external multi-master-serial-bus-system. The IIC protocol software is not part of the TOE.
- General Purpose Input/Output (GPIO)
  The GPIO module supports a number of general purpose I/O signals in parallel and independent of each other. Each of the I/O signals can be configured

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 two CPUs (Central Processing Units), acting as one, the MMU (Memory Management Unit) and the MED (Memory Encryption/Decryption Unit). The Core implements also the Post Failure Detection (PFD) covering CPU, Cache and MED. The two CPUs control each other in order to detect faults and serve by this for data integrity. The TOE implements a full 16 MByte linear addressable memory space for each privilege level, a simple scalable Memory Management concept and a scalable stack size. The flexible memory concept consists of a ROM, RAM and the non-volatile memory (NVM), which we call SOLID FLASH™ NVM. The ROM is not available for the user and contains the main parts of firmware components only.

The firmware is composed out of the Boot-up software (BOS), the Resource Management System (RMS) and the Flash Loader (FL). The BOS applies the essential configuration, internal testing and the start-up. The RMS implements a low level application interface (API) to the Smartcard Embedded Software and provides handling and managing routines for RAM, MMU, Branch table, configuration and further functions. The Flash Loader allows downloading user software to the SOLID FLASH™ NVM during the manufacturing process and also at user premises - if ordered.

This TOE implements a Hybrid Random Number Generator (HDRNG). This HDRNG equals to the expression Hybrid Physical True Random Number Generator (hybrid PTRNG) as defined by the BSI. In the following, the BSI expression hybrid PTRNG is used. The hybrid PTRNG implements a true physical random source and has evidenced its conformance to the classes of AIS31 [13] as declared in chapter 7.1.1.1.
The produced genuine random numbers are available as a security service for the user and are also used for internal purposes. Together with the guidelines in [6] the hybrid PTRNG operates in the following modes of operation and is conformant to the named classes:

- True Random Number Generation, meeting AIS31 PTG.2
- Hybrid Random Number Generation, meeting AIS31 PTG.3

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

The hybrid PTRNG is deemed for any application requiring excellent physical random data entropy.
The two cryptographic co-processors serve the need of modern cryptography: The symmetric co-processor (SCP) combines both AES and DES with one, two or triple-key hardware acceleration.
The Asymmetric Cryptographic Co-processor, called Crypto2304T, provides optimized high performance calculations for the user software executing cryptographic operations and is also used by the optional cryptographic libraries for Rivest-Shamir-Adleman (RSA) and Elliptic Curve (EC) cryptography.

The optional software part of the TOE consists of the cryptographic RSA-, EC-, the supporting Toolbox-, HSL-libraries and Toolbox provide certain functionality via an API to the Smartcard Embedded Software. The private parts of the cryptographic libraries are only used internally and have no user interface. If neither the RSA- nor the EC library is delivered, also the belonging private parts are not on board. The Toolbox does not have private library parts.
The TOE can be delivered including - in free combinations - or not including any of the functionality of the cryptographic libraries EC and RSA. This holds also for the HSL and the Toolbox library.
The RSA library is used to provide a high level interface to the RSA cryptography implemented on the hardware component Crypto2304T and includes countermeasures against fault injection and side channel attacks. The routines are used for the generation of RSA Key Pairs (RsaKeyGen), the RSA signature verification (RsaVerify), the RSA signature generation (RsaSign) and the RSA modulus recalculation (RsaModulus). The hardware Crypto2304T unit provides the basic long number calculations (add, subtract, multiply, square) with high performance. The RSA library is delivered as object code and in this way integrated in the user software. The RSA library can perform RSA operations from 512 to 4096 bits.
Following the national BSI 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 Crypto2304T and includes countermeasures against fault injection and side channel 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 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 Brainpool [16] and NIST [24] Elliptic Curves with key lengths of 224, 233, 256, 283, 320, 384, 409, 512 and 521 Bits. The definition of the key lengths follows the national AIS32 regulation regarding the 100 bit security level by the BSI. The former 80 bit level is achieved by the key lengths of 160, 163, and 192 Bits.
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 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.
Beside the inclusion and support of cryptographic libraries this TOE comes with the optional Hardware Support Library (HSL) significantly simplifying the management of the SOLID FLASH™ NVM functionality. The HSL constitutes an application interface (API) accessing the HSM state machine and abstracting low level properties like special function registers and settings of specific hardware features. In short the HSL provides a user friendly also use case oriented interface considering endurance, reliability and performance. In certain configurations the HSL provides also functions implementing tearing safe behaviour of the SOLID FLASH™ NVM. If used the user has no need to care about cases where the TOE is suddenly cut off the power supply even during managing the

SOLID FLASH™ NVM.
Anyhow, the HSL remains as an optional library as even sudden power off situations does never lead to exploitable conditions of the TOE. In the worse the TOE ends operation in case of a faulty programmed SOLID FLASH™ NVM location due to the Integrity Guard.

Note that this TOE can come with both cryptographic co-processors accessible, or with a blocked SCP or with a blocked Crypto2304T, or with both cryptographic co-processors blocked. The blocking depends on the user's choice. No accessibility of the deselected cryptographic co-processors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic co-processors. 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).
To fulfill the highest security requirements 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. This TOE utilizes digital security features to include customer friendly security, combined with a robust design overcoming the disadvantages on analogue protection technologies. The TOE provides full on-chip encryption covering the complete core, busses, memories and cryptographic co-processors leaving no plain data on the chip. A further security feature has been implemented for this TOE protecting also the involved addresses transferred over the memory bus. Therefore the attractiveness for attackers is a step further 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 critical 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 briefly 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 out of the security functional requirements as part of the security policy and the security assurance requirements. These are the formal steps applied during the evaluation and certification showing that the TOE meets the targeted requirements. In addition, simplified 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 Security IC Platform Protection Profile [9] and are referenced here. These requirements build up a minimal standard common for all Security ICs.
The security functions are defined here in the security target as property of this specific TOE. Here it is shown how this specific TOE fulfils the requirements for the common standard defined in the Common Criteria documents [10], [11], [12] and in the Security IC Platform Protection Profile [9].

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 [9] 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 Security Interface Controllers as an integrated circuit (IC), meeting the highest requirements in terms of performance and security. The TOE products are manufactured by Infineon Technologies AG in 65 nm CMOS-technology. 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 the PP [9].
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, system peripherals, a control block and the peripherals. The following picture provides a simplified overview upon the hardware components of this TOE which are subsequently briefly described:

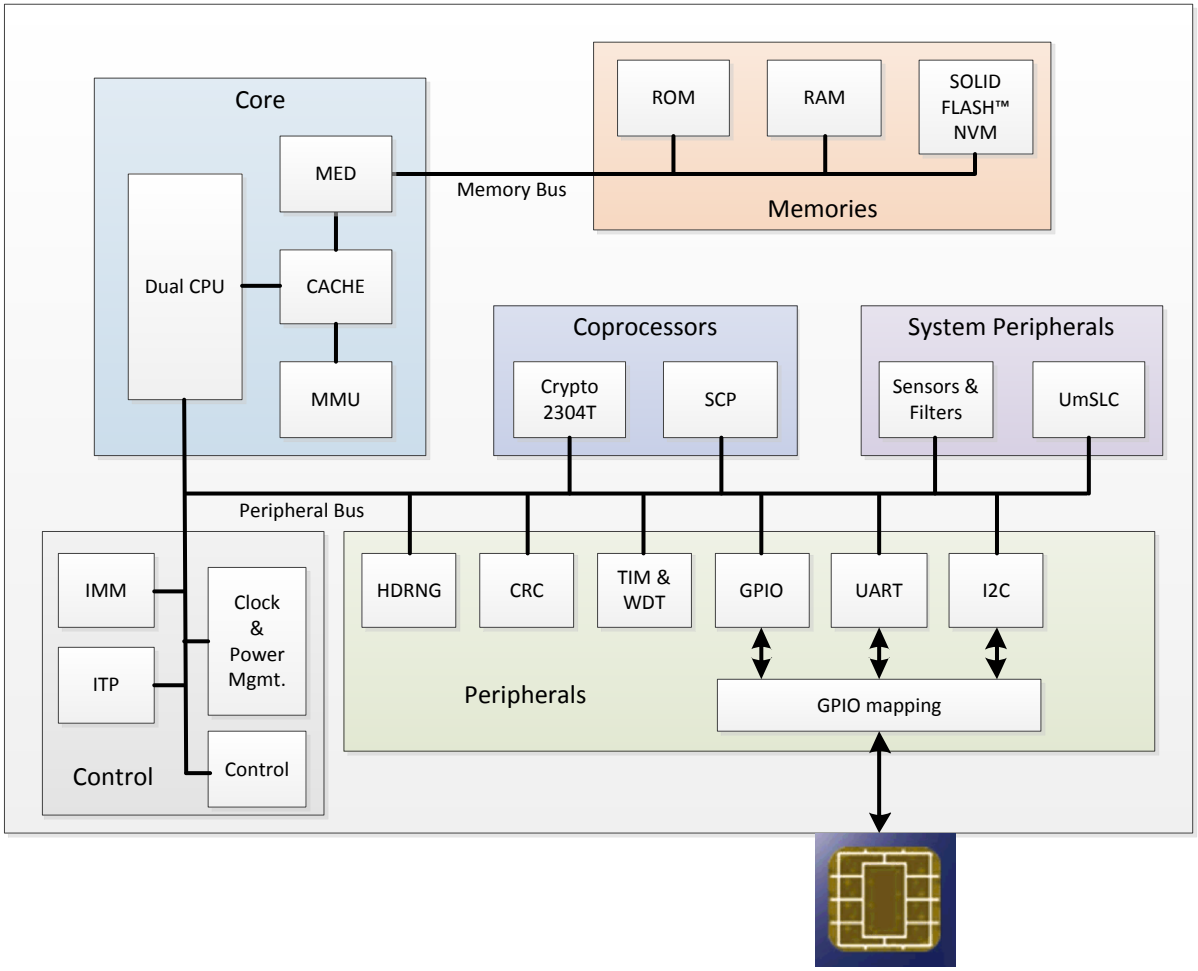


Figure 1 Simplified block diagram of the TOE

Introduction
The main components of the core system are the dual CPU (Central Processing Units), the MMU (Memory Management Unit) and the MED (Memory Encryption/Decryption Unit). The co-processor block contains the cryptographic processors for RSA/EC and DES/AES processing, while the peripheral block contains the random number generation, the module for the Cyclic Redundancy Check (CRC), the timers and watchdogs and last but not least the external interfaces service.
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). All data and addresses transferred over the two bus systems are encrypted respectively masked.

The Core
The dual CPU, constituted out of two CPUs and acting as one from users view, is based on a 16-bit architecture based on the MCS® 251 instruction set with an execution time faster than a standard MCS® 251 at the same clock frequency. The instruction set for the architecture is also largely compatible with the well-known 80251 microcontroller family. Anyhow, the CPU has a special internal architecture and timing that differs from the standard 80251 and it provides additional powerful instructions, meeting the requirements for new operating system generations. Despite its compatibility the CPU implementation is entirely proprietary and not standard.
The CPU accesses the memory via the integrated Memory Encryption and Decryption unit (MED). The Post Failure Detection (PFD) covers the modules CPU, Cache and MED, 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 application to the memories can be controlled with the memory management unit (MMU). Errors in the memories are automatically detected (EDC) and in terms of the SOLID FLASH™ NVM 1-Bit-errors are also corrected (ECC). The two processors 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 full error detection capability for the complete data path, which does not leave any parts of the circuitry unprotected.
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 Busses
The bus system comprises two separate bus entities: a memory bus and peripheral bus for high-speed communication internally between the modules and to the outer world with the peripherals. All transfer of data and addresses via the memory and the peripheral bus systems is protected by means of encryption respectively masking leaving no plain contents anywhere on the chip.

The cryptographic Coprocessors
The TOE implements two cryptographic co-processors: The symmetric cryptographic co-processor (SCP) combines both AES and DES with one, two or triple-key hardware acceleration. The Asymmetric Cryptographic Co-processor, called Crypto2304T, provides optimized high performance calculations for the user software executing cryptographic operations and is also used by the optional cryptographic libraries for RSA and Elliptic Curve (EC) cryptography. These co-processors are especially designed for smart card applications with respect to the security and power consumption. The SCP module computes the complete DES algorithm within a few clock cycles and is especially designed to counter attacks like DPA, EMA and DFA.
Note that this TOE can come with both cryptographic co-processors accessible, or with a blocked SCP or with a blocked Crypto2304T, or with both cryptographic co-processors blocked. The blocking depends on the customer

demands prior to the production of the hardware. No accessibility of the deselected cryptographic co-processors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic co-processors.

The Memories
The BOS (boot-up software), RMS (Resource Management System) 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 (BOS), and also the RMS functions are grouped together in a common privilege level. These privilege levels are protected by a hardwired Memory Management Unit (MMU) setting.
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 user software can be implemented in various options depending on the user's choice and 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.
All content regardless whether stored or transferred remains encrypted and EDC protected. Also the addresses are protected by cryptographic protection means.
The TOE uses also Special Function Registers SFR. These SFR registers are used for general purposes and chip configuration. The start-up register values are stored in the SOLID FLASH™ NVM, in the configuration page area.

The System Peripherals
The system peripheral block serves for operation within the specified ranges and manages the alarms and self-testing. Note that there is a small set of sensors left in order to detect excessive deviations from the specified operational range, while not being over-sensitive. These digital features do not need adjustment or calibration and are deemed to increase the robustness of the chip against environmental influences even more. Conditions that would not be harmful for the operation would therefore in most cases not disturb the proper function.
By implementing the integrity guard concept, the sensors are no more required for the TOE security. The sensors are therefore assigned to be security supporting but do not implement a security mechanism on their own. The only sensor contributing to a security mechanism is the frequency sensor.
After the BOS has finished, the operating system or application can call the User Mode Security Life Control (UMSLC) test. The UMSLC tests several modules, various functions and sensors for correct operation. Some of them have a user configurable interface.

The Control
The Interface Management Module (IMM) handles all interfaces in a unified manner and simplifies by this the variety of interfaces for the user. It provides simultaneous maintenance of a multitude of various interfaces in a non-conflicting manner simultaneously if so configured. The Interrupt and Peripheral Event Channel Controller (ITP) manages individual interrupt requests signaled as events by peripherals. The controller can be associated with different interrupt events enabling to select between executing a standard interrupt service routine or a fast data transfer between memory locations over a so-called peripheral event channel (PEC). The control-block implements a summary of all control interfaces respectively SFRs used by various modules.

The Peripherals
This block implements the various interface options, communication protocols and operation modes as outlined in chapter 1.2.
In addition to the interfaces it implements the Hybrid Random Number Generator (HDRNG). This HDRNG equals to the expression Hybrid Physical True Random Number Generator (hybrid PTRNG) as defined by the BSI. In the following, the BSI expression hybrid PTRNG is used. The hybrid PTRNG implements a true physical random source and has evidenced its conformance to the classes of AIS31 [13] as declared in chapter 7.1.1.1.

The produced genuine random numbers are available as a security service for the user and are also used for internal purposes. Together with the guidelines in [6] the hybrid PTRNG operates in the following modes of operation and is conformant to the named classes:

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

The hybrid PTRNG is deemed for any application requiring excellent physical random data entropy.
Several timer modules are implemented used for example to control the communication via the UART, other interfaces behavior, for asynchronous wake-up and similar timed events.
The timer permits easy implementation of communication protocols such as T=1 and all other time-critical operations. The UART-controlled I/O interface allows the security controller and the terminal interface to be operated independently. The watchdog timers implement a configurable time out for various purposes. More information can be found in the hardware reference manual HRM [1].
The cyclic redundancy check (CRC) module is used to compute a checksum over any input data and allows by that explicit checking integrity of a piece of data.

Feature Summary
The following is a list of central features provided by this TOE:

- 24-bit linear addressing
- Up to 16 MByte of addressable memory
- Data and addresses protected against eavesdropping
- Register-based architecture
  (registers can be accessed as bytes, words (2 bytes), and double words (4 bytes))
- 2-stage instruction pipeline
- Based MCS® 251 instruction set and largely compatible with the well-known 80251 microcontroller family
- Extensive additional set of powerful instructions, including 16- and 32-bit arithmetic and logic instructions
- Cache with single-cycle access searching
- 16-bit self-checking dual CPU
- Hybrid Physical True Random Number Generation for random numbers at highest entropy quality
- Extended Temperature Range

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

2.2 Scope of the TOE

The TOE comprises:

- The silicon die, respectively the Integrated Circuit (IC) respectively the hardware of this TOE.
- The TOE is also delivered in various configurations, achieved by means of blocking by the customer and/or depending on the customer order.
- All according firmware and
- Optional software in various combinations as ordered
- All configurations of any individual TOE product

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. 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. This depends on the user order. 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 listed 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 (see Figure 1) as defined in the hardware reference manual HRM [1] comprises:

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)
Memory Management Unit (MMU)

Memories

Read-Only Memory (ROM), not available for the user
Random Access Memory (RAM)
SOLID FLASH™ NVM, the flash cell based nonvolatile memory

Buses

Memory Bus
Peripheral Bus

Coprocessors

Crypto2304T for asymmetric algorithms like RSA and EC (optionally blocked)
Symmetric Cryptographic Co-processor for DES and AES Standards (optionally blocked)

Control
- Interface Management Module (IMM)
- Interrupt and Peripheral Event Channel Controller (ITP)
- Clock & Power Management
- Control

System Peripherals
- Sensors & Filters
- User mode Security Life Control (UmSLC)

Peripherals
- Hybrid Physical True Random Number Generator (HPTRNG) implementing also a Deterministic Random Number Generator (DRNG)
- Timers and Watchdogs
- Cyclic Redundancy Check module (CRC)
- Universal Asynchronous Receiver/Transmitter (UART)
- Inter-Integrated Circuit module (I2C)
- General Purpose Input Output (GPIO)

2.2.2 Firmware and software of the TOE

The firmware comes with two alternative Firmware-Identifiers. The second and new Firmware-Identifier does not change anything on the TOE except the version number of the Firmware-Identifier. I.e. the entire firmware on the TOE equals entirely for the two Firmware-Identifiers so that it is from user perspective regardless which Firmware-Identifier is chosen. The effective change is on Infineon Technologies production testing only which results by an automatism in this version increase.

The entire firmware of the TOE consists of different parts:
One part comprises the Resource Management System (RMS) with routines for managing the Cache, RAM, MMU, the branch table, configuration and the testing functions. The RMS is the IC Dedicated Support Software as defined in the PP [9]. The RMS routines are stored from Infineon Technologies AG in a reserved area of the ROM but parts of it are also stored in the SOLID FLASH™ NVM. There is no ROM space available for the user.

The second part is the Boot Software (BOS), consisting of initialization and various testing routines and providing the different operation modes of the TOE. The BOS is the IC Dedicated Test Software as defined in the PP [9]. The BOS routines are stored in the especially protected test ROM but parts of it are also stored in the SOLID FLASH™ NVM. The BOS is not accessible for the user software.

The third part is the Flash Loader. This piece of software enables the 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. 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. Already the MMU blocks calls of the Flash Loader software at derivatives coming without Flash Loader. In derivatives with Flash Loader the related function is performed.

The optional software part of the TOE consists of the RSA-, the EC, the Toolbox- and the HSL libraries.

The RSA library is used to provide a high level interface to the RSA cryptography implemented on the hardware component Crypto2304T and includes countermeasures against SPA, DPA and DFA attacks. The routines are

used for the generation of RSA Key Pairs (RsaKeyGen), the RSA signature verification (RsaVerify), the RSA signature generation (RsaSign) and the RSA modulus recalculation (RsaModulus). The module provides the basic long number calculations (add, subtract, multiply, square with 1100 bit numbers) with high performance.
The RSA library is delivered as object code and in this way integrated in the user software. The RSA library can perform RSA operations from 512 to 4096 bits. Depending on the customer's choice, the TOE can be delivered with the 4096 code portion or with the 2048 code portion only. The 2048 code portion is included in both. Part of the evaluation are the RSA straight operations with key length from 1976 bits to 2048 bits, and the RSA CRT[1] operations with key lengths of 1976 Bits to 4096 Bits.
Parts of the evaluation are the RSA straight operations with key length from 1976 bits to 2048 bits, and the RSA CRT[2] operations with key lengths of 1976 bits to 4096 bits.
The EC library is used to provide a high level interface to Elliptic Curve cryptography and includes countermeasures against SPA, DPA and DFA attacks. The routines are used for ECDSA signature generation, ECDSA signature verification, ECDSA key generation and Elliptic Curve Diffie-Hellman key agreement. In addition, the EC library provides an interface to an addition function for primitive elliptic curve operations like ECC Add and ECC Double. ECC curves over prime field Fp, as well as over GF(2^n) finite field are supported too. 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 Brainpool [16] and NIST [24] Elliptic Curves with key lengths of 224, 233, 256, 283, 320, 384, 409, 512 and 521 Bits. The definition of the key lengths follows the national AIS32 regulation regarding the 100 bit security level by the BSI. The former 80 bit level is achieved by the key lengths of 160, 163, and 192 Bits.
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 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.

Beside the inclusion and support of cryptographic libraries this TOE comes with the optional Hardware Support Library (HSL) significantly simplifying the management of the SOLID FLASH™ NVM functionality. The HSL constitutes an application interface (API) accessing the HSM state machine and abstracting low level properties like special function registers and settings of specific hardware features. In short the HSL provides a user friendly also use case oriented interface considering endurance, reliability and performance.
Beyond the low level driver the basic method "In-place Update" with optional tearing safe methodology leverages the dedicated advantages of the new SOLID FLASH™ NVM technology. The HSL library is delivered as object code.
We define tearing as an untimed power cut off which in the worse could also occur during writing to or erasing of pages in the SOLID FLASH™ NVM.
If the HSL comes with the TOE and the user implements the offered configuration and dedicated functions tearing save behaviour of the SOLID FLASH™ NVM is provided. In these cases the user does not need to care about tearing events since either the old data or the new data are correctly in place.
Even in the cases where the user decides not to use the HSL and did also not implement own routines preserving the consistency of the SOLID FLASH™ NVM, the hardware protection means prevent from operation of

[2] Chinese Remainder Theorem

inconsistent data. Therefore, in no cases a tearing event leads to an exploitable situation respectively vulnerability.
Anyhow, the user should be aware and is recommended to use either the HSL or implement own routines managing tearing events since if there would occur a faulty programmed SOLID FLASH™ NVM location the TOE ends operation at that point.

Note 1:
The cryptographic libraries RSA and EC are delivery options. Therefore the TOE may come with free combinations of or without these libraries. 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).
End of note.

The firmware and software parts of the TOE comprise:

Firmware

Boot Software (BOS)
Resource Management System (RMS)
Flash Loader

Optional Software

RSA cryptographic library
EC cryptographic library
Toolbox library
HSL

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 ISO pads, the CLK and power supply pads, as well as the pads used for contact based interfacing.
- The data-oriented I/O interface to the TOE is formed by the pads used for contact based communication.
- The interface to the firmware is constituted by special registers used for hardware configuration and control (Special Function Registers, SFR).
- The interface of the TOE to the operating system is constituted by the RMS compatible software 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 BOS test routine call, i.e. entry to the test modes.
- 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 by the Toolbox library interface
- The interface to the HSL is defined by the functions of the Hardware Support Library.

Note that the interfaces to the cryptographic libraries (RSA and EC) are optionally, depending on the customer order.

2.2.4 Guidance documentation

The following provides a brief overview of the document set constituting the user guidance for this TOE. The exact document titles and versions are given in chapter 9.

- The Hardware Reference Manual HRM [1] is the user data book of the TOE and contains the relevant module, function and feature description
- The Production and Personalization User Manual [2] contains detailed information about the usage of the Flash Loader
- The document Programmers Reference Manual [3] describes the usage and interface of the Resource Management System RMS. The Resource Management System (RMS) provides basic configuration and testing services to the user.
- The document [4] asymmetric Cryptographic Library for Crypto@2304T user interface 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. This document comes with an additional errata section.
- The document [5] Crypto@2304T User Manual 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 [6] Security Guidelines User Manual provides the guidance and recommendations to develop secure software for and secure usage of this TOE.
- The document [7] Errata Sheet contains latest updates and corrections of the TOE relevant for the user and it is a kind addendum to the hardware reference manual HRM [1]. The Errata Sheet can be changed during the life cycle of the TOE. New Errata Sheet releases are reported in a monthly updated list provided from Infineon Technologies AG to the user. This list is not part of the certification process. Part of the TOE certification is the released version valid at the point in time the certificate was issued.
- The document [15] Hardware Support Library (HSL) provides an application interface (API) accessing the HSM state machine and abstracting low level properties like special function registers and settings of specific hardware features.
- Finally the certification report by BSI 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 user documentation, the Security Guidelines User Manual [6].

2.2.5 Forms of delivery

The TOE can be delivered:

- in form of complete modules
- in form of plain wafers
- in any IC case (for example TSSOP28, VQFN32, VQFN40, CCS-modules, etc.)
- in no IC case or package, simply as bare dies
- or in whatever type of package

The form of delivery does not affect the TOE security and it can be delivered in any type, as long as the processes applied and sites involved have been subject of the appropriate audit.

The delivery can therefore be at the end of phase 3 or at the end of phase 4 which can also include pre-personalization steps according to PP [9]. Nevertheless in both cases the TOE is finished and the extended test features are removed. In this document are always both cases mentioned to avoid incorrectness but from the security policy point of view the two cases are identical.
The delivery to the software developer (phase 2 ➔ phase 1) contains the development package and is delivered in form of documentation as described above, data carriers containing the tools and emulators as development and debugging tool.
Part of the software delivery could also be the Flash Loader program, provided by Infineon Technologies AG, running on the TOE and receiving the transmitted information of the user software to be loaded into the SOLID FLASH™ NVM. The download is only possible after successful authentication and the user software can also be downloaded in an encrypted way. In addition, the user is after he finalized the download and prior deliver to third party obligated to permanently lock further use of the Flash Loader. Note that it depends on the procurement order, whether the Flash Loader program is present or not.

The belonging user guidance documents are delivered in electronic form: Either by user downloads from a secure server or alternatively on request as encrypted email attachment.

2.2.6 Production sites

The TOE may be handled in different production sites but the silicon of this TOE is produced in Tainan, Taiwan only, as listed below. To distinguish the different production sites of various products in the field, the site is coded into the identification data. The exact coding of the generic chip identification data is described in the hardware reference manual HRM [1].
The delivery measures are described in the ALC_DVS aspect.

Table 4 Production site in chip identification

Production Site	Chip Identification
Tainan, Taiwan	Byte number 13: $0A_H$

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 and in particular, conformance is claimed for:

Common Criteria part 2 **extended** [11] and Common Criteria part 3 **conformant** [12].

3.2 PP Claim

This Security Target is in **strict conformance** to the Security IC Platform Protection Profile [9].
The targeted EAL6+ level includes already the highest assurance families AVA_VAN.5 and ALC_DVS.2 from Common Criteria part 3 [12]. To achieve an additional augmentation, this Security Target is **assurance package augmented** compared to the Security IC Platform Protection Profile [9].
The augmentation is achieved - with regard to CCv3.1 Part 3 [12]: Security assurance components by including:

Table 5 Augmentations of the assurance level of the TOE

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

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

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

The security assurance requirements of the TOE are according to the Security IC Platform Protection Profile [9] and to Part 3 of the Common Criteria version v3.1 [12].

3.3 Package Claim

This Security Target claims conformance to the following additional packages taken from the Security IC Platform Protection Profile [9]:

- Package "Authentication of the Security IC", section 7.2
- Package "Loader", Package 1: Loader dedicated for usage in secured environment only, section 7.3.1. This package is optional and fulfilled only by TOE products coming with Flash Loader.
- Package "Loader", Package 2: Loader dedicated for usage by authorized users only, section 7.3.2. This package is optional and fulfilled only by TOE products coming with Flash Loader.
- Package "TDES"; section 7.4.1
- Package "AES"; section 7.4.2

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

The assurance level of this TOE is:
EAL6 augmented (EAL6+)
with the component ALC_FLR.1 and additional packages

3.4 Conformance Rationale

This security target claims **strict** conformance only to the PP [9].
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 behaviour of the security functionality
- the IC Dedicated Software with the parts
- the IC Dedicated Test Software,
- the IC Dedicated Support Software.

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

3.4.1 Security Problem Definition:

Following the PP [9], the security problem definition is enhanced by adding additional threats, organization security policies and an augmented assumption. Including these add-ons, the security problem definition of this security target is consistent with the statement of the security problem definition in the PP [9], as the security target claimed strict conformance to the PP [9].

3.4.2 Conformance Rationale:

The augmented organizational security policy P.Add-Functions, coming from the additional security functionality of the cryptographic libraries, the augmented assumption A.Key-Function, related to the usage of key-depending function, and the threat memory access violation T.Mem-Access, due to specific TOE memory access control functionality, have been added. These add-ons have no impact on the conformance statements regarding CC [10] and PP [9], with following rational:

- The security target remains conformant to CC [10], claim 482 as the possibility to introduce additional restrictions is given.
- The security target fulfils the strict conformance claim of the PP [9] due to the application notes 5, 6 and 7 which apply here. By those notes the addition of further security functions and security services are covered, even without deriving particular security functionality from a threat but from a policy.

3.4.3 Adding Objectives

Due to additional security functionality coming from

- the cryptographic libraries
  - O.Add-Functions,
- the memory access control
  - O.Mem-Access
- and objective related to the Flash Loader
  - O.Authentication,
  - O.Cap_Avail_Loader,
  - O.Ctrl_Auth_Loader and
  - O.Prot_TSF_Confidentiality

additional security objectives have been introduced.
These add-ons have no impact on the conformance statements regarding CC [10] and PP [9] with following rational:

The security target remains conformant to CC [10], claim 482 as the possibility to introduce additional restrictions is given.

- The security target fulfils the strict conformance of the PP [9] due to the application note 9 applying here. This note allows the definition of high-level security goals due to further functions or services provided to the Security IC Embedded Software.

3.4.4 AES and TDES

The PP [9] implements the optional policy cryptographic services P.Crypto_Service with its packages "TDES" and "AES". This TOE provides these optional packages requiring secure hardware based cryptographic services for the IC Embedded Software as outlined in chapter 7.1.4.
Due to these optional additional security functionalities the security objectives O.TDES and O.AES have been introduced. These add-ons have no impact on the conformance statements regarding CC [10] and PP [9], with following rational:

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

3.4.5 Loader

The PP [9] implements the optional policy for applying a Loader. The Loader is used to load data into the SOLID FLASH™ NVM.
The Flash Loader provides the service for authentication and implements the:

- Package for Authentication of the Security IC
  - FIA_API.1 Authentication Proof of Identity of the TOE against a user.
    This means that the user clearly can identify the TOE on his external request. This fulfils the objective O.Authentication, authentication to external entities, and obligates an objective to the environment OE.TOE_Auth, external entities authenticating of the TOE as outlined in the PP [9].

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

- This TOE provides a Flash Loader complying with the optional packages:
- Package 1: Loader dedicated for usage in secured environment only
- Package 2: Loader dedicated for usage by authorized users only" as outlined in sections 7.2 and 7.3 of the PP [9]
- Due to these optional additional security functionalities the security objectives
  - "O.Cap_Avail_Loader", Capability and availability of the Loader,
  - "O.Ctrl_Auth_Loader", access control and authenticity for the Loader" and
  - "OE.Loader_Usage Secure communication and usage of the Loader"
  - "O.Prot_TSF_Confidentiality", Protection of the confidentiality of the TSF
  - "OE.Lim_Block_Loader", Limitation of capability and blocking the Loader

have been introduced.

These add-ons have no impact on the conformance statements regarding CC [10] and PP [9], with following rational:
The security target fulfils the strict conformance claim of the PP [9] due to the application notes 9 applying here. By this note the addition of further security functions and security services are covered, even without deriving particular security functionality from a threat or a policy.

3.4.6 Summary

Due to the above rational, the security objectives of this security target are consistent with the statement of the security objectives in the PP [9], as the security target claims package augmentation to the PP [9].
All security functional requirements defined in the PP [9] are included and completely defined in this ST.
The following security functional requirements are taken from the Common Criteria part 2 [11] document and respectively from the package definitions taken from the PP [9]:

Table 6 Security Functional Requirements

Security Functional Requirement	Description
FAU_SAS.1	Audit data storage
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_CKM.4/AES (1)	Cryptographic key destruction – AES
FCS_CKM.4/TDES (1)	Cryptographic key destruction – TDES
FCS_COP.1	Cryptographic operation
FCS_COP.1/AES (1)	Cryptographic operation – AES
FCS_COP.1/TDES (1)	Cryptographic operation – TDES
FCS_RNG.1	Generation of Random Numbers
FDP_SDC.1	Stored data confidentiality
FDP_ACC.1	Subset access control
FDP_ACC.1/Loader (2)	Subset access control – Loader
FDP_ACF.1 (4)	Security attribute based access control
FDP_ACF.1/Loader (2)	Security attribute based access control - Loader
FDP_IFC.1	Subset information flow control
FDP_ITT.1	Basic internal transfer protection
FDP_SDI.1	Stored data integrity monitoring
FDP_SDI.2	Stored data integrity monitoring and action
FDP_UCT.1 (2)	Basic data exchange confidentiality
FDP_UIT.1 (2)	Data exchange integrity
FIA_API.1	Authentication Proof of Identity
FMT_LIM.1	Limited capabilities
FMT_LIM.1/Loader (3)	Limited capabilities
FMT_LIM.2/Loader (3)	Limited availability
FMT_LIM.2	Limited availability
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_SMF.1	Specification of Management functions
FPT_FLS.1	Failure with preservation of secure state
FPT_ITC.1 (2)	Inter-TSF trusted channel
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_PHP.3	Resistance to physical attack
FRU_FLT.2	Limited fault tolerance

(1) Taken from the according packages of the PP [9]: package "TDES", package "AES" and package "Hash functions".
(2) Taken from the according Package 2: Loader dedicated for usage by authorized users only of the PP [9]
(3) Taken from the according package 1: Loader dedicated for usage in secured environment only of the PP [9]
(4) Implemented by the Flash Loader if on board of the TOE

The following security functional requirement is included and completely defined in this ST, section 6.

FPT_TST.2	Subset TOE security testing[1]

All assignments and selections of the security functional requirements are done in the PP [9] and in this Security Target.

3.5 Application Notes

The functional requirements

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

are iterations of the FCS_RNG.1 as defined in the Protection Profile [9] according to "Anwendungshinweise und Interpretationen zum Schema (AIS)" respectively "Functionality classes and evaluation methodology for physical random number generators", AIS31 [13].

[1] Requirement from the PP [9]

4 Security Problem Definition (ASE_SPD)

The content of the PP [9] 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 [9] section 3.2, respectively for T.Masquerade_TOE in chapter 7.2.1.

Table 7 Threats according PP [9]

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

4.1.1 Additional Threat due to TOE specific Functionality

The additional functionality of introducing sophisticated privilege levels and access control allows the secure separation between the operation system(s) and applications, the secure downloading of applications after personalization and enables multitasking by separating memory areas and performing access controls between different applications. Due to this additional functionality "area based memory access control" a new threat is introduced.
The Smartcard Embedded Software is responsible for its User data of the Composite TOE according to the assumption "Treatment of User data of the Composite TOE (A.Resp-Appl)". However, the Smartcard Embedded Software may comprise different parts, for instance an operating system and one or more applications. In this case, such parts may accidentally or deliberately access data (including code) of other parts, which may result in a security violation.
The TOE shall avert the threat "Memory Access Violation (T.Mem-Access)" as specified below:

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

The additional functionality of a Loader as defined in the PP [9], section 7.3 requires to address the following threat, as defined in the document "PP0084: Interpretation" [PP0084].

The TOE shall avert the threat "Diffusion of open Samples (T.Open_Samples_Diffusion)" as specified below:

Table 8 Additional threats due to TOE specific functions and augmentations

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

Table 9 Additional threats due to TOE specific functions and augmentations

T.Mem-Access	Memory Access Violation
T.Open_Samples_Diffusion	Diffusion of open samples

4.1.2 Assets regarding the Threats

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

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

SC4 is an additional security service provided by this TOE which is the availability of random numbers. These random numbers are generated either by a true random number or a deterministic random number generator or by both, when a true random number is used as seed for the deterministic random number generator. Note that the generation of random numbers is a requirement of the PP [9].
To be able to protect the listed assets the TOE shall protect its security functionality as well. Therefore critical information about the TOE shall be protected. Critical information includes:

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

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

- logical design data,
- physical design data,
- IC Dedicated Software, Security IC Embedded Software, Initialization Data and Pre-personalization Data,
- specific development aids,

- test and characterization related data,
- material for software development support, and
- reticles and products in any form

as long as they are generated, stored, or processed by the TOE Manufacturer.
For details see PP [9] section 3.1.

4.2 Organizational Security Policies

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

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

Due to the augmentations of PP [9] and the chosen packages additional policies are introduced and described in the next chapter.

Table 10 Organizational Security Policies according PP [9]

P.Process-TOE	Identification during TOE Development and Production

4.2.1 Augmented Organizational Security Policy

Due to the augmentations of the PP [9] and the chosen packages additional policies are introduced.
The TOE provides specific security functionality, which can be used by the Smartcard Embedded Software. In the following specific security functionality is listed which is not derived from threats identified for the TOE's environment because it can only be decided in the context of the smartcard application, against which threats the Smartcard Embedded Software will use the specific security functionality.
The IC Developer / Manufacturer must apply the 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 2:
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 any combination 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.
End of note.

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

P.Crypto-Service	**Cryptographic services of the TOE**

	The TOE provides secure hardware based cryptographic services for the IC Embedded Software: • Triple Data Encryption Standard (TDES) • Advanced Encryption Standard (AES)

Note 3:
This TOE can come with both crypto co-processors accessible, or with a blocked SCP or with a blocked Crypto2304T, or with both crypto co-processors blocked. The blocking depends on the customer demands prior to the production of the hardware. In case the SCP is blocked, no AES and DES computation supported by hardware is possible. In case the Crypto2304T is blocked, no RSA and EC computation supported by hardware is possible. No accessibility of the deselected cryptographic co-processors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic co-processors.
End of note.

The IC Developer / Manufacturer must apply the organizational security policy "Limiting and Blocking the Loader Functionality (P.Lim_Block_Loader)" as specified below:

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

4.3 Assumptions

The TOE assumptions on the operational environment are defined and described in PP [9] section 3.4.
The assumptions concern the phases where the TOE has left the chip manufacturer.
The support of cipher schemas requires an additional assumption.

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

4.3.1 Augmented Assumptions

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

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

Note that here the routines which may compromise keys when being executed are part of the Smartcard Embedded Software. In contrast to this the threats T.Leak-Inherent and T.Leak-Forced address (i) the cryptographic routines which are part of the TOE. For details please refer to PP [9] section 3.4.

5 Security objectives (ASE_OBJ)

This section shows the subjects and objects where are relevant to the TOE.
A short overview is given in the following.
The user has the following standard high-level security goals related to the assets:

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

5.1 Security objectives for the TOE

The security objectives of the TOE are defined and described in PP [9] section 4.1, 7.2.1, 7.3.1, 7.3.2, 7.4.1 and 7.4.2.

Table 11 Objectives for the TOE according to PP [9]

O.Phys-Manipulation	Protection against Physical Manipulation
O.Phys-Probing	Protection against Physical Probing
O.Malfunction	Protection against Malfunction
O.Leak-Inherent	Protection against Inherent Information Leakage
O.Leak-Forced	Protection against Forced Information Leakage
O.Abuse-Func	Protection against Abuse of Functionality
O.Identification	TOE Identification
O.RND	Random Numbers
O.Cap_Avail_Loader	Capability and availability of the Loader Valid only for the TOE derivatives delivered with activated Flash Loader.
O.Authentication	Authentication to external entities Valid only for the TOE derivatives delivered with activated Flash Loader
O.Ctrl_Auth_Loader	Access control and authenticity for the Loader - valid only for the TOE derivatives delivered with activated Flash Loader
O.TDES	Cryptographic service Triple-DES
O.AES	Cryptographic service AES

Note 4:
The objectives O.Cap_Avail_Loader, O. Authentication, O.Ctrl_Auth_Loader and O.Prot_TSF_Confidentiality apply only at TOE products coming with activated Flash Loader enabled for software or data download by the user. In other cases the Flash Loader is not available anymore and the user software or data download is completed. Depending on the capabilities of the user software these objectives may then reoccur as subject of the composite TOE.
End of note.

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 5:
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 any combination 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.
End of note.

Note 6:
This TOE can come with both crypto co-processors accessible, or with a blocked SCP or with a blocked Crypto2304T, or with both crypto co-processors blocked. The blocking depends on the customer demands prior to the production of the hardware. In case the SCP is blocked, no AES and DES computation supported by hardware is possible. In case the Crypto2304T is blocked, no RSA and EC computation supported by hardware is possible. No accessibility of the deselected cryptographic co-processors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic co-processors.
End of note.

The TOE shall provide "Area based Memory Access Control (O.Mem-Access)" as specified below.

O.Mem Access	**Area based Memory Access Control** The TOE must provide the Smartcard Embedded Software with the capability to define restricted access memory areas. The TOE must then enforce the partitioning of such memory areas so that access of software to memory areas and privilege levels is controlled as required, for example, in a multi-application environment.

The additional functionality of a Loader as defined in the PP [9], section 7.3 requires to address the following objective, as defined in the document "PP0084: Interpretation" [PP0084].

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

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

Table 12 Additional objectives due to TOE specific functions and augmentations

O.Add-Functions	Additional specific security functionality
O.Mem-Access	Area based Memory Access Control
O.Prot_TSF_Confidentiality	Protection of the confidentiality of the TSF

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 [9] section 4.2, 4.3, 7.2.1and 7.3.
The operational environment of the TOE shall provide "Limitation of capability and blocking the Loader "OE.Lim_Block_Loader", "External entities authentication of the TOE "OE.TOE_Auth" and "Secure communication and usage of the Loader "OE.Loader¬Usage" as specified below:

OE.Lim_Block_Loader	**Limitation of capability and blocking the Loader** The Composite Product Manufacturer will protect the Loader functionality against misuse, limit the capability of the Loader and terminate irreversibly the Loader after intended usage of the Loader.
OE.TOE_Auth	**Authentication to external entities** The operational environment shall support the authentication verification mechanism and know authentication reference data of the TOE.
OE.Loader_Usage	**Secure communication and usage of the Loader** The authorized user must support the trusted communication with the TOE by confidentiality protection and authenticity proof of the data to be loaded and fulfilling the access conditions required by the Loader.

Note 7:
The objectives OE.Lim_Block_Loader, OE.TOE_Auth and OE.Loader_Usage for the development and operation environment apply only at TOE products coming with activated Flash Loader enabled for user data download. In other cases the Flash Loader is not available anymore and the user data download is completed. Depending on the capabilities of the user software this objective may then reoccur as subject of the composite TOE.
End of note.

The table below lists the security objectives.

Table 13 Security Objectives for the Environment according to the PP [9]

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

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

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

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

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

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

5.3 Security Objectives Rationale

The security objectives rationale of the TOE are defined and described in PP [9] section 4.4. For organizational security policy P.Add-Functions, OE.Plat-Appl and OE.Resp-Appl the rationale is given in the following description.

Table 14 Security Objectives Rationale

Assumption, Threat or Organizational Security Policy	Security Objective
A.Key-Function	OE.Resp-Appl
P.Add-Functions	O.Add-Functions
P.Crypto-Service	O.TDES
P.Crypto-Service	O.AES
P.Ctrl_Loader	O.Ctrl_Auth_Loader O.Authentication
P.Ctrl_Loader	OE.Loader_Usage OE.TOE_Auth
P.Lim_Block_Loader	O.Cap_Avail_Loader
P.Lim_Block_Loader	OE.Lim_Block_Loader
T.Masquerade	O.Authentication OE.TOE_Auth
T.Mem-Access	O.Mem-Access
T.Open_Samples__Diffusion	O.Prot_TSF_Confidentiality O.Leak-Inherent O.Leak-Forced

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

Nevertheless the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced define how to implement the specific security functionality required by P.Add-Functions. (Note that these objectives support that the specific security functionality is provided in a secure way as expected from P.Add-Functions.) Especially O.Leak-Inherent and O.Leak-Forced refer to the protection of confidential data (User data 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.

Compared to the PP [9] a further clarification has been made for the security objective "Treatment of user data of the Composite TOE (OE.Resp-Appl)": By definition cipher or plain text data and cryptographic keys are user data of the Composite TOE. So, the Smartcard Embedded Software will protect such data if required and use keys and functions appropriately in order to ensure the strength of cryptographic operation. Quality and confidentiality must be maintained for keys that are imported and/or derived from other keys. This implies that appropriate key management has to be realized in the environment. That is expressed by the assumption A.Key—Function which is covered from OE.Resp–Appl. These measures make sure that the assumption

A.Resp-Appl is still covered by the security objective OE.Resp-Appl although additional functions are being supported according to P.Add-Functions.

Compared to the PP [9] 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 [9] section 7.3 considers the life cycle phases of the TOE also with the organizational policy P.Lim_Block_Loader and P.Ctlr_Loader as the TOE must be protected against unauthorized usage and control and against download of malicious software before, during and after the user downloads his software. This is formalized with the objectives O.Cap_Avail_Loader, O.Authentication and O.Ctrl_Auth_Loader requiring authentication of the TOE to external entities and a trusted communication channel. The O.Authentication implements a mutual authentication and involves the environment therefore.
The implemented mutual authentication requires first to authenticate the TOE to the external user. This requires also knowledge by the user about the sequence of the protocol, interpretation of the transferred data and how to start the authentication of the TOE. This authentication mean counters the threat T.Masquerade_TOE as only the genuine TOE is able to identify itself correctly to the enabled user, which covers O.Authentication.
The second step of the mutual authentications mean implements the authentication of the user to the TOE. Only the user enabled to present the correct authentication data and knowing about the sequence, data interpretation and signaling of the authentication to the TOE is able to proceed further on. This enforces OE.TOE_Auth, requiring the support of the verification mechanism and known authentication reference data by the operational environment.

It is normal business that products enabled for software download by the user are either on their way to the user or are already stored at user premises. At both situations it cannot be excluded that an attacker could manage to steal such products enabled for software downloads. The ability to download software on a chip without operating system and/or application is defined as open sample.
This situation generates the threat T.Open_Samples_Diffusion which is defined as follows:
The download of analysis software could enable an attacker to characterize the product and to construct an attack path out of the gained information.
This threat is countered by the Flash Loader by following rational:
As long as the Flash Loader is active, controlled usage to the Flash Loader functionality (P.Ctrl_Loader) is enforced which protects the TOE from achieving the status of being an open sample. And more, even the attacker could observe, meaning in the sense of measurements during, or induce faults during an authorized download, the Flash Loader protects the user data of the download by confidentiality and integrity protection means. The Flash Loader functionalities of mutual authentication, establishing a dedicated trusted communication channel, the encryption and integrity protection means cover the objectives O.Prot_TSF_Confidentiality, O.Leak-Inherent and O.Leak-Forced.

The objective O.Ctrl_Auth_Loader Access control and authenticity for the Loader is covered by following rational: The identification of the communication entities of the Flash Loader requires the presence of dedicated identification data for passing successfully the mutual authentication. This enforces the policy P.Ctrl_Loader comprising the aspect of the mutual authentication. After successful authentication the user is enabled to change the keys used for authentication and downloading the user data. This first user is defined as the administrator. The TOE can then further be operated for example by a service partner who is defined as being the Download Operator. The equal protecting means as for the Administrator apply here again but due to the key change different roles are established. The Download Operator downloads then the encrypted user data

with the Flash Loader into the defined and accessible SOLID FLASH™ NVM area. This area is access protected by the MMU.

This objective O.Leak-Inherent is covered with following rational:
This threat is countered with the mutual authentication mean as only the correct identified user is able to download the user intended software and data. Since it is not practical for an attacker to authenticate correctly a threatening download of attack software is countered. By that possible confidential user data already stored on the TOE remain protected from disclosure by this method.
If the user is the attacker, or does not follow the user guidance, or bad designed user software implements weaknesses, the user data remain protected anyway, since even after passing the mutual authentication of the loader the download is conducted encrypted only. And even more, a different encryption is applied to store the data in the SOLID FLASH™ NVM. Since also the number of Flash Loader trials is limited even comprehensive side channel analysis would not leave sufficient information.

This objective O.Leak-Forced is covered with following rational:
Another method to gain information is to force information leakage of confidential data processed in the TOE. Such forcing requires malfunction or physical manipulation. Inducing errors of any kind during data processing will be discovered by the Integrity Guard with high probability which leads to a security reset. Failures induced during the mutual authentication or encrypted download process of the Flash Loader will also be discovered as the perturbation of the sequences leads to fail of the process with trial counter decrement or a fail of the integrity check of the downloaded data will occur. It would anyway not be practical to induce targeted errors at any process managing data due to the permanent and differently data encryption and integrity protection on the TOE.
Physical static manipulation requires the presence of worthwhile target. This is on one hand hard to identify and would require intensive reverse engineering due to the topological means such as synthesis of the TOE and other means. But, if we assume than an attacker could identify such spot, the physical preparation was successful too and thus it was possible to probe the targeted signal, then, even assumed the attacker could analyze the traffic on the signal, the results would be worthless since the signal data is encrypted or masked. Thus, the data remains confidentiality protected even outside the TOE, since the analyst neither has neither the encryption algorithm nor the key.

All requirements are fulfilled by the Flash Loader due the strong mutual authentication means enabling only the authorized user for the download, due to the download of encrypted data only and due to the final locking command to be applied by the user before delivery. As a consequence the operational environment objectives OE.Lim_Block_Loader, OE.TOE_Auth and OE.Loader_Usage obligate the composite manufacturer to protect the authentication data (e.g. keys) against misuse and limit the capability of the Loader.
In addition, the user guidance implements the obligation to permanent disable the Flash Loader prior delivery to the end-user.

The package 1 defines the final locking of the Flash Loader prior delivery to the end-user and the usage in secure environment. The package 2 defines that the Flash Loader can be used also in insecure environment. By claiming both packages the user has the choice to apply the active Flash Loader either in insecure or in secure environment and achieves by that a maximum of flexibility. Anyhow, the user is obligated to lock the Flash Loader prior delivery to the end-user in both cases. This is an obligation implemented by the user guidance.
The Flash Loader provides the required functionality to be applied by the composite manufacturer for covering these objectives.

The objectives O.Cap_Avail_Loader, O.Authentication, O.Loader_Usage and O.Prot_TSF_Confidentiality and the organizational policies P.Lim_Block_Loader and P.Ctlr_Loader as discussed in the PP [9] section 7.2 and 7.3 apply only at TOE products at the life cycle phase delivery, if these products come with activated Flash Loader enabled for software or data download by the user. In other cases the Flash Loader is not available anymore and

the user software or data download is completed. Depending on the capabilities of the user software these objectives may then reoccur as subject of the composite TOE.

The PP [9] includes the organizational security policy P.Crypto-Service Cryptographic services of the TOE in a different extend as it formalizes the objectives O.TDES and O.AES.
For the objective O.TDES a concrete standard reference (NIST) with operational modes is given the implementation must follow and also the cryptographic key destruction is regulated. The implementation complies to the given security functional requirements and the objective O.TDES is met.
For the objective O.AES a concrete standard reference (NIST) with a selection of key lengths is given the implementation must follow and also the cryptographic key destruction is regulated. The implementation complies to the given security functional requirements and the objective O.AES is met.
For the objective O.AES 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.AES 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 Protection Profile for the assumptions, policy and threats defined there.

6 Extended Component Definition (ASE_ECD)

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

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

The extended components FCS_RNG, FMT_LIM, FAU_SAS, FDP_SDC and FIA_API are defined and described in PP [9] section 5 and the extended component FIA_API is defined and described in PP [9] section 7.2.
The component FPT_TST.2 is defined in the following.

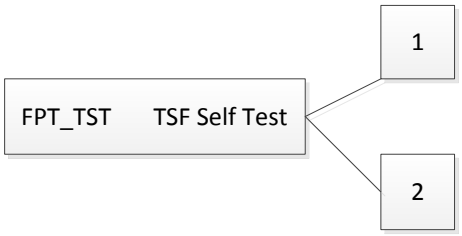
6.1 Component "Subset TOE security testing (FPT_TST.2)"

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

TSF self-test (FPT_TST)

Family Behavior	The Family Behavior is defined in [12] section 15.14 (442, 443).
Component leveling	
FPT_TST.1:	The component FPT_TST.1 is defined in [3] section 15.14 (444, 445, 446).
FPT_TST.2:	Subset TOE security testing, provides the ability to test the correct operation of particular security functions or mechanisms. These tests may be performed at start-up, periodically, at the request of the authorized user, or when other conditions are met. It also provides the ability to verify the integrity of TSF data and executable code.
Management FPT_TST.2	The following actions could be considered for the management functions in FMT: Management of the conditions under which subset TSF self-testing occurs, such as during initial start-up, regular interval or under specified conditions Management of the time of the interval appropriate.
Audit: FPT_TST.2	There are no auditable events foreseen.
FPT_TST.2	**Subset TOE testing**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.2.1:	The TSF shall run a suite of self-tests [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, and/or at the conditions [assignment: conditions under which self-test should occur]] to demonstrate the correct operation of [assignment: functions and/or mechanisms].

7 Security Requirements (ASE_REQ)

For this section the PP [9] section 6 can be applied completely.

7.1 TOE Security Functional Requirements

The security functional requirements (SFR) for the TOE are defined and described in the PP [9] section 6.1 and in the following description.
Following table provides an overview of the functional security requirements of the TOE, defined in the in PP [9] section 6.1. In the last column it is marked if the requirement is refined. The refinements are also valid for this ST.

Table 15 Security Functional Requirements defined in respectively taken from packages of the PP [9]

Security Functional Requirement		Refined y/n or Defined in PP [9]
FAU_SAS.1	"Audit storage"	Defined
FCS_CKM.4/AES (1)	"Cryptographic key destruction – AES"	No
FCS_CKM.4/TDES (1)	"Cryptographic key destruction – TDES"	No
FCS_COP.1/AES (1)	"Cryptographic operation – AES"	No
FCS_COP.1/TDES (1)	"Cryptographic operation – TDES"	No
FCS_RNG.1/DRNG	"Random number generation - DRNG"	Defined
FCS_RNG.1/HPRG	"Random number generation – HPRG"	Defined
FCS_RNG.1/KSG	"Random number generation - KSG"	Defined
FCS_RNG.1/TRNG	"Random number generation - TRNG"	Defined
FDP_ACC.1/Loader (3)	"Subset access control – Loader"	Defined
FDP_ACF.1/Loader (3)	"Security attribute based access control – Loader"	Defined
FDP_IFC.1	"Subset information flow control"	No
FDP_ITT.1	"Basic internal transfer protection"	Yes
FDP_SDC.1	"Stored data confidentiality"	Defined
FDP_SDI.2	"Stored data integrity monitoring and action"	No
FDP_UCT.1 (3)	"Basic data exchange confidentiality"	No
FDP_UIT.1 (3)	"Data exchange integrity"	No
FIA_API.1 (4)	"Identification and Authentication"	Defined
FMT_LIM.1	"Limited capabilities"	No
FMT_LIM.1/Loader (2)	"Limited Capabilities"	Defined
FMT_LIM.2	"Limited availability"	No
FMT_LIM.2/Loader (2)	"Limited Availability"	Defined
FPT_FLS.1	"Failure with preservation of secure state"	Yes
FPT_ITT.1	"Basic internal TSF data transfer protection	Yes
FPT_PHP.3	"Resistance to physical attack"	Yes
FRU_FLT.2	"Limited fault tolerance"	Yes
FTP_ITC.1 (3)	"Inter-TSF Trusted Channel"	No

(1) Taken from the PP [9] package "TDES" and package "AES".

(2) From PP[9]: Package 1: Loader dedicated for usage in secured environment only
(3) From PP[9]: Package 2: Loader dedicated for usage by authorized users only
(4) From PP[9]: Package Authentication of the Security IC

Following table provides an overview about the augmented security functional requirements, which are added additional to the TOE and defined in this ST. All requirements are taken from Common Criteria Part 2 [11], with the exception of the requirement FPT_TST.2 which is defined in this ST completely and FDP_SDI.2 which is taken from the PP [9] as well.

Table 16 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"

All assignments and selections of the security functional requirements of the TOE are done in PP [9] and in the following description.
The security functional requirements FMT_LIM.1/Loader, FMT_LIM.2/Loader, FIA_API.1, FTP_ITC.1, FDP_UCT.1, FDP_UIT.1, FDP_ACC.1/Loader and FDP_ACF.1/Loader applying only at TOE products coming with activated Flash Loader enabled for user data download. In other cases the Flash Loader is not available anymore and the user data download is completed. Depending on the capabilities of the user software these security functional requirements may then reoccur as subject of the composite TOE.

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

Please note that the national regulation are outlined in PP [9] chapter 7.5.1 and in AIS31 [13]. These regulations apply for this TOE.

Note 8:
The functional requirements FCS_RNG.1/TRNG, FCS_RNG.1/HPRG, FCS_RNG.1/DRNG, FCS_RNG.1/KSG, are iterations of the FCS_RNG.1 defined in the PP [9] according to "Anwendungshinweise und Interpretationen zum Schema (AIS)" respectively "A proposal for: Functionality classes for random number generators" [13].
End of note.

Note 9:
The Physical True Random Number Generator PTRNG implements total failure test of the random source and a continuous RNG test according to:
National Institute of Standards and Technology, Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication (FIPS) 140-2, 2002-03-12, chapter 4.9.2.
End of note.

Together with the guidelines in [6] the hybrid PTRNG of this TOE provides random numbers conformant to several quality metrics as defined in [13]. Depending on the user configuration the TOE provide the according random number quality. For each addressed quality metric of [13] the definitions are made in the following:

7.1.1.1.1 True Random Number Generation, meeting [13] PTG.2

FCS_RNG.1/TRNG	**Random Number Generation**
Hierarchical to:	No other components
Dependencies:	No dependencies
FCS_RNG.1/TRNG	Random numbers generation **Class PTG.2** according to [13]
FCS_RNG.1.1/TRNG	The TSF shall provide a *physical* random number generator that implements:
PTG.2.1	*A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.*
PTG.2.2	*If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.*
PTG.2.3	*The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.*
PTG.2.4	*The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.*
PTG.2.5	*The online test procedure checks the quality of the raw random number sequence. It is triggered continuously. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.*
FCS_RNG.1.2/TRNG	The TSF shall provide *numbers in the format 8- or 16-bit* that meet
PTG.2.6	*Test procedure A, as defined in [13] 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.*

7.1.1.1.2 Hybrid Random Number Generation, meeting AIS31 PTG.3

FCS_RNG.1/HPRG	**Random Number Generation**
Hierarchical to:	No other components
Dependencies:	No dependencies
FCS_RNG.1/HPRG	Random numbers generation **Class PTG.3** according to [13]
FCS_RNG.1.1/HPRG	The TSF shall provide a *hybrid physical* random number generator that implements:
PTG.3.1	*A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure has been detected no random numbers will be output.*
PTG.3.2	*If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.*
PTG.3.3	*The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test and the seeding of the DRG.3 post-processing algorithm have been finished successfully or when a defect has been detected.*
PTG.3.4	*The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.*
PTG.3.5	*The online test procedure checks the raw random number sequence. It is triggered continuously. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.* *Note:* *Continuously means that the raw random bits are scanned continuously.* *The algorithmic post-processing belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function. The output data rate of the post-processing algorithm shall not exceed its input data rate.* *End of note.*
FCS_RNG.1.2/HPRG	The TSF shall provide *numbers in the format 8- or 16-bit* that meet
PTG.3.7	*The test procedure A of AIS 31. The internal numbers were passing and the statistical test suites cannot practically distinguish the internal random numbers from output sequences of an ideal RNG.*
PTG.3.8	*The internal random numbers shall use the PTRNG of class PT.2 as random source for the post processing.* *Note:* *The internal random numbers produced by the employed PTG.2-conform PTRNG are adaptively compressed raw bits, where the compression rate is controlled by a so-called entropy estimator. The concept ensures that the random numbers provided by the PTRNG have high entropy, i.e., each delivered random byte will have more the 7.976 bit of entropy. In addition, the PTRNG produced random numbers have been tested against test procedures A and B under varying environment conditions.* *End of note.*

7.1.1.1.3 Deterministic Random Number Generation (DRNG) AIS31 DRG.3

FCS_RNG.1/DRNG	**Random Number Generation**
Hierarchical to:	No other components
Dependencies:	No dependencies
FCS_RNG.1/DRNG	Random numbers generation **Class DRG.3** according to [13]
FCS_RNG.1.1/DRNG	The TSF shall provide a *deterministic* random number generator that implements:
DRG.3.1	*If initialized with a random seed using a PTRNG of class PTG.2 as random source the internal state of the RNG shall have at least 100 bit of entropy.* *Note:* *Furthermore, the length of the internal state shall have at least 200 bit. (For the DRG.3 under consideration, the internal state has 351 bit.). The seed is provided by a certified PTG.2 physical TRNG with guaranteed 7,976 bit of entropy per byte.* *End of note.*
DRG.3.2	*The RNG provides forward secrecy.*
DRG.3.3	*The RNG provides backward secrecy even if the current internal state is known.*
FCS_RNG.1.2/DRNG	The TSF shall provide *numbers in the format 8- or 16-bit* that meet
DRG.3.4	*The RNG, initialized with a random seed, where the seed has at least 100 bit of entropy and is derived by a PTG.2 certified PTRNG. The RNG generates output for which any consecutive 234 bits strings of bit length 128 are mutually different with a probability that is greater than* $1 - 2^{(-16)}$.
DRG.3.5	*Statistical test suites cannot practically distinguish the random numbers from the output sequences of an ideal RNG. The random numbers must pass test procedure A and the U.S. National Institute of Standards and Technology (NIST) test suite for RNGs used for cryptographic purposes [S17] containing following 16 tests:* *Frequency (Monobit) Test, Frequency Test within a Block, Runs Tests, Test for the Longest-Run-of-Ones in a Block, Binary Matrix Rank Test, Discrete Fourier Transform (Spectral) Test, Non-overlapping (Aperiodic) Template Matching Test, Overlapping (Periodic) Template Matching Test, Maurer´s "Universal Statistical" Test, Liner Complexity Test, Serial Test, Approximate Entropy Test, Cumulative Sums (Cusums) Test, Random Excursions Test and Random Excursions Variant Test.*

7.1.1.1.4 Deterministic Random Number Generation (DRNG) AIS31 DRG.2

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

FCS_RNG.1/KSG	**Random Number Generation**
Hierarchical to:	No other components
Dependencies:	No dependencies
FCS_RNG.1/KSG	Random numbers generation **Class DRG.2** according to [13]
FCS_RNG.1.1/KSG	The TSF shall provide a *deterministic* random number generator that implements:
DRG.2.1	*If initialized with a random seed using a PTRNG of class PTG.2 as random source, the applied seed shall have at least 100 bits of entropy, the internal state of the RNG shall have at least the size of 200 bit - in this case the size of the internal state amounts to 351 bit, has the work factor for breaking the algorithm of 2127 due to the restriction on the maximum amount of keystream computed from a given seed, require guess work amounts to 2127 as well.*
DRG.2.2	*The RNG provides forward secrecy.* *Note:* *A linear complexity of the keystream of Achterbahn-128 that is lower bounded by 2^{98} (see Theorem 1 on page 27 in B. Gammel, R. Göttfert, O. Kniffler: Achterbahn-128/80, eSTREAM submission, June 2006). As a consequence an attacker needs to know at least $2 \times 2^{98} = 2^{99}$ consecutive random bits in order to determine future random bits.* *A correlation attack requires $2^{48.54}$ key stream bits along with a time complexity greater than 2^{119}. (See R. Göttfert and B. Gammel: On the frame length of Achterbahn-128/80, Proceedings of the 2007 IEEE Information Theory Workshop on Information Theory for Wireless Networks, pp. 1-5, IEEE, 2007.) To prevent such an attack, the generator produces at most 2^{40} random bytes (=2^{43} random bits) for a given seed. Thus the required $2^{48.54}$ random bits are not available. Therefore, the property of forward secrecy is fulfilled.* *End of note.*
DRG.2.3	*The RNG provides backward secrecy.* *Note:* *For a correlation attack knowledge of at least 2^{48} consecutive present or future random bits is required. Then, with a working factor of 2^{119} operations, the internal state can be computed. However, such an attack is not possible since the data complexity of the attack is $2^{48.54}$ and most of 2^{43} random bits are generated by the generator for each seed. Thus, the generator provides backward secrecy.* *End of Note.*
FCS_RNG.1.2/KSG	The TSF shall provide *numbers in the format 8- or 16-bit* that meet
DRG.2.4	*The RNG, initialized with a random seed of length at least 100 bit delivered by an PTRNG of the class PTG.2, generates output for which any consecutive 234 strings of the length 128 bits are mutually different with probability greater than $1-2^{(-16)}$.*

DRG.2.5	*Statistical test suites cannot practically distinguish the random numbers from the output sequences of an ideal RNG. The random numbers must pass test procedure A and the statistical tests mentioned in item DRG4.7.* *Note:* *The random numbers have been shown to fulfill all statistical tests of the AIS 20/31 statistical tests of procedure A. The random numbers are in the format 8- or 16 Bit.* *End of Note.*

7.1.1.2 FAU_SAS

During testing at the end of Phase 3 before TOE Delivery, the TOE shall be able to store some data (for instance about the production history or identification data of the individual die or other data to be used after delivery). Therefore, the security functional component Audit storage (FAU_SAS.1) has been added and is described in the PP [9].
The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below, PP [9]:

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

7.1.2 Subset of TOE testing

The security is strongly dependent on the correct operation of the security functions. Therefore, the TOE shall support that particular security functions or mechanisms are tested in the operational phase (Phase 7). The tests can be initiated by the Smartcard Embedded Software and/or by the TOE.
The TOE shall meet the requirement "Subset TOE testing (FPT_TST.2)" as specified below (Common Criteria Part 2 extended).

FPT_TST.2	**Subset TOE testing**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.2.1	The TSF shall run a suite of self-tests *at the request of the authorized user* to demonstrate the correct operation *of the alarm lines and/or following environmental sensor mechanisms:* • *More details are given in the confidential Security Target [8].*

7.1.3 Memory access control

Usage of multiple applications in one Smartcard often requires code and data separation in order to prevent that one application can access code and/or data of another application. For this reason the TOE provides Area based Memory Access Control. The underlying memory management unit (MMU) is documented in section 4 in the hardware reference manual HRM [1].
The security service being provided is described in the Security Function Policy (SFP) **Memory Access Control Policy**. The security functional requirement **"Subset access control (FDP_ACC.1)"** requires that this policy is in place and defines the scope were it applies. The security functional requirement **"Security attribute based access control (FDP_ACF.1)"** defines security attribute usage and characteristics of policies. It describes the rules for the function that implements the Security Function Policy (SFP) as identified in FDP_ACC.1. The decision whether an access is permitted or not is taken based upon attributes allocated to the software. The Smartcard Embedded Software defines the attributes and memory areas. The corresponding permission control information is evaluated "on-the-fly" by the hardware so that access is granted/effective or denied/inoperable.
The security functional requirement **"Static attribute initialization (FMT_MSA.3)"** ensures that the default values of security attributes are appropriately either permissive or restrictive in nature. Alternative values can be specified by any subject provided that the **Memory Access Control Policy** allows that. This is described by the security functional requirement **"Management of security attributes (FMT_MSA.1)"**. The attributes are determined during TOE manufacturing (FMT_MSA.3) or set at run-time (FMT_MSA.1).
From TOE's point of view the different roles in the Smartcard Embedded Software can be distinguished according to the memory based access control. However the definition of the roles belongs to the user software.
The following Security Function Policy (SFP) **Memory Access Control Policy** is defined for the requirement "Security attribute based access control (FDP_ACF.1)":

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

The 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 information is given in the confidential Security Target [8].

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

FDP_ACC.1	**Subset access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1	The TSF shall enforce the *Memory Access Control Policy* on *all subjects (software running at the defined and assigned privilege levels), all objects (data including code stored in memories) and all the operations defined in the Memory Access Control Policy, i.e. privilege levels*.

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

FDP_ACF.1	**Security attribute based access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1	The TSF shall enforce the *Memory Access Control Policy* to objects based on the following: *Subject*: *- software running at the IFX, OS1 and OS2 privilege levels required to securely operate the chip. This includes also privilege levels running interrupt routines.* *- software running at the privilege levels containing the application software* *Object*: *- data including code stored in memories* *Attributes*: *- the memory area where the access is performed to and/or* *- the operation to be performed*.
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *evaluate the corresponding permission control information of the relevant memory range before and during the access so that accesses to be denied cannot be utilized by the subject attempting to perform the operation*.
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none*.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the *following additional rules: none*.

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

FMT_MSA.3	**Static attribute initialisation**
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the *Memory Access Control Policy* to provide *well defined*[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

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 chapter 7.4.1.1.
The following additional specific security functionality is implemented in the TOE:

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

The RSA cryptographic library is offered in two parts: The 2k part of the RSA library can be used for key lengths of up to 2048 + 64 bits and the 4k part of the RSA library can be used for key lengths of up to 4096 + 128 bits. The additional function of the EC library, providing the primitive elliptic curve operations, does not add specific security functionality.

Note 10:
This TOE can come with both crypto co-processors accessible, or with a blocked SCP or with a blocked Crypto2304T, or with both crypto co-processors blocked. The blocking depends on the customer demands prior to the production of the hardware. In case the SCP is blocked, no AES and DES computation supported by hardware is possible. In case the Crypto2304T is blocked, no RSA and EC computation supported by hardware is possible. No accessibility of the deselected cryptographic co-processors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic co-processors.
End of note.

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

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 [22] Section 9, Para.4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context.
Therefore, for these functions it shall be checked whether the related cryptographic operations are appropriate for the intended system. Some further hints and guidelines can be derived from the "Technische Richtlinie BSI TR-02102", www.bsi.bund.de.
Any cryptographic functionality that is marked in the column "Security level above 100 Bits" of the following table with a "no" achieves a security level of lower than 100 Bits (in general context).

Table 17 Cryptographic TOE Functionality

Cryptographic Mechanism	Standard Reference	Key size in Bits to input	Security level above 100 Bits
TDES	[17], [18], [29], [31]	|k| = 168 in operating mode: CBC	Yes
	[17], [18], [29], [31]	|k| = 168 plus key length for ELB in operating mode: CBC-MAC-ELB	Yes
	[17], [18], [29], [31]	|k| = 168 in operating mode: CBC-MAC	No
	[18], [29]	|k| = 168 in operating mode: ECB	No
	Proprietary	|k| = 168 BLD mode	No
AES	[18], [29], [30], [31]	|k| = 128, 192, 256 in operating modes: CBC, CBC-MAC	Yes
	[18], [29], [30], [31]	|k| = 128, 192, 256 plus the key length for ELB in operating mode: CBC-MAC—ELB	Yes
	[18], [29], [30]	|k| = 128, 192, 256 in operating mode: ECB	No
	Proprietary	|k| = 128, 192, 256 BLD mode	No
	Proprietary	|k| = 128 Recrypt mode (AES)	Yes
Flash Loader	[29], [23]	AES in PCBC mode |k| = 128	Yes
Hybrid Physical True Random Number Generation	[13]	n.a.	n.a.

Cryptographic Mechanism	Standard Reference	Key size in Bits to input	Security level above 100 Bits
RSA encryption / decryption/ key generation /signature generation / verification (only modular exponentiation part)	[19], [27]	Modulus length = 1976 – 4096 The 2k part of the RSA library can be used for key lengths of up to 2048 + 64 bits. The 4k part of the RSA library can be used for key lengths of up to 4096 + 128 bits.	Yes
ECDH	[16], [21], [24], [26], [27]	Key sizes of 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits [24] ➔P-{224, 256, 384, 521}, K-{233, 409}, B-{233, 283, 409} [16] ➔ lP {224,256,320,384,512}r1, P{224,256,320,384,512}t1	Yes
ECDH	[16], [21], [24], [26], [27]	Key sizes of 160, 163, and 192 [24] ➔ P-192, K-163 [16] ➔lP{160, 192}r1, lP{160, 192}t1	No
ECDSA key generation	[16], [20], [24], [25], [27]	Key sizes of: 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits [24] ➔ P-{224, 256, 384, 521}, K-{233, 409}, B-{233, 283, 409} [16] ➔ lP{224,256,320,384,512}r1, lP{224,256,320,384,512}t1	Yes
ECDSA key generation	[16], [20], [24], [25], [27]	Key sizes of 160, 163, and 192 [24] ➔ P-192, K-163 [16] ➔ lP{160, 192}r1, lP{160, 192}t1	No
ECDSA signature generation	[16], [20], [24], [25], [27]	Key sizes of: 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits [24] ➔ P-{224, 256, 384, 521}, K-{233, 409}, B-{233, 283, 409} [16] ➔ lP{224,256,320,384,512}r1, lP{224,256,320,384,512}t1 [20] ➔ According to section 7.3	Yes
ECDSA signature generation	[16], [20], [24], [25], [27]	Key sizes of 160, 163, and 192 [24] ➔ P-192, K-163 [16] ➔ lP{160, 192}r1, lP{160, 192}t1 [20] ➔ According to section 7.3	No

Cryptographic Mechanism	Standard Reference	Key size in Bits to input	Security level above 100 Bits
EDCSA signature verification	[16], [20], [24], [25], {27]	Key sizes of: 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits [24] ➔ P-{224, 256, 384, 521}, K-{233, 409}, B-{233, 283, 409} [16] ➔ lP{224,256,320,384,512}r1, lP{224,256,320,384,512}t1 [20] ➔ According to section 7.3	Yes
EDCSA signature verification	[16], [20], [24], [25], [27]	Key sizes of 160, 163, and 192 [24] ➔ P-192, K-163 [16] ➔ lP{160, 192}r1, lP{160, 192}t1 [20] ➔ According to section 7.3	No

7.1.4.2 Triple-DES Operation

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

FCS_COP.1/TDES	Cryptographic operation
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data of the Composite TOE without security attributes, or FDP_ITC.2 Import of user data of the Composite TOE with security attributes, or FCS_CKM.1 Cryptographic key management] FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1.1/TDES	The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *TDES in* • *the Electronic Codebook Mode (ECB)* • *the Cipher Block Chaining Mode (CBC)* • *the Cipher Block Chaining Message Authentication Code (CBC-MAC)* • *the Cipher Block Chaining Message Authentication Code Encrypt Last Block (CBC-MAC-ELB)* • *the Blinding Mode (BLD)* • *the Recrypt Mode* and cryptographic key sizes of *168 bit* that meet the following standards: • *National Institute of Standards and Technology (NIST) 800-67 Rev. 1 [17]* • *ISO/IEC 18033-3 [29]* • *ECB, CBC:* *National Institute of Standards and Technology (NIST) SP 800-38A [18]* • *CBC-MAC, CBC-MAC-ELB:* *ISO/IEC 9797-1 Mac Algorithm 1 and 2 respectively [31]* • *BLD, Recrypt Mode* *Proprietary, description given in the hardware reference manual HRM [1]*

Note 11:
The BLD and Recrypt operation modes are described in the hardware reference manual HRM [1] while the implementations of the other modes follow the referenced standards. Also the BLD is compliant to the referenced standards but is operated in a masked way.
End of note.

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

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

7.1.4.3 AES Operation

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

FCS_COP.1/AES	Cryptographic operation
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data of the Composite TOE without security attributes, or FDP_ITC.2 Import of user data of the Composite TOE with security attributes, or FCS_CKM.1 Cryptographic key 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* • *the Electronic Codebook Mode (ECB)* • *the Cipher Block Chaining Mode (CBC)* • *the Cipher Block Chaining Message Authentication Code (CBC-MAC)* • *the Cipher Block Chaining Message Authentication Code Encrypt Last Block (CBC-MAC-ELB)* • *the Blinding Mode (BLD)* • *the Recrypt Mode* and cryptographic key sizes *of 128 bit or 192 bit or 256 bit* that meet the following standards: • *ISO/IEC 18033-3 [29]* • *FIPS 197 [30]* • *ECB, CBC:* *National Institute of Standards and Technology (NIST) SP 800-38A [18]* • *CBC-MAC, CBC-MAC-ELB:* *ISO/IEC 9797-1 Mac Algorithm 1 and 2 respectively [31]* • *BLD, Recrypt Mode* *Proprietary, description given in the hardware reference manual HRM [1]*

Note 13:
The BLD and Recrypt operation modes are described in the hardware reference manual HRM [1] while the implementations of the other modes follow the referenced standards. Also the BLD is compliant to the referenced standards but is operated in a masked way.
End of note.

FCS_CKM.4/AES	**Cryptographic key destruction – AES**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM4.1/AES	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwriting or zeroing* that meets the following:
Dependencies:	*None*

Note 14:
The key destruction can be done by overwriting the key register interfaces or by software reset of the SCP which provides immediate zeroing of all SCP key registers.
End of Note.

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**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data of the Composite TOE without security attributes, or FDP_ITC.2 Import of user data of the Composite TOE with security attributes] 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 bits* that meet the following: ***Encryption:*** *1. According to section 5.1.1 RSAEP in PKCS [19]:* • *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 [19] 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) 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 [19] 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 [19]:* *supported for n < $2^{4096+128}$* • *5.2.2(1) not supported* *2. According to section 8.2.5 IEEE [27]:* • *Supported for n < $2^{4096+128}$* • *8.2.5(1) not supported*

Please consider also the statement of chapter 7.1.4.1.

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)".

The RSA cryptographic library is offered in two parts: The 2k part of the RSA library can be used for key lengths of up to 2048 + 64 bits and the 4k part of the RSA library can be used for key lengths of up to 4096 + 128 bits.

FCS_CKM.1/RSA	Cryptographic key generation
Hierarchical to:	No other components.
Dependencies:	FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes
FCS_CKM.1.1/RSA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *implemented by following functions:* • *CryptoRSAKeyGenMask_CRT plus CryptoGeneratePrimeMask* • *CryptoRSAKeyGenMask_D plus CryptoGeneratePrimeMask* • *CryptoRSAKeyGenMask_N plus CryptoGeneratePrimeMask* and specified cryptographic key sizes of *1976– 4096 bits* that meet the following*:* *1. According to sections 3.1 and 3.2 in PKCS [19], 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 < $2^{4096+128}$* *3. 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 < $2^{2048+128}$*

Note 15:
The minimum key length of 1976 follows the national recommendations by the BSI. The key length requirements can differ between the countries.
End of note.

Note 16:
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.
End of note.

Note 17:
The TOE can be delivered with or without the RSA library. In the case of coming without the RSA library the TOE does not provide the Additional Specific Security Functionality Rivest-Shamir-Adleman Cryptography (RSA) realized with the security functional requirements FCS_COP.1/RSA and FCS_CKM.1/RSA. In case of a blocked Crypto2304T the optionally delivered cryptographic and the supporting Toolbox cannot be used in that TOE product.
End of note.

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 Brainpool [16] and NIST [24] Elliptic Curves with key lengths of 224, 233, 256, 283, 320, 384, 409, 512 and 521 Bits. The definition of the key lengths follows the national AIS32 regulation regarding the 100 bit security level by the BSI. The former 80 bit level is achieved by the key lengths of 160, 163, and 192 Bits. 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 $p \in \left[2^{41-1};\ 2^{521}\right]$ 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) operation

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**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data of the Composite TOE without security attributes, or FDP_ITC.2 Import of user data of the Composite TOE with security attributes] 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 *224, 233, 256, 283, 320, 384, 409, 512 or 521 bits* that meet the following: ***ECDSA Signature Generation:*** *1. According to section 7.3 Signing Process in ANSI [20]* • *Step d) and e) are 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 sections 6.4.3 Signature Process in ISO/IEC [25]* • *Chapter 6.4.3.3 is not supported* • *Chapter 6.4.3.5 is not supported* ○ *the hash-code of H of the message has to be provided by the caller as input for our function.* • *Chapter 6.4.3.7 is not supported* *Chapter 6.4.3.8 is not supported* *3. According to section 7.2.7 ECSP-DSA in IEEE [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* ***Signature Verification:*** *1. According to section 7.4.1 in ANSI [20]* • *Step b) and c) are 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 BasepointerOrder n to the calculated values u1 and u2.* *2. According to sections 6.4.4 Signature Verification Process in ISO/IEC [25]* • *Chapter 6.4.4.2 is not supported* • *Chapter 6.4.4.3 is 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 [27].*

Note 18:
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.
End of note.

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**
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 *implemented by following functions which can be used independently of each other:* • *ECC_ECDSAKeyGen* • *ECC_ECDSAKeyGenMask* *specified in [20], [25] and [27]* and specified cryptographic key sizes *224, 233, 256, 283, 320, 384, 409, 512 or 521 bits* that meet the following: ECDSA *Key Generation:* *1. According to the appendix "A4.3 Elliptic Curve Key Pair Generation" in ANSI [20]:* *The optional cofactor h is not supported.* *2. According to section "6.4.2 Generation of signature key and verification key" in ISO/IEC [25].* *3. According to appendix "A.16.9 An algorithm for generating EC keys" in IEEE [27]*

Note 19:
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.
End of note.

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.

FCS_COP.1/ECDH	Cryptographic operation
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data of the Composite TOE without security attributes, or FDP_ITC.2 Import of user data of the Composite TOE with security attributes, or FCS_CKM.1 Cryptographic key 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 *224, 233, 256, 283, 320, 384, 409, 512 or 521 bits* that meet the following: *1. According to section "5.4.1 Standard Diffie-Hellman Primitive" in ANSI [21]* *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 "Appendix D.6 Key agreement of Diffie-Hellman" type in ISO/IEC [26]* *The function enables the operations described in appendix D.6* *3. According to section "7.2.1 ECSVHDP-DP" in IEEE [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 20:
The certification covers the standard Brainpool [16] and NIST [24] Elliptic Curves with key lengths of 224, 233, 256, 283, 320, 384, 409, 512 or 521 Bits, 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.
End of note

Note 21:
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.
End of note.

Note 22:
The TOE can be delivered with or without the EC library. In the case the TOE comes without, it does not provide the Additional Specific Security Functionality Elliptic Curve Cryptography realized with the security functional requirements FCS_COP.1/ECSA, FCS_COP.1/ECDH and FCS_CKM.1/EC. In case of a blocked Crypto2304T, the RSA and EC cryptographic library cannot be used. In case of a blocked Crypto2304T the optionally delivered cryptographic RSA and EC, as well as the supporting Toolbox cannot be used in that TOE product.
End of note.

Note 23:
The EC primitives allow the selection of various curves. The selection of the curves depends to the user.
End of note.

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 *of the Composite TOE stored in containers* controlled by the TSF for *inconsistencies between stored data and corresponding EDC* on all objects, based on the following attributes: *EDC value for the RAM, ROM and SOLID FLASH™ NVM*.

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

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

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

FDP_SDC.1	**Stored data confidentiality**
Hierarchical to:	No other components
Dependencies:	No dependencies
FDP_SDC.1.1	The TSF shall ensure the confidentiality of the information of the user data *of the Composite TOE* while it is stored in the *RAM, ROM, Cache and SOLID FLASH™ NVM.*

7.2 Support of the Flash Loader

The TOE provides the Flash Loader to download user data into the SOLID FLASH™ NVM, either during production of the TOE or at customer site. The Flash Loader is dedicated for usage by authorized users only in secured and insecure environment during the production up to "Phase 6 Security IC Personalisation".
The Flash Loader has to be permanently deactivated before entering "Phase 7 Security IC end-usage".
For this reason the TOE shall meet the requirements as defined and described in the PP [9] section "7.3 Packages for Loader" and "7.2 Package "Authentication of the Security IC":

- "Limited capabilities (FMT_LIM.1/Loader)",
- "Limited availability – Loader (FMT_LIM.2/Loader)",
- "Authentication Proof of Identity (FIA_API.1)",
- "Inter-TSF trusted channel (FTP_ITC.1)",
- "Basic data exchange confidentiality (FDP_UCT.1)",
- "Data exchange integrity (FDP_UIT.1)",
- "Subset access control – Loader (FDP_ACC.1/Loader)" and

- "Security attribute based access control – Loader (FDP_ACF.1/Loader)"

as defined in the PP [9], section 7.2 and 7.3.

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

- Loader SFP:
  provides the mutual authentication between the TOE and the administrator user or download operator user and the download of the user data into the memory of the TOE.

- The Flash Loader supports the following two subjects:
  - Administrator user:
    is enabled performing mutual authentication with the keys Kc and Kd, to manage (set, exchange, delete) the keys Kc, Kd and Kfdi and to process the download of the user data into the memory of the TOE.
  - Download operator user:
    is enabled performing mutual authentication with Kd, to exchange the key Kd and to perform the download of the user data into the memory of the TOE. He can also delete Kfdi.

- The Flash Loader supports the following object:
  - User data:
    Data loaded into the memory of the TOE.

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

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

The TOE shall meet the requirement "Limited availability – Loader (FMT_LIM.2/Loader)" as specified below:

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 "Limited availability – Loader (FIA_API.1)" as specified below:

FIA_API.1	**Authentication Proof of Identity**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide an *authentication mechanism according to [33] ISO/IEC 9798-2 section 6.2.2 Mechanism 4: Three-path authentication based on the security attributes (keys) Kc or Kd.*

Additional requirement to the environment with regard to GBIC: If the GBIC process is to be applied, the keys Kc, Kd and Kfdi shall be generated with sufficient entropy considering the requirements by GBIC as outlined in section 10 Annex to prove the identity of the TOE to an external entity.

The TOE shall meet the requirement "Limited availability – Loader (FTP_ITC.1)" as specified below:

FTP_ITC.1	**Inter-TSF trusted channel**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and the *administrator user, enabled performing mutual authentication with the keys Kc and Kd, to manage (set, exchange, delete) the keys Kc, Kd and Kfdi and to process the download of the user data into the memory of the TOE and the Download operator user, enabled performing mutual authentication with Kd, to exchange the key Kd, to perform the download of the user data into the memory of the TOE and to delete Kfdi* that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit *another trusted IT product* to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for *deploying Loader for downloading user data.*

The TOE shall meet the requirement "Limited availability – Loader (FDP_UCT.1)" as specified below:

FDP_UCT.1	**Basic data exchange confidentiality**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_UCT.1.1	The TSF shall enforce the *Loader SFP* to *receive* user data in a manner protected from unauthorised disclosure.

The TOE shall meet the requirement "Limited availability – Loader (FDP_UIT.1)" as specified below:

FDP_UIT.1	**Data exchange integrity**
Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control].
FDP_UIT.1.1	The TSF shall enforce the *Loader SFP* to *receive* user data in a manner protected from *modification, deletion or insertion* errors.
FPP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether *modification, deletion or insertion* have occurred.

The TOE shall meet the requirement "Limited availability – Loader (FDP_ACC.1/Loader)" as specified below:

FDP_ACC.1/Loader	**Subset access control - Loader**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control.
FDP_ACC.1.1/Loader	The TSF shall enforce the *Loader SFP* on *(1) The subjects* *Administrator user, enabled performing mutual authentication with the keys Kc and Kd, to manage (set, exchange, delete) the keys Kc, Kd and Kfdi and to process the download of the user data into the memory of the TOE and the Download operator user, enabled performing mutual authentication with Kd, to exchange the key Kd, to perform the download of the user data into the memory of the TOE and to delete Kfdi,* *(2) The objects* *User data, data loaded into the memory of the TOE, in SOLID FLASH™ NVM,* (3) *The operation deployment of the Loader.*

Additional requirement to the environment with regard to GBIC: If the GBIC process is to be applied, the keys Kc, Kd and Kfdi shall be generated with sufficient entropy considering the requirements by GBIC as outlined in section 10 Annex to prove the identity of the TOE to an external entity.

The TOE shall meet the requirement "Limited availability – Loader (FTP_ACF.1/Loader)" as specified below:

FDP_ACF.1/Loader	**Security attribute based access control - Loader**
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/Loader	The TSF shall enforce the *Loader SFP* to objects based on the following: *(1) the subjects Administrator user, enabled performing mutual authentication with the keys Kc and Kd, to manage (set, exchange, delete) the keys Kc, Kd and Kfdi and to process the download of the user data into the memory of the TOE with security attributes key Kc and* *the Download operator user, enabled performing mutual authentication with Kd, to exchange the key Kd, to perform the download of the user data into the memory of the TOE with security attributes Key Kd and to delete Kfdi,* *(2) the objects User data, data loaded into the memory of the TOE in the*

	SOLID FLASH™ NVM with security attributes key Kfdi.
FDP_ACF.1.2/Loader	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *(1) evaluate the corresponding access control information of the relevant subject, administrator user and download operator user, before the access, so that accesses to be denied cannot be utilized by the subject attempting to perform the operation. The subsequent download is then protected by the key Kfdi.*
FDP_ACF.1.3/Loader	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: None
FDP_ACF.1.4/Loader	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: None

Note 24:
Regarding FDP_ACF.1.4/Loader it is added in the User Guidance that the Flash Loader has to be permanently deactivated prior delivery to the end-user.
End of note.

Note 25:
The security functional requirements FMT_LIM.1/Loader, FMT_LIM.2/Loader, FIA_API.1, FTP_ITC.1, FDP_UCT.1, FDP_UIT.1, FDP_ACC.1/Loader and FDP_ACF.1/Loader apply only at TOE products coming with activated Flash Loader enabled for user data download. In other cases the Flash Loader is not available anymore and the user 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 permanent locking of the Flash Loader after finalizing the download and prior delivery to the end-user is added to package 2 with LIM1/Loader and FMT_LIM.2/Loader.
End of note.

7.3 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 [9] is expressed with bold letters.

Table 18 Assurance Components

Aspect	Acronym	Description	Refinement
Development	ADV_ARC.1	Security Architecture Description	In PP [9]
	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 [9]
	AGD_PRE.1	Preparative procedures	in PP [9]
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 [9]
	ALC_DVS.2	Sufficiency of security measures	in PP [9]
	ALC_LCD.1	Developer defined life-cycle model	
	ALC_TAT.3	**Compliance with implementation standards – all parts**	
	ALC_FLR.1	**Basic Flaw Remediation**	
Security Target Evaluation	ASE_CCL.1	Conformance claims	
	ASE_ECD.1	Extended components definition	
	ASE_INT.1	ST introduction	
	ASE_OBJ.2	Security objectives	
	ASE_REQ.2	Derived security requirements	
	ASE_SPD.1	Security problem definition	
	ASE_TSS.1	TOE summary specification	
Tests	**ATE_COV.3**	**Rigorous analysis of coverage**	In ST
	ATE_DPT.3	**Testing: modular design**	
	ATE_FUN.2	**Ordered functional testing**	
	ATE_IND.2	Independent testing – sample	
Vulnerability Assessment	AVA_VAN.5	Advanced methodical vulnerability testing	in PP [9]

7.3.1 Refinements

Some refinements are taken unchanged from the PP [9]. In some cases a clarification is necessary. In Table 17 an overview is given where the refinement is done.
The refinements from the PP [9] have to be discussed here in the Security Target, as the assurance level is increased. The refinements from the PP [9] are included in the chosen assurance level EAL 6 augmented with ALC_FLR.1.

7.3.1.1 *Development (ADV)*

ADV_IMP Implementation Representation:
The refined assurance package ADV_IMP.1 implementation representation of the TSF requires the availability of the entire implementation representation, a mapping of the design description to the implementation representation with a level of detail that the TSF can be generated without further design decisions. In addition, the correspondence of design description and implementation representation shall be demonstrated.
The covered higher assurance package ADV_IMP.2 requires a complete and not curtailed mapping of the implementation representation of the TSF, and the mapping of the design description to the entire implementation representation. In addition, the correspondence of design description and the implementation representation shall be demonstrated. The ADV_IMP.1 aspect and refinement remains therefore valid. The enhancement underlines the refinement in the PP [9] and by that the entirely complete design i.e. not curtailed representation with according mapping was provided, demonstrated and reviewed.

ADV_INT TSF Internals:
The assurance package ADV_INT.2 well-structured internals is extended to ADV_INT.3 minimally complex internals requiring the documentation to minimally complex internals with the intension that the entire TSF has been designed and implemented using sound engineering principles. The ADV_INT.2 aspect remains applicable as well structured internals are fundamental for achieving sound engineering principles. ADV_INT.2 and its refinements in the PP [9] remain therefore valid. The assurance and evidence was provided accordingly.
ADV_FSP Functional Specification:
The ADV_FSP.4 package requires a functional description of the TSFIs and there assignment to SFR-enforcing, SFR-supporting, SFR-non-interfering, including related error messages, the assurance package. The enhancement of ADV_FSP.5 requires additionally a complete semi-formal functional specification with additional error information. In addition the package includes a tracing from the functional specification to the SFRs, as well as the TSFIs descriptions including error messages not resulting from an invocation of a TSFI. These aspects from ADV_FSP.5 are independent from the ADV_FSP.4 refinements from the PP [9] but constitute an enhancement of it. By that the aspects of ADV_FSP.4 and its refinement in the PP [9] apply also here. The assurance and evidence was provided accordingly.

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

ADV_SPM.1	Formal TOE security policy model
Hierarchical to:	No other components
Dependencies:	ADV_FSP.4 Complete function description
ADV_SPM.1.1D	The developer shall provide a formal security policy model for the *Memory Access Control Policy and the corresponding SFRs* • *FDP_ACC.1 Subset Access Control* • *FDP_ACF.1 Security attribute based access control* • *FMT_MSA.1 Management of Security Attributes* • *FMT_MSA.3 Static Attribute Initialization.* *Moreover, the following SFRs shall be addressed by the formal security policy model:* • *FDP_SDI.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.

ADV_TDS TOE Design:
The assurance package ADV_TDS.4 Semiformal modular design is extended to ADV_TDS.5 Complete semiformal modular design requires the complete semiformal design description. As the package ADV_TDS.5 is an enhancement of ADV_TDS.4 the package and its refinements in the PP [9] remain valid. The assurance and evidence was provided accordingly.

ALC_DEL Delivery Procedure
Considering the GBIC requirement as outlined in section 10 Annex this assurance class is refined with the confirmation that the delivery process of the Flash Loader keys - as referenced in the section 10 Annex - is separated from the chip delivery to the user.

7.3.1.2 *Life-cycle Support (ALC)*

ALC_CMS Configuration Management Scope:
The Security IC embedded firmware and the optional software are part of TOE and delivered together with the TOE as the firmware and optional software are stored in the ROM and/or SOLID FLASH™ NVM. The presence of the optional parts belongs to the user order. Both, the firmware and software delivered with the TOE are controlled entirely by Infineon Technologies. In addition, the TOE offers the possibility that the user can download his software at his own premises. These parts of the software are user controlled only and are not part of this TOE. The download of this solely user controlled software into the SOLID FLASH™ NVM is protected by strong authentication means. In addition, the download itself could also be encrypted. By the augmentation of ALC_CMS.4 to ALC_CMS.5 the configuration list includes additional the development tools. The package ALC_CMS.5 is therefore an enhancement to ACL_CMS.4 and the package with its refinement in the PP [9] remains valid. The assurance and evidence was provided accordingly.

ALC_CMC Configuration Management Capabilities:
The PP refinement from the assurance package ALC_CMC.4 Production support, acceptance procedures and automation points out that the configuration items comprise all items defined under ALC_CMS to be tracked under configuration management. In addition a production control system is required guaranteeing the traceability and completeness of different charges and lots. Also the number of wafers, dies and chips must be tracked by this system as well as procedures applied for managing wafers, dies or complete chips being removed from the production process in order to verify and to control predefined quality standards and production parameters. It has to be controlled that these wafers, dies or assembled devices are returned to the same production stage from which they are taken or they have to be securely stored or destroyed otherwise.
The additionally covered extended package of ALC_CMC.5 Advance Support requires advanced support considering the automatisms configuration management systems, acceptance and documentation procedures of changes, role separation with regard to functional roles of personnel, automatisms for tracking and version controlling in those systems, and includes also production control systems. The additional aspects of ADV_CMC.5 constitute an enhancement of ACL_CMC.4 and therefore the aspects and ACL_CMC.4 refinements in the PP [9] remain valid. The assurance and evidence was provided.

ALC_DVS Development Security:
The assurance package ALC_DVS.1 identification of security measures is extended to ALC_DVS.2 requiring the evidence of sufficiency of security measures. The evidence was given and reviewed that the design and implementation and its development environment is protected with regard to confidentiality and integrity. The ALC_DVS.2 package is an enhancement of ALC_DVS.1. Therefore, this package and its refinement in the PP [9] remain valid. The assurance and evidence was provided accordingly.
Considering the GBIC requirements as outlined in section 10 this assurance class is refined with the confirmation that the:

- keys are generated with sufficient entropy
- the keys are stored within a HSM as integral part of the vendor environment
- the keys are stored in the non-volatile memory of the chip

ALC_DEL Delivery Procedure
Considering the GBIC requirements, this assurance class is refined with the confirmation that the delivery process of the Flash Loader keys for the users - as referenced in the section 10 - is separated from the chip respectively goods delivery to the user.

ALC_TAT Tools and Techniques:
The assurance package ALC_TAT.2 Compliance with implementation standards is extended to ALC_TAT.3 Compliance with implementation standards - all parts requiring that all implemented parts are compliant to implementation standards. The evidence has been given that all parts have been developed and implemented according to implementation standards, processes and rules.

7.3.1.3 *Tests (ATE)*

ATE_COV Test Coverage:
The PP refined assurance package ATE_COV.2 Analysis of coverage addresses the extent to which the TSF is tested, and whether or not the testing is sufficiently extensive to demonstrate that the TSF operates as specified. It includes the test documentation of the TSFIs in the functional specification. In particular the refinement requires that The TOE must be tested under different operating conditions within the specified ranges. In addition, the existence and effectiveness of mechanisms against physical attacks should be covered by evidence that the TOE has the particular physical characteristics. This is furthermore detailed in the PP [9].
This assurance package ATE_COV.2 has been enhanced to ATE_COV.3 to cover the rigorous analysis of coverage. This requires the presence of evidence that exhaustive testing on rigorous entirely all interfaces as documented in the functional specification was conducted. By that ATE_COV.2 and refinements as given in the PP [9] 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.

ATE_FUN Functional Tests:
The assurance package ATE_FUN.1 Functional testing is extended to ATE_FUN.2 Ordered functional testing requiring which means to include considerations of dependency aspects. The package ATE_FUN.2 is an enhancement to ATE_FUN.1 in terms of describing dependencies and sequences of the functional testing documented with ATE_FUN.1. Therefore, the refinements in the PP [9] remain valid. The testing systems, processes and tooling have been analyzed and reviewed with regard to intrinsic dependencies.

7.3.1.4 *AVA_VAN Vulnerability Analysis*

The assurance package AVA_VAN remains unchanged compared to the forerunner processes and requires advanced methodical vulnerability analysis.

7.4 Security Requirements Rationale

7.4.1 Rationale for the Security Functional Requirements

The objectives O.Authentication and OE.TOE_Auth are discussed in the PP [9] chapter 7.2.1.
The objectives O.Cap_Avail_Loader and OE.Lim_Block_Loader and the covering security functional requirements FMT_LIM.1/Loader and FMT_LIM.2/Loader are discussed in the PP [9] chapter 7.3.1.
The policy P.Ctrl_Loader and the objectives O.Ctrl_Auth_Loader and OE.Loader_usage are discussed in the PP [9] chapter 7.3.2.
The objective O.Add-Function enables to include additional functionality which is used here to include the organizational policy P.Crypto-Service with the extended objectives O.TDES and O.AES. These extended objectives are discussed also in the PP [9] see chapters 7.4.1 to 7.4.3.
The additional objectives O.Prot_TSF_Confidentiality is defined in chapter 5.1 and 5.3 in this document.
PP [9] chapter 6.1 includes also the definition of FDP_SDI.2 „Stored data integrity monitoring and action".
While the above mentioned security functional requirements rationale of the TOE are defined and described in PP [9] section 6.3.1, the additional introduced SFRs are listed and discussed below:

Table 19 Rational for additional SFR in the ST

Objective	TOE Security Functional Requirements
O.Add-Functions	FCS_COP.1/RSA „Cryptographic operation" FCS_COP.1/ECDSA „Cryptographic operation" FCS_COP.1/ECDH „Cryptographic operation" FCS_CKM.1/RSA „Cryptographic key generation " FCS_CKM.1/EC „Cryptographic key generation"
O.Phys-Manipulation	FPT_TST.2 „Subset TOE security testing"
O.Mem-Access	FDP_ACC.1 "Subset access control" FDP_ACF.1 "Security attribute based access control" FMT_MSA.3 "Static attribute initialisation" FMT_MSA.1 "Management of security attributes" FMT_SMF.1 "Specification of Management Functions"
O.Malfunction	FDP_SDI.1 „Stored data integrity monitoring"
O.RND	FCS_RNG.1/TRNG "Generation of Random Numbers -TRNG" FCS_RNG.1/HPRG "Generation of Random Numbers - HPRG" FCS_RNG.1/DRNG "Generation of Random Numbers -DRNG" FCS_RNG.1/KSG "Generation of Random Numbers - KSG"
O.Prot_TSF_Confidentiality	FTP_ITC.1 "Inter-TSF-trusted channel" FDP_ACC.1/Loader "Subset access control –Loader" FDP_ACF.1/Loader "Security attribute based access control – Loader"

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 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/EC are suitable to meet the security objective.

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

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

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

All these requirements have to be fulfilled to support OE.Resp-Appl for FCS_COP.1/TDES (DES algorithm) and for FCS_COP.1/AES (AES algorithm).
The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced define how to implement the specific security functionality. However, key-dependent functions could be implemented in the Smartcard Embedded Software.

The usage of cryptographic algorithms requires the use of appropriate keys. Otherwise these cryptographic functions do not provide security. The keys have to be unique with a very high probability, and must have a certain cryptographic strength etc. In case of a key import into the TOE (which is usually after TOE delivery) it has to be ensured that quality and confidentiality are maintained. Keys for DES and AES are provided by the environment. 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 justification related to the security objective "Protection against Physical Manipulation (O.Phys-Manipulation)" is as follows:
The security functional requirement FPT_TST.2 will detect attempts to conduce a physical manipulation on the monitoring functions of the TOE. The objective of FPT_TST.2 is O.Phys-Manipulation. The physical manipulation will be tried to overcome security enforcing functions.

The security functional requirement "Subset access control (FDP_ACC.1)" with the related Security Function Policy (SFP) "Memory Access Control Policy" exactly require the implementation of an area based memory

access control as required by O.Mem-Access. The related TOE security functional requirements FDP_ACC.1, FDP_ACF.1, FMT_MSA.3, FMT_MSA.1 and FMT_SMF.1 cover this security objective. The implementation of these functional requirements is represented by the dedicated privilege level concept.

The justification of the security objective and the additional requirements show that they do not contradict to the rationale already given in the Protection Profile for the assumptions, policy and threats defined there. Moreover, these additional security functional requirements cover the requirements by the PP [9] user data of the Composite TOE protection of chapter 1.2.5 claim 35 and 36 which are not refined by the PP [9]. Nevertheless, the developer of the Smartcard Embedded Software must ensure that the additional functions are used as specified and that the User data of the Composite TOE processed by these functions are protected as defined for the application context. The TOE only provides the tool to implement the policy defined in the context of the application.

The justification related to the security objective "Protection against Malfunction due to Environmental Stress (O.Malfunction)" is as follows:
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 malfunction of the TOE using corrupt data is prevented. Therefore FDP_SDI.1 is suitable to meet the security objective.
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.. Therefore FDP_SDI.2 is suitable to meet the security objective O.Phys-Manipulation.

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 [9] chapter 5.1. The requirement implements a quality metric which is defined by national regulations. The implemented random number generation fulfils the definitions of AIS 31 [13] 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 CC part 2 defines the component FIA_SOS.2, which is similar to FCS_RNG.1, as follows:

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

The justification related to the Flash Loader security objectives are as follows. Note that the following objectives and related rationales apply only at TOE products coming with activated Flash Loader enabled for software or data download by the user. In other cases the Flash Loader is not available anymore and the user data download is completed. Depending on the capabilities of the user software these security functional requirements may then reoccur as subject of the composite TOE.
The Flash Loader related objectives are:

The objective O.Authentication requires the presence of an authentication mechanism proving the identity of a given security IC to an external entity. This objective is covered by the functional requirement FIA_API

Authentication Proof of Identity. The Flash Loader implements this functionality and outputs identification data to external requesting entity. The user guidance describes in more detail how this authentication request is applied and conducted by the external entity. As the functional requirements are met by the Flash Loader the objective is covered.

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 irreversibly terminates 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 objectives O.Ctrl_Auth_Loader and O.Prot_TSF_Confidentiality require that a trusted communication channel with an authorized user, a confidentiality protection during the download and authentication of the user data and access control for the usage of the Loader functionality are provided by the Loader.
Without successfully passing the authentication functionality of the Flash Loader no usage of the Flash Loader is possible. Passing the authentication successfully assigns also a user role to the current user.
The Flash Loader implements mutual authentication functionality and if successfully passing this mutual authentication, the TOE and the external user are established as trusted entities. Furthermore, the Flash Loader enforces the exchange of the download key by the user which provides clear separation from the hardware vendor and preserves confidentiality of the user data download. In addition, the Flash Loader preserves the integrity of the downloaded data against for example induced errors by hashing functionality.
As the functional requirements are met by the Flash Loader the objective is covered.

7.4.1.1 Dependencies of Security Functional Requirements

The dependencies of the security functional requirements are defined and described in PP [9] section 6.3.2, with FDP_SDI.2, and with regard to the Flash Loader related security functional requirements, the description is given at the individual package chapters 7.2.3, 7.3.1 and 7.3.2.

FDP_ITT.1	FDP_IFC.1	FPT_ITT.1	FPT_PHP.3	FPT_FLS.1
FRU_FLT.2	FMT_LIM.1	FMT_LIM.2	FCS_RNG.1	FAU_SAS.1
FDP_SDI.2	FDP_SDC.1	FMT_LIM.1/Loader	FMT_LIM.2/Loader	FDP_ACC.1/Loader
FDP_ACF.1/Loader				

The security functional requirements FIA_API.1 and FTP_ITC.1 have no dependencies.
The security functional requirements FIA_API.1, FMT_LIM.1/Loader, FMT_LIM.2/Loader, FTP_ITC.1, FDP_UCT.1, FDP_UIT.1, FDP_ACC.1/Loader and FDP_ACF.1/Loader apply only at TOE products which are delivered with activated Flash Loader.

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

Table 20 Dependency for cryptographic operation requirement

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FCS_COP.1/RSA	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) FCS_CKM.4	Yes, see comment 2
FCS_CKM.1/RSA	FCS_CKM.2 or FCS_COP.1	Yes
	FCS_CKM.4	Yes, see comment 2
FCS_COP.1/ECDSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM1], FCS_CKM.4	Yes, see comment 2
FCS_CKM.1/EC	FCS_CKM.2 or FCS_COP.1	Yes
	FCS_CKM.4	Yes, see comment 2
FCS_COP.1/ECDH	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM1], FCS_CKM.4	Yes, see comment 2
FCS_COP.1/TDES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM1], FCS_CKM.4	Yes, see comment 2
FCS_CKM.4/TDES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, see comment 2
FCS_COP.1/AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM1], FCS_CKM.4	Yes, see comment 2
FCS_CKM.4/AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, see comment 2
FPT_TST.2	No dependencies	Yes
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FMT_MSA.3 FDP_ACC.1	Yes Yes
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes Not required, see comment 1
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes see comment 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_UCT.1	[FPT_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	Yes Yes
FDP_UIT.1	[FPT_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	Yes Yes
FDP_ACC.1/Loader	FDP_ACF.1/Loader	Yes
FDP_ACF.1/Loader	FMT_MSA.3 FDP_ACC.1/Loader	Yes, see comment 3

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

Comment 2:
These requirements all address the appropriate management of cryptographic keys used by the specified cryptographic function and are not part of the PP [9]. Most requirements concerning key management shall be fulfilled by the environment since the Smartcard Embedded Software is designed for a specific application context and uses the cryptographic functions provided by the TOE.
For the security functional requirement FCS_COP.1/TDES and FCS_COP.1/AES the respective dependencies FCS_CKM.1, FCS_CKM.4 and FDP_ITC.1 or FDP_ITC.2 have to be fulfilled by the environment because the TOE does not provide the accompanying functionality; i.e. delete, generate and import keys. That means that the environment shall meet the requirements FCS_CKM.4 as defined in Common Criteria Part 2 [11], section 10.1 and shall meet at least one of the requirements FCS_CKM.1, FDP_ITC.1 or FDP_ITC.2 as defined in Common Criteria Part 2 [11], section 10.1 and 11.7.
The cryptographic key destruction can be done by overwriting the key register interfaces or by software reset of the SCP which provides immediate zeroing of all SCP key registers. Please refer also to the application notes 41 and 42 in the PP [9].

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

Comment 4:
These requirements all address the appropriate management of cryptographic keys used by the specified cryptographic function and are not part of the PP [9]. Most requirements concerning key management shall be fulfilled by the environment since the Smartcard Embedded Software is designed for a specific application context and uses the cryptographic functions provided by the TOE.
For the security functional requirement FCS_COP.1/RSA, FCS_COP.1/ECDSA and FCS_COP.1/ECDH the respective dependency FCS_CKM.1 has to be fulfilled by the TOE with the security functional requirement FCS_CKM.1/RSA (for FCS_COP.1/RSA) and FCS_CKM.1/EC (for FCS_COP.1/ECDSA and FCS_COP.1/ECDH) as defined in section 7.1.4. The respective dependency FCS_CKM.4 has to be fulfilled by the environment because the TOE does not provide the functionality to delete keys. That mean, that the environment shall meet the requirement FCS_CKM.4 as defined in Common Criteria Part 2 [11], section 10.1. Additionally the requirement FCS_CKM.1 can be fulfilled by the environment as defined in Common Criteria Part 2 [11], section 10.1.
For the security functional requirement FCS_CKM.1/RSA and FCS_CKM.1/EC the respective dependency FCS_COP.1 is fulfilled by the TOE. The respective dependency FCS_CKM.4 has to be fulfilled by the environment because the TOE does not provide this functionality. That mean, that the environment shall meet the requirement FCS_CKM.4 as defined in Common Criteria Part 2 [11], section 10.1.
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 any combination 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 is no cryptographic library and provides no additional specific security functionality. The IT environment has to fulfill the requirements of this section depending if the TOE comes with or without a/the library/ies.
End of comment.

7.4.2 Rationale of the Assurance Requirements

The chosen assurance level EAL6 is augmentation with the requirements coming from ALC_FLR.1. In Table 17 the different assurance levels are shown as well as the augmentations. The augmentations are in compliance with the Protection Profile [9].
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" [14] shall be taken as a basis for the vulnerability analysis of the TOE.
Due to the targeted long life time of the Infineon Technologies products, a comprehensive flaw remediation process and database is in place to maintain the TOE also in future. Reported flaws of any kind, meaning, regardless whether the flaws reported have a more directed towards quality, functional or security, are tracked by a dedicated database and related processes.
And more, in order to continuously improve also future products reported flaws are analyzed whether they could affect also future products. Due to its overall importance for future development, the assurance class ALC_FLR.1 is included in this certification process.
This evaluation assurance package was selected to permit a developer gaining maximum assurance from positive security engineering based on good commercial practices as well as the assurance that the TOE is maintained during its targeted life time. The evaluation assurance package follows the EAL6 assurance classes as given in Common Criteria Part 3 [12].

7.4.2.1 *ALC_FLR.1 Basic Flaw Remediation*

Flaws of any kind are entered into a dedicated database with related processes to solve those.
At the point in time where a flaw is entered, it is automatically logged who entered a flaw and who is responsible for solving it. In addition, it is also documented if, when and how an individual flaw has been solved.
Flaws are prioritized and assigned to a responsibility.
The assurance class ALC_FLR.1 has no dependencies.

8 TOE Summary Specification (ASE_TSS)

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

- SF_DPM Device Phase Management
- SF_PS Protection against Snooping
- SF_PMA Protection against Modification Attacks
- SF_PLA Protection against Logical Attacks
- SF_CS Cryptographic Support

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

8.1 SF_DPM: Device Phase Management

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

In addition, chip identification modes are implemented being active in all TOE life cycle phases. The chip identification data (O.Identification) is stored in a in the not changeable and access protected configuration page area of the SOLID FLASH™ NVM. In the same area further TOE configuration data is stored. In addition, user initialization data can be stored in the SOLID FLASH™ NVM 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 in dependency of the corresponding phase identifiers. The decision of accessing a certain mode is defined as phase entry protection as defined conditions have to be met. The phases follow also a defined and flow 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 and finalize the user data. Using the download functionality of the Flash Loader requires passing a successful authentication process and a key exchange. The key exchange ensures that only the user defines the encryption key which is used during the download. If the conditions are met, user code and data can be flashed into the SOLID FLASH™ NVM area as specified by the associated control information of the Flash Loader software. The download into the chip is done in an encrypted way only.
The usage of the Flash Loader is only possible after a successful mutual authentication process of the external entity and the TOE itself.
In case the user has ordered TOE derivatives without Flash Loader, the software download by the user (phase 5 or phase 6) is disabled and all user data of the Composite TOE has been flashed on the TOE at Infineon premises. In both cases the integrity of the loaded data is checked with a hashing process. The data to be loaded is transferred always in encrypted form.
After finalizing the load operation and prior delivery to the end-user, the Flash Loader shall be permanently deactivated. The permanent deactivation is named locking and is a user obligation documented in the user guidance. This locking removes any possibility to use or reactivate the Flash Loader and provides a clear separation between the firmware domain and the user software domain regarding downloads: Software updates after delivery to the end user are exclusively in the responsibility of the user software.

The covered security functional requirement are FMT_LIM.1/Loader "Limited capabilities", FMT_LIM.2/Loader "Limited availability-Loader", FIA_API.1 "Authentication Proof of Identity", FTP_ITC.1 "Inter-TSF trusted channel", FDP_UCT.1 "Basic data exchange confidentiality", FDP_UIT.1 "Data exchange integrity, FDP_ACC.1/ "Loader Subset access control – Loader" and FDP_ACF.1/Loader "Security attribute based access control – Loader".
These Flash Loader related security functional requirements apply only at TOE products coming with activated Flash Loader enabled for user data download by the user. In other cases the Flash Loader is not available anymore and the user data download is completed.

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, belonging memory keys and access rights are initialized by the BOS with predefined values. The covered security functional requirement is FMT_MSA.3 "Static attribute initialization".

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

During the testing phase in production within the secure environment the entire SOLID FLASH™ NVM is deleted. The covered security functional requirement is FPT_PHP.3 "Resistance to physical attack".
Each operation phase is protected by means of authentication and encryption. The covered security functional requirements are FDP_ITT.1 "Basic internal transfer protection" and FPT_ITT.1 "Basic internal TSF data transfer protection".

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

8.2 SF_PS: Protection against Snooping

Memories
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 and the encryption of the memories cover also the stored error detection values, and with regard to the SOLID FLASH™ NVM, also the error correction values. Induced errors will lead with very high probability to an encryption and/or decryption fail in the MED and to the appropriate action.
In contrast to the linear virtual address range, the physical SOLID FLASH™ NVM pages are transparently mapped to different physical address ranges and controlled by the MMU. Thus the data is continuously protected during transfer and storage by encryption and the mapping means of the address ranges. On top this, the address scrambling provides a completely user transparent chip-individual physical memory layout of the SOLID FLASH™ NVM. By that even in the unlike event of two equal TOE derivatives coming with equal software, equal MMU settings and equal MMU mapping, finding an equal piece of data – for example a previously identified target - at the equal physical location in the SOLID FLASH™ NVM on the second chip is extremely unlikely and from attackers perspective not practical. This address scrambling is entirely independent from the user software and the MMU.
MED

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. This includes also the possibility of user chosen keys for SOLID FLASH™ NVM areas. The only key remaining static over the product life cycle is the specific ROM key, changing in case of a mask change only. 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. Note that the ROM contains the firmware only and no user data of the Composite TOE.
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"FPT_FLS.1, "Failure with preservation of secure state" and FDP_SDC.1 "Stored data confidentiality".
Peripheral Bus
In addition the data transferred over the memory bus to and from (bi-directional encryption) the CPU, Co-processors, the special SFRs and selected peripheral devices connected to the peripheral bus are encrypted automatically with a dynamic key change.
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 FPT_FLS.1 "Failure with preservation of secure state".
CPU
The TOE computes and handles data even in the core only encrypted respectively masked. At no time plain data is processed – except when communicating to the outer world. By this plain data is only available at the interface modules. The dual CPU computes entirely masked. More information is given in the confidential Security Target [8].
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 FPT_FLS.1 "Failure with preservation of secure state".
SCP/Cache
The symmetric cryptographic co-processor (SCP) is also entirely masked. The Cache being in ongoing use during core operation is also entirely encrypted. More information is given in the confidential Security Target [8]. The encryption covers the data processing policy and FDP_IFC.1 "Subset information flow control". The covered security functional requirements are FPT_PHP.3, FDP_IFC.1, FPT_ITT.1 and FDP_ITT.1.
MMU
In addition to their protection during processing of code and data, their storage in the SOLID FLASH™ NVM is protected with a further mean too: Even if users operate with direct and static addressing for storing their secrets, the addresses are always translated to virtual addresses. More information is given in the confidential Security Target [8].
The covered security functional requirements are FPT_PHP.3 "Resistance to physical attacks", FPT_ITT.1 "Basic internal TSF data transfer protection", FDP_ITT.1 "Basic internal transfer protection" and FPT_FLS.1 "Failure with preservation of secure state".
Proprietary CPU
A proprietary dual CPU implementation with a non-public bus protocol 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.
Important parts of the chip are especially designed to counter leakage or side channel attacks like DPA/SPA or EMA/DEMA. Therefore, even identifying and collecting physical data is difficult to perform, since timing and current consumption are almost independent of the processed data, as those are protected by a bunch of other internal protecting means.
Synthesis
In the design a number of components are automatically synthesized and mixed up to disguise and complicate analysis. The covered security functional requirement is FPT_PHP.3 "Resistance to physical attack".

Secure Wiring/I² shield
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, rendering probing attacks with high feasibility to not practical. This provides the so called intelligent implicit active shielding "I²-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".
FSE
A low system frequency sensor FSE is implemented to prevent the TOE from single stepping. The sensor is tested by the user mode security life control UMSLC.
The covered security functional requirements are FPT_PHP.3 "Resistance to physical attack" and FPT_FLS.1 "Failure with preservation of secure state".
The **SF_PS** "Protection against Snooping" covers the security functional requirements FPT_PHP.3, FDP_SDC.1, FDP_IFC.1, FPT_ITT.1, FDP_ITT.1 and FPT_FLS.1.

8.3 SF_PMA: Protection against Modifying Attacks

First of all we can say that all security mechanisms effective against snooping **SF_PS** apply also here since a reasonable modification of data is almost impossible on dynamically encrypted, masked, scrambled, transparently relocated, randomized and topologically protected hardware. Due to this the covered security functional requirements are FPT_PHP.3, FDP_SDC.1, FDP_IFC.1, FPT_ITT.1, FDP_ITT.1 and FPT_FLS.1.

The TOE is equipped with an error detection code (EDC) which covers the memory system of RAM, ROM and SOLID FLASH™ NVM and includes also the MED and MMU. Thus introduced failures could 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 an EDC value is calculated and stored as well. This contributes to 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".

The Cache integrity is protected by a different method as the other memories and provides also error detection and appropriate reaction in case of induced errors. This contributes to FDP_SDI.2 "Stored data integrity monitoring and action".

The TOE is protected against fault and modifying attacks. The core provides the functionality of double-computing and result comparison of all tasks to detect incorrect calculations. The detection of an incorrect calculation is stored and the TOE enters a defined secure state which causes the chip internal reset process.
The implementation of 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 at the correct place with the correct timing – despite all other countermeasures like dynamic masking, encryption and others. The comparison and the register files are also protected by various measures. The covered security functional requirements are FPT_FLS.1 "Failure with preservation of secure state", FPT_PHP.3 "Resistance to physical attack", FPT_ITT.1 "Basic internal TSF data transfer protection" and FDP_ITT.1 "Basic internal transfer protection".

During start up, the BOS performs various configurations and subsystem tests. After the BOS has finished, the operating system or application can call the RMS function User Mode Security Life Control (UMSLC) test. This function provides the testing of the security features enabled to generate an alarm and can be released actively by the user software during normal chip operation any time. Attempts to modify the security features will be

detected from this test and lead to the appropriate reaction. 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, for example by the intelligent intrinsic shield (I^2), the processing of the TOE is immediately stopped and the TOE enters a secure state called security reset. The I^2 shield is also part of the UmSLC. The covered security functional requirements are "Failure with preservation of secure state", 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 allow the user to check the correct processing time and the integrity of the program flow of the user software.
Another measure against modifying and perturbation respectively differential fault attacks (DFA) is the implementation of backward calculation in the SCP. By this induced errors are discovered.
The covered security functional requirements are FPT_FLS.1 "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 is 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 defined privilege levels. Addresses and privilege level must match and induced errors and/or manipulation lead to appropriate error message and action. 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 initialization" and FMT_SMF.1 "Specification of Management Functions".

All the measures of controlling the access rights, checking the integrity of data and code, the coverage of the integrity protecting values by means of encryption, the continuously masked calculation and operation stands for the Integrity Guard. The implemented measures interact like a gearing mechanism and by that an induced error will be discovered with very high feasibility followed by the appropriate reaction. While single bit faults may be corrected automatically, other faults which cannot be corrected lead to an alarm, and 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".

If the hardware support library HSL comes with the TOE and the low level driver and/or the "In-Place-Update" functionality are used in certain configurations as outlined in the PRM [3], the TOE behavior is protected against sudden power off events and its behavior is tearing safe.
In this case tearing safe implements an atomicity in the concerned operations resulting that if the process of writing to the SOLID FLASH™ NVM is interrupted by an accidental or intentional power loss or reset, the SOLID FLASH™ NVM data will be either the original data or will be in the new data. The interruption possibly involves some recovery steps that have to be taken before the data is accessed. After successful completion of the concerned operations the relevant data are always in a defined status. If errors are detected during the processing a secure state is entered.
The covered security functional requirement is FPT_FLS.1 "Failure with preservation of secure state".

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

8.4 SF_PLA: Protection against Logical Attacks

The memory access control of the TOE uses a memory management unit (MMU) to control the access to the available physical memory by using virtual memory addresses and to segregate the code and data to a privilege level model. The MMU controls the address permissions of up to seven privileged levels and gives the software the possibility to define different access rights for the user available privileged levels. The address permissions of the privilege levels are controlled by the MMU. In case of an access violation the MMU will trigger a reset and then a trap service routine can react on the access violation. The policy of setting up the MMU and specifying the memory ranges for the privilege levels – with the exception of the IFX level - is defined from the user software (OS). More information is given in the confidential Security Target [8].
Therefore, the TOE provides support for secure separation of memory areas covering the security functional requirements FPT_PHP.3 "Resistance to physical attack", 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_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 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", FPT_ITT.1 "Basic internal transfer protection", FDP_IFC.1 "Subset information flow control" and FPT_FLS.1 "Failure with preservation of secure state".

Beside the access protection and key management, also the use of illegal operation code is detected and will release a security reset. The 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_PHP.3, FPT_ITT.1, FDP_IFC.1, FPT_FLS.1 and FMT_SMF.1.

8.5 SF_CS: Cryptographic Support

The TOE is equipped with several hardware accelerators and software modules to support the standard symmetric and asymmetric cryptographic operations. This security function is introduced to include the cryptographic operation in the scope of the evaluation as the cryptographic function respectively mathematic algorithm itself is not used from the TOE security policy. On the other hand these functions are of special interest for the use of the hardware as platform for the software. The components are a co-processor supporting the DES and AES algorithms and a combination of a co-processor 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 26:
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 any combination 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.
End of note.

Note 27:
This TOE can come with both crypto co-processors accessible, or with a blocked SCP or with a blocked Crypto2304T, or with both crypto co-processors blocked. The blocking depends on the customer demands prior to the production of the hardware. In case the SCP is blocked, no AES and DES computation supported by hardware is possible. In case the Crypto2304T is blocked, no RSA and EC computation supported by hardware is possible. No accessibility of the deselected cryptographic co-processors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic co-processors.
End of note.

8.5.1 Triple DES

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

National Institute of Standards and Technology (NIST), SP 800-67 [17]
ISO/IEC 18033-3 [29]

The TOE implements the following alternative block cipher modes for the user:
The Electronic Codebook Mode (ECB), the Cipher Block Chaining Mode (CBC), the Blinding Feedback Mode (BLD), the Cipher Block Chaining Mode Message Authentication Code (CBC-MAC), the CBC-MAC- encrypt-last-block (CBC-MAC-ELB) and in the Recrypt Mode.

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

ISO/IEC 9797-1 Mac Algorithm 1 [31]

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

National Institute of Standards and Technology (NIST), SP 800-38A [18]

Note that the BLD follows also the standard, but in a masked way.
The key destruction as required by FCS_CKM.4 can be done by overwriting the key register interfaces or by software reset of the SCP which provides immediate zeroing of all SCP key registers.
Please consider also the statement of chapter 7.1.4.1.
The covered security functional requirements are FCS_COP.1/TDES and FCS_CKM.4/TDES.

8.5.2 AES

The TOE supports the encryption and decryption in accordance with the specified cryptographic algorithm Advanced Encryption Standard (AES) and cryptographic key sizes of 128 bit or 192 bit or 256 bit that meet the standard:

ISO/IEC 18033-3 [29]
FIPS 197 [30]

The TOE implements the following alternative block cipher modes for the user:
The Electronic Codebook Mode (ECB), the Cipher Block Chaining Mode (CBC), the Blinding Feedback Mode (BLD), the Cipher Block Chaining Mode Message Authentication Code (CBC-MAC), the CBC-MAC- encrypt-last-block (CBC-MAC-ELB) and in the Recrypt Mode.

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

ISO/IEC 9797-1 Mac Algorithm 1 and 2 respectively [31]

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 [18]

The key destruction as required by FCS_CKM.4 can be done by overwriting the key register interfaces or by software reset of the SCP which provides immediate zeroing of all SCP key registers.
Please consider also the statement of chapter 7.1.4.1.
The covered security functional requirement is FCS_COP.1/AES and FCS_CKM.4/AES.

8.5.3 RSA

Encryption, Decryption, Signature Generation and Verification

The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm Rivest-Shamir-Adleman (RSA) and cryptographic key sizes 1024 - 4096 bits that meet the following standards:

Encryption: 1. According to section 5.1.1 RSAEP in PKCS [19]: • 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 [19] 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) 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 [19] 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 [19]:* *supported for $n < 2^{4096+128}$* • *5.2.2(1) not supported* *2. According to section 8.2.5 IEEE [27]:* • *Supported for $n < 2^{4096+128}$* • *8.2.5(1) not supported*

Please consider also the statement of chapter 7.1.4.1.

Asymmetric Key Generation

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *RSA specified in PKCS#1 [19]* and specified cryptographic key sizes of 1976 – *4096 bits* that meet the following *standard:*

RSA key generation:
1. According to sections 3.1 and 3.2 in PKCS [19], for u = 2, i.e. without any (r_i, d_i, t_i), i > 2:
3.1 supported for $n < 2^{4096+128}$
3.2.(1) supported for $n < 2^{2048+64}$
3.2.(2) supported for $p \times q < 2^{4096+128}$
According to section 8.1.3.1 in IEEE [27]:
8.1.3.1(1) supported for $n < 2^{2048+64}$
8.1.3.1(2) supported for $p \times q < 2^{4096+128}$
8.1.3.1(3) supported for $p \times q < 2^{2048+128}$

FCS_CKM.1/RSA is covered by the standards as stated above.

Note 28:
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.
End of note.

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

8.5.4 Elliptic Curves EC

The certification covers the standard Brainpool [16] and NIST [24] Elliptic Curves with key lengths of 233, 256, 283, 320, 384, 409, 512 or 521 Bits, 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 $p \in \lfloor 2^{41-1};\ 2^{521} \rceil$ as well as curves based on a finite field GF(2^n) with size $n \in [41-1; 521]$ are supported.

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 192 - 521 bits that meet the following standard:

ECDSA Signature Generation: *1. According to section 7.3 Signing Process in ANSI [20]* • *Step d) and e) are 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):* o *The jumps to step a) were substituted by a return of the function with an error code, the jumps are emulated by another call to our function.* *2. According to sections 6.4.3 Signature Process in ISO/IEC [25]* • *Chapter 6.4.3.3 is not supported* • *Chapter 6.4.3.5 is not supported* o *The hash-code of H of the message has to be provided by the caller as input for our function.* • *Chapter 6.4.3.7 is not supported* • *Chapter 6.4.3.8 is not supported* *3. According to section 7.2.7 ECSP-DSA in IEEE [27]* • *Deviation of step (3) and (4):* o *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*
Signature Verification: *1. According to section 7.4.1 in ANSI [20]* • *Step b) and c) are not supported.* • *The output of step c) has to be provided as input to our function by the caller.* • *Deviation of step d):* o *Beside noted calculation, our algorithm adds a random multiple of BasepointerOrder n to the calculated values u1 and u2.* *2. According to sections 6.4.4 Signature Verification Process in ISO/IEC [25]* • *Chapter 6.4.4.2 is not supported* • *Chapter 6.4.4.3 is not supported:* o *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 [27].*

Asymmetric Key Generation

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Elliptic Curve EC specified in [20], [25] and [27] and specified cryptographic key sizes 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits that meet the following standard:

ECDSA *Key Generation:*

1. According to the appendix "A4.3 Elliptic Curve Key Pair Generation" in ANSI [20]:

- *The optional cofactor h is not supported.*

2. According to section "6.4.2 Generation of signature key and verification key" in ISO/IEC [25].

3. According to appendix "A.16.9 An algorithm for generating EC keys" in IEEE [27]

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 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits that meet the following standard:

1. According to section "5.4.1 Standard Diffie-Hellman Primitive" in ANSI [21]

- *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 "Appendix D.6 Key agreement of Diffie-Hellman" type in ISO/IEC [26]

- *The function enables the operations described in appendix D.6*

3. According to section "7.2.1 ECSVHDP-DP" in IEEE [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 29:
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.
End of note.
The covered security functional requirements are FCS_COP.1/ECDSA, FCS_CKM.1/EC and FCS_COP.1/ECDH.

8.5.5 Toolbox Library

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

8.5.6 Hybrid PTRNG

Random data is essential for cryptography as well as for security mechanisms. The TOE is equipped with a Hybrid Physical True Random Number Generator (HPTRNG, FCS_RNG.1). The random data can be used from the Smartcard Embedded Software and is also used from the security features of the TOE, i.e. masking. The HPTRNG implements various topological means, masked bus interface and is self-checking.
The produced genuine random numbers are available as a security service for the user and are also used for internal purposes. Together with the security guidelines in [6] the hybrid PTRNG operates in the following modes of operation and is conformant to the named classes:

- True Random Number Generation, meeting AIS31 PTG.2
- Hybrid Random Number Generation, meeting AIS31 PTG.3

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

The details of AIS31 are given in [13].

The Hybrid PTRNG implements protected a protected peripheral bus interface is a synthesized module and covers therefore FPT_PHP.3 "Resistance to physical attack". The transferred random data are masked as well as other configuration data transferred over the peripheral bus. This covers FDP_ITT.1 "Basic internal transfer protection" and FPT_ITT.1 "Basic internal TSF data transfer protection". The correct function of the Hybrid PTRNG is subject of internal self testing and in case of errors a secure state is achieved to protect the user from random data with bad entropy. Therefore, the output of the Hybrid PTRNG is conformant to the above claimed classes or there is no random data output. This covers FPT_FLS.1 "Failure with preservation of secure state".

The hybrid PTRNG covers the security functional requirements FCS_RNG.1 "Random Number Generation", FPT_PHP.3 "Resistance to physical attack", FDP_ITT.1 "Basic internal transfer protection", FPT_ITT.1 "Basic internal TSF data transfer protection" and FPT_FLS.1 "Failure with preservation of secure state".

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

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

The justification and overview of the mapping between security functional requirements (SFR) and the TOE's security functionality (SF) is given in sections the sections above. The results are shown in 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 21 Mapping of SFR and SF

Security Functional Requirement	SF_DPM	SF_PS	SF_PMA	SF_PLA	SF_CS
FAU_SAS.1	X				
FCS_CKM.1/EC					X
FCS_CKM.1/RSA					X
FCS_CKM.4/AES					X
FCS_CKM.4/TDES					X
FCS_COP.1/AES					X
FCS_COP.1/ECDH					X
FCS_COP.1/ECDSA					X
FCS_COP.1/RSA					X
FCS_COP.1/TDES					X
FCS_RNG.1/TRNG					X
FCS_RNG.1/HPRG					X
FCS_RNG.1/DRNG					X
FCS_RNG.1/KSG					X
FDP_ACC.1	X		X	X	
FDP_ACC.1/Loader	X				
FDP_ACF.1	X		X	X	
FDP_ACF.1/Loader	X				
FDP_IFC.1		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_UCT.1	X				
FDP_UIT.1	X				
FIA_API.1	X				
FMT_LIM.1	X				
FMT_LIM.1/Loader	X				
FMT_LIM.2	X				
FMT_LIM.2/Loader	X				
FMT_MSA.1	X		X	X	
FMT_MSA.3	X		X	X	
FMT_SMF.1	X		X	X	
FPT_FLS.1		X	X	X	X
FPT_ITT.1	X	X	X		X
FPT_PHP.3	X	X	X	X	X

Security Functional Requirement	SF_DPM	SF_PS	SF_PMA	SF_PLA	SF_CS
FPT_TST.2			X		
FRU_FLT.2			X		
FTP_ITC.1	X				

8.7 Security Requirements are internally Consistent

For this chapter the PP [9] section 6.3.4 can be applied completely.
In addition to the discussion in section 6.3 of PP [9] the security functional requirement FCS_COP.1 is introduced. The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the cryptographic algorithms implemented according to the security functional requirement FCS_COP.1. Therefore, these security functional requirements support the secure implementation and operation of FCS_COP.1.
As disturbing, manipulating during or forcing the results of the test checking the security functions after TOE delivery, this security functional requirement FPT_TST.2 has to be protected. An attacker could aim to switch off or disturb certain sensors or filters and preserve the detection of his manipulation by blocking the correct operation of FPT_TST.2. The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the security functional requirement FPT_TST.2. Therefore, the related security functional requirements support the secure implementation and operation of FPT_TST.2.
The requirement FPT_TST.2 allows testing of some security mechanisms by the Smartcard Embedded Software after delivery. In addition, the TOE provides an automated continuous user transparent testing of certain functions.
The implemented privilege level concept represents the area based memory access protection enforced by the MMU. As an attacker could attempt to manipulate the privilege level definition as defined and present in the TOE, the functional requirement FDP_ACC.1 and the related other requirements have to be protected themselves. The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the area based memory access control function implemented according to the security functional requirement described in the security functional requirement FDP_ACC.1 with reference to the Memory Access Control Policy and details given in FDP_ACF.1. Therefore, those security functional requirements support the secure implementation and operation of FDP_ACF.1 with its dependent security functional requirements.
The requirements FDP_SDI.1.1 and FDP_SDI.2.1 enable for 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 and References

Note that the final versions of these documents are defined at the end of the evaluation process and that the documents are listed in the certification report as well.

No.	Vers.	As of	Document Title
1	4.2	2016-11-15	16-bit Security Controller Family - V02, Hardware Reference Manual (HRM)
2	3.2	2016-08-05	16-bit Security Controller in 65nm, Production & Personalization, User's Manual
3	9.6	2017-07-04	16-bit Security Controller, 65-nm Technology, Programmer's Reference Manual (PRM)
4	v2.06.003	2016-12-12	CL52 Asymmetric Crypto Library for Crypto@2304T, RSA/ECC/Toolbox, 16-bit Security Controller, User Interface with additional errata section
		2017-05-10	Additional errata section
5	1.4.1	2014-11-10	16-bit Security Controller, Crypto@2304T V3, User Manual
6	1.00-1545	2016-12-01	16-bit Security Controller - V02, Security Guidelines (SG)
7	Rev. 4.0	2017-08-17	16-bit Security Controller - V02, Errata Sheet
8	This document		The confidential Security Target for this TOE.
9	1.0	2014-01-13	Security IC Protection Profile PP-0084 "Security IC Platform Protection Profile with Augmentation Packages", BSI-CC-PP-0084-2014, available at https://www.bund.bsi.de
10	3.1 Rev 5	2012-09	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model; Version 3.1 Revision 5, April 2017, CCMB-2017-04-001
11	3.1 Rev 5	2012-09	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements; Version 3.1 Revision 5, April 2017, CCMB-2017-04-002
12	3.1 Rev 5	2012-09	Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements; Version 3.1 Revision 5, April 2017, CCMB-2017-04-003
13	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
14	2.9	2013-01	Application of Attack Potential to Smartcard, mandatory technical document, CCDB-2013-05-002, http://www.commoncriteriaportal.org
15	v01.22.4346	2016	Hardware Support Library for SLCx2 (HSL)

No.	Vers.	As of	Document Title
16	RFC 5639	2010-03	RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, IETF Trust and the persons identified as the document authors, March 2010, http://www.ietf.org/rfc/rfc5639.txt
17	800-67 Rev. 1	2012-01	National Institute of Standards and Technology (NIST), Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Revised January 2012, Technology Administration, U.S. Department of Commerce
18	NIST SP800-38A	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)
19	v2.1	2002-06-14	PKCS #1: RSA Cryptography Standard, RSA Laboratories, RFC3447
20	ANSI 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
21	ANSI X.9.63	2011-12-21	American National Standard for Financial Services X9.63-2011, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, American National Standards Institute
22	I	2009-08-14	Act on the Federal Office for Information Security (BSI-Gesetz - BSIG), Bundesgesetzblatt I p. 2821; BSIG Section 9, Para.4, Clause 2
23			Intentionally left blank
24	FIPS Pub 186-4	2013-07	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)
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 Crytography, 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.
28			Intentionally left blank
29	ISO/IEC 18033	2005	ISO/IEC 18033-3: 2005, Information technology – Security techniques - Encryption algorithms - Part 3: Block ciphers [18033] (for AES)
30	FIPS 197	2001-11-26	Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE / National Institute of Standards and Technology, November 26, 2001
31	ISO/IEC 9797-1	2011-03-01	ISO/IEC 9797-1: 2011, Information technology – Security techniques - Message Authentication Codes (MACs) Part 1 Mechanisms using a block cipher
32	1.0	2015-02-13	Nachweis der Einhaltung der Sicherheitsanforderungen für Chipkarten im Zulassungsverfahren der Deutschen Kreditwirtschaft (DK) (German only)
33	ISO/IEC 9798-2	2015-02-14	Information Technologies - Security Techniques - Entity Authentication, part 2: Mechanisms using symmetric encipherment algorithms, 3rd edition 2008-12-15

10 Annex: Consideration of additional Requirements by the GBIC Approval Scheme

After alignment and harmonization with the BSI, the German Banking Industry Committee (GBIC) respectively the Deutsche Kreditwirtschaft (DK) accepts Common Criteria certificates and related national processes but adds additional requirements coming from [32] chapter 7 which are considered in the following.

Translation:

1. The hardware vendor has to support confidentiality and integrity protected processes that
   a. Generate keys with sufficient entropy
   b. Store those keys in a HSM within the vendor environment
   c. Store those keys in the non-volatile memory of the chip
   d. Deliver these keys separated from the chip delivery to the user
2. The loading of software and data into the chip memories is only possible after passing a secure authentication

These security requirements are especially affective for the security functionality of the key K_{chip} respectively Kc coming from the personalization concept of the Publishing Houses (Verlage). For the complete coverage during the Common Criteria it is required that already the firmware of the TOE provides the security functionality for K_{chip}.
In the course of migration to Common Criteria these security requirements must be modelled in the Security Target.
End of translation.

Regarding requirement 1:

GBIC issues therewith additional requirement for sufficient entropy of the used keys. This requires the presence of dedicated device and process in order to provide evidence that the keys used have been generated appropriately. The key used in this context are generated by a dedicated hardware security module (HSM) with appropriate certification. This covers requirement 1.a.

The requirement 1.b is sufficiently addressed by the refinements regarding development security (ALC_DVS) taken from PP [9].

All data loaded into the chip is encrypted and integrity protected stored in the SOLID FLASH ™ NVM. This covers the requirement 1.c.

The requirement 1.d implies the presence of a dedicated GBIC process with additional protection means for the key handling and management after its generation in the HSM. Infineon Technologies has implemented a dedicated process with role separation, access protection, transport protection during the internal different instances and implements a separate specific process for protected delivery of the used keys to the user. Therefore, the requirement 1.d. is sufficiently addressed by refinements regarding delivery procedure (ALC_DEL) if the security functionality of the corresponding key is part of the TOE.

Regarding requirement 2:

This requirement implements the authentication aspects of the chip against the external world and vice versa, which is covered by following packages taken from the PP [9]:

FIA_API "Authentication Proof of Identity ",

"Package 2: Loader dedicated for usage by authorized users only" and additionally the TOE implements the

"Package 1: Loader dedicated for usage in secured environment only" of the PP [9].

The rational shows that all GBIC specific requirements are met by the TOE.

Note for the additional objectives for GBIC respectively DK

- The requirement for sufficient entropy requires the presence of dedicated device and process in order to provide evidence that the key K_{chip} has been generated appropriately. As the key K_{chip} is generated by a dedicated hardware security module (HSM) with appropriate certification the objective O.GBIC_Key is covered.
- The used HSM is certified by:
  FIPS 140-2 Consolidated Validation Certificate, consolidated certificate No. 0006. 2011/06/30, by the National Institute of Standards and Technology of the United States of America and the Communications Security Establishment of the Government of Canada.
- The additional requirements imply the presence of a dedicated GBIC process with additional protection means for the key handling and management after its generation in the HSM. Infineon Technologies has implemented a dedicated process with role separation, access protection, transport protection during the internal different instances and implements a separate specific process for protected delivery of the key K_{chip} to the user. This covers the objective O.Process_GBIC.
- The GBIC requirement 2 is covered by the flash loader package 1 of PP [9] as justified in section 5.3.

Additional requirements issued by the general GBIC directive in September 2016

The related directive with file number 80-11 affects the software vendors respectively personalization step and implements specific requirements. The rational is given by the fact that it can occur that an exclusively contact based product, deemed for LCCS of MF for SECCOS ICC and ICC products referring to SECCOS 7, is based on a dual interface controller. Since not all contact-based-only applications block the access to the contactless interface, specific requirements are set immediately effective.
These requirements affect user software developers and the product personalization only and thus they are not repeated here.
Anyhow, the given requirements target the complete disabling of the contactless interfaces if the product is used contact based only and define the specific configuration of the LCCS-Byte of the MF with the hexadecimal value "35" for those contact based products, referring on SECCOS ICC and ICC products for SECCOS 7.
When using this TOE, the user can easily follow these requirements since this dual interface controller can permanently block the contactless interface by user applicable configuration means. And, in addition, dedicated product derivatives are available by order option coming with the contact based interface only.

11 Hash Signatures of Cryptographic Libraries

Following listings document the hash signatures of the respective optional cryptographic library software version. For convenience purpose several hash algorithms were used.

11.1 RSA, EC, Toolbox Version v2.06.003:

Cl52-LIB-base-XSMALL-HUGE.lib:
MD5=165554e1b2c2a3918fedd4ccaf4756ef
SHA1=6a47aeba0840a29b9dcf8e09b1662d9e110767c4
SHA256=e172936204dc4d2a3b79bb27a915017f7b5c49366b8333a7b19d0345aff3c9d8

Cl52-LIB-ecc-XSMALL-HUGE.lib:
MD5=23f70c52fe712ff9f71d1ed7d31e338a
SHA1=5f52a8802dff6e29c754f71f62b55915efcd293e
SHA256=3bf8e9d79578c94163dfe7f751e2ebd917adcbadea45338b1cd48f9417907584

Cl52-LIB-2k-XSMALL-HUGE.lib:
MD5=df1e79efd5a8d8c05f70c68f165e0606
SHA1=e939a32b841edf991d69e97373afb3ea541f7b09
SHA256=6d85ee8b56118602a9803cd7d829c55af080f4d96c2c4b014c7df64173f4c564

Cl52-LIB-4k-XSMALL-HUGE.lib:
MD5=747955e3945069be053f001f0c4071cd
SHA1=e4cbb3ab4371df6de99d21fd5c5a95dd217456bc
SHA256=cc928ac2c86d342098961a6cb4c74bf229de317ccf73994df719f6d91ad69042

Cl52-LIB-toolbox-XSMALL-HUGE.lib:
MD5=efdf2ced3d3a5e0ed729d6284276ccd0
SHA1=61995654bdebc4d4a72b80e1ea5729ab437acc1f
SHA256=0db886bac26b47927e1966d4394fdbb4e72fbd74d1ea1738d7cb7470b7463b96

11.2 The Hardware Support Library

Hsl.lib:
MD5=57b0eb1f5e54922be46218431da53e4d
SHA-1=3cb599186885e3e167295bf7db583652d9e143b9
SHA-256=f898ac7ad4ba43732ec05e9ab7de752811c2a9553c078b5187ccba8b2a67843b

12 List of Abbreviations

AES	Advanced Encryption Standard
AIS31	"Anwendungshinweise und Interpretationen zu ITSEC und CC Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren"
API	Application Programming Interface
APDU	Application Protocol Data Unit
BOS	Boot-up Software
BSI	German: Bundesamt für Sicherheit in der Informationstechnik English: Federal Office for Information Security
CC	Common Criteria
CI	Chip Identification Mode (BOS-CI)
CIM	Chip Identification Mode (BOS-CI), same as CI
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
Crypto2304T	Asymmetric Cryptographic Processor
CRT	Chinese Remainder 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
SOLID FLASH™ NVM	Nonvolatile memory based on flash cell technology
EMA	Electromagnetic analysis
FL	Flash Loader
Flash	SOLID FLASH™ Memory
HW	Hardware
HSL	Hardware Support Library
IC	Integrated Circuit
ICO	Internal Clock Oscillator
ID	Identification
IMM	Interface Management Module
ITP	Interrupt and Peripheral Event Channel Controller
I/O	Input/Output
IRAM	Internal Random Access Memory
ITSEC	Information Technology Security Evaluation Criteria
M	Mechanism
MCS	Mifare compatible software

MED	Memory Encryption and Decryption
MMU	Memory Management Unit
NVM	Non Volatile Memory
O	Object
OS	Operating system
PEC	Peripheral Event Channel
PFD	Post Failure Detection Unit
PRNG	Pseudo Random Number Generator
PROM	Programmable Read Only Memory
PTRNG	Physical Random Number Generator
RAM	Random Access Memory
RFI	Radio Frequency Interface
RMS	Resource Management System
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rives-Shamir-Adleman Algorithm
SCP	Symmetric Cryptographic Processor
SF	Security Feature
SFR	Special Function Register, as well as Security Functional Requirement The specific meaning is given in the context
SPA	Simple power analysis
SW	Software
SO	Security objective
T	Threat
TM	Test Mode (STS)
TOE	Target of Evaluation
TRNG	True Random Number Generator
TSC	TOE Security Functions Control
TSF	TOE Security Functionality
UART	Universal Asynchronous Receiver/Transmitter
UM	User Mode (STS)
UmSLC	User mode Security Life Control
WDT	Watch Dog Timer
XRAM	eXtended Random Access Memory
TDES	Triple DES Encryption Standard also known as 3DES

13 Glossary

Application Program/Data	Software which implements the actual TOE functionality provided for the user or the data required for that purpose
Bill-Per-Use	Bill-Per-Use concept allowing the user to configure the chips
Central Processing Unit	Logic circuitry for digital information processing
Chip	Integrated Circuit]
Chip Identification Data	Data stored in the SOLID FLASH™ NVM containing the chip type, lot number (including the production site), die position on wafer and production week and data stored in the ROM containing the STS version number
Chip Identification Mode	Operational status phase of the TOE, in which actions for identifying the individual chip by transmitting the Chip Identification Data take place
Controller	IC with integrated memory, CPU and peripheral devices
Crypto2304T	Cryptographic coprocessor for asymmetric cryptographic operations (RSA, Elliptic Curves)
Cyclic Redundancy Check	Process for calculating checksums for error detection
End User	Person in contact with a TOE who makes use of its operational capability
Firmware	Is software essential to put the chip into operation. The firmware is located in the ROM and parts of it in the SOLID FLASH™ NVM
Flash Loader	Software enabling to download software after delivery
Hardware	Physically present part of a functional system (item)
Integrated Circuit	Component comprising several electronic circuits implemented in a highly miniaturized device using semiconductor technology
Internal Random Access Memory	RAM integrated in the CPU
Mechanism	Logic or algorithm which implements a specific security function in hardware or software
Memory Encryption and Decryption	Method of encoding/decoding data transfer between CPU and memory
Memory	Hardware part containing digital information (binary data)
Microprocessor	CPU with peripherals
Object	Physical or non-physical part of a system which contains information and is acted upon by subjects
Operating System	Software which implements the basic TOE actions necessary to run the user application
Programmable Read Only Memory	Non-volatile memory which can be written once and then only permits read operations
Random Access Memory	Volatile memory which permits write and read operations
Random Number Generator	Hardware part for generating random numbers
Read Only Memory	Non-volatile memory which permits read operations only
Resource Management System	Part of the firmware containing SOLID FLASH™ NVM programming routines, AIS31 test bench etc.
SCP	Is the symmetric cryptographic coprocessor for symmetric cryptographic operations (TDES, AES).

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	Is a plastic card in credit card format with built-in chip. Other form factors are also possible, i.e. if integrated into mobile devices
Software	Information (non-physical part of the system) which is required to implement functionality in conjunction with the hardware (program code)
Subject	Entity, generally in the form of a person, who performs actions
Target of Evaluation	Product or system which is being subjected to an evaluation
Test Mode	Operational status phase of the TOE in which actions to test the TOE hardware take place
Threat	Action or event that might prejudice security
User Mode	Operational status phase of the TOE in which actions intended for the user takes place

14 Revision History

Major changes since the last revision

Version	Description of change
0.1	Initial version
0.2	Update of asymmetric cryptographic library, update of ANSI X9.63 standard reference, removal of unused standard references
0.3	ACL user guidance comes with additional errata section
0.4	Inclusion of second alternative FW-Identifier, User Guidance documents update, correction in table 7.1.4.1

Edition 2017-08-22

Published by
Infineon Technologies AG
81726 Munich, Germany

Do you have a question about this document?
Email: erratum@infineon.com

Document reference

IMPORTANT NOTICE
The information contained in this Security Target is given as a hint for the implementation of the product only and shall in no event be regarded as a description or warranty of a certain functionality, condition or quality of the product. Before implementation of the product, the recipient of this application note must verify any function and other technical information given herein in the real application. Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind (including without limitation warranties of non-infringement of intellectual property rights of any third party) with respect to any and all information given in this Security Target.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer's technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

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

WARNINGS
Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies' products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.