Public Security Target
IFX_CCI_000011h
IFX_CCI_00001Bh
IFX_CCI_00001Eh
IFX_CCI_000025h
G12

Common Criteria EAL6 augmented / EAL6+

Resistance to attackers with HIGH attack potential

including optional software libraries:
Flash Loader according Package1 and Package2,
NRG, HSL, ACL, SCL and CIPURSE™ CL

Author: Jürgen Noller, CSS S PS

Revision 1.5 as of 2021-11-05

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 IFX_CCI_000011h IFX_CCI_00001Bh IFX_CCI_00001Eh IFX_CCI_000025h G12, covering one hardware platform with following Common Criteria Identifierers (CCI):

- IFX_CCI_000011h
- IFX_CCI_00001Bh
- IFX_CCI_00001Eh
- IFX_CCI_000025h

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) in the following description.

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 public Security Target has the Revision 1.5 and is dated 2021-11-05.

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

- the Asymmetric Cryptographic Library (ACL) includes RSA2048/4096 libraries in the versions v2.08.006 and v3.03.003, which are providing RSA[1] cryptography . The ACL supports also smaller key lengths, but lengths below 1976 bits are not included in the certification due to national regulation by the BSI,
- the Asymmetric Cryptographic Library (ACL) includes the EC library in the versions v2.08.006 and v3.03.003, which provides EC[2] cryptography.
- the Asymmetric Cryptographic Library (ACL) includes the Toolbox library in the versions v2.08.006 and v3.03.003, which provides basic mathematical functions for a simplified user interface to the Crypto@2304T.
  The Toolbox library is not part of the TOE Security Functionality (TSF) of this TOE.
- the Symmetric Cryptographic Library (SCL) in the version v2.13.001 provides a simplified interface and utilizes the full services of the SCP to the user,
- the Hardware Support Library (HSL) in the version v2.01.6198 provides a simplified interface and utilizes the full services of the SOLID FLASH™ NVM to the user,
- the CIPURSE™ Cryptographic Library (CIPURSE™ CL) in the version v02.00.0005 provides the user OSPT alliance CIPURSE™ V2 conformant communication functionality between a PICC and a PCD,
- the NRG[1] Software (NRGS), which is not part of the TOE Security Functionality (TSF) of this TOE, including the Management of NRG Cards, Management of NRG Cards Extension, NRG Reader Mode Support and NRG OS in the version v04.03.3431,

---

[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.

- with specific IC dedicated software (firmware) and with specific guidance documentation according section 2.2.4 and 9.

The design step of this TOE is G12.

The Security Target is based on the Protection Profile PP-0084 "Security IC Platform Protection Profile with Augmentation Packages" [1] 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 ARM core 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 of the TOE

	Version	Date	Registration
Security Target	Revision 1.5	2021-11-05	Public Security Target IFX_CCI_000011h IFX_CCI_00001Bh IFX_CCI_00001Eh IFX_CCI_000025h G12
Target of Evaluation			The hardware controller with following identifiers CCIs: • IFX_CCI_000011h • IFX_CCI_00001Bh • IFX_CCI_00001Eh • IFX_CCI_000025h in the design step G12 with Firmware Identifier 80.201.04.1 in the delivery format: as defined in section 2.2.5 and the following **optional** libraries all the delivery format: binary RSA2048 v2.08.006 and v3.03.003 RSA4096 v2.08.006 and v3.03.003 EC v2.08.006 and v3.03.003 Toolbox v2.08.006 and v3.03.003 SCL v2.13.001 HSL v2.01.6198 CIPURSE™ CL v02.00.0005 and the following **optional** NRG Software libraries, which

---

[1] The term "NRG" in this document means "ISO/IEC 14443-3 type A with CRYPTO1". This applies to the entire document whenever the term is used.

	Version	Date	Registration
			are not part of the evaluated security functionality (TSF), in the delivery format: binary, as defined in section 2.2.5
			NRG OS v04.03.3431
			Management of NRG Cards v04.03.3431
			Management of NRG Cards Extension v04.03.3431
			NRG Reader Mode Support v04.03.3431
			and the belonging user guidance as listed in 2.2.4
			all in the delivery format: *.pdf or *.chm, as defined in section 2.2.5
Protection Profile	1.0	2014-06-17	Security IC Platform Protection Profile with Augmentation Packages BSI-CC-PP-0084-2014
User Guidance			Section 2.2.4 Guidance documentation describes briefly the contents of the individual documents of the User Guidance Documentation, while the individual documents are versioned and entitled in section 9 Literature and References. The there listed set of user guidance documents belongs to the TOE.
Common Criteria	3.1 Revision 5	April 2017	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCMB-2017-04-001 Part 2: Security functional requirements CCMB-2017-04-002 Part 3: Security Assurance Components CCMB-2017-04-003

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, referenced in Table 1 at row Target of Evaluation, can be identified with the Generic Chip Identification Mode (GCIM). The TOE hardware platform is identified by the Common Criteria Certification Identifier bytes of the GCIM as given in the 32-bit Security Controller - V07 Hardware Reference Manual [7]: The unique hexadecimal values as stated in the title are:

- IFX_CCI_000011h

- IFX_CCI_00001Bh

- IFX_CCI_00001Eh

- IFX_CCI_000025h

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

The interpretation of the output GCIM data is clearly explained in the user guidance, "32-bit Security Controller - V07 Hardware Reference Manual" [7] and in the "32-bit Security Controllers SLC37 (65 nm Technology) Programmer´s Reference Manual" [11].

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

Despite these configuration possibilities, all products are derived from the equal hardware design results, the TOE. The differences between the derivatives have no impact on the TOEs security policies. Details are explained in the user guidance "32-bit Security Controller - V07 Hardware Reference Manual" [7].

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

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

To each of the TOE relevant optional different mask set variants, an individual value is assigned, which is part of the data output of the Generic Chip Identification Mode (GCIM). By that the various hardware mask sets can be clearly identified and differentiated by the GCIM output. The interpretation of the output GCIM data is clearly explained in the user guidance, "32-bit Security Controller - V07 Hardware Reference Manual" [7].

There are no other differences between the mask sets the TOE is produced with, and all these changes have no impact on the TOEs security policies and related functions. Details are explained in the user guidance "32-bit Security Controller - V07 Hardware Reference Manual" [7] and in the "32-bit Security Controller - V07 Errata Sheet" [12].

The TOE product allows for a maximum of configuration possibilities defined by the customer order or his blocking following the market needs. For example, a TOE can come in one project with the fully available SOLID

FLASH™ NVM or in another project with any other SOLID FLASH™ NVM -size below the physical implementation size, or with a different RAM size. And more, the user has the free choice, whether he needs the Symmetric Cryptographic Coprocessor SCP or not. 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 Symmetric Cryptographic Coprocessor for DES and AES Standards,
- the availability of the Crypto@2304T coprocessor for RSA and EC Standards
- the availability and free combinations of the cryptographic libraries RSA, EC, Toolbox and SCL,
- the availability of the HSL,
- the availability of the Flash Loader,
- the availability of the CIPURSE™ Cryptographic Library,
- the availability of various interface options, and
- the possibility to tailor the product by blocking on his own premises (BPU),
- the possibility to apply the PIN-Letter in combination with the Flash Loader,
- the availability of the NRGS (NRG OS , Management of NRG Cards, Management of NRG Cards Extension, NRG Reader Mode Support) libraries, which are not part of the TSF of this TOE.

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

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

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

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

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

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

As written above, the software realizing the user allowed blocking, is implemented and delivered in the TOE – depending on the order - and is part of the evaluation and certificate. This software is an additional part of the Flash Loader software, but also the other firmware has seen a small enhancement to enable for BPU.
If BPU is available, the blocking is done by the user at user premises, usually by taking an enhancement of the user own personalization flow and applying the according APDUs. These APDUs are predefined by Infineon Technologies and can also depend on the customer order. Only these APDUs can block the chip according to the user demands.

Infineon Technologies AG provides special software, running in parallel when doing the blocking. This software summarizes all devices and final configurations allowing for the later commercial balancing. The balancing depends on the number of chips and their individual final blockings the user has made over a defined time

span. This special software can be used only for the commercial balancing, is not present on the TOE, not security relevant and therefore not part of this certificate.

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

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

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

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

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

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

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

Extra authentication means applied in the PIN-Letter status of the Flash Loader preserve that only the intended user with the intended PIN-Letter can configure with user specific information and enable the normal Flash Loader functions in a second step. By that the user orders the products and receives - in a protected way - the belonging PIN-Letter. PIN-Letter and delivered chips must match.
By delivery the user warehouse gets filled and depending on market demands the user can immediate apply the authentication means of the PIN-Letter. If passing, the TOE products become user specific configured and the Flash Loader can be used for this specific user in a second step.

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

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

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

The "32-bit Security Controller - V07 Hardware Reference Manual" [7] provides an overview about the configuration options respectively ranges.

Note that there is no separate user available on-chip ROM module anymore. The user software and data are 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 comparable respectively equal reliability and endurance, compared to a conventional ROM.

Beside the above listed flexible ranges, the user guidance contains a number of predefined configurations for those customers not using the BPU option. All of these configurations belong to the TOE as well and are of course made of equal hardware and are inside the above declared ranges. Today's predefined configurations of the TOE are listed in the "32-bit Security Controller - V07 Hardware Reference Manual" [7]. These predefined products come with the most requested configurations and allow to produce volumes on stock in order to simplify logistic processes.

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

Note that the TOE answers to the Non-ISO-ATR with the Generic Chip Identification Mode (GCIM) answer. This GCIM outputs a coded clear identifier for the chip type, the design step and further configuration information. The document "32-bit Security Controller - V07 Hardware Reference Manual" [7] is part of the user guidance and enables for the clear interpretation of the read out GCIM data.

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

In addition, dedicated special function registers (SFR) allow reading out the present configuration in detail. The output data together with the "32-bit Security Controller - V07 Hardware Reference Manual" [7] enables for clear identification of a product and its configuration. All these steps for gathering identification and detailed configuration information can be done by the user himself, without involving Infineon Technologies AG.

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

The firmware part includes the Boot Software (BOS) for test and initialization purposes (see section 2.2.2), at startup of the TOE, the optional Flash Loader for downloading user software (user data) to the SOLID FLASH™ NVM and the NRG Base.
The BOS functions are located in the ROM and in the SOLID FLASH™ NVM. The ROM contains no user data.

The optional software part is differentiated into the cryptographic libraries RSA[1], EC[2], SCL[3] and the supporting libraries Toolbox, Base, HSL, CIPURCE™ CL and the NRG Library (Management of NRG Cards, Management of NRG Cards Extension, NRG Reader Mode Support, NRG OS, which are not part of the TSF of this TOE).

The RSA, EC and Toolbox libraries in two alternative versions, provide certain functionality via an API to the Smartcard Embedded Software. The Base library is no delivery option for the user and therefore not listed in Table 1, because the library is used internally by the RSA, EC and Toolbox libraries and is part of the TOE in any case if one of the three libraries RSA, EC and Toolbox is delivered, if none of them is delivered also the Base library is not part of the TOE.
The Toolbox provides the following basic long integer arithmetic and modular functions in software, supported by the cryptographic coprocessor Crypto@2304T: Addition, subtraction, division, multiplication, comparison, reduction, modular addition, modular subtraction, modular multiplication, modular inversion and modular exponentiation. The Toolbox library is not part of the TOE Security Functionality (TSF) of this TOE and does not provide any security functional requirement.

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

The SCL library provides certain functionality via an API to the Smartcard Embedded Software.

The TOE can be delivered including - in free combinations - or not including any of the functionality of the cryptographic libraries SCL, EC, RSA and the supporting Toolbox library. If RSA or EC or Toolbox is delivered, automatically the Base library is part of the shipment too.

If the user decides not to use one or all of the crypto library(s), the specific library(s) is (are) not delivered to the user and, in the case that RSA or EC are not delivered, the accompanying "Additional Specific Security Functionality (O.Add Functions)" Rivest-Shamir-Adleman (RSA) and/ or EC is/are not provided by the TOE.

The Base library provides the low level interface to the asymmetric cryptographic coprocessor and is available if one of the RSA, EC or Tollbox libraries is part of the TOE.

The Symmetric Cryptographic Library (SCL) offers a high level interface to perform the cryptographic operations DES/TDES, AES and MAC with different key lengths on the Symmetric Cryptographic Coprocessor (SCP) for this TOE. The SCL implements already several block cipher modes as declared in this document and covering a wide range of applications, the SCL offers in addition the flexibility to implement additional block cipher modes defined by the user.

---

[1] Rivest-Shamir-Adleman asymmetric cryptographic algorithm

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

[3] Symmetric Crypto Library

This library provides a simplified interface to the hardware Symmetric Cryptographic Coprocessor (SCP) and preserves the security and performance requirements as required by the user.
Note that the definition of the key lengths follows the national AIS32 regulation regarding the 100 bit security level by the BSI[1]. This excludes the single DES operation from the certification.

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

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 applied the user has no need to care about cases where the TOE is unintentionally removed from the power supply even during managing the SOLID FLASH™ NVM.
Anyhow, the HSL remains as an optional library, as even sudden power off situations do not lead to exploitable conditions of the TOE. In the worse, the TOE ends operation in case of a faulty programmed SOLID FLASH™ NVM location.

The order option CIPURSE™ Cryptographic Library (CIPURSE™ CL) provides cryptographic functionality to implement a CIPURSE™ V2 conformant protocol.
This protocol provides a secure mutual authentication of two entities, namely the terminal (denoted as PCD = Proximity Coupling Device (CIPURSE™-compliant terminal)) and a smart card or a token in other form factors which is called PICC. PICC stands for Proximity Integrated Circuit Card (CIPURSE™-compliant card).
Beside the mutual authentication, the protocol implements measures to maintain the integrity of the transferred data and preserves in parallel the confidentiality of the transferred data.
By that the CIPURSE™ CL supports the user to implement systems conformant to the CIPURSE™ open standard implementing a secured, interoperable and flexible transit fare collection solution, including ISO 7816, ISO/IEC 14443-4 communication and AES-128 bit cryptography for multiple payment types.

The NRG Software (NRGS) as a further order option implements the routines for a NRG interface which are not part of the TSF of this TOE. The NRGS provides an operating system handling the emulation of a NRG card. One part of the NRGS is permanently stored in the ROM and the second part consisting of patch and API is located in the SOLID FLASH™ NVM. The second part is only present if the NRGS is part of the delivery. If the NRGS is not part of the delivery the ROM part is present but not used. The NRGS implements tearing safe behaviour in context with the SOLID FLASH™ NVM management and is therefore independent from the HSL.

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

All optional software libraries are stored respectively can be loaded into the SOLID FLASH™ NVM.

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

---

[1] German: Bundesamt für Sicherheit in der Informationstechnik, English: Federal Office for Information Security

1.2 Target of Evaluation overview

The TOE comprises the Infineon Technologies AG security controller with specific IC dedicated firmware and optional software libraries and with specific guidance documentation according section 2.2.4 and 9.

The TOE is a member of the Infineon Technologies AG 32-bit ARM-based Security Controller family meeting high requirements in terms of performance and security. This family has been developed with a modular concept and different memory configurations, sets of peripherals and interfaces as well as different security features to satisfy market requirements. A summary product description is given in this Security Target (ST).

The TOE offers all functions that are required and useful in security systems, and integrated peripherals that are needed in high-end chipcard applications, such as embedded security and Mobile Payment. The TOE implements a dedicated security 32-bit RISC CPU designed on the basis of the ARMv7_M architecture. The core system is then composed by the 32-bit CPU as a variant of the ARM® SecurCore™ SC300™, the Cache system, the Memory Protection Unit and the Memory Encryption/Decryption Unit. The TOE implements a full 32-bit addressing with up to 4 GByte linear addressable memory space, a simple scalable memory management concept and a scalable stack size. Additionally the TOE provides a memory access control policy enforced by the Memory Protection Unit. The TOE embeds its own ROM, RAM and Non Volatile Memory, protected by the Infineon's SOLID FLASH™ NVM memory system also called NVM in the following description.

The TOE offers a wide range of peripherals, such as a UART (using the ISO7816 interface), several timers and watchdogs, a CRC module, a Tick Counter, a Hybrid Random Number Generator (HRNG) and two dedicated coprocessors for symmetric (e.g. Triple-DES, AES) and asymmetric (e.g. RSA, EC) cryptographic algorithms. The CRC module is not part of the TOE Security Functionality (TSF) of this TOE.
Additionally a range of communication interfaces, such as GPIO, I2C, SPI, SWP and a NRG interface (implemented by the NRG Base and the optional NRG Software, which are not part of the TSF of this TOE) are offered.

The firmware is composed of the Boot Software (BOS), Flash Loader (FL) and NRG Base. The BOS firmware (BOS) is used for initialization purposes and the FL allows the fast downloading of the user software/data into the NVM during the manufacturing process. The BOS is implemented in a separated access protected area of the ROM and SOLID FLASH™ NVM being part of the TOE. The NRG Base includes support for card emulation mode and reader mode and consist of the the two parts NRG Base and the optional NRG Software, which are not part of the TSF of this TOE.

This TOE implements a Hybrid Random Number Generator (HRNG). This HRNG equals to the expression Hybrid Physical True Random Number Generator (hybrid PTRNG) as defined by the BSI. In the following, the BSI expression hybrid PTRNG is used. The hybrid PTRNG implements a true physical random source and has evidenced its conformace to different classes of AIS31 [6] as declared in section 7.1.1.

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

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

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

The two cryptographic coprocessors serve the need of modern cryptography: The symmetric coprocessor (SCP) combines both AES and Triple-DES with dual-key or triple-key hardware acceleration. The asymmetric cryptographic coprocessor, called Crypto2304T in this document, supports RSA and Elliptic Curve (EC) cryptography with high performance.

The optional software part of the TOE consists of the cryptographic libraries CIPURSE™ Cryptographic Library, Symmetric Cryptographic Library, RSA, EC and Toolbox, the Hardware Support Library (HSL) and the NRG Library (Management of NRG Cards, Management of NRG Cards Extension, NRG Reader Mode Support and NRG OS, which are not part of the TSF of this TOE). If RSA or EC or Toolbox or combinations hereof are part of the shipment, automatically the Base library is included.

The RSA library in two alternative versions, 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 (SPA, DPA and DFA attacks). The routines are used for the generation of RSA key pairs, the RSA signature verification, the RSA signature generation and the RSA modulus recalculation. The hardware 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 4224 bits.

The EC library in two alternative versions, 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 EC. The EC library is delivered as object code and in this way integrated in the user software. The certification covers the standard Brainpool [S2] and NIST [S1] Elliptic Curves with key lengths of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 Bits, due to national AIS32 regulations by the BSI. 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 in two alternative versions, 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 Crypto@2304T: Addition, subtraction, division, multiplication, comparison, reduction, modular addition, modular subtraction, modular multiplication, modular inversion and modular exponentiation. The Toolbox library is not part of the TOE Security Functionality (TSF) of this TOE and does not provide any security functional requirement.The Toolbox library is deemed for software developers as support for simplified implementation of long integer and modular arithmetic operations. The Toobox library is delivered as object code and in this way integrated in the user software.

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

The Base library in two alternative versions, provides the low level interface to the asymmetric cryptographic coprocessor is delivered as object code and in this way integrated in the user software.

The Symmetric Cryptographic Library (SCL) offers a high level interface to perform the cryptographic operations DES/TDES, AES and MAC with different key length on the symmetric cryptographic coprocessor (SCP) for this TOE. The SCL implements already several block cipher modes as declared in this document and covers a wide range of applications, but the SCL offers in addition the flexibility to implement additional user defined block cipher modes.
This library provides a simplified interface to the hardware Symmetric Cryptographic Coprocessor (SCP) and preserves the security and performance requirements as required by the user.
Even in the basic configuration the SCL meets the targeted security level, which can be further increased by means of configuration options.
The key lengths used for the DES/TDES, AES and MAC functionality follow the national AIS32 regulation regarding the 100 bit security level issued by the BSI. This regulation excludes the single DES operation from the certification as it is considered to be not sufficiently secure from algorithm perspective.
Thus the certification covers the SCL cryptographic functionality of the AES algorithm with key lengths of 128, 192 and 256 bits and the TDEA or TripleDES (TDES) algorithm with an effective key size of 112 and 168 bits.

Note that this TOE can come with both cryptographic coprocessors accessible, or with a blocked SCP, or with a blocked Crypto2304T, or with both cryptographic coprocessors blocked. The blocking depends on the user's choice. No accessibility of the deselected cryptographic coprocessor is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic coprocessors. The TOE can also be delivered without a specific optional software library. In this case the TOE does not provide the functionality of the respective software library and the Additional Specific Security Functionality Rivest-Shamir-Adleman Cryptography (RSA) or/and Elliptic Curve Cryptography (EC) and/or CIPURSE™ Cryptographic Library.   If the Crypto2304T coprocessor is blocked the functionality of the RSA2048/4096 and EC and Toolbox libraries and the Additional Specific Security Functionality Rivest-Shamir-Adleman Cryptography (RSA) and Elliptic Curve Cryptography (EC) are not available. If the SCP coprocessor is blocked, the functionality of the Symmetric Cryptographic Library and the functionality related to the CIPURSE™ Cryptographic Library are not available.

Additionally the optional HSL library supports the user with an application interface (API) for 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. The HSL library is delivered as object code and in this way integrated in the user software.

The NRG Software (NRGS) as a further order option implementing the routines for a NRG interface, which are not part of the TSF of this TOE. The NRGS implements an operating system handling the emulation of a NRG card using the Single Wire Protokol. One part of the NRGS is permanently stored in the ROM and the second part implementing the API is located in the SOLID FLASH™ NVM. The second part is only present if the NRGS is part of the delivery. If the NRGS is not part of the delivery the ROM part is present but not used. The NRGS implements tearing safe behaviour in context with the SOLID FLASH™ NVM management and is therefore independent from the HSL. The NRGS do not provide any TOE security functionality. To use the optional NRGS the Single Wire Protokol shall not be blocked.

The optional CIPURSE™ Cryptographic Library (CIPURSE™ CL) provides cryptographic functionality to implement a CIPURSE™ V2 conformant protocol. This protocol provides a secure mutual authentication of two entities, namely the terminal (denoted as PCD = Proximity Coupling Device (CIPURSE™-compliant terminal)) and a smart card or a token in other form factors which is called PICC. PICC stands for Proximity Integrated Circuit Card (CIPURSE™-compliant card). Beside the mutual authentication, the protocol implements measures to maintain the integrity of the transferred data and preserves in parallel the confidentiality of the transferred data. By that the CIPURSE™ CL supports the user to implement systems conformant to the CIPURSE™ open standard implementing a secured, interoperable and flexible transit fare collection solution, including ISO 7816, ISO/IEC 14443-4 communication and AES-128 bit cryptography for multiple payment types. The optional CIPURSE™ CL is conformant to the CIPURSE™ open standard [S21] for both, the PICC and then PCD software parts. It implements the by the OSPT alliance standardized application interface for the card and the terminal side. The CIPURSE™ CL implements the by the OSPT alliance standardized application interface for the card and the terminal side.

The scope of the certification of this TOE covers all parts of the CIPURSE™ CL which are later implemented by the user on the user card respectively token based on this TOE and the functionality of the PCD software part which is implemented in the terminal side. The PCD software operates also on the hardware of this TOE which is implemented in the terminal.

To fulfill the high security standards for smartcards today and also in the future, this TOE utilizes an integral security concept comprising countermeasure mechanisms specially designed against possible attack scenarios. The TOE provide a robust set of sensors for the purpose of monitoring proper chip operating conditions and detecting fault attack scenarios. The sensors are complemented with digital error detection

mechanisms such as parities, error detection codes and instruction stream signatures and a one bit error correction functionality is provided for the SOLID FLASH™ NVM. Probing and forcing attacks will be counteracted by a shield approach, implemented by an Infineon-specific shielding combined with secure wiring of security critical signals and by encryption of all memories inside the chip (RAM, ROM, NVM). A decentralized alarm propagation and system deactivation principle is implemented, further decreasing the risk of manipulating and tampering. Additionally, an online check of parts of the security mechanisms is available by specific Special Function Resisters (UMSLC). Side-channel attacks (e.g. Timing Attack, SPA, DPA, EMA) are typically defeated using a combination of hardware and software mechanisms, for this the TOE provides several supporting features e.g. trash register writes and instruction interrupt prevention. The optional Instruction Stream Signature Checking (ISS) is a powerful countermeasure against fault attacks that try to manipulate the execution sequence of the instruction stream.

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 up 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, the functionality of the TOE matching the requirements is described.

The assets, threats, security objectives and the security functional requirements are defined in this Security Target and in the Security IC Platform Protection Profile [1] and are referenced here. These requirements build up a minimal standard common for all Smartcards.

The security functions are defined here in the security target as property of this specific TOE. Here it is shown how this specific TOE fulfils the requirements for the common standard defined in the Common Criteria documents [2], [3], [4] and in the Security IC Platform Protection Profile [1].

2   Target of Evaluation Description

The TOE description helps to understand the specific security environment and the security policy. In this context the assets, threats, security objectives and security functional requirements can be employed. The following is a more detailed description of the TOE than in Security IC Platform Protection Profile [1] 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

The TOE consists of security controller meeting high 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 Protection Profile [1].

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

The TOE consists of a core system, memories, coprocessors, buses, peripherals and control logic. In the following a briefly description of the hardware components is given.

The Core

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

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

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

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

The Busses

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

The cryptographic Coprocessors

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

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

The Memories

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

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

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

The Peripherals

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

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

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

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

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

The timers permits easy i----mplementation of communication protocols such as T=1 and all other time-critical operations. The UART-controlled I/O interface allows the smart card controller and the terminal interface to be operated independently. The watch-dog timers implement a configurable time out for various purposes. More information can be found in the "32-bit Security Controller - V07 Hardware Reference Manual "[7].

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

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

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

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

In addition to the interfaces the Hybrid Random Number Generator (HRNG) is implemented. This HRNG equals to the expression Hybrid Physical True Random Number Generator (hybrid PTRNG) as defined by the BSI. In the following, the BSI expression hybrid PTRNG is used. The hybrid PTRNG implements a true physical random source and has evidenced its conformance to different classes of AIS31 [6] as declared in section 7.1.1.

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

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

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

Guidance Documentation

The user guidance documentation of the TOE is given in section 2.2.4 and 9 .

Optional Libraries

The NRG Software (NRGS) include the optionally libraries NRG OS, Management of NRG Cards, Management of NRG Cards Extension and NRG Reader Mode Support, which are not part of the TSF of this TOE. The Management of NRG Cards provides an API for the management and generation of NRG Cards (note that the Management of NRG Cards Extension provides an additionally command). The library enables an access to external NRG cards. The libraries NRG OS and NRG Reader Mode Support can be used independently, for the use of the libraries Management of NRG Cards and Management of NRG Cards Extension the library NRG OS is also necessary.
The NRG Software is not part of the evaluated TOE Security Functionality (TSF) of this TOE.

The cryptographic libraries for RSA2048, RSA4096 and EC providing a high-level interface to the RSA and EC cryptography implemented on the hardware component Crypto2304T and including countermeasures against SPA, DPA and DFA attacks. The optional library Toolbox provides the basic long integer arithmetic and modular functions in software, supported by the cryptographic coprocessor. The Toolbox library is not part of the TOE Security Functionality (TSF) of this TOE.

The Symmetric Crypto Library (SCL) is used to provide a high level interface to DES/TDES, AES and MAC symmetric cryptographic operations. It uses the SCP of the underlying hardware but implements also countermeasures against all known weaknesses of the SCP.

The HSL library supports the user with an application interface (API) for significantly simplifying the management of the SOLID FLASH™ NVM functionality, including service routines for the tearing safe write into the SOLID FLASH™ NVM and considering also endurance, reliability and performance.

The CIPURSE™ Cryptographic Library (CIPURSE™ CL) provides cryptographic functionality to implement a CIPURSE™ V2 conformant protocol. It uses the SCP of the underlying hardware but implements also countermeasures against all known weaknesses of the SCP.

The TOE with its integrated security features meets the requirements of all smart card applications such as information integrity, access control, mobile telephone and identification, as well as uses in electronic funds transfer and healthcare systems.

To sum up, the TOE is a powerful security controller with a large amount of memory and special peripheral devices with improved performance, optimized power consumption, different interfaces 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.
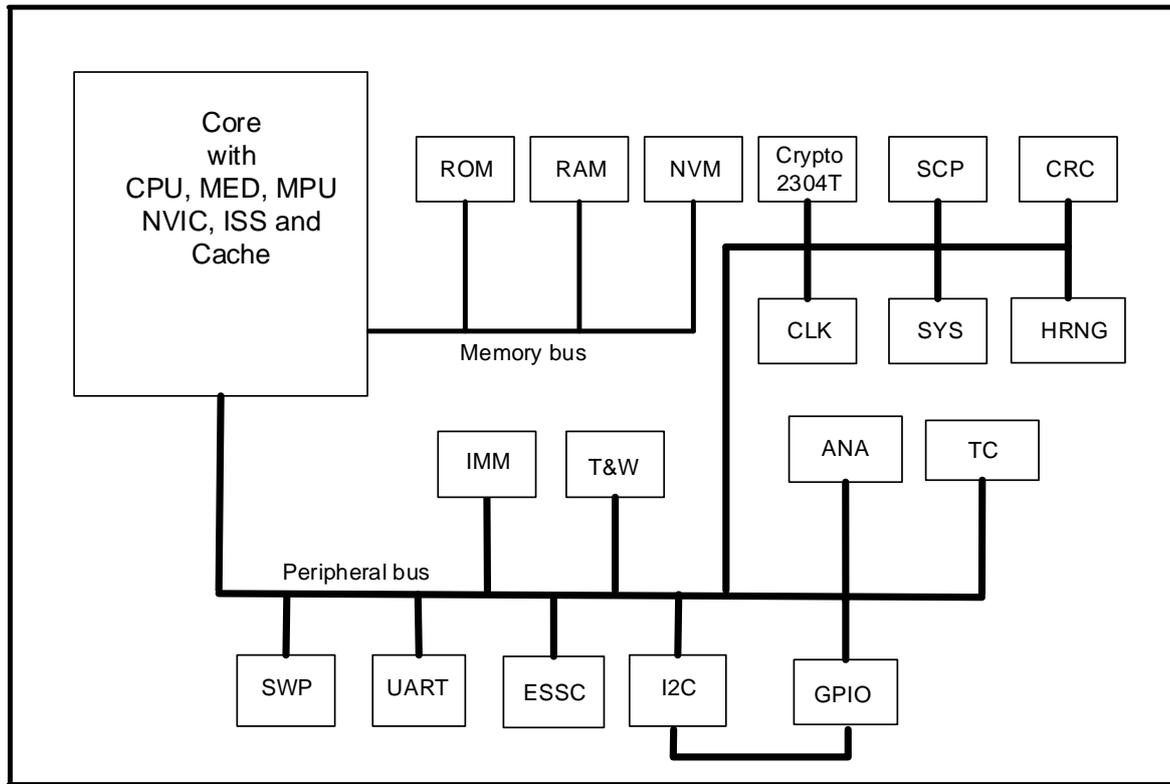
Core	Core System	ROM	Read Only Memory
NVM	SOLID FLASH™ NVM	RAM	Random Access Memory
CLK	Clock Unit	SYS	System Module
Crypto	Crypto2304T	SCP	Symmetric Crypto Processor
CRC	Cyclic Redundancy Check	HRNG	Hybrid Random Number Generator
T&W	Timer and Watchdog	UART	UART
I2C	Inter-Integrated Cirquit (I2C)	GPIO	General Purpose IO
SWP	Single Wire Protocol	ANA	Analog Units
IMM	Interface Management Module	TC	Tick Counter
ESSC	Enhancd Synhronous Serial Slave Controller		

Figure 1   Simplified block diagram of the TOE

2.2 Scope of the TOE

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

Therefore, this TOE includes:

- The silicon die, respectively the Integrated Circuit (IC) respectively the hardware of this TOE in several versions
- The TOE is also delivered in various configurations, achieved by means of blocking by the customer and/or depending on the customer order
- All configurations and resulting derivatives generated out of the mask sets described as above
- The according firmware on all derivatives and
- The optional software in various combinations as ordered
- All configurations of any individual TOE product
- The guidance documentation according section 2.2.4 and 9.

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. 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 guidance documents as listed in section 2.2.4 and 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 PP [1] is comprised of:

Core System

Proprietary 32-bit CPU implementation of ARM Secure Core SC300 based on ARMv7-M Instruction set architecture including the Instruction Stream Signature Checking (ISS)

Cache for code and data buffering

Memory Encryption/Decryption Unit (MED)

Memory Protection Unit (MPU)

Nested Vectored Interrupt Controller (NVIC)

Memories

Read-Only Memory (ROM, for internal firmware)

Random Access Memory (RAM)

SOLID FLASH™ NVM (NVM)

Note that the TOE has implemented an Electrical Erasable Programmable Read Only Memory (EEPROM) as Non-Volatile-Memory (NVM) This EEPROM module is configured to act as a flash memory and is trademarked as the SOLID FLASH™ NVM.

Peripherals

Universal Asynchronous Receiver/Transmitter (UART)

Single-Wire Protocol (SWP)

Inter Integrated Circuit (I2C) interface

General Purpose Input Output (GPIO)

Interface Management Module (IMM)

Enhanced Synchronous Serial Slave Controller (ESSC) supporting an SPI–compatible interface

Hybrid Random Number Generator (HRNG)

Timers and Watchdog including a checkpoint register (T&W)

System Module (SYS)

Clock Unit (CLK)

Tick Counter (TC)

Coprocessors

Crypto2304T coprocessor for asymmetric algorithms like RSA and EC

Symmetric Crypto Coprocessor for DES and AES Standards

Checksum module (CRC)

Analog Module (ANA)

Temperature Sensor

Backside Light Detector

Frequency Sensor

Voltage Sensor

User Mode Security Life Control (UMSLC)

Buses

Memory bus

Peripheral bus and PAU

2.2.2 Firmware and software of the TOE

For this TOE the entire firmware and software of the TOE consists of different parts including optional parts. As the differences between the various parts are transparent to the user from functional and interface perspective, the descriptions for the firmware and cryptographic library pieces hold true, regardless which part the user may have chosen. The exact versions of firmware respectively software alternatives are given in Table 1 Identification of the TOE.

One part comprises the Boot Software (BOS, IC Dedicated Test Software in PP [1]), consisting of initialization and various testing routines and providing the different operation modes of the TOE. The BOS routines are stored in a separated access protected area of the ROM and SOLID FLASH™ NVM. The BOS is not accessible for the user software.

The second part is the Flash Loader, a piece of software enabling the download of the user software or parts of it to the SOLID FLASH™ NVM memory. The Flash Loader routines are stored in a separated access protected area of the SOLID FLASH™ NVM. Depending on the order, the Flash Loader comes with the BPU-software enabling for TOE configuration at user premises. Additionally a sample mode, the PIN-Letter, is implemented as an additional PIN-Letter state of operation. Extra authentication means applied in the PIN-Letter status of the Flash Loader preserve that only the intended user with the intended PIN-Letter can configure with user specific information and enable the normal Flash Loader functions in a second step. By that the user orders the products and receives - in a protected way - the belonging PIN-Letter. PIN-Letter and delivered chips must match, in any mismatch the Flash Loader blocks any authentication. The Flash Loader provides mutual authentication of the user and the TOE and a key management functionality. The download of user data is provided in encrypted form only and the intrgrity of the loaded data is checked during and after the download. After completion of the download and/or final configuration of the TOE, and prior delivery to the end user (Phase 7: Security IC End-usage), 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. If the TOE is delivered without the Flash Loader functionality, the Flash Loader is deactivated permanently by the manufacturer Infineon Technologies AG. In derivatives with Flash Loader the related function is performed.

The third part is the NRG Base if the NRG interface option is active. If the NRG interface is deactivated the NRG Base is present but not used.

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

The optional software part of the TOE consists of the libraries HSL, SCL, RSA2048, RSA4096, EC, Toolbox which is not part of the TSF of this TOE, Base, CIPURSE™ CL and the NRGS (Management of NRG Cards, Management of NRG Cards Extension, NRG Reader Mode Support and NRG OS, which are not part of the TSF of this TOE).

The RSA library (RSA2048 or RSA4096) in two alternative versions, 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, the RSA signature verification, the RSA signature generation and the RSA modulus recalculation. The module provides the basic long number calculations (add, subtract, multiply, square with 1100-bit numbers) with high performance. The RSA library is delivered as object code and in this way integrated in the user software. The RSA library can perform RSA operations from 512 to 4224 bits (encryption up to 2048+64 bit key length). Depending on the customer's choice, the TOE can be delivered with the 4096 code portion (RSA4096) or with the 2048 code portion (RSA2048) only. The 2048 code portion is included in both. Part of the evaluation are the RSA straight operations with key lengths from 1024 bits to 2112 bits, and the RSA CRT[1] operations with key lengths of 1024 bits to 4224 bits.

---

[1] CRT: Chinese Remainder Theorem

The EC library in two alternative versions, 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 [S2] and NIST [S1] Elliptic Curves with key lengths of 224, 233, 256, 283, 320, 384, 409, 512 or 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 in two alternative versions, 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 Crypto@2304T: Addition, subtraction, division, multiplication, comparison, reduction, modular addition, modular subtraction, modular multiplication, modular inversion and modular exponentiation. The Toolbox library is deemed for software developers as support for simplified implementation of long integer and modular arithmetic operations. The Toolbox library is not part of the TOE Security Functionality (TSF) of this TOE and does not provide any security functional requirement.

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

The Base Library in two alternative versions, provides the low level interface to the asymmetric cryptographic coprocessor.

The Symmetric Cryptographic Library offers a high level interface to perform the cryptographic operations DES/TDES, AES and MAC with different key lengths on the symmetric cryptographic coprocessor (SCP) for this TOE. The SCL implements already several block cipher modes as declared in this document and covers a wide range of applications, but the SCL offers in addition the flexibility to implement additional user defined block cipher modes. The library provides a simplified interface to the hardware Symmetric Cryptographic Coprocessor (SCP) and preserves the security and performance requirements as required by the user. Even in the basic configuration the SCL meets the targeted security level, which can be further increased by means of configuration options.
The key lengths used for the AES and DES functionality follow the national AIS32 regulation regarding the 100 bit security level issued by the BSI[1]. This regulation excludes the single DES operation from the certification as it is considered to be not sufficiently secure from algorithm perspective.
Thus the certification covers the SCL cryptographic functionality of the AES algorithm with key lengths of 128, 192, 256 bits and the TDEA or TripleDES (TDES) algorithm with an effective key size of 112 and 168 bits.

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 HSL 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.

The HSL implements beyond the low level driver the basic method "In-place-Update" and additionally the basic method "Incremental Write". The "In-place-Update" includes the tearing safe methodology and leveraging the dedicated advantages of the new SOLID FLASH™ NVM technology.

---

[1] German: Bundesamt für Sicherheit in der Informationstechnik, English: Federal Office for Information Security

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.

In the case where the user decides not to use the tearing save function of the HSL, the user should be aware to implement own routines managing tearing events since if there would occur a faulty programmed SOLID FLASH™ NVM location the TOE may ends operation at that point.

The NRG as a further order option implementing the routines for a NRG interface, which are not part of the TSF of this TOE. The NRGS implements an operating system handling the emulation of a NRG card together with the Single Wire Protokoll. One part of the NRGS is permanently stored in the ROM and the second part consisting of patch and API is located in the SOLID FLASH™ NVM. The second part is only present if the NRGS is part of the delivery. If the NRGS is not part of the delivery the ROM part is present but not used. The NRGS implements tearing safe behaviour in context with the SOLID FLASH™ NVM management and is therefore independent from the HSL. The NRGS is not part of the evaluated security functionality of the TOE.

The option CIPURSE™ Cryptographic Library (CIPURSE™ CL) provides cryptographic functionality to implement a CIPURSE™ V2 conformant protocol.

This protocol provides a secure mutual authentication of two entities, namely the terminal (denoted as PCD = Proximity Coupling Device (CIPURSE™-compliant terminal)) and a smart card or a token in other form factors which is called PICC. PICC stands for Proximity Integrated Circuit Card (CIPURSE™-compliant card).

Beside the mutual authentication, the protocol implements measures to maintain the integrity of the after passing successfully the authentication transferred data. It depends on the chosen operation mode whether the user requires integrity protection only, for example if the exchange is used in a secure environment only, or whether complete protection including the encrypted transfer of user data between the two authentication entities is an issue. Both modes are part of the CIPURSE™ open standard and offered as integrity protection mode and as confidential communication mode.

By that the CIPURSE™ CL supports the user to implement systems conformant to the CIPURSE™ open standard implementing a secured, interoperable and flexible transit fare collection solution, including ISO 7816, ISO/IEC 14443-4 communication and AES-128 bit cryptography for multiple payment types.

The order CIPURSE™ CL is conformant to the CIPURSE™ open standard [S21] for both, the PICC and then PCD software parts. . It implements the by the OSPT alliance standardized application interface for the card and the terminal side.

The CIPURSE™ CL implements the by the OSPT alliance standardized application interface for the card and the terminal side.

The scope of this certification of this TOE covers all parts of the CIPURSE™ CL which are later implemented by the user on the user card respectively token based on this TOE and the functionality of the PCD software part which is implemented in the terminal side. The PCD software operates also on the hardware of this TOE which is implemented in the terminal.

The certification comprises the entire functionality of the CIPURSE™ CL implemented and operated on the TOE hardware. On one hand the TOE can operate the PICC side software part as a token and on the other hand, a second TOE product operates the PCD side software part if used inside a terminal or similar system.

The environment on the terminal, the terminal systems, their security and their interfaces to the background systems are not in the scope of this certification. The user operating system and further applications implemented on the TOE are also out of scope of this certification.

To summarize, if used with the PCD software the certification view equals to the case where the TOE is running the PICC software: The TOE operates one of the optional software parts of the CIPURSE™ CL – regardless whether PICC or PCD part - and is enabled to communicate via the selected interfaces. The surrounding environment is in both cases out of scope.

Note 1:
The cryptographic libraries RSA, EC and Toolbox 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 the RSA, EC or Toolbox libraries the TOE does not provide the Additional Specific Security Functionality Rivest-Shamir-Adleman Cryptography (RSA) and/or Elliptic Curve Cryptography (EC).
The Toolbox and Base Library are no cryptographic libraries and provide no additional specific security functionality. The Toolbox library is not part of the TSF of this TOE.

The cryptographic library SCL is a delivery option.
Therefore the TOE may come with free combinations with the other libraries of or without these libraries. In the case of coming without the SCL the TOE does not provide the specific security functionality implemented by this software. Even in case of a TOE coming without SCL, the symmetric cryptographic functionality defined by FCS_COP.1/AES and FCS_COP.1/TDES is unchanged covered by the hardware symmetric cryptographic coprocessor SCP.

The cryptographic library CIPURSE™ CL is a delivery option.
Therefore the TOE may come with free combinations with the other libraries of or without these libraries. In the case of coming without the CIPURSE™ CL the TOE does not provide the specific security functionality implemented by this software.

End of note.

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:
    - The ISO 7816 pads consist particularly of the contacted RES, I/O, CLK lines and supply lines VCC and GND. The contact based communication is according to ISO 7816/ETSI/EMV.
    - The I2C communication can be driven via the ISO 7816 pads. In this case no other communication using the ISO 7816 pads is possible.
    - The GPIO interface consists of 5 pads which can be individually configured and combined in various ways.
    - Also the I2C communication can be exclusively driven via the GPIO pads. In this case no other communication using the GPIO pads is possible.
    - The SWP interface is build out of one pad to support the SWP slave functionality.
    - The Serial Peripheral Interface (SPI) compatible provided by the Enhanced Synchronous Serial Controller
- The data-oriented I/O interface to the TOE is formed by the I/O pad.
- The interface to the firmware is constituted by special registers used for hardware configuration and control (Special Function Registers, SFR).
- The interface of the TOE to the operating system is constituted by the instruction set of the TOE.
- The interface of the TOE to the test routines is formed by the BOS test routine call, i.e. entry to test mode (OS TM entry).
- The interface to the RSA calculations is defined by the RSA library (optionally).
- The interface to the EC calculations is defined by the EC library (optionally).
- The interface to the Toolbox basic arithmetic functions is defined by the Toolbox library (optionally).
- The NRG interface is defined by the NRGS (Management of NRG Cards, Management of NRG Cards Extension, NRG Reader Mode Support, NRG OS) (all optionally), which are not part of the TSF of this TOE.

- The interface to the HSL is defined by the Hardware Support Library (optionally).
- The interface to the SCL is defined by the functions f the Symmetric Cryptographic Librarary (optionally).
- The interface to the CIPURSE™ CL is defined by the functions of the cryptographic library (optionally).

2.2.4   Guidance documentation

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

- 32-bit Security Controller - V07 Hardware Reference Manual [7] (HRM), is the user data book of the TOE and contains the relevant module, function and feature description;
- ARMv7-M Architecture Reference Manual [5] (ARM), is the user data book for the core of the TOE
- Production and personalization 32-bit ARM-based security controller User´s Manual [14] (PPM), contains detailed information about the usage of the Flash Loader
- 32-bit Security Controllers SLC37 (65 nm Technology) Programmer´s Reference Manual [11] (PRM), describes the usage and interfaces of the TOE
- 32-bit Security Controller – V07 Security Guidelines [23](SG), provides the guidance and recommenddations to develop secure software for and secure usage of this TOE
- 32-bit Security Controller – V07 Errata Sheet [12] (ERS), contains latest updates and corrections of the TOE relevant for the user and it is a kind addendum to the 32-bit Security Controller - V07 Hardware Reference Manual [7]. The Errata Sheet can be changed during the life cycle of the TOE. New Errata Sheet releases are reported in a monthly updated list provided from Infineon Technologies AG to the user. This list is not part of the certification process. Part of the TOE certification is the released version valid at the point in time the certificate was issued
- ACL37-Crypto2304T-C65 Asymmetric Crypto Library RSA / ECC / Toolbox 32-bit Security Controller User Interface [89] (ACL-1, optional), and
ACL37-Crypto2304T-C65 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox 32-bit Security Controller User interface manual [89] (ACL-2, optional),   are describing the architecture of cryptographic coprocessor on register level. It also provides a functional description of the register architecture, instruction set and gives programming guidance
- SLxx7-C65 Hardware Support Library [60] (HSL, optional) provides an application interface (API) to support the user by the handling of the SOLID FLASH™ NVM functionality
- SCL37-SCP-v4-C65 Symmetric Crypto Library for SCP-v4 AES/DES/MAC 32-bit Security Controller User interface manual [139] (SCL, optional), contains all user interfaces required to have a simplified and secure use of the symmetric cryptographic coprocessor.
- The user guidance of the optional library NRGS is included in the 32-bit Security Controllers SLC37 (65 nm Technology) Programmer´s Reference Manual [11] and in the 32-bit Security Controller – V07 Security Guidelines [23]
- CIPURSE™ Crypto Library CCL37xCIP v02.00.0005 CIPURSE™ V2 User Interface [141] (CCL, optional), provides detailed information and the complete application interface for the user for implementation of an OSPT™ compliant PCD / PICC communication solution
- 32-bit Security Controller Crypto@2304T V3 User Manual [104] (CUM), provides the interface to the asymmetric cryptographic coprocessor Crypto2304T

2.2.5 Forms of delivery

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

Table 3 Forms of delivery

TOE Component	Delivered Format	Delivery Method	Comment
Hardware			
IFX_CCI_000011h IFX_CCI_00001Bh IFX_CCI_00001Eh IFX_CCI_000025h all in the design G12	- complete modules, - plain wafers, - bare dies, - in any IC case, - in whatever type of package	Postal transfer in cages	All materials are delivered to distribution centers in cages, locked
Firmware			
BOS	–	–	This firmware part of stored on the delivered hardware
NRG Base	–	–	This firmware part of stored on the delivered hardware and not part of the TSF of this TOE
Flash Loader	–	–	This firmware part of stored on the delivered hardware
Software			
RSA2048 Library	L251 Library File (object code)	Secured download	Optional; depending on order
RSA4096 Library	L251 Library File (object code)	Secured download	Optional; depending on order
EC Library	L251 Library File (object code)	Secured download	Optional; depending on order
Toolbox Library	L251 Library File (object code)	Secured download	Optional; depending on order
Base Library	L251 Library File (object code)	Secured download	Optional; depending on presence of RSA, EC and Toolbox
SCL	L251 Library File (object code)	Secured download	Optional; depending on order. Consists of three library files
CIPURSE™ Library	L251 Library File (object code)	Secured download	Optional; depending on order
NRGS	L251 Library File (object code)	Secured download	Optional; depending on order and not part of the TSF of this TOE

HSL	L251 Library File (object code)	Secured download	Optional; depending on order
Guidance Documentation (full name see section 2.2.4)			
ARM [5]	Personalized PDF	Secured download	
HRM [7]	Personalized PDF	Secured download	–
PPM [14]	Personalized PDF	Secured download	–
PRM [11]	Personalized PDF	Secured download	–
SG [23]	Personalized PDF	Secured download	-
ERS [12]	Personalized PDF	Secured download	–
ACL-1 and ACL-2 [89]	Personalized PDF	Secured download	Optional, delivered if at least one of the RSA, EC or Toolbox libraries is ordered
SCL [139]	Personalized PDF	Secured download	Optional; delivered if the SCL library is ordered
HSL [60]	Personalized CHM	Secured download	Optional; delivered if the HSL library is ordered
CCL [141]	Personalized PDF	Secured download	Optional; delivered if the CIPURSE™ library is ordered
CUM [104]	Personalized PDF	Secured download	-

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

The form of delivery does not affect the TOE security and it can be delivered in any type, as long as the processes applied and sites involved have been audited as compliant to the Common Criteria scheme. The delivery can therefore be at the end of phase 3 or at the end of phase 4 which can also include pre-personalization steps according to PP [1]. Nevertheless in both cases the TOE is finished and the extended test features are removed. In this document are always both cases mentioned to avoid incorrectness but from the security policy point of view the two cases are identical.

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

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 Generic Chip Ident Mode (GCIM) data. The exact coding of the generic chip identification data is described in the "32-bit Security Controller - V07 Hardware Reference Manual" [7], section Chip Identification Mode.

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 (Fab number): $0A_H$

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 part 1 [2], part 2 [3], part 3 [4] and in particular, conformance is claimed for:

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

3.2 PP Claim

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

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

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

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

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

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

Table 5   Augmentations of the assurance level of the TOE

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

3.3 Package Claim

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

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

Note 2:

> This package is optional and fulfilled only by TOE products coming with a Flash Loader. Furthermore, it should be noted that in contrast to the functional package introduced in the PP [1], the availability of the authentication mechanism is not given after locking the Flash Loader. The intended use case of the authentication is to prevent a customer from flashing user data on a non-genuine TOE. No

authentication mechanism can be provided after the Flash Loader is locked.

After locking of the Flash Loader, the related threats and objectives for the operational environment and SFRs related to the TOE authentication are regarded as not applicable, due to the fact that it is out of scope of the intended use-case and the authentication functionality is no longer available.

End of note.

Depending on the availability of the optional Symmectric Cryptographic Coprocessor:

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

These packages are optional and fulfilled by TOE products coming with an activated Symmetric Cryptographic Coprocessor. The additionally available optional SCL does not change the conformance of the packages.

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 [1].

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

- the circuitry of the IC (hardware including the physical memories),
- configuration data, initialization data related to the IC Dedicated Software and the behavior of the security functionality
- the IC Dedicated Software with the parts
- the IC Dedicated Test Software,
- the IC Dedicated Support Software
- the guidance documentation according section 2.2.4 and 9.

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

3.4.1 Security Problem Definition

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

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, the threat memory access violation T.Mem-Access, due to specific TOE memory access control functionality, and the threat T.Open_Samples_Diffusion, due to the Flash Loader functionality have

been added. These add-ons have no impact on the conformance statements regarding CC [2] and PP [1], with following rational:

- The security target remains conformant to CC [2], claim 482 as the possibility to introduce additional restrictions is given.
- The security target fulfills the strict conformance claim of the PP [1] due to the application notes 4, 5 and 6 which apply here. By those notes the addition of further security functions and security services are covered, even without deriving particular security functionality from a threat but from a policy.

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
- the objectives related to the Flash Loader
    - O.Authentication,
    - O.Cap_Avail_Loader,
    - O.Ctrl_Auth_Loader,
    - O.Prot_TSF_Confidentiality
- and objectives related to CIPURSE™ Cryptographic Library
    - O.Add-Functions,

additional security objectives have been introduced.

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

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

3.4.4   AES and TDES

The PP [1] implements the optional policy cryptographic services P.Crypto_Service with its packages "TDES" and "AES". This TOE provides these optional packages requiring secure hardware based cryptographic services for the IC Embedded Software as outlined in section 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 [2] and PP [1], with following rational:

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

3.4.5 Loader

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

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

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

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

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

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

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

Due to these optional additional security functionalities the security objectives

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

These add-ons have no impact on the conformance statements regarding CC [2] and PP [1] as defined in section 3.4.2.

3.4.6   Summary

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

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

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

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

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

Table 6   Security Functional Requirements

Security Functional Requirement	Description	Source
FDP_ACC.1	Subset access control	CCP2 [3]
FDP_ACF.1	Security attribute based access contol	CCP2 [3]
FMT_MSA.1	Management of security attributes	CCP2 [3]
FMT_MSA.3	Static attribute initialization	CCP2 [3]
FMT_SMF.1	Specification of Management functions	CCP2 [3]
FCS_CKM.1/RSA-1	Cryptographic key generation – RSA-1	CCP2 [3]
FCS_CKM.1/RSA-2	Cryptographic key generation – RSA-2	CCP2 [3]
FCS_CKM.1/EC-1	Cryptographic key generation – EC-1	CCP2 [3]
FCS_CKM.1/EC-2	Cryptographic key generation – EC-2	CCP2 [3]
FCS_CKM.1/CCL	Cryptographic key generation - CCL	CCP2 [3]
FCS_CKM.4/TDES (5)	Cryptographic key destruction – TDES	PP [1]
FCS_CKM.4/AES (5)	Cryptographic key destruction – AES	PP [1]
FCS_CKM.4/CCL	Cryptographic key destruction – CCL	CCP2 [3]
FCS_COP.1/RSA-1	Cryptographic operation – RSA-1	CCP2 [3]
FCS_COP.1/RSA-2	Cryptographic operation – RSA-2	CCP2 [3]
FCS_COP.1/ECDSA-1	Cryptographic operation – ECDSA-1	CCP2 [3]
FCS_COP.1/ECDSA-2	Cryptographic operation – ECDSA-2	CCP2 [3]
FCS_COP.1/ECDH-1	Cryptographic operation – ECDH-1	CCP2 [3]
FCS_COP.1/ECDH-2	Cryptographic operation – ECDH-2	CCP2 [3]
FCS_COP.1/TDES (5)	Cryptographic operation - TDES	PP [1]
FCS_COP.1/AES (5)	Cryptographic operation - AES	PP [1]

FCS_COP.1/TDSCL	Cryptographic operation – TDES - SCL	CCP2 [3]
FCS_COP.1/AESCL	Cryptographic operation – AES - SCL	CCP2 [3]
FCS_COP.1/CMAC	Cryptographic operation – CMAC - SCL	CCP2 [3]
FCS_COP.1/RMAC	Cryptographic operation – RMAC - SCL	CCP2 [3]
FCS_COP.1/CCL	Cryptographic operation – CCL	CCP2 [3]
FCS_RNG.1/KSG	Generation of Random Numbers - KSG	PP [1]
FCS_RNG.1/TRNG	Generation of Random Numbers -TRNG	PP [1]
FCS_RNG.1/HPRG	Generation of Random Numbers - HPRG	PP [1]
FCS_RNG.1/DRNG	Generation of Random Numbers -DRNG	PP [1]
FDP_SDI.2	Stored data integrity monitoring and action	PP [1]
FDP_SDC.1	Stored data confidentiality	PP [1]
FAU_SAS.1	Audit data storage	PP [1]
FMT_LIM.1	Limited capabilities	PP [1]
FMT_LIM.2	Limited availability	PP [1]
FMT_LIM.1/Loader (8)	Limited capabilities	PP [1]
FMT_LIM.2/Loader (8)	Limited availability - Loader	PP [1]
FRU_FLT.2	Limited fault tolerance	PP [1]
FPT_FLS.1	Failure with preservation of secure state	PP [1]
FPT_PHP.3	Resistance to physical attack	PP [1]
FDP_ITT.1	Basic internal transfer protection	PP [1]
FPT_ITT.1	Basic internal TSF data transfer protection	PP [1]
FDP_IFC.1	Subset information flow control	PP [1]
FIA_API.1 (7)	Authentication Proof of the Identity	PP [1]
FTP_ITC.1 (6)	Inter-TSF trusted channel	PP [1]
FDP_UCT.1 (6)	Basic data exchange confidentiality	PP [1]
FDP_UIT.1 (6)	Data exchange integrity	PP [1]
FDP_ACC.1/Loader (6)	Subset access control - Loader	PP [1]
FDP_ACF.1/Loader (6)	Security attribute based access control - Loader	PP [1]

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

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

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

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

The following security functional requirements are included and completely defined in this ST, section 6.

FPT_TST.2	Subset TOE security testing

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

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

3.5 Application Notes

The functional requirements

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

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

4 Security Problem Definition (ASE_SPD)

The content of the PP [1] applies to this section 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 [1] section 3.2 and 7.2.

Table 7   Threats according PP [1]

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

4.1.1 Additional Threat due to TOE specific Functionality

Threat Memory Access Violation

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

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

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

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

Threat Diffusion of Open Samples

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

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

T.Open_Samples_Diffusion	Diffusion of open samples An attacker may get access to open samples of the TOE and use them to gain information about the TSF (loader, memory, management unit, ROM code, …). He may also use the open samples to characterize the behavior of the IC and its security functionalities (for example: characterization of side channel profiles, perturbation crytography, …). The execution of dedicated security features (for example: execection 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 8   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 [1].

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

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

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

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

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

For details see PP [1] section 3.1.

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.

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

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

Table 9   Organizational Security Policies according PP [1]

P.Process-TOE	Identification during TOE Development and Production

4.2.1   Augmented Organizational Security Policy

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

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

The IC Developer / Manufacturer must apply the 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) • CIPURSE™ Cryptographic Library (CCL) • Cipher based Message Authentication Code (CMAC) • Cipher based Retail-MAC (RMAC)

Note 3:
The cryptographic libraries CCL, SCL, RSA and EC 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 CCL, RSA and EC, the TOE does not provide the Additional Specific Security Functionality Rivest-Shamir-Adleman Cryptography (RSA) and/or Elliptic Curve Cryptography (EC) and/or CIPURSE™ Cryptographic Library.
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 4:

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

End of note.

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

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

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

4.3 Assumptions

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

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

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 [1] section 3.4.

4.3.2   Note regarding CIPURSE™ CL

The CIPURSE™ CL as cryptographic functionality establishes a cryptographic secured communication channel between two identified entities. Depending on the implementation and usage, the CIPURSE™ CL can act either in the PICC or in the PCD role. In any case the secrets applied for establishing and usage of the secured channel must be treated in an appropriate way by both entities PICC and PCD.
This means that it is essential on user side that the critical data for establishing this cryptographic secured communication channel is generated and stored in an appropriate way and that integrity and confidentiality is maintained.
These preconditions are treated in the PP [1] section 3.4 Assumption with A.Resp-Appl.

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 [1] section 4.1, 7.2.1, 7.3.1, 7.3.2, 7.4.1 and 7.4.2 and in this section.

Table 10   Objectivs for the TOE according to PP [1]

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

Note 5:
The O.Cap_Avail_Loader applies to every TOE product, the objectives O. Authentication, O.Ctrl_Auth_Loader

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

The TOE 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)
	• CIPURSE™ Cryptographic Library (CCL)
	• Cipher base Message authentication code (CMAC)
	• Retail-MAC (RMAC)

Note 6:
The cryptographic libraries CCL, SCL, RSA and EC 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 CCL, SCL, RSA and EC, the TOE does not provide the Additional Specific Security Functionality Rivest-Shamir-Adleman Cryptography (RSA) and/or Elliptic Curve Cryptography (EC) and/or Cipher based Message Authentication Code (CMAC) and/or Retail-MAC (RMAC) and/or CIPURSE™ Cryptographic Library.
End of note.

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

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

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

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

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

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

Table 11   Additional objectives due to TOE specific functions and augmentation

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 from PP for development and environment

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

For secure use of the CIPURSE™ CL it is essential that on user side the common secret is generated and stored in an appropriate way and that integrity and confidentiality of this user secret is maintained. These preconditions are treated in the PP [1] section 3.1 claims 67 and 68.

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

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

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

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

Note 8:
The objectives OE.Lim_Block_Loader, OE.TOE_Auth and OE.Loader_Usage for the development and operation environment apply only at TOE products coming with activated Flash Loader enabled for user data download by the user. In other cases the Flash Loader is not available anymore and the user data download is completed. Depending on the capabilities of the user software this objective may then reoccur as subject of the composite TOE.
End of note.

5.3 Security Objectives for the environment

The CIPURSE™ CL requires the presence of a common secret on both communication entities. This is covered by assigning the OE.Resp-Appl defined in PP [1], section 4.3 Security Objectives for the Security Embedded Software with an additionally clarification.

OE.Resp-Appl	Treatment of User data of the Composite TOE
	Please refer to chapter 5.3.1 for clarification

Note 9:
The CIPURSE™ CL is a delivery option. In case the user has ordered the CIPURSE™ CL, the user is responsible to implement the CIPURSE™ CL into his user software. In addition, the user has to generate and treat the common secret in an appropriate way. The objective common secret is therefore similar to the OE.Resp-Appl. Anyhow, processes and treatment is exclusively subject of the user and his logistic processes.
End of note.

Note 10:
If the user decides to use the integrity protection mode of the CIPURSE™ CL then the confidentiality of the user data to be transferred is solely subject of the user.
End of note.

Note 11:
The CIPURSE™ CL as cryptographic functionality establishes a cryptographic secured communication channel between two identified entities. Depending on the implementation and usage, the CIPURSE™ CL can act either in the PICC or in the PCD role. In any case the secrets applied for establishing and usage of the secured channel must be treated in an appropriate way by both entities PICC and PCD.
This means that it is essential on user side that the critical data for establishing this cryptographic secured communication channel is generated and stored in an appropriate way and that integrity and confidentiality is maintained.
These preconditions are treated in the PP [1] section 3.4 Assumption with A.Resp-Appl.
End of note.
The table below lists the security objectives.

Table 12   Security Objectives for the Environment according the PP [1]

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

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

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

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

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

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

5.4   Security Objectives Rationale

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

Table 13   Security Objective Rationale

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

P.Add-Functions

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.

A.Key-Function

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

T.Mem-Access

Compared to the PP [1] an enhancement regarding memory area protection has been established. The clear definition of privilege levels for operated software establishes the clear separation of different restricted memory areas for running the firmware, downloading and/or running the operating system and to establish a clear separation between different applications. Nevertheless, it is also possible to define a shared memory section where separated applications may exchange defined data. The privilege levels clearly define by using a

hierarchical model the access right from one level to the other. These measures ensure that the threat T.Mem-Access is clearly covered by the security objective O.Mem-Access.

T.Open_Samples_Diffusion

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

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 family FDP_SDC at the class FDP User Data Protection
- the component FPT_TST.2 at the class FPT Protection of the TSF
- the family FIA_API at the class FIA Identification and Authentication

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

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 [3] provides the security functional component "TSF testing (FPT_TST.1)". The component FPT_TST.1 provides the ability to test the TSF's correct operation.

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

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 [3]). This component allows that particular parts of the security mechanisms and functions provided by the TOE can be tested after TOE Delivery or are tested automatically and continuously during normal operation transparent for the user.

This security functional component is used instead of the functional component FPT_TST.1 from Common Criteria Part 2 [3]. For the user it is important to know which security functions or mechanisms can be tested. The functional component FPT_TST.1 does not mandate to explicitly specify the security functions being tested. In addition, FPT_TST.1 requires verifying the integrity of TSF data and stored TSF executable code which might violate the security policy.

The functional component "Subset TOE testing (FPT_TST.2)" is specified as follows (Common Criteria Part 2 extended [3]).

6.2.1 TSF self-test (FPT_TST)

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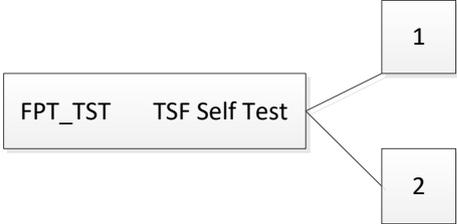
FPT_TST.1:	The component FPT_TST.1 is defined in [3] section 15.14 (444, 445, 446).
FPT_TST.2:	Subset TOE security testing, provides the ability to test the correct operation of particular security functions or mechanisms. These tests may be performed at start-up, periodically, at the request of the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

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

7 Security Requirements (ASE_REQ)

For this section the PP [1] section 6 can be applied completely.

7.1 TOE Security Functional Requirements

The security functional requirements (SFR) for the TOE are defined and described in the PP [1] section 6.1, 7.2, 7.3, 7.4.1, 7.4.2 and in the following description.

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

The refinements are also valid for this ST.

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

Table 14   Security functional requirements defined / refined / augmented by source

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

Security Functional Requirement	Description	Source	Defined in Source / Refined in ST / Completed in ST / Augmented in ST
FIA_API.1	"Authentication Proof of Identity"	PP [1]	completed
FTP_ITC.1	"Inter-TSF trusted channel"	PP [1]	completed
FDP_UCT.1	"Basic data exchange confidentiality"	PP [1]	defined
FDP_UIT.1	"Data exchange integrity"	PP [1]	defined
FDP_ACC.1/Loader	"Subset access control – Loader"	PP [1]	completed
FDP_ACF.1/Loader	"Security attribute based access control – Loader"	PP [1]	completed
FCS_COP.1/TDES	"Cryptographic operation – TDES"	PP [1]	refined/completed
FCS_COP.1/TDSCL	"Cryptographic operation – TDES by SCL"	PP [1]	refined/completed
FCS_COP.1/AES	"Cryptographic operation – AES"	PP [1]	refined/completed
FCS_COP.1/AESCL	"Cryptographic operation – AES by SCL"	PP [1]	refined/completed
FCS_COP.1/CMAC	"Cryptographic operation – CMAC by SCL"	PP [1]	refined/completed
FCS_COP.1/RMAC	"Cryptographic operation – RMAC by SCL"	PP [1]	refined/completed
FCS_COP.1/RSA-1	"Cryptographic operation – RSA by ACL-1"	CCP2 [3]	augmented
FCS_COP.1/RSA-2	"Cryptographic operation – RSA by ACL-2"	CCP2 [3]	augmented
FCS_COP.1/ECDSA-1	"Cryptographic operation – ECDSA by ACL-1"	CCP2 [3]	augmented
FCS_COP.1/ECDSA-2	"Cryptographic operation – ECDSA by ACL-2"	CCP2 [3]	augmented
FCS_COP.1/ECDH-1	"Cryptographic operation – ECDH by ACL-1"	CCP2 [3]	augmented
FCS_COP.1/ECDH-2	"Cryptographic operation – ECDH by ACL-2"	CCP2 [3]	augmented
FCS_COP.1/CCL	"Cryptographic operation – CCL"	CCP2 [3]	augmented
FCS_CKM.1/RSA-1	"Cryptographic key generation – RSA by ACL-1"	CCP2 [3]	augmented
FCS_CKM.1/RSA-2	"Cryptographic key generation – RSA by ACL-2"	CCP2 [3]	augmented
FCS_CKM.1/EC-1	"Cryptographic key generation –EC by ACL-1"	CCP2 [3]	augmented
FCS_CKM.1/EC-2	"Cryptographic key generation –EC by ACL-2"	CCP2 [3]	augmented
FCS_CKM.1/CCL	"Cryptographic key generation - CIPURSE™ CL"	CCP2 [3]	augmented
FCS_CKM.4/TDES	"Cryptographic key destruction – TDES"	PP [1]	completed
FCS_CKM.4/AES	"Cryptographic key destruction – AES"	PP [1]	completed
FCS_CKM.4/CCL	"Cryptographic key destruction – CCL"	CCP2 [3]	augmented
FMT_MSA.1	"Management of security attributes"	CCP2 [3]	augmented
FMT_MSA.3	"Static attribute initialization"	CCP2 [3]	augmented
FMT_SMF.1	"Specification of Management functions "	CCP2 [3]	augmented
FPT_TST.2	"TOE security testing"	CCP2 [3]	augmented

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

Notes:

- The security functional requirements FCS_COP.1/RSA-1, FCS_COP.1/RSA-2, FCS_CKM.1/RSA-1 and FCS_CKM.1/RSA-2 apply only if the corresponding asymmetric cryptographic library RSA2048/4096 is part of the TOE.
- The security functional requirements FCS_COP.1/ECDSA-1, FCS_COP.1/ECDSA-2, FCS_COP.1/ECDH-1, FCS_COP.1/ECDH-2, FCS_CKM.1/EC-1 and FCS_CKM.1/EC-2 apply only if the corresponding asymmetric cryptographic library EC is part of the TOE.
- The security functional requirements FCS_COP.1/TDSCL, FCS_COP.1/AESCL, FCS_COP.1/CMAC and FCS_COP.1/RMAC apply only if the corresponding symmetric cryptographic library SCL is part of the TOE.
- The security functional requirements FIA_API.1, FTP_ITC.1, FDP_UCT.1, FDP_UIT.1, FDP_ACC.1/Loader and FDP_ACF.1/Loader applying only at TOE products coming with activated Flash Loader enabled for user data download. In other cases the Flash Loader is not available anymore and the user data download is completed. Depending on the capabilities of the user software these security functional requirements may then reoccur as subject of the composite TOE.
- The security functional requirements FCS_COP.1/CCL, FCS_CKM.1/CCL and FCS_CKM.4/CCL apply only if the optional software CIPURSE™ Cryptographic Library is on board.

7.1.1 Extended Components FCS_RNG.1 and FAU_SAS.1

7.1.1.1 FCS_RNG Generation of random numbers

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

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

Note 12:
The functional requirements FCS_RNG.1/TRNG, FCS_RNG.1/HPRG, FCS_RNG.1/DRNG, FCS_RNG.1/KSG, are iterations of the FCS_RNG.1 defined in the Protection Profile [1] according to "Anwendungshinweise und Interpretationen zum Schema (AIS)" respectively "A proposal for: Functionality classes for random number generators" [6].
End of note.

Note 13:
The Hybrid Physical Random Number Generator (hybrd PTRNG) implements total failure testing of the random source data and a continuous random number generator test according to:
National Institute of Standards and Technology, Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication (FIPS) 140-2, 2002-03-12 section 4.9.2.
End of note.

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

7.1.1.2   True Random Number Generation, meeting [6] PTG.2

FCS_RNG.1/TRNG	**Random Number Generation**
Hierarchical to:	No other components
Dependencies:	No dependencies
FCS_RNG.1/TRNG	Random numbers generation **Class PTG.2** according to [6]
FCS_RNG.1.1/TRNG	The TSF shall provide a <u>physical</u> random number generator that implements:
PTG.2.1	<u>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.</u>
PTG.2.2	<u>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.</u>
PTG.2.3	<u>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.</u>
PTG.2.4	<u>The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.</u>
PTG.2.5	<u>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.</u>
FCS_RNG.1.2/TRNG	The TSF shall provide <u>numbers in the format 8- or 16-bit</u> that meet
PTG.2.6	<u>Test procedure A, as defined in [6] does not distinguish the internal random numbers from output sequences of an ideal RNG.</u>
PTG.2.7	<u>The average Shannon entropy per internal random bit exceeds 0.997.</u>

7.1.1.3 Hybrid Random Number Generation, meeting [6] PTG.3

FCS_RNG.1/HPRG	**Random Number Generation**
Hierarchical to:	No other components
Dependencies:	No dependencies
FCS_RNG.1/HPRG	Random numbers generation **Class PTG.3** according to [6]
FCS_RNG.1.1/HPRG	The TSF shall provide a <u>hybrid physical</u> random number generator that implements:

PTG.3.1   A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure has been detected no random numbers will be output.

PTG.3.2   If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.

PTG.3.3   The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test and the seeding of the DRG.3 post-processing algorithm have been finished successfully or when a defect has been detected.

PTG.3.4   The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.

PTG.3.5   The online test procedure checks the raw random number sequence. It is triggered continuously. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.

PTG.3.6   The algorithmic post-processing algorithm belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function, and the output data rate of the post-rocessing algorithm shall not exceed its input data rate.

FCS_RNG.1.2/HPRG	The TSF shall provide <u>numbers in the format 8- or 16-bit</u> that meet

PTG.3.7   Statistical test suites cannot practically distinguish the internal random numbers from output sequences of an ideal RNG. The internal random numbers must pass test procedure A.

PTG.3.8   The internal random numbers shall use PTRNG of class PTG.2 as random source for the post-processing.

Note to PTG.3.5:
Continuously means that the raw random bits are scanned continuously.
The algorithmic post-processing algorithm belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function, and the output data rate of the post-processing algorithm shall not exceed its input data rate.
End of note.

Note to PTG.3.8:
The internal random numbers produced by the employed PTG.2-conform PTRNG are adaptively compressed raw bits, where the compression rate is controlled by a so-called entropy estimator. The concept ensures that the random numbers provided by the PTRNG have high entropy, i.e., each delivered random byte will have more the 7.976 bit of entropy. In addition, the PTRNG produced random numbers have been tested against test procedures A and B under varying environment conditions conditions.
End of note.

7.1.1.4   Deterministic Random Number Generation, meeting [6] DRG.3

FCS_RNG.1/DRNG	**Random Number Generation**
Hierarchical to:	No other components
Dependencies:	No dependencies
FCS_RNG.1/DRNG	Random numbers generation **Class DRG.3** according to [6]
FCS_RNG.1.1/DRNG	The TSF shall provide a <u>deterministic</u> random number generator that implements:
DRG.3.1	<u>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.</u>
DRG.3.2	<u>The RNG provides forward secrecy.</u>
DRG.3.3	<u>The RNG provides backward secrecy even if the current internal state is known.</u>
FCS_RNG.1.2/DRNG	The TSF shall provide random numbers that meet:
DRG.3.4	<u>The RNG, initialized with a random seed, where the seed has at least 100 bit of entropy and is derived by a PTG.2 certified PTRNG. The RNG generates output for which any consecutive 2^{34} bits strings of bit length 128 are mutually different with a probability that is greater than $1 - 2^{(-16)}$.</u>

DRG.3.5	Statistical test suites cannot practically distinguish the random numbers from the output sequences of an ideal RNG. The random numbers must pass test procedure A and the U.S. National Institute of Standards and Technologiy (NIST) test suite for RNGs used for cryptographic purposes [S17] containing following 16 tests:
	Frequency (Monobit) Test, Frequency Test within a Block, Runs Tests, Test for the Longest-Run-of-Ones in a Block, Binary Matrix Rank Test, Discrete Fourier Transform (Spectral) Test, Non-overlpping (Aperiodic) Template Matching Test, Overlapping (Periodic) Template Matching Test, Maurer´s "Universal Statistical" Test, Liner Complexity Test, Serial Test, Approximate Entropy Test, Cumulative Sums (Cusums) Test, Random Excursions Test and Random Excursions Variant Test.

Note to DRG.3.1:
Furthermore, the length of the internal state shall have at least 200 bit. (For the DRG.3 under consideration, the internal state has 351 bit.). The seed is provided by a certified PTG.2 physical TRNG with guaranteed 7,976 bit of entropy per byte.
End of note.

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

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

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

FCS_RNG.1.2/KSG	The TSF shall provide random numbers that meet:
DRG.2.4	<u>The RNG, initialized with a random seed of length at least 100 bit delivered by an PTRNG of the class PTG.2, generates output for which any consecutive 2^{34} strings of the length 128 bits are mutually different with probability greater than $1-2^{(-16)}$.</u>
DRG.2.5	<u>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.</u>

Note to DRG.2.2:

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

End of note.

Note to DRG.2.3:

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

End of note.

Note to DRG.2.5:

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

End of note.

7.1.1.6   FAU_SAS

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

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

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

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

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 [3]).

FPT_TST.2	**Subset TOE testing**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.2.1	The TSF shall provide a suite of self-test features <u>at the request of the authorized user</u> to demonstrate the correct operation <u>of the alarm lines and/or following environmental sensor mechanisms:</u> • <u>Please refere to the Confidential Security Target [16]</u>

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 protection unit (MPU) is documented in section 4 in the "32-bit Security Controller - V07 Hardware Reference Manual" [7].

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

The security functional requirement **"Static attribute initialization (FMT_MSA.3)"** ensures that the default values of security attributes are appropriately either permissive or restrictive in nature. Alternative values can be specified by any subject provided that the **Memory Access Control Policy** allows that. This is described by

the security functional requirement **"Management of security attributes (FMT_MSA.1)".** The attributes are determined during TOE manufacturing (FMT_MSA.3) or set at run-time (FMT_MSA.1).

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

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

Memory Access Control Policy

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

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

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

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

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

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

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

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 <u>Memory Access Control Policy</u> to objects based on the following: <u>Subject:</u> <u>- software running at privilege mode</u> <u>- software running at user mode</u> <u>Object:</u> <u>- data including code stored in memories</u> <u>Attributes:</u> <u>- the memory area where the access is performed to and the corresponding permission control information and/or</u> <u>- the operation to be performed.</u>
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: <u>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.</u>
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: <u>none.</u>

FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: <u>none.</u>

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 <u>Memory Access Control Policy</u> to provide <u>well defined(11)</u> default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow <u>the subject</u> <u>- software running at privilege mode (12),</u> to specify alternative initial values to override the default values when an object or information is created.

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

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

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

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

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

FMT_SMF.1	Specification of management functions
Hierarchical to:	No other components
Dependencies:	No dependencies
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: <u>the subject</u> <u>- software running at privilege mode</u> (12) <u>shall be able to access the configuration registers of the MPU.</u>

7.1.4 Support of Cipher Schemes

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

FCS_COP.1 Cryptographic operation requires a cryptographic operation to be performed in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard; dependencies are discussed in section 7.3.1.5.

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

- Rivest-Shamir-Adleman (RSA)
- Elliptic Curve Cryptography (EC)
- Advanced Encryption Standard (AES)
- Triple Data Encryption Standard (TDES)
- Cipher based Message Authentication Code (CMAC)
- Retail-MAC (RMAC)
- CIPURSE™ Cryptographic Library (CCL)

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 (encryption up to 2048 +64 bit key length).

The additional function of the EC library, providing the primitive elliptic curve operations *ECC add* and *ECC double*, does not add specific security functionality.

Note 14:
In case a user deselects the RSA and/or EC library, the TOE provides basic HW-related routines for RSA and/or EC calculations. For secure library implementations the user has to implement additional countermeasures. End of note.

Note 15:
This TOE can come with both crypto coprocessors accessible, or with a blocked SCP, or with a blocked Crypto2304T, or with both cryptographic coprocessors blocked. The blocking depends on the customer demands prior to the production of the hardware. In case the SCP is blocked, no AES, DES and MAC computation supported by hardware and no CIPURSETM Cryptographic Library functionality is possible. In case the Crypto2304T is blocked, no RSA and EC computation supported by hardware is possible. No accessibility of the deselected cryptographic coprocessor is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic coprocessors.

In case the SWP interface is blocked, the CIPURSE™ Cryptographic Library usage is not possible.
End of note.

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

7.1.4.2 Triple-DES Operation

The following operations of the TOE shall meet the requirements "Cryptographic operation (FCS_COP.1)" and "Cryptographic key destruction" (FCS_CKM.4) as specified below:

FCS_COP.1/TDES	Cryptographic operation
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key management] FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1.1/TDES	The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm Triple Data Encryption Standard (TDES) in

- the Electronic Codebook Mode (ECB)
- the Cipher Block Chaining Mode (CBC)
- the Cipher Block Chaining Message Authentication Code (CBC-MAC)
- the Cipher Block Chaining Message Authentication Code Encrypt Last Block (CBC-MAC-ELB)

and cryptographic key sizes of 112 or 168 bit that meet the following:

- National Institute of Standards and Technology (NIST) SP 800-67 Rev. 2 [S4]
- the ECB, CBC:
National Institute of Standards and Technology (NIST) SP 800-38A [S5]
- the CBC-MAC, CBC-MAC-ELB:
ISO/IEC 9797-1 Mac Algorithm 1 and 2 respectively [S14]

Note 16:
The FCS_COP.1/TDES refers to the direct hardware DES interface of the Symmetric Crypto coprocessor (SCP).
End of note.

FCS_COP.1/TDSCL	Cryptographic operation
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key management] FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1.1/TDSCL	The TSF shall perform <u>encryption and decryption</u> in accordance with a specified cryptographic algorithm <u>Triple Data Encryption Standard (TDES) in</u>

- the Electronic Codebook Mode (ECB)
- the Cipher Block Chaining Mode (CBC)
- the Counter Mode (CTR)
- the Cipher Feedback Mode (CFB)
- the Propagating Cipher Block Chaining Mode (PCBC)

and cryptographic key sizes of <u>112 or 168 bit</u> that meet the following:

- National Institute of Standards and Technology (NIST) SP 800-67 Rev. 2 [S4]
- the ECB, CBC, CTR and CFG:
  National Institute of Standards and Technology (NIST) SP 800-38A [S5]
- the PCBC:
  Bruce Schneier, Applied Cryptography, Second Edition, John Wiley & Sons,1996 [S23]. This standard should be implemented considering the 32-bit Security Controller – V07 Security Guidelines [23] only

Note 17:
The FCS_COP.1/TDSCL refers to the DES interface provided by the Symmetric Crypto Library (SCL).
End of note.

FCS_COP.1/CMAC	Cryptographic operation - CMAC
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/CMAC	The TSF shall perform *computation of a cipher based message authentication code* in accordance with a specified cryptographic algorithm *CMAC using*
	
	• *AES or*
	• *TDES*
	
	and cryptographic key sizes *of 128 bit or 192 bit or 256 bit for AES and 168 bit for TDES* that meet the following standards:
	
	• *CMAC: National Institute of Standards and Technology (NIST) SP 800-38B [S7]*
	• *AES*
	   o *Federal Information Standards Publication 197 [S8]*
	   o *TDES*
	   o *National Institute of Standards and Technology SP 800-67 [S4]*

FCS_COP.1/RMAC	Cryptographic operation - RMAC
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/RMAC	The TSF shall perform *computation of a cipher based Retail-MAC* in accordance with a specified cryptographic algorithm *Retail-MAC using* • *TDES* and cryptographic key sizes *of 112 bit for TDES* that meet the following standards: o ISO/IEC 9797-1:2011 Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher *[S14]*

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 <u>overwriting or zeroing</u> that meets the following: <u>none</u>

Note 18:

For FCS_COP.1/TDES, FCS_COP.1/TDSCL, FCS_COP.1/CMAC and FCS_COP.1/RMAC the key destruction can be done by overwriting the key register interfaces or by software reset of the SCP which provides immediate zeroing of all SCP key registers.
End of note.

Note 19:

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

The TOE can be delivered with the optional Symmetric Cryptographic Library (SCL). If the optional SCL is not available then the FCS_COP.1/TDSCL, FCS_COP.1/CMAC and FCS_COP.1/RMAC are not applicable.
End of note.

7.1.4.3   AES Operation

The following operations of the TOE shall meet the requirements "Cryptographic operation (FCS_COP.1)" and "Cryptographic key destruction" (FCS_CKM.4) as specified below:

FCS_COP.1/AES	Cryptographic operation
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/AES	The TSF shall perform <u>decryption and encryption</u> in accordance with a specified cryptographic algorithm <u>Advanced Encryption Standard (AES) in</u> • <u>the Electronic Codebook Mode (ECB)</u> • <u>the Cipher Block Chaining Mode (CBC)</u> • <u>the Cipher Block Chaining Message Authentication Code (CBC-MAC)</u> • <u>the Cipher Block Chaining Message Authentication Code Encrypt Last Block (CBC-MAC-ELB)</u> and cryptographic key sizes of <u>128 bit or 192 bit or 256 bit</u> that meet the following:

- FIPS 197 [S8]
- the ECB, CBC:
  National Institute of Standards and Technology (NIST) SP 800-38A [S5]
- the CBC-MAC, CBC-MAC-ELB:
  ISO/IEC 9797-1 Mac Algorithm 1 and 2 respectively [S14]

Note 20:
The FCS_COP.1/AES refers to the direct hardware AES interface of the Symmetric Crypto coprocessor (SCP).
End of note.

FCS_COP.1/AESCL	Cryptographic operation
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/AESCL	The TSF shall perform decryption and encryption in accordance with a specified cryptographic algorithm Advanced Encryption Standard (AES) in

- the Electronic Codebook Mode (ECB)
- the Cipher Block Chaining Mode (CBC)
- the Counter Mode (CTR)
- the Cipher Feedback Mode (CFB)
- the Propagating Cipher Block Chaining (PCBC)

and cryptographic key sizes of 128 bit or 192 bit or 256 bit that meet the following:

- FIPS 197 [S8]
- the ECB, CBC, CTR and CFB:
  National Institute of Standards and Technology (NIST) SP 800-38A [S5]
- the PCBC:
  Bruce Schneier, Applied Cryptography, Second Edition, John Wiley & Sons,1996 [S23]. This standard should be implemented considering the 32-bit Security Controller – V07 Security Guidelines [23] only

Note 21:
The FCS_COP.1/AESCL refers to the AES interface provided by the Symmetric Cryptographic Library (SCL).
End of note.

FCS_CKM.4/AES	Cryptographic key destruction
Hierarchical to:	No other components.

Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM4.1/AES	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method <u>overwriting or zeroing</u> that meets the following: <u>none</u>

Note 22:
For FCS_COP.1/AES, FCS_COP.1/AESCL and FCS_COP.1/CMAC the key destruction can be done by overwriting the key register interfaces or by software reset of the SCP which provides immediate zeroing of all SCP key registers.
End of note.

Note 23:
The TOE can be delivered with the SCP accessible or blocked. In case the SCP is blocked, no AES computation supported by hardware is possible and the FCS_COP.1/AES, FCS_COP.1/AESCL, FCS_COP.1/CMAC and FCS_CKM.4/AES are not applicable.

The TOE can be delivered with the optional Symmetric Cryptographic Library (SCL). If the optional SCL is not available then the FCS_COP.1/AESCL and FCS_COP.1/CMAC are not applicable.
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.

Valid for the ACL in two versions v2.08.006 (ACL-1) and v3.03.003 (ACL-2).

Please consider also the statement of section 7.1.4.1.

FCS_COP.1/RSA-1 or FCS_COP.1/RSA-2	Cryptographic operation
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/RSA-1 or FCS_COP.1.1/RSA-2	The TSF shall perform <u>encryption, decryption, signature generation and signature verification</u> in accordance with a specified cryptographic algorithm <u>Rivest-Shamir-Adleman (RSA)</u> and cryptographic key sizes <u>1024 - 4224 bits</u> that meet the following:

Encryption:

1. According to section 5.1.1 RSAEP in PKCS#1 [S9]:

- Supported for $n < 2^{2048 + 64}$

- 5.1.1(1) not supported

2. According to section 8.2.2 IFEP-RSA in IEEE [S10]:

- Supported for $n < 2^{2048 + 64}$

Decryption (with or without CRT):

1. According to section 5.1.2 RSADP in PKCS#1 [S9] for u = 2, i.e., without any (ri, di, ti), 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 IFDP-RSA in IEEE 1363 [S10]:

- 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 #1[S9] for u = 2, i.e., without any (ri, di, ti), 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 1363 [S10]:

- 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 [S9]:

- supported for $n < 2^{4096 + 128}$
- 5.2.2(1) not supported

2. According to section 8.2.5 IFVP-RSA1 in IEEE 1363 [S10]:

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

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)".

Valid for the ACL in two versions v2.08.006 (ACL-1) and v3.03.003 (ACL-2).

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-1 or FCS_CKM.1/RSA-2	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/RSA-1 or FCS_CKM.1.1/RSA-2	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm RSA key generation according to Infineon Technologies key generation algorithm and specified cryptographic key sizes of 1024 – 4224 bits that meet the following:

1. According to sections 3.1 and 3.2 in PKCS #1[S9]

for u = 2, i.e. without any (ri, di, ti), i > 2:

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

<div style="border">

2. According to section 8.1.3.1 in IEEE 1363 [S10]:

- 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 $p \times q < 2^{2048 + 128}$

</div>

Note to FCS_CKM.1.1/RSA-1 and FCS_CKM.1.1/RSA-2:
the RSA key generation is implemented by following functions:

CryptoRSAKeyGen

CryptoRSAKeyGenMask_CRT plus CryptoGeneratePrime or CryptoGeneratePrimeMask (valid for RSA-1)

CryptoRSAKeyGenMask_D plus CryptoGeneratePrime or CryptoGeneratePrimeMask (valid for RSA-1)

CryptoRSAKeyGenMask_N plus CryptoGeneratePrime or CryptoGeneratePrimeMask (valid for RSA-1)

CryptoRsaKeyGenMask_PQ plus CryptoRsaKeyGenMask_CRT or CryptoRsaKeyGenMask_D or
CryptoRsaKeyGenMask_D   (valid for RSA-2)

CryptoGeneratePrime plus CryptoRsaKeyGenMask_CRT or CryptoRsaKeyGenMask_D or
CryptoRsaKeyGenMask_D   (valid for RSA-2)

The function CryptoGeneratePrime has been assigned to the appropriate security level by BSI. The proprietary CryptoGeneratePrimeMask function has not been cryptographic-analytically evaluated and certified by BSI. However, the AVA_VAN.5 evaluation did not reveal any weaknesses, neither in concept nor in implementation. The targeted AVA_VAN.5 is achieved therefore.
End of note.

Note 24:
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 section 7.1.4.1.
End of note.

Note 25:
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-1, FCS_COP.1/RSA-2, FCS_CKM.1/RSA-1 and FCS_CKM.1/RSA-2.
End of note.

Note 26:
The minimum key length follows the national recommendations by the BSI which means that RSA key length below 1976 bits are not included in the certificate. The key length requirements can differ between the countries. Please note that the BSI expects this key length as appropriate until 2022 and recommends for longer usage times key length of 3000 bits or higher.
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 [S1] and NIST [S2] Elliptic Curves with key lengths of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 Bits, due to national AIS32 regulations by the BSI. 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 $p \in \left\lfloor 2^{41-1}; 2^{521} \right\rfloor$ as well as curves based on a finite field GF(2^n) with size $n \in [41-1; 521]$ are supported.

7.1.4.7 Elliptic Curve DSA (ECDSA) operation

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

Valid for ACL v2.08.006.

FCS_COP.1/ECDSA-1	Cryptographic operation
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ECDSA-1	The TSF shall perform signature generation and signature verification in accordance with a specified cryptographic algorithm ECDSA and cryptographic key sizes 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits that meet the following: **ECDSA Signature Generation:** 1. According to section 7.3 Signing Process in ANSI X9.62 [S11] • 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 14888-3 [S13]

- Section 6.4.3.3 is not supported

- Section 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

- Section 6.4.3.7 is not supported

- Section 6.4.3.8 is not supported

3. According to section 7.2.7 ECSP-DSA in IEEE 1363 [S10]

Deviation of step (3) and (4):

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

ECDSA Signature Verification:

1. According to section 7.4.1 Verification with the Public Key in ANSI X9.62 [S11]

- 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 14888-3 [S13]

- Section 6.4.4.2 is not supported

- Section 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 1363 [S10]

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

Valid for ACL v3.03.003 (ACL-2).

FCS_COP.1/ECDSA-2	Cryptographic operation
Hierarchical to:	No other components.

Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ECDSA-2	The TSF shall perform <u>signature generation and signature verification</u> in accordance with a specified cryptographic algorithm <u>ECDSA</u> and cryptographic key sizes <u>160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits</u> that meet the following: **ECDSA Signature Generation:** <u>1. According to section 7.3 Signing Process in ANSI X9.62 [S11]</u> - <u>Step d) and e) are not supported</u> - <u>The output of step e) has to be provided as input to our function by the caller.</u> <u>2. According to sections 6.4.3 Signature Process in ISO/IEC 14888-3 [S13]</u> - <u>Section 6.4.3.3 is not supported</u> - <u>Section 6.4.3.5 is not supported</u> - <u>the hash-code of H of the message has to be provided by the caller as input for our function</u> - <u>Section 6.4.3.7 is not supported</u> - <u>Section 6.4.3.8 is not supported</u> <u>3. According to section 7.2.7 ECSP-DSA in IEEE 1363 [S10]</u> **ECDSA Signature Verification:** <u>1. According to section 7.4.1 Verification with the Public Key in ANSI X9.62 [S11]</u> - <u>Step b) and c) are not supported</u> - <u>The output of step c) has to be provided as input to our function by the caller</u> - <u>Deviation of step d):</u> - <u>Beside noted calculation, our algorithm adds a random multiple of BasepointerOrder n to the calculated values u1 and u2.</u> <u>2. According to sections 6.4.4 Signature Verification Process in ISO/IEC 14888-3 [S13]</u> - <u>Section 6.4.4.2 is not supported</u> - <u>Section 6.4.4.3 is not supported:</u> - <u>The hash-code H of the message has to be provided by the caller as input to our function</u>

3. According to section 7.2.8 ECVP-DSA in IEEE 1363 [S10]	

Note 27:

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)".

Valid for the ACL in two versions v2.08.006 (ACL-1) and v3.03.003 (ACL-2).

FCS_CKM.1/EC-1 or FCS_CKM.1/EC-2	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-1 or FCS_CKM.1.1/EC-2	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm EC key generation and specified cryptographic key sizes 160, 163, 192, 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 X9.62 [S11]: • The optional cofactor h is not supported 2. According to section 6.4.2 Generation of signature key and verification key in ISO/IEC 14888-3 [S13] 3. According to appendix A.16.9 An algorithm for generating EC keys in IEEE 1363 [S10]

Note to FCS_CKM.1.1/EC-1 and FCS_CKM.1.1/EC-2:

For FCS_CKM.1.1/EC-1 the EC key generation is implemented by following functions which can be used independently of each other:

- ECC_ECDSAKeyGen
- ECC_ECDSAKeyGenMask

For FCS_CKM.1.1/EC-2 the EC key generation is implemented by the function ECC_ECDSAKeyGenMask.

End of note.

Note 28:
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.

Valid for the ACL in two versions v2.08.006 (ACL-1) and v3.03.003 (ACL-2).

FCS_COP.1/ECDH-1 or FCS_COP.1/ECDH-2	Cryptographic operation
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ECDH-1 or FCS_COP.1.1/ECDH-2	The TSF shall perform elliptic curve Diffie-Hellman key agreement in accordance with a specified cryptographic algorithm ECDH and cryptographic key sizes 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits that meet the following: 1. According to section 5.4.1 Standard Diffie-Hellman Primitive" in ANSI X9.63[S3] • 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 11770-3 [S12] • The function enables the operations described in appendix D.6 3. According to section 7.2.1 ECSVDP-DH in IEEE 1363 [S10] • 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:
The certification covers the standard Brainpool [S2] and NIST [S1] Elliptic Curves with key lengths of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 Bits, due to national AIS32 regulations by the BSI. 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 30:
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 31:
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-1, FCS_COP.1/ECSA-2, FCS_COP.1/ECDH-1, FCS_COP.1/ECDH-2, FCS_CKM.1/EC-1 and FCS_CKM.1/EC-2.
End of note.

Note 32:
The EC primitives allow the selection of various curves. The selection of the curves depends to the user.
End of note.

7.1.4.10   CIPURSE™ CL Cryptographic Functions

The optional CIPURSE™ CL (CCL) meets the following security functional requirements.

The CIPURSE™ CL implementation shall meet the security functional requirement FCS_CKM.1/CCL as specified below:

FCS_CKM.1/CCL	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/CCL	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm:
	• In the mode confidential communication:
	   session key derivation and key derivation for the exchange protocol
	• In the mode integrity protection:
	   session key derivation
	and specified cryptographic key sizes of <u>128 bits</u> that meet the following:
	• CIPURSE™ V2 Cryptographic Protocol [S22] chapters 5.2 and 6.2

The CIPURSE™ CL implementation shall meet the security functional requirement FCS_CKM.4/CCL as specified below:

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

Note 33:
The key destruction is triggered from the CCL to the SCP at every entry and exit. The key storage in the CCL is wiped with zero values.
End of note.

The CIPURSE™ CL shall meet security functional requirements "Cryptographic Operation" FCS_COP.1/CCL as specified below:

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

FCS_COP.1.1/CCL	The TSF shall perform

> - an authentication protocol and a cryptographic protected protocol for integrity protection and confidential communication

in accordance with a specified cryptographic algorithm

> - CIPURSE™ V2 Cryptographic Protocol [S22], chapter 5 Authentication and 6 Secure Data Exchange Protocol

and cryptographic key sizes *of 128 Bit* that meet the following:

> - Federal Information Processing Standards Publication 197 [S8]
> - NIST Special Publication SP 800-38A [S5]
> - CIPURSE™ V2 Cryptographic Protocol [S22] chapter 5.2 Session key Derivation
> - CIPURSE™ V2 Cryptographic Protocol [S22] chapter 6.2 Key Derivation for the first frame
> - in case of integrity protection mode: CIPURSE™ V2 Cryptographic Protocol [S22] chapter 6.3 Integrity Protection
> - in case of confidential communication mode: CIPURSE™ V2 Cryptographic Protocol [S22] chapter 6.4 Confidential Communication

Note 34:
The CIPURSE™ CL is a delivery option. The TOE can be delivered with or without the CIPURSE™ CL. In the case the TOE comes without, it does not provide the Additional Specific Security Functionality CIPURSE™ Cryptographic Library (CCL) realized with the security functional requirements FCS_COP.1/CCL, FCS_CKM.1/CCL and FCS_CKM.4/CCL.
End of note.

7.1.5 Data Integrity

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

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

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

FDP_SDC.1	Stored data confidentiality
Hierarchical to:	No other components
Dependencies:	No dependencies
FDP_SDC.1.1	The TSF shall ensure the confidentiality of the information of the user data while it is stored in the <u>RAM, Cache and SOLID FLASH™ NVM except the memory area of the SOLID FLASH™ NVM from address 10007000H to 100077FFH.</u>

7.1.6 Support by the Flash Loader

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

- Limited capabilities (FMT_LIM.1/Loader),
- Limited availability – Loader (FMT_LIM.2/Loader),
- Authentication Proof of Identity (FIA_API.1),
- Inter-TSF trusted channel (FTP_ITC.1),
- Basic data exchange confidentiality (FDP_UCT.1),
- Data exchange integrity (FDP_UIT.1),
- Subset access control – Loader (FDP_ACC.1/Loader),
- Security attribute based access control – Loader (FDP_ACF.1/Loader)
- as defined in the PP [1], section 7.2 and 7.3.

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

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

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

- The Administrator user is enabled performing mutual authentication with the keys Kc and Kd, to manage (set, exchange, delete) the keys Kc, Kd and Kfdi and to process the download of the User data into the memory of the TOE.

- Download operator user is enabled performing mutual authentication with Kd, to exchange the key Kd and to perform the download of the User data into the memory of the TOE. He can also delete Kfdi.

The Flash Loader supports the following object:

- user data: Data loaded into the memory of the TOE.
- The Flash Loader supports the following security attributes:
- Keys Kc and Kd used for the mutual authentication process.
- Key Kfdi used to encrypt/decrypt the user data.

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

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

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

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

Note 35:
Regarding FMT_LIM.1.1/Loader it is added in the User Guidance that the Flash Loader has to be permanently deactivated prior delivery to the end user (Phase 7).
End of note.

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

FIA_API.1	Authentication Proof of Identity
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide a <u>authentication mechanism according ISO/IEC 9798-2 [S18], section 6.2.2 Mechanism 4 - Three-pass authentication based on the security attributes Kc and Kd</u> to prove the identity of the TOE to an external entity.

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

FTP_ITC.1	Inter-TSF trusted channel
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and <u>the Administrator user and the Download operator user as described in the Loader SFP</u> that is logically distinct from other communication channels and provides assured identificaton of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit <u>another trusted IT product</u> to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for <u>deploying Loader for downloading the user data</u>.

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

FDP_UCT.1	Basic data exchange confidentiality
Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control].
FDP_UCT.1.1	The TSF shall enforce the <u>Loader SFP</u> to <u>receive</u> user data in a manner protected from unauthorised disclosure.

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

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

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

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

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

FDP_ACF.1/Loader	Security attribute based access control – Loader
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/Loader	The TSF shall enforce the <u>Loader SFP</u> to objects based on the following: • <u>(1) the subjects Administrator user and the Download operator user with security attributes Kc, Kd and Kfdi</u> • <u>(2) the objects user data in data loaded into the SOLID FLASH™ NVM memory of the TOE with security attributes Kfdi.</u>
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 36:
The security functional requirements FIA_API.1, FTP_ITC.1, FDP_UCT.1, FDP_UIT.1, FDP_ACC.1/Loader and FDP_ACF.1/Loader apply only at TOE products coming with activated Flash Loader enabled for user data download. In other cases the Flash Loader is not available anymore and the user data download is completed. Depending on the capabilities of the user software these security functional requirements may then reoccur as subject of the composite TOE.
The permanent locking of the Flash Loader after finalizing the download and prior delivery to the end-user is covered with FMT_LIM1/Loader and FMT_LIM.2/Loader.
End of note.

7.2 TOE Security Assurance Requirements

The evaluation assurance level is EAL6 augmented with ALC_FLR.1.

In the following table, the security assurance requirements are given. The augmentation of the assurance components compared to the Protection Profile [1] is expressed with bold letters.

Table 15 Assurance components

Aspect	Acronym	Description	Refinement
Development	ADV_ARC.1	Security Architecture Description	in PP [1]
	ADV_FSP.5	**Complete semi-formal functional specification with additional error information**	in ST [16]
	ADV_IMP.2	**Complete mapping of the implementation representation of the TSF**	in ST [16]
	ADV_INT.3	**Minimally complex internals**	
	ADV_TDS.5	**Complete semi-formal modular design**	
	ADV_SPM.1	**Formal TOE security policy model**	
Guidance Documents	AGD_OPE.1	Operational user guidance	in PP [1]
	AGD_PRE.1	Preparative procedures	in PP [1]
Life-Cycle Support	**ALC_CMC.5**	**Advanced support**	in ST [16]
	ALC_CMS.5	**Development tools CM coverage**	in ST [16]
	ALC_DEL.1	Delivery procedures	in PP [1]
	ALC_DVS.2	Sufficiency of security measures	in PP [1]
	ALC_LCD.1	Developer defined life-cycle model	
	ALC_TAT.3	**Compliance with implementation standards – all parts**	
	ALC_FLR.1	**Basic Flaw Remediation**	
Security Target Evaluation	ASE_CCL.1	Conformance claims	
	ASE_ECD.1	Extended components definition	
	ASE_INT.1	ST introduction	
	ASE_OBJ.2	Security objectives	
	ASE_REQ.2	Derived security requirements	
	ASE_SPD.1	Security problem definition	
	ASE_TSS.1	TOE summary specification	
Tests	**ATE_COV.3**	**Rigorous analysis of coverage**	in ST [16]
	ATE_DPT.3	**Testing: modular design**	
	ATE_FUN.2	**Ordered functional testing**	
	ATE_IND.2	Independent testing - sample	
Vulnerability Assessment	AVA_VAN.5	Advanced methodical vulnerability analysis	in PP [1]

7.2.1 Refinements

Some refinements are taken unchanged from the PP [1]. In some cases a clarification is necessary. In Table 18 an overview is given where the refinement is done.

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

7.2.1.1 Development (ADV)

ADV_IMP Implementation Representation:

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

ADV_FSP Functional Specification:

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

7.2.1.2 Life-cycle Support (ALC)

ALC_CMS Configuration Management Scope:

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

ALC_CMC Configuration Management Capabilities:

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

ALC_DVS Development Security:

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

7.2.1.3   Tests (ATE)

ATE_COV Test Coverage:

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

7.2.2   ADV_SPM Formal Security Policy Model

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

ADV_SPM.1	Formal TOE security policy model
Hierarchical to:	No other components
Dependencies:	ADV_FSP.4 Complete function description
ADV_SPM.1.1D	The developer shall provide a formal security policy model for the

Memory Access Control Policy and the corresponding SFRs

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

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

- FDP_SDI.2 Stored data integrity monitoring and action
- FDP_SDC.1 Stored data confidentiality
- FDP_ITT.1 Basic Internal Transfer Protection
- FDP_IFC.1 Information Flow Control
- FPT_ITT.1 Basic internal TSF data transfer protection
- FPT_PHP.3 Resistance to physical attack
- FPT_FLS.1 Failure with preservation of secure state
- FRU_FLT.2 Limited fault tolerance
- FMT_LIM.1 Limited capabilities
- FMT_LIM.2 Limited availability
- FAU_SAS.1 Audit storage
    - FMT_SMF.1 Specification of Management Functions
    - FMT_LIM.1/Loader Limited capabilities
    - FMT_LIM.2/Loader Limited availability – Loader
    - FIA_API.1 Authentication Proof of Identity
    - FTP_ITC.1 Inter-TSF trusted channel
    - FDP_UCT.1 Basic data exchange confidentiality
    - FDP_UIT.1 Data exchange integrity
    - FDP_ACC.1/Loader Subset access control - Loader
    - FDP_ACF.1/Loader Security attribute based access control - Loader
    -

ADV_SPM.1.2D	For each policy covered by the formal security policy model, the model shall identify the relevant portions of the statement of SFRs that make up that policy.
ADV_SPM.1.3D	The developer shall provide a formal proof of correspondence between the model and any formal functional specification.
ADV_SPM.1.4D	The developer shall provide a demonstration of correspondence between the model and the functional specification.

7.3 Security Requirements Rationale

7.3.1 Rationale for the Security Functional Requirements

The objectives O.Authentication and OE.TOE_Auth are discussed in the PP [1] section 7.2.1.
The objectives O.Cap_Avail_Loader and OE.Lim_Block_Loader and the covering security functional requirements FMT_LIM.1/Loader and FMT_LIM.2/Loader are discussed in the PP [1] section 7.3.1.
The policy P.Ctrl_Loader and the objectives O.Ctrl_Auth_Loader and OE.Loader_usage are discussed in the PP [1] section 7.3.2.
The 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 [1] see chapters 7.4.1 to 7.4.3.
The additional objective O.Prot_TSF_Confidentiality is defined in section 5.1 and 5.3 of this document.
The PP [1] section 6.1 includes also the definition of FDP_SDI.2 „Stored data integrity monitoring and action".

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

Table 16   Rational for additional SFR in the ST

Objective	TOE Security Functional Requirements
O.Add-Functions	FCS_COP.1/RSA-1 "Cryptographic operation by ACL-1"
	FCS_COP.1/ECDSA-1 "Cryptographic operation by ACL-1"
	FCS_COP.1/ECDH-1 "Cryptographic operation by ACL-1"
	FCS_CKM.1/RSA -1 "Cryptographic key generation by ACL-1"
	FCS_CKM.1/EC-1 "Cryptographic key generation by ACL-1"
	FCS_COP.1/RSA-2 "Cryptographic operation by ACL-2"
	FCS_COP.1/ECDSA-2 "Cryptographic operation by ACL-2"
	FCS_COP.1/ECDH-2 "Cryptographic operation by ACL-2"
	FCS_CKM.1/RSA -2 "Cryptographic key generation by ACL-2"
	FCS_CKM.1/EC-2 "Cryptographic key generation by ACL-2"
	FCS_COP.1/CMAC "Cryptographic operation - CMAC"
	FCS_COP.1/RMAC "Cryptographic operation - RMAC"
	FCS_COP.1/CCL "Cryptographic Operation"
	FCS_CKM.1/CCL "Cryptographic key generation"
	FCS_CKM.4/CCL "Cryptographic key destruction"
O.Phys-Manipulation	FPT_TST.2 "Subset TOE security testing"

Objective	TOE Security Functional Requirements
O.Mem-Access	FDP_ACC.1 "Subset access control" FDP_ACF.1 "Security attribute based access control" FMT_MSA.3 "Static attribute initialisation" FMT_MSA.1 "Management of security attributes" FMT_SMF.1 "Specification of Management Functions"
O.RND	FCS_RNG.1/TRNG "Generation of Random Numbers -TRNG" FCS_RNG.1/HPRG "Generation of Random Numbers - HPRG" FCS_RNG.1/DRNG "Generation of Random Numbers -DRNG" FCS_RNG.1/KSG "Generation of Random Numbers - KSG"
O.Prot_TSF_Confidentiality	FTP_ITC.1 "Inter-TSF-trusted channel" FDP_ACC.1/Loader "Subset access control –Loader" FDP_ACF.1/Loader "Security attribute based access control – Loader" FDP_UCT.1 "Basic data exchange confidentiality" FDP_UIT.1 "Data exchange integrity"
O.TDES	FCS_COP.1/TDSCL "Cryptographic operation"
O.AES	FCS_COP.1/AESCL "Cryptographic operation"

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

7.3.1.1 Cryptographic Aspects

The justification related 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. This holds true for the RSA2024/4096 and EC libraries which implements the generation of RSA keys FCS_CKM.1/RSA -1 and FCS_CKM.1/RSA -2 and the generation of EC keys FCS_CKM.1/EC-1 and FCS_CKM.1/EC-2.

The implementation covers the functional requirements and meets the objective O.Add Functions.

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

All these requirements have to be fulfilled to support OE.Resp-Appl for FCS_COP.1/TDES, FCS_COP.1/TDSCL (both DES algorithm) and for FCS_COP.1/AES, FCS_COP.1/AESCL (both AES algorithm) and for FCS_COP.1/CMAC and FCS_COP.1/RMAC.
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 , AES and MAC 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.

7.3.1.2   Hardware related Aspects

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

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

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

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

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

The presence of true random numbers is the security goal 4 (SG4) which is formalized in the objective O.RND Random Numbers. This objective must be covered by fulfillment of the security functional requirement FCS_RNG. This is defined in the PP [1] section 5.1. The rational for the functional requirement FCS_RNG is discussed in the PP [1], section 6.3.1. The requirement implements a quality metric which is defined by national regulations. The implemented random number generation fulfills the definitions of AIS31 [6] in the quality classes as outlined in section 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: <u>a defined quality metric</u>].
FIA_SOS.2.2	The TSF shall be able to enforce the use of TSF generated secrets for [assignment: <u>list of TSF functions</u>].

7.3.1.3 Flash Loader related Aspects

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

The TOE provides protection against disclosure of confidential operations of the Security IC through the use of a dedicated code loaded on open samples with the security functional requirement FTP_ITC.1 "Inter-TSF-trusted channel". The FTP_ITC.1 installs a communication channel between the TOE and the user which is logically distinguished from other channels. The security functional requirements FDP_UCT.1 "Basic data exchange confidentiality" and FDP_UIT.1 "Data exchange integrity" providing the confidentiality and integrity of the transferred user data with crypograhic methodes. Additionally th e security functional requirements

FDP_ACC.1/Loader "Subset access control –Loader" and FDP_ACF.1/Loader "Security attribute based access control – Loader" providing the access control policy for the roles Administrator user and Download operator user.

7.3.1.4 CIPURSE™ Cryptographic Library related Aspects

The objective O.Add-Functions implements the fundament for the subsequent establishment of a protected communication between two entities. The clear authentication of an allowed communication entity is achieved by FCS_ COP.1/CCL as a common secret must be established and present at the allowed communication partners. The authentication is mutual wise. The authentication response of a request contains specific data which only the communication partner can identify, operate and proceed accordingly.
A user of the CIPURSE™ CL will face that no other action or functionality of the CIPURSE™ CL is possible until the user has been successfully authenticated. This strong authentication mechanism implements FCS_COP.1/CCL and covers the objective O.Add-Functions.
Last but not least, in case of authentication failure an error message is returned and the CIPURSE™ CL functionality cannot be used.

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

All these requirements have to be fulfilled to support OE.Resp-Appl for FCS_COP.1/CCL .
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. The keys management for CIPURSE ™ is provided by the TOE implementing FCS_CKM.1/CCL and FCS_CKM.4/CCL.
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.

7.3.1.5 Dependencies of Security Functional Requirements

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

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

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

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

Table 17 Dependency for cryptographic operation requirement

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FCS_COP.1/RSA-1 FCS_COP.1/RSA-2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	Yes, see comment 4
FCS_CKM.1/RSA-1 FCS_CKM.1/RSA-2	[FCS_CKM.2 or FCS_COP.1],	Yes
	FCS_CKM.4	Yes, see comment 4
FCS_COP.1/ECDSA-1 FCS_COP.1/ECDSA-2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	Yes, see comment 4
FCS_CKM.1/EC-1 FCS_CKM.1/EC-2	[FCS_CKM.2 or FCS_COP.1]	Yes
	FCS_CKM.4	Yes, see comment 4
FCS_COP.1/ECDH-1 FCS_COP.1/ECDH-2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	Yes, see comment 4
FCS_COP.1/TDES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	Yes, see comment 2
FCS_COP.1/TDSCL	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	Yes, see comment 2
FCS_CKM.4/TDES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, see comment 2
FCS_COP.1/AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM1], FCS_CKM.4	Yes, see comment 2
FCS_COP.1/AESCL	[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
FCS_COP.1/CMAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM1] FCS_CKM.4	Yes, see comment 2
FCS_COP.1/RMAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM1] FCS_CKM.4	Yes, see comment 2
FCS_COP.1/CCL	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM1], FCS_CKM.4	Yes, see comment 5
FCS_CKM.1/CCL	[FCS_CKM.2 or FCS_COP.1]	Yes, see comment 5
FCS_CKM.4/CCL	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, see comment 5
FPT_TST.2	No dependencies	Yes
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FMT_MSA.3, FDP_ACC.1	Yes
FMT_MSA.3	FMT_MSA.1	Yes
	FMT_SMR.1	NA, see comment 1

FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	Yes
	FMT_SMR.1	NA, see comment 1
	FMT_SMF.1	Yes
FMT_SMF.1	None	NA
FMT_LIM.1/Loader	FMT_LIM.2/Loader	Yes
FMT_LIM.2/Loader	FMT_LIM.1/Loader	Yes
FTP_ITC.1	None	Yes, see comment 3
FDP_UCT.1	[FPT_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	Yes
FDP_UIT.1	[FPT_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	Yes
FDP_ACC.1/Loader	FMT_ACF.1/Loader	Yes
FDP_ACF.1/Loader	FMT_MSA.3	Yes, see comment 3

Comment 1:

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

End of comment.

Comment 2:

These requirements all address the appropriate management of cryptographic keys used by the specified cryptographic function and are not part of the PP [1]. Most requirements concerning key management shall be fulfilled by the environment since the Smartcard Embedded Software is designed for a specific application context and uses the cryptographic functions provided by the TOE.
For the security functional requirement FCS_COP.1/TDES and FCS_COP.1/AES the respective dependency FCS_CKM.4 is fulfilled by the TOE.
For the security functional requirement FCS_COP.1/TDSCL, FCS_COP.1/AESCL, FCS_COP.1/CMAC and FCS_COP.1/RMAC the respective dependency FCS_CKM.4/TDES and FCS_CKM.4/AES are fullfilled by the Symmectric Cryptographic Library.
The cryptographic key destruction can be done by overwriting the key register interfaces or by software reset of the SCP which provides immediate zeroing of all SCP hardware key registers. The Symmetric Cryptographic Library also destroys dynamic cipher block code object in the memory, which leads to the memory clearance and key destruction. Please refer also to the application notes 41 and 42 in the PP [1].
For the security functional requirement FCS_COP.1/TDES, FCS_COP.1/AES, FCS_CKM.4/TDES, FCS_CKM.4/AES, FCS_COP.1/TDSCL, FCS_COP.1/AESCL, FCS_COP.1/CMAC and FCS_COP.1/RMAC the dependencies FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 have to be fulfilled by the environment because the TOE does not provide the accompanying functionality (e.g. generate and import keys). That mean, that the environment shall meet the requirements FCS_CKM.1, FDP_ITC.1 or FDP_ITC.2 as defined in [3], section 10.1 and 11.7.

The Symmetric Cryptographic Library is a delivery option. Therefore the TOE may come without this library. In the case of coming without this library the FCS_COP.1/TDSCL, FCS_COP.1/AESCL, FCS_COP.1/CMAC and FCS_COP.1/RMAC are not provided by the TOE. The IT environment has to fulfill the requirements of this section depending if the TOE comes with or without this library.

End of comment.

Comment 3:

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

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

End of comment.

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 [1]. Most requirements concerning key management shall be fulfilled by the environment since the Smartcard Embedded Software is designed for a specific application context and uses the cryptographic functions provided by the TOE.

For the security functional requirement FCS_COP.1/RSA-1, FCS_COP.1/RSA-2, FCS_COP.1/ECDSA-1, FCS_COP.1/ECDSA-2, FCS_COP.1/ECDH-1 and FCS_COP.1/ECDH-2 the respective dependency FCS_CKM.1 has to be fulfilled by the TOE with the security functional requirement FCS_CKM.1/RSA-1 (for FCS_COP.1/RSA-1) and FCS_CKM.1/RSA-2 (for FCS_COP.1/RSA21) and FCS_CKM.1/EC-1 (for FCS_COP.1/ECDSA-1 and FCS_COP.1/ECDH-1) and FCS_CKM.1/EC-2 (for FCS_COP.1/ECDSA-2 and FCS_COP.1/ECDH-2)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 [3], section 10.1. Additionally the requirement FCS_CKM.1 can be fulfilled by the environment as defined in [3], section 10.1.

For the security functional requirement FCS_CKM.1/RSA-1, FCS_CKM.1/RSA-2, FCS_CKM.1/EC-1 and FCS_CKM.1/EC-2 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 [3], section 10.1.

The cryptographic libraries RSA and EC 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 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.

Comment 5:

The security of the cryptographic functions FCS_CKM.1/CCL, FCS_CKM.4/CCL and FCS_COP.1/CCL relies on the secure use of the CIPURSE™ CL: This means that it is essential on user side that the common secret is generated and stored in an appropriate way and that integrity and confidentiality of this user secret is maintained. These preconditions are treated in the PP [1] section 3.1 claims 67 and 68.
The key destruction FCS_CKM.4/CCL applies only for the keys generated during and for a session and not for the common secret.

End of comment.

7.3.2   Rationale of the Assurance Requirements

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

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

In order to provide a meaningful level of assurance and that the TOE provides an adequate level of defense against such high potential attacks, the evaluators have access to all information regarding the TOE including the TSF internals, the low level design and source code including the testing of the modular design. Additionally the mandatory technical document "Application of Attack Potential to Smartcards" [10] shall be taken as a basis for the vulnerability analysis of the TOE.

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

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

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

7.3.2.1   ALC_FLR.1 Basic Flaw Remediation

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

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

Flaws are prioritized and assigned to a responsibility.

The assurance class ALC_FLR.1 has no dependencies.

8 TOE Summary Specification (ASE_TSS)

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

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

- SF_DPM   Device Phase Management
- SF_PS   Protection against snooping
- SF_PMA   Protection against Modifying Attacks
- SF_PLA   Protection against Logical Attacks
- SF_CS   Cryptographic Support

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

8.1 SF_DPM: Device Phase Management

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

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

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

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

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

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

The covered security functional requirement are FMT_LIM.1/Loader "Limited capabilities", FMT_LIM.2/Loader "Limited availability-Loader", FIA_API.1 "Authentication Proof of Identity", FTP_ITC.1 "Inter-TSF trusted channel", FDP_UCT.1 "Basic data exchange confidentiality", FDP_UIT.1 "Data exchange integrity, FDP_ACC.1/ "Loader Subset access control – Loader" and FDP_ACF.1/Loader "Security attribute based access control – Loader".

The Flash Loader related security functional requirements FIA_API.1, FTP_ITC.1, FDP_UCT.1, FDP_UIT.1, FDP_ACC.1/Loader and FDP_ACF.1/Loader apply only at TOE products coming with activated Flash Loader enabled for user data download by the user. In other cases the Flash Loader is not available anymore and the user data download is completed.

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

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

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

8.2 SF_PS: Protection against Snooping

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

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

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

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

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

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

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

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

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

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

8.3   SF_PMA: Protection against Modifying Attacks

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

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

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

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

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

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

During start up, the TOE performs various configurations and subsystem tests. After the start up has finished, the operating system or the application can activate the testfunctions (UMSLC), provided by specific Special Function Registers, also during normal operation. These testfunctions can be used to check the alarm lines and/or functions and sensors for correct operation as given in the 32-bit Security Controller - V07 Hardware Reference Manual [7].

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

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

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

If the optional Hardware Support Library (HSL) is part of the TOE, and the service routines for the tearing safe write into the SOLID FLASH™ NVM covered by the operation "Inplace Update" as outlined in the version specific user guidance document HSL [60], 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 requirements are FPT_PHP.3 "Resistance to physical attack" and FPT_FLS.1 "Failure with preservation of secure state".

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

8.4 SF_PLA: Protection against Logical Attacks

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

The covered security functional requirements are FDP_ACC.1 "Subset access control", FDP_ACF.1 "Security attribute based access control", FMT_MSA.1 "Management of security attributes", FMT_MSA.3 "Static attribute initialisation", FPT_FLS.1 "Failure with preservation of secure state" and FMT_SMF.1 "Specification of Management functions".

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

8.5　SF_CS: Cryptographic Support

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

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 37:
The cryptographic libraries SCL, RSA and EC 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). In the case of coming without the SCL library the TOE does not provide FCS_COP.1/TDSCL, FCS_COP.1/AESCL, FCS_COP.1/CMAC and FCS_COP.1/RMAC functionality.
End of note.

Note 38:
This TOE can come with both crypto coprocessors accessible, or with a blocked SCP, or with a blocked Crypto2304T, or with both cryptographic coprocessors blocked. The blocking depends on the customer demands prior to the production of the hardware. In case the SCP is blocked, no AES, DES and MAC computation supported by hardware is possible. In case the Crypto2304T is blocked, no RSA and EC computation supported by hardware is possible. No accessibility of the deselected cryptographic coprocessor is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic coprocessors.
End of note.

Note 39:
The cryptographic library CIPURSE™ CL is a delivery option.
Therefore the TOE may come with free combinations with the other libraries of or without this library. In the case of coming without the CIPURSE™ CL the TOE does not provide the specific security functionality implemented by this software.
End of note.

8.5.1　Triple DES

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

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

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

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

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

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

The implementation of ECB and CBC modes follow the standard:

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

The FCS_COP.1/TDSCL, which features are described in the following, is implemented by using the interface of the optional SCL library. The SCL contains additional software countermeasures to harden the restance against side channel and fault attacks. The TOE supports the encryption and decryption in accordance with the specified cryptographic algorithm Triple Data Encryption Standard (TDES) with cryptographic key sizes of 112 or 168 bit meeting the standards:

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

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

the Electronic Codebook Mode (ECB), the Cipher Block Chaining Mode (CBC), the Counter Mose (CTR), the Cipher Block – Feedback Mode (CFB) and the Propagating Cipher Block Chaining (PCBC) Mode.

The implementation of ECB, CBC, CFB and CTR modes follow the standard:

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

The PCBC mode refers to the standard:

- Bruce Schneier, Applied Cryptography, Second Edition, John Wiley & Sons, 1996 [S23].

This standard should be implemented considering the 32-bit Security Controller – V07 Security Guidelines [23] only.

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

Please consider also the statement of section 7.1.4.1.

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

8.5.2   AES

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

- FIPS 197 [S8].

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

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

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

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

The implementation of ECB and CBC complies with the standard:

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

The FCS_COP.1/AESCL, which features are described in the following, is implemented by using the interface of the optional SCL library. The SCL contains additional software countermeasures to harden the restance against side channel and fault attacks. The TOE supports the encryption and decryption in accordance with the specified cryptographic algorithm Advanced Encryption Standard (AES) and cryptographic key sizes of 128 bit or 192 bit or 256 bit that meet the standard:

- FIPS 197 [S8].

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

the Electronic Codebook Mode (ECB), the Cipher Block Chaining Mode (CBC), the Counter Mode (CTR), the Cipher Feedback Mode (CFB) and the Propagating Cipher Block Chaining Mode (CPCBC).

The implementation of ECB, CBC, CTR and CFB modes complies with the standard:

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

The implementation of PCBC mode complies with the standard:

- Bruce Schneier, Applid Cryptography, Second Edition, John Wiley & Sons, 1996 [S23].

This standard should be implemented considering the 32-bit Security Controller – V07 Security Guidelines [23] only.

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

Please consider also the statement of section 7.1.4.1.

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

8.5.3 CMAC

The SCL of the TOE supports the computation of cipher based message authentication codes CMAC hat meet the standard:

CMAC: National Institute of Standards and Technology (NIST) SP 800-38B [S7]

The CMAC algorithm uses for the computation either the AES or TDES algorithms according to following standards:

- AES
  - o Federal Information Standards Publication 197 [S8]
- TDES
  - o National Institute of Standards and Technology 800-67 Rev.1 [S4]

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

8.5.4   RMAC

The optional SCL of the TOE supports the computation of cipher based message authentication codes Retail-MAC hat meet the standard:

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

The Retail-MAC algorithm uses for the computation the TDES algorithms according to following standards:

- TDES
  - National Institute of Standards and Technology 800-67 Rev.1 [S4]

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

8.5.5   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 - 4224 bits that meet the following standards:

Encryption:

1. According to section "5.1.1 RSAEP" in PKCS#1 [S9]:

- Supported for $n < 2^{2048+64}$
- 5.1.1(1) not supported

2. According to section "8.2.2 IEFEP-RSA" in IEEE 1363 [S10]:

- Supported for $n < 2^{2048+64}$

Decryption (with or without CRT):

1. According to section "5.1.2 RSADP" in PKCS#1 [S9],
   for u = 2, i.e., without any (ri;di; ti); 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 $p\_q < 2^{4096+128}$
- 5.1.2(2.b) (ii)&(v) not applicable due to u = 2

2. According to section "8.2.3 IFDP-RSA" in IEEE 1363 [S10]:

- 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#1 [S9],
   for u = 2, i.e., without any (ri, di, ti), i >2,

- 5.2.1(1) not supported

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

2. According to section "8.2.4 IFSP-RSA1" in IEEE 1363 [S10]:

- 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#1 [S9]:

- Supported for $n < 2^{4096+128}$
- 5.2.2(1) not supported

2. According to section "8.2.5 IFVP-RSA1" in IEEE 1363 [S10]:

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

Please consider also the statement of section7.1.4.1.

The covered security functional requirement are FCS_COP.1/RSA-1 and FCS_COP.1/RSA-2.

Asymmetric Key Generation

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm RSA specified in PKCS#1 and specified cryptographic key sizes of 1024 - 4224 bits that meet the following standard:

1. According to sections 3.1 and 3.2 in PKCS#1 [S9],
for u = 2, i.e., without any (ri;di; ti); i > 2:

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

2. According to section 8.1.3.1 in IEEE 1363 [S10]:

- 8.1.3.1(I) supported for $n < 2^{2048+64}$
- 8.1.3.1(II) supported for $p \times q < 2^{4048+128}$
- 8.1.3.1(I) supported for $p \times q < 2^{2048+64}$

Note 40:
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 section 7.1.4.1.
End of note.

The covered security functional requirement are FCS_CKM.1/RSA-1 and FCS_CKM.1/RSA-2.

8.5.6   Elliptic Curves EC

The certification covers the standard Brainpool [S2] and NIST [S1] Elliptic Curves with key lengths of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 Bits, due to national AIS32 regulations by the BSI. Note that 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 $p \in \lfloor 2^{41-1}; 2^{521} \rfloor$ 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 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits that meet the following standard:

ECDSA Signature Generation:

 1. According to section "7.3 Signing Process" in ANSI X9.62 [S11]:

- Step d) and e) not supported.
- The output of step e) has to be provided as input to our function by the caller.
- Deviation of step c) and f):

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

 2. According to section "6.4.3 Signature process" in ISO/IEC 14888-3 [S13]:

- 6.4.3.3 not supported.
- 6.4.3.5 not supported:

   – the hash-code H of the message has to be provided by the caller as input to our function.

- 6.4.3.7 not supported.
- 6.4.3.8 not supported.

3. According to section "7.2.7 ECSP-DSA" in IEEE 1363 [S10]:

- Deviation of step (3) and (4):

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

ECDSA Signature Verification:

 1. According to section "7.4.1 Verification with the Publix Key" in ANSI X9.62–2005 [S11]

- Step b) and c) not supported.
- The output of step c) has to be provided as input to our function by the caller.
- Deviation of step d):
    – Beside noted calculation, our algorithm adds a random multiple of BasepointOrder n to the
      calculated values u1 and u2.

2. According to section "6.4 Signature Verification Process" in ISO/IEC 14888-3 [S13]:

- 6.4.4.2 not supported.

- 6.4.4.3 not supported:
  – the hash-code H of the message has to be provided by the caller as input to our function.
- 3. According to section "7.2.8 ECVP-DSA" in IEEE 1363 [S10].

Please consider also the statement of section7.1.4.1.

The covered security functional requirement are FCS_COP.1/ECDSA-1 and FCS_COP.1/ECDSA-2.

Asymmetric Key Generation

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Elliptic Curve EC specified in ANSI X9.62-2005 and ISO/IEC 14888-3:2006 and specified cryptographic key sizes 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits bits that meet the following standard:

ECDSA Key Generation:

1. According to appendix "A.4.3 Elliptic Curve Key Pair Generation" in ANSI X9.62 [S11]:

- Optional cofactor h is not supported.

2. According to section "6.4.2 Generation of signature key and verification key" in ISO/IEC 14888-3 [S13].

3. According to appendix "A.16.9 An algorithm for generating EC keys" in IEEE 1363-2000 [S10].

Please consider also the statement of section7.1.4.1.

The covered security functional requirement are FCS_CKM.1/EC-1 and FCS_CKM.1/EC-2.

Asymmetric Key Agreement

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

Diffie-Hellmann Key Agreememt

1. According to section "5.4.1 Standard Diffie-Hellman Primitive" in ANSI X9.63 [S3]:

- Unlike section 5.4.1(3), our implementation not only returns the x-coordiinate of the shared secret, but rather the x-coordinate and y-coordinate.

2. According to section "Appendix D.6 Key agreement of Diffie-Hellman type" in ISO/IEC 11770-3: [S12]:

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

3. According to section "7.2.1 ECSVDP-DH" in IEEE 1363 [S10]:

- Unlike section 7.2.1, our implementation not only returns the x-coordinate of the shared secret, but rather the x-coordinate and y-coordinate.

Please consider also the statement of section7.1.4.1.

The covered security functional requirement are FCS_COP.1/ECDH-1 and FCS_COP.1/ECDH-2.

Note 41:
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-1, FCS_COP.1/ECDSA-2, FCS_CKM.1/EC-1, FCS_CKM.1/EC-2, FCS_COP.1/ECDH-1 and FCS_COP.1/ECDH-2.

8.5.7 CIPURSE™ Cryptographic Library

The optional CIPURSE™ Cryptographic Library (CIPURSE™ CL) provides cryptographic functionality to implement a CIPURSE™ V2 conformant protocol [S22].
This protocol provides a secure mutual authentication of two entities, namely the terminal (denoted as PCD = Proximity Coupling Device (CIPURSE™-compliant terminal)) and a smart card or a token in other form factors which is called PICC. PICC stands for Proximity Integrated Circuit Card (CIPURSE™-compliant card).
Beside the mutual authentication, the protocol implements cryptographic measures which can be choosen by the user to maintain the integrity of the transferred data or to preserve the confidentiality and integrity of the transferred data.

The implemented cryptographic operation applies following standards:

- Federal Information Processing Standards Publication 197 [S8]
- NIST Special Publication SP 800-38A [S5]
- CIPURSE™ V2 Cryptographic Protocol [S22] chapter 5.2 Session key Derivation
- CIPURSE™ V2 Cryptographic Protocol [S22] chapter 6.2 Key Derivation for the first frame
- CIPURSE™ V2 Cryptographic Protocol [S22] chapter 6.3 Integrity Protection
- CIPURSE™ V2 Cryptographic Protocol [S22] chapter 6.4 Confidential Communication

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

8.5.8 Hybrid Random Number Generator

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

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

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

The hybrid PTRNG covers the security functional requirements FCS_RNG.1 "Random Number Generation" (FCS_RNG.1/TRNG, FCS_RNG.1/HPRG, FCS_RNG.1/DRNG, FCS_RNG.1/KSG), FPT_PHP.3 "Resistance to physical

attack", FDP_ITT.1 "Basic internal transfer protection", FPT_ITT.1 "Basic internal TSF data transfer protection" and FPT_FLS.1 "Failure with preservation of secure state".

The **SF_CS** "Cryptographic Support" covers the security functional requirements FCS_COP.1/TDES, FCS_COP.1/TDSCL, FCS_CKM.4/TDES, FCS_COP.1/AES, FCS_COP.1/AESCL, FCS_CKM.4/AES, FCS_COP.1/CMAC, FCS_COP.1/RMAC, FCS_COP.1/RSA-1, FCS_COP.1/RSA-2, FCS_CKM.1/RSA-1, FCS_CKM.1/RSA-2, FCS_COP.1/ECDSA-1, FCS_COP.1/ECDSA-2, FCS_CKM.1/EC-1, FCS_CKM.1/EC-2, FCS_COP.1/ECDH-1, FCS_COP.1/ECDH-2, FCS_COP.1/CCL, FCS_CKM.1/CCL, FCS_CKM.4/CCL, 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 18   Mapping of SFR and SF

Security Functional Requirement	SF_DPM	SF_PS	SF_PMA	SF_PLA	SF_CS
FAU_SAS.1	X				
FMT_LIM.1	X				
FMT_LIM.2	X				
FDP_ACC.1	X			X	
FDP_ACF.1	X			X	
FTP_ITC.1	X				
FDP_UCT.1	X				
FIA_API.1	X				
FMT_LIM.1/Loader	X				
FMT_LIM.2/Loader	X				
FDP_UIT.1	X				
FDP_ACC.1/Loader	X				

FDP_ACF.1/Loader	X				
FPT_PHP.3		X	X		X
FDP_ITT.1	X	X	X		X
FPT_ITT.1	X	X	X		X
FDP_SDC.1		X	X		
FDP_SDI.2			X		
FDP_IFC.1		X	X		
FMT_MSA.1	X			X	
FMT_MSA.3	X			X	
FMT_SMF.1	X			X	
FRU_FLT.2			X		
FPT_TST.2			X		
FPT_FLS.1		X	X	X	X
FCS_RNG.1/TRNG					X
FCS_RNG.1/HPRG					X
FCS_RNG.1/DRNG					X
FCS_RNG.1/KSG					X
FCS_COP.1/TDES					X
FCS_COP.1/TDSCL					X
FCS_COP.1/CMAC					X
FCS_COP.1/RMAC					X
FCS_COP.1/AES					X
FCS_COP.1/AESCL					X
FCS_COP.1/RSA-1					X
FCS_COP.1/RSA-2					X
FCS_COP.1/ECDSA-1					X
FCS_COP.1/ECDSA-2					X
FCS_COP.1/ECDH-1					X
FCS_COP.1/ECDH-2					X
FCS_COP.1/CCL					X
FCS_CKM.1/RSA-1					X
FCS_CKM.1/RSA-2					X
FCS_CKM.1/EC-1					X
FCS_CKM.1/EC-2					X

FCS_CKM.1/CCL					X
FCS_CKM.4/TDES					X
FCS_CKM.4/AES					X
FCS_CKM.4/CCL					X

8.7 Security Requirements are internally Consistent

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

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

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

The requirement FPT_TST.2 allows testing of some security mechanisms by the Smartcard Embedded Software after delivery. In addition, the TOE provides an automated continuous user transparent testing of certain functions.

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

9 Literature and References

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

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

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

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

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

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

[7] 32-bit Security Controller - V07 Hardware Reference Manual, Infineon Technologies AG, Revision 6.0, 2019-06-13

[10] Joint Interpretation Library, Application of Attack Potential to Smartcard, mandatory technical document, CCDB-2013-05-002, http://www.commoncriteriaportal.org

[11] 32-bit Security Controllers SLC37 (65 nm Technology) Programmer's Reference Manual, Infineon Technologies AG, Revision 4.7, 2021-04-19

[12] 32-bit Security Controller- V07 Errata Sheet, Infineon Technologies AG, Revision 6.1, 2021-02-26

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

[16] Confidential Security Target IFX_CCI_000011h IFX_CCI_00001Bh IFX_CCI_00001Eh IFX_CCI_000025h G12, v1.5, 2021-09-07

[23] 32-bit Security Controller – V07 Security Guidelines, Infineon Technologies AG, Version 1.01-2761, 2021-07-19

[60] SLxx7-C65 Hardware Support Library, Infineon Technologies AG, Revision 1.3, 2019-07-05

[89] ACL37-Crypto2304T-C65 Asymmetric Crypto Library RSA / ECC / Toolbox 32-bit Security Controller User Interface, Infineon Technologies AG, Version 2.08.006, October 12, 2021 (ACL-1) and ACL37-Crypto2304T-C65 Asymmetric Crypto Library RSA/ECC/Toolbox 32-bit Security Controller User interface manual, Infineon Technologies AG, Version 3.03.003, 2021-04-13 (ACL-2)

[104] 32-bit Security Controller Crypto@2304T V3 User Manual, Infineon Technologies AG, Revision 1.4.1, 2014-11-10

[139] Symmetric Crypto Library for SCP-v4 AES/DES/MAC 32-bit Security Controller User interface manual, Version v2.13.001, 2021-06-16

[141] CIPURSE™ Crypto Library CCL37xCIP v02.00.0005 CIPURSE™ V2 User Interface, Infineon Technologies AG, Revision 1.4, 2018-03-13

[S1]   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), 2013-07

[S2]   IETF: RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010, http://www.ietf.org/rfc/rfc5639.txt

[S3]   American National Standard for Financial Services ANSI X9.63-2011, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, American National Standards Institute (NIST), December 21, 2011

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

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

[S6]   ISO/IEC 10118-3: 2004, Information technology — Security techniques — Hash-functions – Part 3: Dedicated Hash functions, 2004

[S7]   National Institute of Standards and Technology (NIST) SP 800-38B, October 2016

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

[S9]   Public-Key Cryptography Standards PKCS#1: RSA Cryptography Standard RSA Laboratories, Version v2.2, 2012-10-27

[S10]   IEEE 1363, IEEE Standard Specifications for Public Key Cryptography, IEEE Standards Board. The standard covers specification for public key cryptography including mathematical primitives for secret value deviation, public key encryption and digital signatures and cryptographic schemes based on those primitives, 2000-01-30 (approved)

[S11]   American National Standard for Financial Services ANSI X9.62-2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standards Institute, 2005-11-16

[S12]   ISO/IEC 11770-3:2008, Technical Corrigendum 1, Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques, 2008, published 2009-09-15

[S13]   ISO/IEC 14888-3:2006, Technical Corrigendum 2, Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms, 2006 published 2009-02-15

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

[S15]   ISO/IEC 15946-1, Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General

[S16]   FIPS PUB 140-2, Security Requirements for Cryptographic Modules, U.S. Department of Commerce, National Institute of Standards and Technology, 2002-03-12,

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

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

[S19]   NIST Special Publication SP 800-108, October 2009, Recommendation for Key Derivation Using Pseudorandom Functions (revised)

[S21]   The CIPURSE™ V2 Revision 2.0 standard issued by the OSPT™ alliance. The standard consists of a set of documents as given in the CIPURSE™ V2 Revision 2.0 Documentation Overview. Version 2 http://www.osptalliance.org/resources/documentation

[S22]   CIPURSE™ V2 Cryptographic Protocol issued by the OSPT™ Alliance with Errata and Precision List, Version 1.0 from 1012-09-28 and Version 1.0 from 2014-09-18

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

[S24]   Nachweis der Einhaltung der Sicherheitsanforderungen für Chipkarten im Zulassungsverfahren der Deutschen Kreditwirtschaft (DK) (Germany only), Version 1.0, 2015-02-13

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

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

10   Hash Signatures of Libraries

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

10.1   ACL-1: RSA, EC, Toolbox Version 02.08.006

Cl37-LIB-base.lib:

MD5   =   2ae0c986bc87268b9a011363b16a78f6
SHA1   =   ac80f3ebbba1efc94fb38456012544baeda22b63
SHA256 =   f80e50b6654abf2bf3d1ce657a4ddf449ac4fcc3a26f74883a701816eeeee4bc

Cl37-LIB-ecc.lib:

MD5   =   bcd63a1442f72edb23255c78ac269745
SHA1   =   400b55563113a31061f833eef0e2a05aded0f931
SHA256 =   5092814a5e393da5aae4a68e171240c409e9f658a54657b123bced6df1a2a94d

Cl37-LIB-2k.lib:

MD5   =   46c8d705981bb43b778ca081fa3d0eec
SHA1   =   b972e879722b21dcac9fa298d6f0ffd72a943489
SHA256 =   fac35f7805a6473df19880a3c50189e1c9e6ca55b48aee119d2fb5bcacc6c7ab

Cl37-LIB-4k.lib:

MD5   =   e3ed6546d86d25d5548231590391b88c
SHA1   =   1099cb08ab059d12e46c37c1e42cc751405872c6
SHA256 =   b03b49a219a6e6ffe4af2fa4d615bd2aa0a078ecf8e1a6bea27632c0569f244b

Cl37-LIB-toolbox.lib:

MD5   =   f2c268c6f2c24553b5683923d64cbdff
SHA1   =   7b3ed3e81fb075f59ede60de6388f1d65d4b66d3
SHA256 =   aeaad5b277eedafe04144fe6db3da32ea615ce9f5c67485792f3598b1629b861

10.2   ACL-2: RSA, EC, Toolbox Version 03.03.003

ACL37-Crypto2304T-C65-base.lib:

MD5   =   0665df0c3f4687657fa0a24e5709eae5
SHA1   =   d3ccab68a7db2a8321b1e47a222d892c1a35a599
SHA256=   c930817f8a661497d0698f37b50739723af7c7e2d55e6d0821e25ccc1fcf2496

ACL37-Crypto2304T-C65-ecc.lib:

MD5   =   2a954becde58f3900045d50edc94fe50
SHA1   =   eede253bafd1208dd0b4e81b03cc1f1d393ddcc6
SHA256=   672a02e730e3a62c77248fffb37fc9ac45d4f68c5451b247bd66a7fdbb419b15

ACL37-Crypto2304T-C65-rsa2k.lib:

MD5   =   a161714a117be13f0696732c8800c41f
SHA1   =   8f2f25b6330d8fdd03358b56ce5f795dcff497ee
SHA256=   3b4fbec76bcbd159a97d4c7a1cbfa3954a31982d7894cc5efcd117da4d6da438

ACL37-Crypto2304T-C65-rsa4k.lib:

MD5   =   eb66b8e11b2779b23fa3e54fe5b0a652
SHA1   =   c24cab6779de80ac27d5b2432ce0b9628c871744
SHA256=   a6f8f8c32c5efb466e2007d77c3abda4ffb00ef6825b2240e1a7ee13bd82661c

ACL37-Crypto2304T-C65-toolbox.lib:

MD5   =   7a14f46629815d5e6e851c4b483bc1e3
SHA1   =   6f80d689a31cc89da8294b6c4e4ec2d34c81318c
SHA256=   cc0f2f485a2c1b6fab210346d26992f3f9cfd93e0ae26675987c3a2ee0ab3625

10.3   HSL – Hardware Support Library Version 2.01.6198

HSL.lib:

MD5   =   becd1b4d8a058313dce703cdf0377882
SHA1   =   3f4f65be9cd98b095d1f8ebee86abc2ae92e14c6
SHA256 =   9a412a090177bb73fdb553c0b2c51f07b4359ee24c7e91edc0c34e7e96d00e6a

10.4   SCL Symmetric Cryptographic Library Version 02.13.001

SCL37-SCP-v4-C65-cipher.lib:

MD5   =   cb1edb2bc75b1021fc988e1e2d9981f7
SHA1   =   459b660c478ed0339752c523e7b7d8fd2218e82f
SHA256=   6746114a36a7f32bc41fab3b98cd9ea789658ad03ddc9c54d0f68bc88db0f56e

SCL37-SCP-v4-C65-mac.lib:

MD5   =   b83d5721050ebb84ce594d69cad316ac
SHA1   =   3e1764a7e3bdbaeece61d40f6d20d3c4cb85107f
SHA256=   54dd15d46184c75db11e462107129a840a854f309c7cbbc135206047d4b6ca66

SCL37-SCP-v4-C65-des.lib:

MD5   =   8edb1dc6f621f1341e409e59a06d685b
SHA1   =   aa147b6c23c38c93c217ef778b088769f6894bc8
SHA256=   78b829bd75b9965e8b732a3b7c12fbd894fc30765e8f92e0be35023b43c32e3c

SCL37-SCP-v4-C65-aes.lib:

MD5   =   69ae45d01ed9277366106f58dccaa222
SHA1   =   c77799b6f9aed49d58d4b44858461553ae009550
SHA256=   eb718a7daf14d9f92df66d8d72bea5ff721f0fe62b33f384a7a9fb90b5cfcc54

10.5　　NRGS – NRG Software Version 04.03.3431

NRG.lib:

MD5　　=　　6b08bf83a9032a7abea5f43b31557d41
SHA1　=　　8aefa402d1aa046020459538b2e8ba6ca6962e9d
SHA256 =　　724f0ab54fc25f0577b4d230f910f253a80031032faa1f93b63c708642154c0f

NRGManagament. Lib:

MD5　　=　　eea47017ccdb672d3a517c6979ccb3a6
SHA1　=　　1422d5535feb4c5709e93e142e93c1c5df3fdd97
SHA256 =　　a401b112aff564dad5404c4f76607bca009119b709b3396f946937a4ba186cd6

NRGManagamentExtension. Lib:

MD5　　=　　6ef8c220518f6bc4aa72bbad08a9d3bd
SHA1　=　　4419604fb43495cac608951efe3ef0756d66085d
SHA256 =　　b9ddf7bad58eaa265e53a6fba07986afbbcdb66b793f899b50f9a909b4485ec0

NRGReaderSoftware.lib:

MD5　　=　　e476937a8a1665f166f9f24f323fb0dd
SHA1　=　　7cafccd8d992990f4ac0e8aececdaf9fbb292478
SHA256 =　　7625fb6ee3f3a223a73fea96fefea1be21706e0e4fe685b87ea146253fc8e2e9

10.6　　CIPURSE^{TM} Cryptographic Library Version v02.00.0005

CCL.lib:

MD5　　=　　86cf407ca7537c7585180a63df8335b3
SHA1　=　　45e6fc6fa43275c0f95c09530731602a528bb87e
SHA256 =　　50fb31021f7b2b5b5993d04d4f9a7f07e65f689e9654e265d28c1b9c3f499921

11 List of Abbreviations

AES	Advanced Encryption Standard
AIS31	"Anwendungshinweise und Interpretationen zu ITSEC und CC Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren"
API	Application Programming Interface
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 Coprocessor
CRT	Chinese Reminder Theorem
DES	Data Encryption Standard
DK	Deutsche Kreditwirtschaft
DPA	Differential Power Analysis
DFA	Differential Failure Analysis
DRNG	Deterministic Random Number Generator
EC	Elliptic Curve Cryptography
ECC	Error Correction Code and Elliptic Curve Cryptography depending on the context
EDC	Error Detection Code
SOLID FLASH™ NVM	Electrically Erasable and Programmable Read Only Memory
EMA	Electromagnetic analysis
FL	Flash Loader
Flash	SOLID FLASH™ Memory
HRNG	Hybrid Random Number Generator
HW	Hardware
HSL	Hardware Support Library
HSM	Hardware Security Module
IC	Integrated Circuit
ICO	Internal Clock Oscillator
ID	Identification

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

12   Glossary

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

Read Only Memory	Non-volatile memory which permits read operations only
SCP	Symmetric Cryptographic CoProcessor for symmetric cryptographic operations (TDES, AES).
Self-Test Software	Part of the firmware with routines for controlling the operating state and testing the TOE hardware
Security Function	Part(s) of the TOE used to implement part(s) of the security objectives
Security Target	Description of the intended state for countering threats
Smart Card	Plastic card in credit card format with built-in chip. Other form factors are also possible, i.e. if integrated into mobile devices
Software	Information (non-physical part) which is required to implement functionality in conjunction with the hardware (program code)
Subject	Entity, generally in the form of a person, who performs actions
Target of Evaluation	Product or system which is being subjected to an evaluation
Test Mode	Operational status phase of the TOE in which actions to test the TOE hardware take place
Threat	Action or event that might prejudice security
User Mode	Operational status phase of the TOE in which actions intended for the user takes place

Revision History

Major changes since the last revision

Version	Description of change
1.1	Final version
1.2	New ACL, HSL , user guidance documents and introduction of NRG terminology
1.3	112 bit TDES key added, new version of Security Guidance
1.4	New ACL and SCL version added, SCL 2.04.001 removed
1.5	Modifications of ECDSA SFR due to implementation differences between ACL libs; new ACL v2.08.006 guidance