

# Security Target Lite

## M7893 B11

Including optional Software Libraries

RSA - EC - SHA-2 - Toolbox

Common Criteria CCv3.1 EAL6 augmented (EAL6+)

Resistance to attackers with HIGH attack potential

**Version:** 0.2

**Date:** 2015-08-31

**Author:** Hans-Ulrich Buchmüller



**Edition 2015-08-31**

**Published by Infineon Technologies AG,  
81726 Munich, Germany.**

**© 2015 Infineon Technologies AG**

**All Rights Reserved.**

#### **Legal Disclaimer**

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

#### **Information**

For further information on technology, delivery terms and conditions and prices, please contact the nearest Infineon Technologies Office ([www.infineon.com](http://www.infineon.com)).

#### **Warnings**

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

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

**Miscellaneous**

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

**Trademarks of Infineon Technologies AG**

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

Trademarks as of January, 2015.

## REVISION HISTORY

0.1	Initial Version
0.2	Update of standard references, editorial changes

## TABLE OF CONTENTS

<b>1</b>	<b>SECURITY TARGET INTRODUCTION (ASE_INT)</b> .....	<b>8</b>
1.1	SECURITY TARGET AND TARGET OF EVALUATION REFERENCE .....	8
1.2	TARGET OF EVALUATION OVERVIEW .....	14
<b>2</b>	<b>TARGET OF EVALUATION DESCRIPTION</b> .....	<b>20</b>
2.1	TOE DEFINITION.....	20
2.2	SCOPE OF THE TOE .....	26
2.2.1	<i>Hardware of the TOE</i> .....	27
2.2.2	<i>Firmware and software of the TOE</i> .....	29
2.2.3	<i>Interfaces of the TOE</i> .....	30
2.2.4	<i>Guidance documentation</i> .....	31
2.2.5	<i>Forms of delivery</i> .....	32
2.2.6	<i>Production sites</i> .....	33
<b>3</b>	<b>CONFORMANCE CLAIMS (ASE_CCL)</b> .....	<b>34</b>
3.1	CC CONFORMANCE CLAIM.....	34
3.2	PP CLAIM .....	34
3.3	PACKAGE CLAIM .....	34
3.4	CONFORMANCE RATIONALE .....	35
3.5	APPLICATION NOTES.....	36
<b>4</b>	<b>SECURITY PROBLEM DEFINITION (ASE_SPD)</b> .....	<b>37</b>
4.1	THREATS.....	37
4.1.1	<i>Additional Threat due to TOE specific Functionality</i> .....	37
4.1.2	<i>Assets regarding the Threats</i> .....	38
4.2	ORGANIZATIONAL SECURITY POLICIES.....	39

4.2.1	<i>Augmented Organizational Security Policy</i> .....	39
4.3	ASSUMPTIONS .....	41
4.3.1	<i>Augmented Assumptions</i> .....	42
<b>5</b>	<b>SECURITY OBJECTIVES (ASE_OBJ)</b> .....	<b>43</b>
5.1	SECURITY OBJECTIVES FOR THE TOE .....	43
5.2	SECURITY OBJECTIVES FOR THE DEVELOPMENT AND OPERATIONAL ENVIRONMENT .....	45
5.2.1	<i>Clarification of "Usage of Hardware Platform (OE.Plat-Appl)"</i> .....	45
5.2.2	<i>Clarification of "Treatment of User Data (OE.Resp-Appl)"</i> .....	46
5.2.3	<i>Clarification of "Protection during Composite product manufacturing (OE.Process-Sec-IC)"</i> .....	46
5.3	SECURITY OBJECTIVES RATIONALE .....	46
<b>6</b>	<b>EXTENDED COMPONENT DEFINITION (ASE_ECD)</b> .....	<b>48</b>
6.1	COMPONENT "SUBSET TOE SECURITY TESTING (FPT_TST)" .....	48
6.2	DEFINITION OF FPT_TST.2 .....	48
6.3	TSF SELF-TEST (FPT_TST) .....	49
6.4	FAMILY "GENERATION OF RANDOM NUMBERS (FCS_RNG)" .....	50
6.5	DEFINITION OF FCS_RNG.1 .....	50
<b>7</b>	<b>SECURITY REQUIREMENTS (ASE_REQ)</b> .....	<b>52</b>
7.1	TOE SECURITY FUNCTIONAL REQUIREMENTS .....	52
7.1.1	<i>Extended Components FCS_RNG.1 and FAU_SAS.1</i> .....	54
7.1.2	<i>Subset of TOE testing</i> .....	56
7.1.3	<i>Memory access control</i> .....	56
7.1.4	<i>Support of Cipher Schemes</i> .....	60
7.1.5	<i>Data Integrity</i> .....	71
7.2	TOE SECURITY ASSURANCE REQUIREMENTS .....	71
7.2.1	<i>Refinements</i> .....	73
7.3	SECURITY REQUIREMENTS RATIONALE .....	77
7.3.1	<i>Rationale for the Security Functional Requirements</i> .....	77
7.3.2	<i>Rationale of the Assurance Requirements</i> .....	84
<b>8</b>	<b>TOE SUMMARY SPECIFICATION (ASE_TSS)</b> .....	<b>85</b>
8.1	SF_DPM: DEVICE PHASE MANAGEMENT .....	85
8.2	SF_PS: PROTECTION AGAINST SNOOPING .....	86
8.3	SF_PMA: PROTECTION AGAINST MODIFYING ATTACKS .....	87
8.4	SF_PLA: PROTECTION AGAINST LOGICAL ATTACKS .....	89
8.5	SF_CS: CRYPTOGRAPHIC SUPPORT .....	89
8.5.1	<i>Triple DES</i> .....	90
8.5.2	<i>AES</i> .....	90

---

8.5.3	RSA .....	90
8.5.4	Elliptic Curves EC .....	91
8.5.5	SHA-2 Operation with Cryptographic Software Library .....	93
8.5.6	Hash Operation with Hardware Module .....	94
8.5.7	Toolbox Library .....	94
8.5.8	Base Library.....	94
8.5.9	PTRNG respectively TRNG .....	95
8.6	ASSIGNMENT OF SECURITY FUNCTIONAL REQUIREMENTS TO TOE'S SECURITY FUNCTIONALITY.....	96
8.7	SECURITY REQUIREMENTS ARE INTERNALLY CONSISTENT.....	97
<b>9</b>	<b>LITERATURE.....</b>	<b>99</b>
<b>10</b>	<b>APPENDIX.....</b>	<b>101</b>
<b>11</b>	<b>LIST OF ABBREVIATIONS.....</b>	<b>103</b>
<b>12</b>	<b>GLOSSARY .....</b>	<b>106</b>

---

**LIST OF TABLES**

Table 1: Identification .....	9
Table 2: Options to implement user software at Infineon production premises .....	11
Table 3: The new interface flexibility.....	25
Table 5: Threats according PP [11] .....	37
Table 6: Additional threats due to TOE specific functions and augmentations.....	38
Table 7: Organizational Security Policies according PP [11] .....	39
Table 8: Assumption according PP [11] .....	41
Table 9: Objectives for the TOE according to PP [11] .....	43
Table 10: Additional objectives due to TOE specific functions and augmentations.....	45
Table 11: Security objectives for the environment according to PP [11] .....	45
Table 12: Security Objective Rationale .....	46
Table 13: Security functional requirements defined in PP [11].....	52
Table 14: Augmented security functional requirements .....	53
Table 15: Cryptographic TOE functionality .....	61
Table 16: Assurance components.....	72
Table 17: Rational for additional SFR in the ST.....	77
Table 18: Dependency for cryptographic operation requirement .....	81
Table 19: Mapping of SFR and SF.....	96
Table 20: Reference hash values of the Cryptographic Libraries.....	101

## 1 Security Target Introduction (ASE\_INT)

### 1.1 Security Target and Target of Evaluation Reference

The title of this document is Security Target Lite, M7893 B11, including optional Software Libraries RSA - EC - SHA-2 – Toolbox, Common Criteria CCv3.1 EAL6 augmented (EAL6+).

This document comprises the Infineon Technologies AG Security Controller (Integrated Circuit IC) M7893 B11 with specific IC dedicated software and optional RSA v1.03.006, EC v1.03.006, SHA-2 v1.01 and Toolbox v1.03.006 software libraries.

The target of evaluation (TOE) M7893 B11 is described in the following. This Security Target has the revision 0.2 and is dated 2015-08-31.

The Target of Evaluation (TOE) is an Infineon Security Controller M7893 B11 with optional RSA2048/4096 v1.03.006, EC v1.03.006, SHA-2 v1.01 libraries and Toolbox v1.03.006 and with specific IC dedicated software (firmware). The design step of this TOE is B11.

The Security Target is based on the Protection Profile “Smartcard IC Platform Protection Profile” [11].

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

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

This TOE concept is based on the architecture, family concept and principles of the TOE M7892 B11 as certified in the process BSI-DSZ-CC-0782-2012 but is enhanced with various interface options, further improved hardware and comes with updated cryptographic libraries. BSI is the abbreviation for Federal Office for Information Security, in German language Bundesamt für Sicherheit in der Informationstechnik.

Table 1: Identification

Item	Version	Date	Registration
Security Target Lite	0.2	2015-08-31	M7893 B11 with optional cryptographic software libraries
Confidential Security Target	0.1	2015-08-20	M7893 B11 with optional cryptographic software libraries
Target of Evaluation			M7893 B11 with FW-Identifier 78.019.03.4 (update) and optional SW: RSA2048 v1.03.006 (optional) RSA4096 v1.03.006 (optional) EC v1.03.006 (optional) SHA-2 v1.01 (optional) Toolbox v1.03.006 (optional) and Guidance documentation
Protection Profile	1.0	2007-06-15	Security IC Platform Protection Profile PP0035
Common Criteria	3.1 Revision 4	2012- September	Common Criteria for Information Technology Security Evaluation <i>Part 1: Introduction and general model</i> CCMB-2012-09-001 <i>Part 2: Security functional requirements</i> CCMB-2012-09-002 <i>Part 3: Security Assurance Components</i> CCMB-2012-09-003

A collection of all referenced documents including the user guidance is given in chapter 9.

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

This TOE is represented by various products, differentiated by various configuration possibilities and order options. Despite these configuration possibilities, all products are derived from the equal hardware design results, the M7893 B11. The GCIM mode is explained and detailed in the user guidance document hardware reference manual HRM [1].

All products are identically from module design and layout, but differ in their possibilities to connect to the power supply, radio frequency antenna, contact based interface options and different packages. Therefore, the TOE is represented and made out of different mask sets and combinations hereof with following TOE internal and security irrelevant differences:

First, there is one metal mask differing only in the input capacity (analogue part) of the radio frequency interface (RFI) allowing adapting different types of antennas. This leads to three versions of this mask and enables to connect a wide range of antennas and to design for different form factors.

Second, one top metal mask alternatively supports different kinds of packages by an optional short cut of the ISO-pads- and the chip core supply. This difference is required for specific applications with restrictions given by standard CC-packages such as VQFN32. This adds two further power supply related options. These differences are comparable to the scenario where for example someone takes a piece of wire and reconnects the pads of the TOE using a soldering bolt.

And last, in order to enable the communication abilities for additional special modules respectively packages with enhanced requirements, different ISO pad usages have been introduced. More details are described in the Errata Sheet [8].

Each of the TOE relevant optional different mask set variants can be identified by the Non-ISO-ATR. 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, Hardware Reference Manual [1].

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 hardware reference manual HRM [1] and in the Errata Sheet [8].

In addition to these hardware differences, the M7893 B11 allows for a maximum of configuration possibilities defined by the customer order following the market needs. For example, a M7893 B11 product can come in one project with the fully available ROM and SOLID FLASH™ Non Volatile Memory (NVM) or in another project without any user available ROM and with any other SOLID FLASH™ NVM-size below the physical implementation size, or with a different RAM size. Even more, the user has the free choice, whether he needs the symmetric co-processor SCP, or the asymmetric co-processor Crypto2304T, or both, or none of them. In addition, the user decides, whether the TOE comes with a free combination of software libraries or without any. And, to be even more flexible, various interface options can be chosen as well. To sum up the major selections, the user defines by his order:

- the available memory sizes of ROM, SOLID FLASH™ NVM and RAM,
- the availability of the cryptographic coprocessors,
- the availability and free combinations of the cryptographic libraries,
- the availability of the Flash Loader for available interfaces like ISO7816, ISO14443, USB or DCLB
- the availability of various further interface options, and

- the possibility to tailor the product by blocking with regard to memory sizes and availability of certain modules on his own premises.

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

Beside fix TOE configurations, which can be ordered as usual, this TOE implements optionally a configuration possibility by blocking, applied by the user at user premises. The realization of this user configuration requires the presence of the Flash Loader software. The presence of this capability defines the customer with his order.

After the final blocking is done and the user additionally may have downloaded his software, the entire Flash Loader software is permanently deactivated. A reactivation of the Flash Loader is not possible. The included firmware provides function to the user to verify the final configuration of the derivate.

All blockings are done by modification of the chip configuration only and without modification of the hardware.

Beside the various TOE configurations further possibilities of how the user inputs his software on the TOE, i.e. the operating system and applications, are in place. This provides a maximum of flexibility and for this an overview is given in the following table:

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

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

5	The user provides the software for implementation into the ROM mask.	The FL is blocked afterwards but can be activated or reactivated by the user or subcontractor to download his software in the Infineon® SOLID FLASH™ memory. Precondition is that the user has provided an own reactivation procedure in software prior chip production to Infineon Technologies AG.
6	The user provides the software for implementation into the ROM mask and provides software for the download into the SOLID FLASH™ NVM to Infineon Technologies AG.	There is no Flash Loader present.
7	The user provides the software for implementation into the ROM mask and provides software for the download into the SOLID FLASH™ NVM to Infineon Technologies AG.	The FL is blocked afterwards but can be activated or reactivated by the user or subcontractor to download his software in the Infineon® SOLID FLASH™ memory. Precondition is that the user has provided an own reactivation procedure in software prior chip production to Infineon Technologies AG.

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

The confidential security target [10] contains an overview about the blocking options of the memory size ranges, certain modules, peripherals and interface options. The blocking option can be applied and configured by Infineon Technologies and partly within defined limits by the user. Within those limitations the TOE configurations can vary under only one identical IC-hardware and one M-number with the above described design steps and without impact on security. All of these possible variations are covered by this certificate.

All possible TOE configurations equal and/or within the specified ranges are covered by the certificate. The hardware reference manual HRM [1] provides an overview about the configuration options respectively ranges.

Note that it is also possible to have no user data in the ROM module. The user software and data are then located in a dedicated and protected part of the SOLID FLASH™ NVM. The long life storage endurance, the automatic management of frequently used memory pages, together with the means for error detection and correction serves for comparable respectively equal reliability and endurance compared to a conventional ROM.

According to the blocking and order options, a not limited number of configurations of the TOE may occur in the field. Basically, 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 hardware, design step and further identification information. The confidential Security Target [10] and the hardware reference manual HRM [1], being part of the user guidance, enables then for the clear interpretation of the read out GCIM data.

In addition, a dedicated firmware allows reading out the present configuration in detail. All these steps for gathering identification and detailed configuration information can be done by the user himself, without involving Infineon Technologies AG.

The TOE consists of the hardware part, the firmware parts and the software parts.

The software parts are differentiated into:

the cryptographic libraries RSA<sup>1</sup>, EC<sup>2</sup> and SHA-2<sup>3</sup> and the supporting libraries Toolbox and Base.

RSA, EC, SHA-2 and Toolbox provide certain functionality via an API to the Smartcard Embedded Software. The Base Library is only used internally by the RSA, EC and Toolbox libraries and has no user interface. If none the three libraries RSA, EC and Toolbox is delivered, also the Base Library is not on board. The SHA-2 library does not use the Base Library.

The firmware parts are the RMS library, the Service Algorithm (SA), the STS firmware for test purpose (see chapter 2.2.2), the Flash Loader for downloading user software to the SOLID FLASH™ NVM and the Mifare compatible software interface. The STS is implemented in a separated Test-ROM being part of the TOE. The RMS and the Flash Loader provide some functionality via an API to the Smartcard Embedded Software.

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

The TOE can be delivered including - in free combinations - or not including any of the functionality of the cryptographic libraries EC, RSA, SHA-2 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 the accompanying "Additional Specific Security Functionality (O.Add-Functions)" *Rivest-Shamir-Adleman (RSA)* and/ or *EC and/or SHA-2* is/are not provided by the TOE.

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

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

---

<sup>1</sup> Rivest-Shamir-Adleman asymmetric cryptographic algorithm

<sup>2</sup> 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.

<sup>3</sup> SHA Secure Hash Algorithm

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

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 RSA, EC, SHA-2 and Toolbox libraries can be implemented together with the Smartcard Embedded Software in the User-ROM mask or respectively loaded into the SOLID FLASH™ NVM. This holds also for the Base Library, if the RSA, EC or Toolbox or combinations hereof is/are part of the shipment.

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

## 1.2 Target of Evaluation overview

The TOE comprises the Infineon Technologies AG Security Multiple Interface Controller M7893 B11 with specific IC dedicated software and optional RSA, EC, SHA-2 and Toolbox libraries.

The TOE is a member of the Infineon Technologies AG high security 78-controller-family meeting the highest requirements in terms of performance and security. A summary product description is given in this Security Target (ST).

The 70 family provides a common architecture upon which specific products can be tailored for markets ranging from low security applications (76 controller family) up to high security and contactless applications (78 controller family).

This TOE is intended to be used in any application and device requiring the highest level of security, for example as secure element in various devices.

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

This TOE provides multiple interface options for various applications and markets. Due to the interface flexibility the product can be used in almost any application, within any device and almost any form factor, i.e. as a build-in device: Due to these multiple communication possibilities, the TOE can be seen as a stand-alone security device being capable to maintain a multitude of data communication interfaces simultaneously. For example, one application communicates via one interface, totally separated from another application, communicating via a second interface, at the same time.

Again these communication and application independency capabilities enable the usage to almost everywhere, where highly secure applications are in use and of course in any other application as well. This TOE is deemed for governmental, corporate, transport and payment markets, or wherever a secure root of trust is required. Various

types of applications can use this TOE, for example in closed loop logical access controls, physical access controls, secure internet access control and internet authentication, or as multi-application token or simply as encrypted storage.

This multiple interface controller provides, depending on the used communication protocols, maximum flexibility in terms of simultaneously respectively parallel available communication ability. A brief description of the interface types is given below and a table with regard to the parallel availability is given in chapter 2.2.3:

#### Contactless Interfaces

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

#### Contact based Interfaces

- ISO/IEC 7816-3  
This is the ISO defined standard contact based communication protocol, using the pads.
- DCLB Digital Contactless Bridge mode  
The DCLB mode enables the use of an external analogue interface or near field communication (NFC) modem via the ISO-pads or alternatively via the GPIO pads. Those external analogue modems are typically deemed for applications running in mobile devices and are not part of this TOE. Whether the DCLB option is available or not is a configuration applied in TOE production which cannot be changed afterwards.
- ACLB Advanced Contactless Bridge mode  
The ACLB mode provides the possibility to leave the analogue communication to the external device - as with DCLB - but the connection is done via the  $L_a$  and  $L_b$  pads to the external device or external contactless reader chip directly. Therefore, an external antenna cannot be connected, if the user decides to use this interface option.
- IIC Inter-Integrated Circuit-bus  
The Inter-Integrated Circuit (IIC) module is able to be connected as slave to an external multi-master-serial-bus-system used to connect the TOE to an external master, using the IIC protocol. The master can also be a multi master IIC system. The IIC protocol software is not part of the TOE.
- GPIO General Purpose Input Output  
The GPIO module supports a number of general purpose I/O signals in parallel and independent of each other. Each of the I/O signals can be configured as push-pull or open-drain output with a fast or slow slew rate. The GPIO interface can be directly accessed by the user software.

In addition, it can be configured which of the other interface module connects to the GPIO signals. But note that below listed interfaces do not require the connection to GPIO. The configurable connection to GPIO signals is just an option. More information is given in the confidential Security Target [10].

- Serial Peripheral Interface SPI master or slave, serial interface

This interface can be configured as SPI master or SPI slave and enables for serial communication. In both cases the data width, the shift direction, the clock polarity and the clock phase are configurable, allowing for easy and flexible adaptation to other SPI enabled peripherals.

- Universal Serial Bus USB

This TOE provides the universal serial bus USB interface ability to communicate with numerous USB-enabled devices. The USB communication uses the ETSI TS 102 600 (IC-USB) standard and provides the full speed of USB 2.0.

Some of the interfaces can be combined and used simultaneously. More information is given in the confidential Security Target [10].

A further option is the Advanced Communication Mode allowing for very high bit rates in the context of using Mifare communication.

In order to increase the contactless interface performance even more, the RFI can be configured in terms of baud rates for reception and transmission and the setting of the sub-carrier frequency used for the load modulation. More details are given in the hardware reference manual HRM [1].

The TOE provides a real 16-bit CPU-architecture and is compatible to the 80251 microcontroller architecture. The major components of the core system are the two CPUs (Central Processing Units), acting as one, the MMU (Memory Management Unit) and MED (Memory Encryption/Decryption Unit). The two CPU parts control each other in order to detect faults and serve by this for data integrity. The TOE implements a full 16 MByte linear addressable memory space for each privilege level, a simple scalable Memory Management concept and a scalable stack size. The flexible memory concept consists of ROM, RAM and the nonvolatile memory (NVM), respectively SOLID FLASH™ NVM. For the SOLID FLASH™ NVM the Unified Channel Programming (UCP) memory technology is used.

The RMS library providing some functionality via an API to the Smartcard Embedded Software contains for example SOLID FLASH™ NVM service routines. The Service Algorithm provides functionality for the tearing save write into the SOLID FLASH™ NVM. The STS firmware is used for test purposes during start-up and the Flash Loader allows downloading user software to the SOLID FLASH™ NVM during the manufacturing process. The firmware parts are implemented in the ROM and in access protected areas of the SOLID FLASH™ NVM.

The BSI has changed names and abbreviations for Random Number Generators, which is clarified as follows: The Physical True Random Number Generator (PTRNG), also named True Random Number Generator (TRNG) is a physical random number generator and meets the requirements of the functionality class AIS31 PTG.2, see [15]. It is used for provision of random number generation as a security service to the user and for internal purposes. The produced genuine random numbers can be used directly or as seed for the Deterministic Random Number Generator (DRNG), former named as Pseudo Random Number Generator (PRNG). The DRNG respectively PRNG is not in the scope of the

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

The TOE implements two cryptographic co-processors: The symmetric cryptographic co-processor (SCP) combines both AES and DES with one, two or triple-key hardware acceleration. The Asymmetric Crypto Co-processor, called Crypto2304T, provides optimized high performance calculations for the user software executing cryptographic operations and is also used by the optional cryptographic libraries for RSA and Elliptic Curve (EC) cryptography.

The software part of the TOE consists of the cryptographic RSA-, EC- and the SHA-2 libraries and the supporting Toolbox and Base libraries. If RSA or EC or Toolbox or combinations hereof are part of the shipment, automatically the Base Library is included.

The RSA library is used to provide a high level interface to RSA (Rivest, Shamir, Adleman) cryptography implemented on the hardware component Crypto2304T and includes countermeasures against SPA, DPA and DFA attacks. The routines are used for the generation of RSA Key Pairs (RsaKeyGen), the RSA signature verification (RsaVerify), the RSA signature generation (RsaSign) and the RSA modulus recalculation (RsaModulus). The hardware Crypto2304T unit provides the basic long number calculations (add, subtract, multiply, square with 1100 bit numbers) with high performance. The RSA library is delivered as object code and in this way integrated in the user software. The RSA library can perform RSA operations from 512 to 4096 bits.

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

The EC library is used to provide a high level interface to Elliptic Curve cryptography implemented on the hardware component Crypto2304T and includes countermeasures against SPA, DPA and DFA attacks. The routines are used for ECDSA signature generation, ECDSA signature verification, ECDSA key generation and Elliptic Curve Diffie-Hellman key agreement. In addition, the EC library provides an additional function for calculating primitive elliptic curve operations like ECC Add and ECC Double. EC curves over prime field  $F_p$ , as well as over  $GF(2^n)$  finite field are supported too. Note that the according user guidance the Elliptic Curve cryptographic functions are abbreviated using ECC.

The EC library is delivered as object code and in this way integrated in the user software. The certification covers the standard NIST [17] and Brainpool [18] Elliptic Curves with key lengths of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 Bits, due to national AIS32 regulations by the BSI. Numerous other curve types, being also secure in terms of side channel attacks on this TOE, exist, which the user optionally can add in the composition certification process.

The SHA-library provides the calculation of a hash value of freely chosen data input in the CPU. The SHA-library is delivered as object code and is in this way available for the user software. This secure hash-algorithm SHA-2 is intended to be used for signature generation, verification and generic data integrity checks. Further essential information about the usage is given in the confidential user guidance.

In addition to the SHA-library, this TOE provides the Hash module to compute extremely fast hash values within just some dozens of clock cycles. The availability of the Hash-module depends on the user. The Hash module provides following hashing algorithms:

- MD-5
- SHA-1
- SHA-256.

This Hash module is intended to be used for signature generation, verification and generic data integrity checks. Following the BSI recommendations the algorithms MD-5 and SHA-1 are not covered by this evaluation. Further essential information about the usage is given in the confidential user guidance.

The TOE can come with the Secure Hash Algorithm by Hardware (optional HW Hash) being available or not. If the Hash module is blocked the hardware implemented Hash Algorithms are not available. The use of the Hash module is independent from the optional SHA-2 library software and also independent of the availability of the cryptographic coprocessors. No accessibility of the Hash module 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 Hash module.

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

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

Note that this TOE can come with both cryptographic co-processors accessible, or with a blocked SCP or with a blocked Crypto2304T, or with both cryptographic co-processors blocked. The blocking depends on the user's choice prior to the production of the hardware. No accessibility of the deselected cryptographic co-processors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic co-processors. The TOE can be delivered without a specific library. In this case the TOE does not provide the Additional Specific Security Functionality Rivest-Shamir-Adleman Cryptography (RSA) or/and Elliptic Curve Cryptography (EC) or/and SHA-2.

To fulfill the highest security standards for smartcards today and also in the future, this TOE implements a progressive digital security concept, which already has been certified in various forerunner processes and which has proven its resistance against attackers with high attack potential. This TOE utilizes digital security features to include customer friendly security, combined with a robust design overcoming the disadvantages on analogue protection technologies. The TOE provides full on-chip encryption of the data path covering the core including the ALUs of the CPU parts, busses, memories and cryptographic co-processors leaving no plaintext on the chip. Therefore the attractiveness for attackers is extremely reduced as encrypted signals are of no use for the attacker – neither for manipulation nor for eavesdropping.

In addition, the TOE is equipped with a comprehensive error detection capability. The double CPU approach allows

error detection even while processing, e.g. a comparator detects, whether a calculation was performed without errors. This approach is designed to cover all relevant parts of the circuitry. The concept allows that the relevant attack scenarios are detected, whereas other conditions that would not lead to an error would mainly be ignored. And more, the TOE is equipped with signal protection implemented by an Infineon-specific shielding combined and further topological means.

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

In the confidential Security Targets [10] the TOE is described and a summary specification is given. The security environment of the TOE during its different phases of the lifecycle is defined. The assets are identified which have to be protected through the security policy. The threats against these assets are described. The security objectives and the security policy are defined, as well as the security requirements. These security requirements are built up of the security functional requirements as part of the security policy and the security assurance requirements. These are the steps during the evaluation and certification showing that the TOE meets the targeted requirements. In addition, the functionality of the TOE matching the requirements is described.

The assets, threats, security objectives and the security functional requirements are defined in this Security Target and in the Protection Profile [11] and are referenced here. These requirements build up a minimal standard common for all Smartcards.

The security functions are defined here in the security target as property of this specific TOE. Here it is shown how this specific TOE fulfills the requirements for the standard defined in the Protection Profile [11].

## 2 Target of Evaluation Description

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

### 2.1 TOE Definition

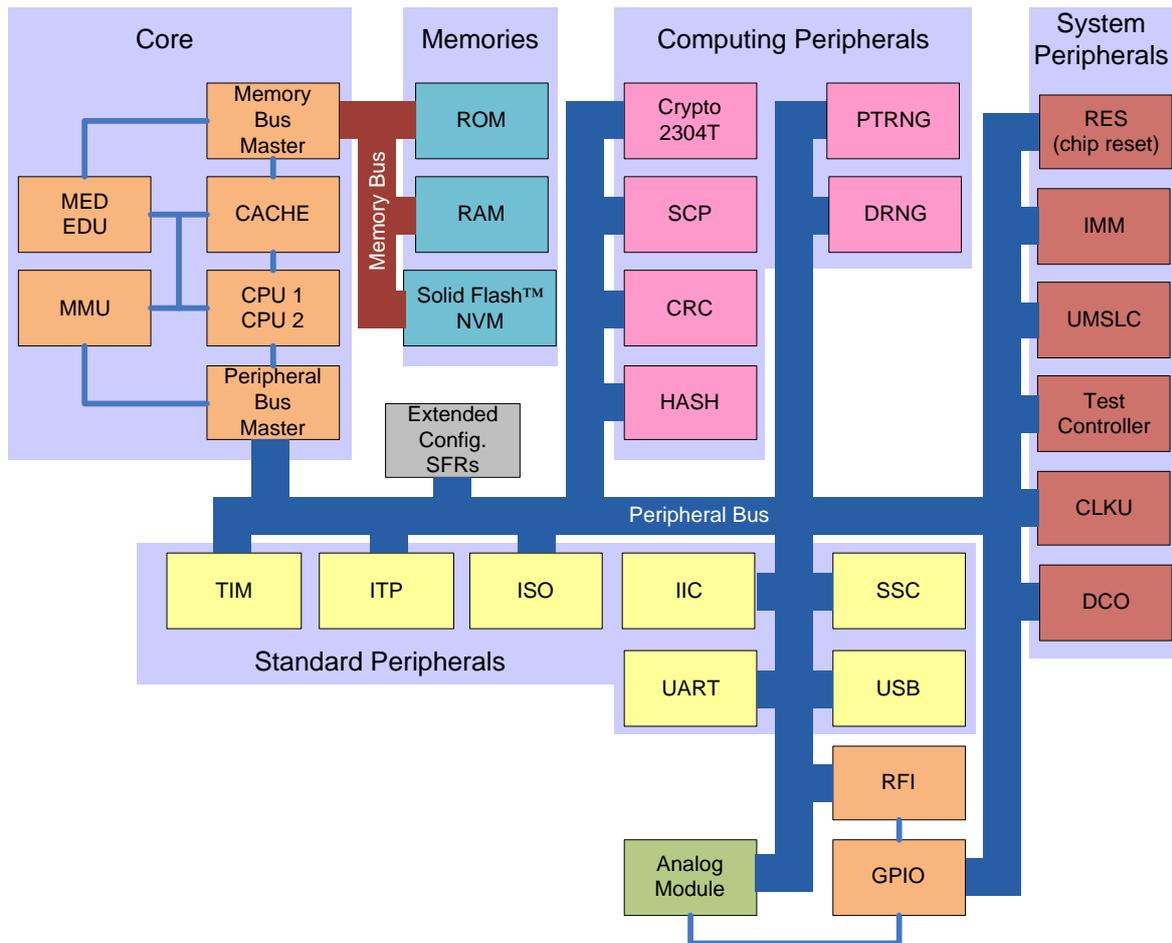
This TOE consists of Security Multiple Interface Controllers as integrated circuits, meeting the highest requirements in terms of performance and security. They are manufactured by Infineon Technologies AG in 90 nm CMOS-technology (L90). This TOE is intended to be used in smart cards and other form factors for particularly security-relevant applications and for its previous use as developing platform for smart card operating systems according to the lifecycle model from the Protection Profile [11]

The term Smartcard Embedded Software is used in the following for all operating systems and applications stored and executed on the TOE regardless whether it is a smartcard or another application of form factor. The TOE is the platform for the Smartcard Embedded Software. The Smartcard Embedded Software itself is not part of the TOE.

The TOE consists of a core system, memories, computing peripherals, system peripherals, standard peripherals, an analogue module and the connecting busses.

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

Figure 1: Block diagram of the TOE



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

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

The CPU accesses the memory via the integrated Memory Encryption and Decryption unit (MED), which transfer the data from the memory encryption schema to the CPU encryption schema without decrypting into intermediate plain data. The error detection unit (EDU) automatically manages the error detection of the individual memories and detects incorrect transfer of data between the memories and the core by means of Error Detection Code (EDC) comparison. The access rights of the firmware, user operating system and application to the memories are controlled and enforced by the memory management unit (MMU). Errors in the memories are automatically detected (EDC) and in terms of the SOLID FLASH™ NVM 1-Bit-errors are also corrected (ECC). The two processors of the CPU control each other in order to detect faults and maintain by this the data integrity. A comparator detects whether a calculation was

performed without errors and allows error detection even while processing. Therefore the TOE is equipped with a comprehensive error detection capability, which is designed to leave no relevant parts of the circuitry unprotected.

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

The error detection unit (EDU) automatically manages the error detection of the individual memories and detects incorrect transfer of data between the memories by means of error code comparison.

Just to sum up, the TOE stores, computes and internally transfers only masked respectively encrypted and integrity protected data, leaving no plain data anywhere on the TOE. The only plain data could be found when it is communicated to the outer world via the multiple interfaces.

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

The memory block contains the ROM, RAM and the SOLID FLASH™ NVM. All data of the memory block is encrypted and all memory types are equipped with an error detection code (EDC), the SOLID FLASH™ NVM in addition with an error correction code (ECC). This TOE stores user code and data in a linear 16-MByte memory space, the SOLID FLASH™ NVM, allowing direct access without the need to swap memory segments in and out of memory using a memory management unit.

The TOE uses also Special Function Registers SFR. These SFR registers are used for general purposes and chip configuration. These registers are located in the SOLID FLASH™ NVM as configuration area page.

The non-volatile ROM contains the firmware parts, accessible for Infineon only, and could optionally include user code and/or data, if transferred to Infineon Technologies prior production. The RAM is a volatile memory which means that the content is lost at power off and used by the core.

The computing peripherals block contains the processors for asymmetric and symmetric cryptographic algorithm and Hash processing, the random number generators and the cyclic redundancy check CRC module.

The PTRNG respectively TRNG is specially designed for smart card applications. The PTRNG respectively TRNG fulfills the requirements from the functionality class PTG.2 of the AIS31 and produces genuine random numbers which then can be used directly or as seed for the PRNG respectively DRNG. The PRNG respectively DRNG is not in the scope of the evaluation.

The TOE implements two cryptographic co-processors: The symmetric cryptographic co-processor (SCP) combines both AES and DES with one, two or triple-key hardware acceleration. The Asymmetric Crypto Co-processor, called Crypto2304T, provides optimized high performance calculations for the user software executing cryptographic

operations and is also used by the optional cryptographic libraries for RSA and Elliptic Curve (EC) cryptography. These co-processors are especially designed for smart card applications with respect to the security and power consumption. The SCP module computes the complete DES algorithm within a few clock cycles and is especially designed to counter attacks like DPA, EMA and DFA.

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

In addition, this TOE provides the Hash module to compute extremely fast hash values within just some dozens of clock cycles. The hash module is based on the hash sub-block of the CEU module<sup>4</sup>, developed by the COM group. Following hashing algorithms can be performed using this module:

- MD-5
- SHA-1
- SHA-256.

This Hash module is intended to be used for signature generation, verification and generic data integrity checks. Following the BSI recommendations the algorithms MD-5 and SHA-1 are not covered by this evaluation. Further essential information about the usage is given in the confidential user guidance.

The TOE can come with the Secure Hash Algorithm by Hardware (optional HW Hash) being available or not. If the Hash module is blocked the hardware implemented Hash Algorithms are not available. The use of the Hash module is independent from the optional SHA-2 library software and also independent of the availability of the cryptographic coprocessors. No accessibility of the Hash module 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 Hash module.

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

The system peripherals block contains mainly the components required for chip operation and the standard peripherals block the components mainly related to the interfaces. Due to their size the contactless interface RFI and the GPIO interface represent a block on their own. The analogue module contains the required analogue circuits such as filters, some robustness sensors and the analogue circuits required for the chip power regulation and generation.

The system peripheral block contains the User Mode Security Life Control and the small remaining set of sensors and filters. This small set of sensors is left in order to detect excessive deviations from the specified operational range,

---

<sup>4</sup> See IPDB, Configurable Encryption Unit (CEU) Architecture Specification Rev. 1.4.2, November 22, 2007

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

The filters are on board to make the TOE more robust against perturbations on the supply lines. The UmSLC enables for checking the proper functions of modules and subsystems essential for the correct operation of the TOE.

The digital controlled oscillator DCO implements a precise and configurable oscillator for proper synchronization of the communication regarding the interfaces, i.e. USB, and the various system frequencies.

Further modules in this block are the reset module (RES) responsible to conduct a TOE reset, the interface management module (IMM), controlling the various interfaces as well as modules supplying clock and power. The test control module is used only during the TOE production and has no user interface.

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

The standard peripherals block contains finally the various interface modules enabling to communicate using the contact based or the contactless interfaces in various combinations and partly even simultaneously. The RFI and GPIO represent blocks on their own but interact also with the controls located in the standard peripherals block.

The timer enables for easy implementation of communication protocols such as T=1 and all other time-critical operations. The timer can be programmed for particular applications, such as measuring the timing behavior of an event. Timer events can generate interrupt requests to be used for peripheral event channel data transfers. The watchdog is implemented to provide the user some additional control of the program flow. More details are given in the hardware reference module HRM [1]

The Interrupt and Peripheral Channel Controller (ITP) arbitrates what CPU action is required to manage individual interrupt requests. The controller can be associated with different interrupt events, allowing it to select between either executing a standard interrupt service routine or a fast data transfer between two memory locations over a so-called peripheral event channel.

The Synchronous Serial Controller (SSC) peripheral provides the Serial Peripheral Interface SPI compatibility. The data format, data shifting, clock settings are programmable. The interface speed (that means, the maximum data transfer rate) depends on the module clock frequency and the selected mode

The Universal Asynchronous Receiver Transmitter UART-controlled I/O interface enables the security controller and the terminal interface to be operated independently, and implements a contact based asynchronous serial interface. The UART supports the T=0 and T=1 protocol according to ISO7816-3.

The analogue block finally contains all analogue design parts required for the clock -and voltage supply and for the various interfaces.

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

The availability of the DCLB and ACLB modes is configured during TOE production and depends on the customer order. Regarding the DCLB enabled derivatives it depends on the operating system of how the pads are configured and used. The individual combinations of the interface options are depicted in the table below. More information is given in the confidential Security Target [10].

Supporting a Mifare compatible interface application requires a dedicated small space of memory. Depending on user’s choice, various Mifare compatible Interface memory sections of 1 or 4 Kbytes each can be defined. The number and location of Mifare compatible interface memory sections is simply limited by the available SOLID FLASH™ NVM space. The Mifare compatible interface memory sections are read/write protected and are defined and generated by the user.

More information about the interfaces and their combinations can be found in the confidential Security Target [10].

An overview upon the various interface options is provided by following table:

Table 3: The new interface flexibility

CL-supply	Pad group	La/Lb						
	Interface	RF						
	Protocol	TI (CIM)	ISO14443 A	ISO14443 B	ISO18092 (Felica)	Mifare		
CB-supply	Pad group	La/Lb						
	Interface	RF / ACLB						
	Protocol	ISO14443 A	ISO14443 B	ISO18092 (Felica)	Mifare			
	Pad group	ISO - CB						
	Interface	ISO 7816		I2C	DCLB			
	Protocol	TI (CIM)	ISO7816	I2C	ISO14443 A	ISO14443 B	ISO18092 (Felica)	Mifare
	Pad group	USB						
	Interface	USB						
	Protocol	USB2.0	IC-USB	TS_102600				
	Pad group	GPIO						
Interface	GPIO		I2C	DCLB				
Protocol	SWIO	SPI	I2C	ISO14443 A	ISO14443 B	ISO18092 (Felica)	Mifare	

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

This secure hash-algorithm SHA-2 is intended to be used for signature generation, verification and generic data integrity checks. Further essential information about the usage is given in the confidential user guidance.

The STS (self-test software), RMS (Resource Management System), Service Algorithm (SA) and Flash Loader together compose the TOE firmware stored in the ROM and the patches hereof in the SOLID FLASH™ NVM. All mandatory

functions for internal testing, production usage and start-up behavior (STS), and also the RMS and SA functions are grouped together in a common privilege level. These privilege levels are protected by a hardwired Memory Management Unit (MMU) setting.

The user software can be implemented in various options depending on the user's choice and described in chapter 1.1. Thereby the user software can be implemented in the ROM and/or the SOLID FLASH™ NVM or coming without user software. In the latter case, the user downloads his entire software on his own using the Flash Loader software.

The TOE sets a new, improved standard of integrated security features, thereby meeting 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 Multiple Interface high security controller with a large amount of memory and special peripheral devices with improved performance, optimized power consumption, free to choose contact based or contactless operation, at minimal chip size while implementing high security. It therefore constitutes the basis for current and future applications.

## 2.2 Scope of the TOE

The TOE comprises several types of hardware each differing by mask set changes and mask set combinations to allow for maximum flexibility in terms of connection to power supplies, external antennas and implementation into different kinds of package and module types. All these changes have no influence on the security or any security policy related to the TOE. More information is given in the confidential Security Target [10].

Therefore, this TOE includes:

- All configurations and resulting derivatives generated out of the mask sets and combinations as described in the confidential Security Target [10]
- with according firmware and
- optional software

as defined in the following chapters.

Despite these module respectively package, communication and power supply related hardware differences and options, the TOE is delivered in various configurations, achieved by means of blocking and depending on the customer order.

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 documents as described in section 2.2.4 and listed in Table 1, are supplied as user guidance.

Not part of the TOE and not part of the certification are:

- the Smartcard Embedded Software respectively user software, and
- some software parts running at user premises cover commercial aspects of user applied blocking.

### 2.2.1 Hardware of the TOE

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

#### Core System

Proprietary double CPU implementation being comparable to the 80251 microcontroller architecture from functional perspective and with enhanced MCS<sup>®</sup> 251 instruction set

Memory Management Unit (MMU)

CACHE with Post Failure Detection

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

Memory Bus Master

Peripheral Bus Master

#### Memories

SOLID FLASH<sup>™</sup> NVM implementing the Unified Channel Programming concept UCP

Read-Only Memory (ROM)

Random Access Memory (RAM)

#### Computing Peripherals

Optional Crypto2304T for asymmetric algorithms like RSA and EC

Optional Symmetric Crypto Co-processor for DES and AES Standards

True Random Number Generator (PTRNG respectively TRNG)

Pseudo Random Number Generator (PRNG respectively DRNG)

Optional Cyclic Redundancy Check (CRC)

Optional Hash module

#### **Peripheral Bus**

#### **Memory Bus**

#### **System Peripherals**

Reset Module – Chip Reset

Interface Management Module (IMM)

User Mode Security Life Control (UMSLC)

Test Controller

Clock and Power Management Unit (CLKU)

Digital Controlled Oscillator (DCO)

#### **Analogue Module**

Modules for power supply of the chip core

Modules for power supply for the various interfaces

Filters

Remaining set of sensors for robustness

Analogue modules of the interface controls

#### **Standard Peripherals**

Timers and Watchdogs

Interrupt and Peripheral Event Channel Controller (ITP and PEC)

ISO communication modules with universal asynchronous receiver/transmitter (UART)

Inter-IC-circuit-bus IIC

Synchronous Serial Controller SSC

Universal Serial Bus (USB)

#### **RF interface (radio frequency power and signal interface)**

#### **General Purpose Input Output GPIO**

#### **Extended Configuration**

If a hardware module is claimed above as optional, it may be available or not to the user by blocking means only. This means that the chip hardware remains always equal, regardless whether such optional module is available or not.

## 2.2.2 Firmware and software of the TOE

The entire firmware of the TOE consists of different parts:

One part comprises the RMS and SA routines used for providing the chip resource management interface for the user. The routines are used for tearing save handling of the SOLID FLASH™ NVM, user testing of the security functions and error correction (Resource Management System, IC Dedicated Support Software in the Protection Profile [11]).

The RMS and SA routines are stored from Infineon Technologies AG in a reserved area of the user ROM and belonging patches (if any) are located in the SOLID FLASH™ NVM.

The second part is the STS, consisting of test and initialization routines (Self-Test Software, IC Dedicated Test Software in the Protection Profile [11]). The STS routines are stored in the ROM and are not accessible for the user software.

The third part is the Flash Loader, a piece of software located in the ROM and allowing downloading the user software or parts of it to the SOLID FLASH™ NVM in a secured way. After completion of the download the Flash Loader can be permanently deactivated by the user.

The fourth part is the Mifare compatible interface routines called via RMS routines if this interface option is active. Note that this interface is always present, but deactivated in case of the non-Mifare compatible interface derivatives. Thus the user interface is identically in both cases and subsequently these interface routines can be called in each of the derivatives. In case this interface is blocked, but the routines are however called, a dedicated error code is returned.

The optional software part of the TOE consists of the RSA-, the EC, the Toolbox and the SHA-2 library.

The RSA library is used to provide a high level interface to the RSA cryptography implemented on the hardware component Crypto2304T and includes countermeasures against SPA, DPA and DFA attacks. The routines are used for the generation of RSA Key Pairs (RsaKeyGen), the RSA signature verification (RsaVerify), the RSA signature generation (RsaSign) and the RSA modulus recalculation (RsaModulus). The module provides the basic long number calculations (add, subtract, multiply, square with 1100 bit numbers) with high performance.

The RSA library is delivered as object code or object code and in this way integrated in the user software. The RSA library can perform RSA operations from 512 to 4096 bits. Depending on the customer's choice, the TOE can be delivered with the 4096 code portion or with the 2048 code portion only. The 2048 code portion is included in both.

Parts of the evaluation are only operations with key length from 1976 bits to 2048 bits, and 4096 bits with or without making use of the CRT<sup>5</sup>. Note that key lengths below 1976 bit are not included in the certificate.

The EC library is used to provide a high level interface to Elliptic Curve cryptography implemented on the hardware component Crypto2304T and includes countermeasures against 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.

---

<sup>5</sup> CRT: Chinese Remainder Theorem

The EC library is delivered as object code and in this way integrated in the user software. The certification covers the standard NIST [17] and Brainpool [18] Elliptic Curves with key lengths of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 Bits, due to national AIS32 regulations by the BSI. Numerous other curve types, being also secure in terms of side channel attacks on this TOE, exist, which the user optionally can add in the composition certification process.

The SHA-2 library provides the calculation of a hash value of freely chosen data input in the CPU. The SHA-2 library is delivered as object code and is in this way available for the user software. This secure hash-algorithm SHA-2 is intended to be used for signature generation, verification and generic data integrity checks. Further essential information about the usage is given in the confidential user guidance.

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

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

#### Note 1:

The cryptographic libraries RSA, EC, SHA-2 and the Toolbox library are delivery options. If one of the libraries RSA, EC and Toolbox or combination hereof are delivered, the Base Lib is automatically part of it. The TOE may come with free combinations of or even without these libraries. In the case of coming without one or any combination of the cryptographic libraries RSA, EC and SHA-2, the TOE does not provide the Additional Specific Security Functionality Rivest-Shamir-Adleman Cryptography (RSA) and/or Elliptic Curve Cryptography (EC) and/or SHA-2.

The Toolbox and Base Library are no cryptographic libraries and provide no additional specific security functionality.  
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 GPIO interface consists of 12 functional and 2 power pads which can be individually configured and combined in various ways.
  - The USB interface is built out of two differential USB-data pads and two power pads.

- A further electrical interface are the La and Lb pads used for the antenna connection and alternatively for the ACLB communication mode connecting an external reader chip which is not part of the TOE.
- The DCLB, the IIC and the SPI communication can be driven via the GPIO or ISO 7816 pads. This has certain dependencies if intended to be used simultaneously with other interfaces. More information is given in the confidential Security Target [10]
- The contactless or radio frequency interface enables contactless communication between a PICC (proximity integration chip card, PICC) and a PCD reader/writer (proximity coupling device, PCD). The required antenna is not part of the TOE.
- The data-oriented I/O interface to the TOE is formed by the I/O pads of ISO 7816, GPIO and USB interfaces and by the various contactless interface options.
- The interface to the firmware is constituted by special registers used for hardware configuration and control (Special Function Registers, SFR).
- The interface of the TOE to the operating system is constituted on one hand by the RMS routine calls and on the other by the instruction set of the TOE.
- The interface of the TOE to the test routines is formed by the STS test routine call, i.e. entry to test mode (STS-TM entry).
- The interface to the RSA calculations is defined from the RSA library interface.
- The interface to the EC calculations is defined from the EC library interface
- The interface to the SHA-2 calculation is defined from the SHA-2 library interface.
- The interface to the Toolbox is defined from the Toolbox library interface.

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

#### 2.2.4 Guidance documentation

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

- The No.1 HRM is the user data book of the TOE and contains the relevant module, function and feature description
- The No. 2 PPUM contains detailed information about the usage of the Flash Loader
- The document No. 3 PRM describes the usage and interface of the Resource Management System RMS.
- The document No. 4 CLUI contains all interfaces of the RSA, EC and Toolbox library and is only delivered to the user in case the RSA library and/or the EC library is/are part of the delivered TOE.
- The document No. 5 SHA-2 contains all interfaces of the SHA-2 library and is only delivered to the user in case the SHA-2 library is part of the delivered TOE. The security guidelines contain all hints and recommendations for a secure programming of the TOE.

- The document No. 6 CUM describes the architecture of cryptographic coprocessor on register level. It also provides a functional description of the register architecture, instruction set and gives programming guidance.
- The document No. 7 SG represents the User Manual for the software programmers.
- The document No. 8 ES contains the description of all interfaces of the software to the hardware relevant for programming the TOE. The SLE70 Family Errata Sheet can be changed during the life cycle of the TOE. This is reported in a monthly updated list provided from Infineon Technologies AG to the user.
- The document No. 9 AMM, Advanced Mode for Mifare-Compatible Technology, additional user guidance how to use the Advanced Mode for Mifare Technology (AMM). This documentation is provisioned to the user if the AMM option has been ordered. This user guidance describes the interface and how to implement and use this communication mode. This is an addendum to the HRM [1].

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

### 2.2.5 Forms of delivery

The TOE can be delivered in form of complete modules, with or without inlay mounting, with or without inlay antenna mounting, in form of plain wafers or in an IC case (for example TSSOP28, VQFN32, VQFN40, CCS-modules, etc.) or in bare dies. In any case, the form of delivery does not affect the TOE security and it can be delivered in any form, as long as the processes applied and sites involved have been subject of the appropriate audit.

The delivery can therefore be at the end of phase 3 or at the end of phase 4 which can also include pre-personalization steps according to the Protection Profile [11]. Nevertheless in both cases the TOE is finished and the extended test features are removed. In this document are always both cases mentioned to avoid incorrectness but from the security policy point of view the two cases are identical.

The delivery to the software developer (phase 2 → phase 1) contains the development package and is delivered in form of documentation as described above, data carriers containing the tools and emulators as development and debugging tool.

Part of the software delivery could also be the Flash Loader program, provided by Infineon Technologies AG, running on the TOE and receiving via the UART interface the transmitted information of the user software to be loaded into the SOLID FLASH™ NVM. The download is only possible after successful authentication. The user software can also be downloaded in an encrypted way. In addition, the user is, after he finalized the download and prior deliver to third party, obligated to permanently lock further use of the Flash Loader. Note that it depends on the procurement order, whether the Flash Loader program is present or not.

### 2.2.6 Production sites

The TOE may be handled in different production sites but the silicon of this TOE is produced in Dresden, Germany. 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 hardware reference manual HRM [1].

The delivery measures are described in the ALC\_DVS aspect.

### 3 Conformance Claims (ASE\_CCL)

#### 3.1 CC Conformance Claim

This Security Target (ST) and the TOE claim conformance to Common Criteria version v3.1 part 1 [12], part 2 [13] and part 3 [14].

Conformance of this ST is claimed for:

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

#### 3.2 PP Claim

This Security Target is in **strict conformance** to the Security IC Platform Protection Profile [11].

The Security IC Platform Protection Profile is registered and certified by the Bundesamt für Sicherheit in der Informationstechnik<sup>6</sup> (BSI) under the reference BSI-PP-0035, Version 1.0, dated 2007-06-15.

The security assurance requirements of the TOE are according to the Security IC Platform Protection Profile [11]. They are all drawn from Part 3 of the Common Criteria version v3.1.

The targeted EAL6+ level includes already the augmentations of the PP [11] AVA\_VAN.5 and ALC\_DVS.2. Further augmentation is achieved - with regard to CCv3.1 Part 3: Security assurance components – as follows:

Table 4: Augmentations of the assurance level of the TOE

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

#### 3.3 Package Claim

This Security Target does not claim conformance to a package of the PP [11].

The assurance level for the TOE is EAL6 augmented with the component ALC\_FLR.1

**The assurance level for the TOE is:**

**EAL6 augmented (EAL6+) with the component ALC\_FLR.1.**

<sup>6</sup> Bundesamt für Sicherheit in der Informationstechnik (BSI) is the German Federal Office for Information Security

### 3.4 Conformance Rationale

This security target claims strict conformance only to one PP, the PP [11].

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

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

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

Security Problem Definition:

Following the PP [11], the security problem definition is enhanced by adding an additional threat, 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 [11], as the security target claimed strict conformance to the PP [11].

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-dependent function, and the threat memory access violation T.Mem-Access, due to specific TOE memory access control functionality, have been added. These add-ons have no impact on the conformance statements regarding CC [12] and PP [11], with following rational:

- The security target remains conformant to CC [12], claim 482 as the possibility to introduce additional restrictions is given.
- The security target fulfills the strict conformance claim of the PP [11] due to the application notes 5, 6 and 7 which apply here. By those notes the addition of further security functions and security services are covered, even without deriving particular security functionality from a threat but from a policy.

Due to additional security functionality, one coming from the cryptographic libraries - O.Add-Functions, and due to the memory access control - O.Mem-Access, additional security objectives have been introduced. These add-ons have no impact on the conformance statements regarding CC [12] and PP [11], with following rational:

- The security target remains conformant to CC [12], claim 482 as the possibility to introduce additional restrictions is given.
- The security target fulfills the strict conformance of the PP [11] due to the application note 9 applying here. This note allows the definition of high-level security goals due to further functions or services provided to the Security IC Embedded Software.

Therefore, the security objectives of this security target are consistent with the statement of the security objectives in the PP [11], as the security target claimed strict conformance to the PP [11].

All security functional requirements defined in the PP [11] are included and completely defined in this ST. The security functional requirements listed in the following are all taken from Common Criteria part 2 [13] and additionally included and completely defined in this ST:

- FDP\_ACC.1 “Subset access control”
- FDP\_ACF.1 “Security attribute based access control”
- FMT\_MSA.1 “Management of security attributes”
- FMT\_MSA.3 “Static attribute initialisation”
- FMT\_SMF.1 “Specification of Management functions”
- FCS\_COP.1 “Cryptographic support”
- FCS\_CKM.1 “Cryptographic key generation”
- FDP\_SDI.1 “Stored data integrity monitoring”
- FDP\_SDI.2 “Stored data integrity monitoring and action”

The security functional requirement

- FPT\_TST.2 “Subset TOE security testing“(Requirement from [13])
- FCS\_RNG.1 “Generation of Random Numbers”

are included and completely defined in this ST, section 6.

All assignments and selections of the security functional requirements are done in the PP [11] 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 requirement FCS\_RNG.1 is a refinement of the FCS\_RNG.1 defined in the Protection Profile [11] according to “Anwendungshinweise und Interpretationen zum Schema (AIS)” respectively “Functionality classes and evaluation methodology for physical random number generators”, AIS31 [15].

## 4 Security Problem Definition (ASE\_SPD)

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

### 4.1 Threats

The threats are directed against the assets and/or the security functions of the TOE. For example, certain attacks are only one step towards a disclosure of assets while others may directly lead to a compromise of the application security. The more detailed description of specific attacks is given later on in the process of evaluation and certification. An overview on attacks is given in PP [11] section 3.2.

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

*Table 5: Threats according PP [11]*

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

#### 4.1.1 Additional Threat due to TOE specific Functionality

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

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

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

**T.Mem-Access**                      Memory Access Violation

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

Table 6: Additional threats due to TOE specific functions and augmentations

T.Mem-Access	Memory Access Violation
--------------	-------------------------

For details see PP [11] section 3.2.

#### 4.1.2 Assets regarding the Threats

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

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

- SC1 Integrity of User Data and of the Security IC Embedded Software (while being executed/processed and while being stored in the TOE’s memories),
- SC2 Confidentiality of User Data and of the Security IC Embedded Software (while being processed and while being stored in the TOE’s memories)
- SC3 Correct operation of the security services provided by the TOE for the Security IC Embedded Software.
- SC4 Continuous availability of random numbers

SC4 is an additional security service provided by this TOE which is the availability of random numbers. These random numbers are generated either by a physical true random number (PTRNG) or a deterministic random number generator (DRNG) 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 [11].

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

- logical design data, physical design data, IC Dedicated Software, and configuration data
- Initialization Data and Pre-personalization Data, specific development aids, test and characterization related data, material for software development support, and 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, Initialisation 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 [11] section 3.1.

## 4.2 Organizational Security Policies

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

P.Process-TOE Protection during TOE Development and Production

An accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries this unique identification.

The organizational security policies are defined and described in PP [11] section 3.3. Due to the augmentations of PP [11] an additional policy is introduced and described in the next chapter.

*Table 7: Organizational Security Policies according PP [11]*

P.Process-TOE	Protection during TOE Development and Production
---------------	--

### 4.2.1 Augmented Organizational Security Policy

Due to the augmentations of the PP [11] an additional policy is introduced.

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

The IC Developer / Manufacturer must apply the policy “Additional Specific Security Functionality (P.Add-Functions)” as specified below.

**P.Add-Functions****Additional Specific Security Functionality**

The TOE shall provide the following specific security functionality to the Smartcard Embedded Software:

- Advanced Encryption Standard (AES)
- Triple Data Encryption Standard (3DES)
- Rivest-Shamir-Adleman Cryptography (RSA),
- Elliptic Curve Cryptography (EC)
- Secure Hash Algorithm SHA-2 (optional SW library)
- Secure Hash Algorithm by Hardware (optional HW Hash)

**Note 2:**

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

End of note.

**Note 3:**

This TOE can come with both crypto co-processors accessible, or with a blocked SCP or with a blocked Crypto2304T, or with both crypto co-processors blocked. The blocking depends on the customer demands prior to the production of the hardware. In case the SCP is blocked, no AES and DES computation supported by hardware is possible. In case the Crypto2304T is blocked, no RSA and EC computation supported by hardware is possible. The use of the SHA-2 library is also possible with both crypto coprocessors blocked. No accessibility of the deselected cryptographic co-processors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic co-processors.

End of note.

**Note 4:**

The TOE can come with the Secure Hash Algorithm by Hardware (optional HW Hash) being available or not. If the Hash module is blocked the hardware implemented Hash Algorithms are not available. The use of the Hash module is independent from the optional SHA-2 library software and also independent of the availability of the cryptographic coprocessors. No accessibility of the Hash module 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 Hash module.

End of note.

### 4.3 Assumptions

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

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

**A.Process-Sec-IC**            Protection during Packaging, Finishing and Personalization

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

**A.Plat-Appl**                Usage of Hardware Platform

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

**A.Resp-Appl**                Treatment of User Data

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

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

*Table 8: Assumption according PP [11]*

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

### 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 see PP [11] section 3.4.

## 5 Security objectives (ASE\_OBJ)

This section shows the subjects and objects where are relevant to the TOE.

A short overview is given in the following.

The user has the following standard high-level security goals related to the assets:

- SG1 maintain the integrity of User Data and of the Security IC Embedded Software
- SG2 maintain the confidentiality of User Data and of the Security IC Embedded Software
- SG3 maintain the correct operation of the security services provided by the TOE for the Security IC Embedded Software
- SG4 provision of random numbers.

### 5.1 Security objectives for the TOE

The security objectives of the TOE are defined and described in PP [11] section 4.1.

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

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

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

**O.Add-Functions      Additional Specific Security Functionality**

The TOE must provide the following specific security functionality to the Smartcard Embedded Software:

- Advanced Encryption Standard (AES)
- Triple Data Encryption Standard (3DES),
- Rivest-Shamir-Adleman (RSA)
- Elliptic Curve Cryptography (EC)
- Secure Hash Algorithm (SHA-2)
- Secure Hash Algorithm by Hardware (optional HW Hash)

**Note 5:**

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

End of note.

**Note 6:**

This TOE can come with both crypto co-processors accessible, or with a blocked SCP or with a blocked Crypto2304T, or with both crypto co-processors blocked. The blocking depends on the customer demands prior to the production of the hardware. In case the SCP is blocked, no AES and DES computation supported by hardware is possible. In case the Crypto2304T is blocked, no RSA and EC computation supported by hardware is possible. The use of the SHA-2 library is also possible with both crypto coprocessors blocked. No accessibility of the deselected cryptographic co-processors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic co-processors.

End of note.

**Note 7:**

The TOE can come with the Secure Hash Algorithm by Hardware (optional HW Hash) being available or not. If the Hash module is blocked the hardware implemented Hash Algorithms are not available. The use of the Hash module is independent from the optional SHA-2 library software and also independent of the availability of the cryptographic coprocessors. No accessibility of the Hash module 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 Hash module.

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.

*Table 10: Additional objectives due to TOE specific functions and augmentations*

O.Add-Functions	Additional specific security functionality
O.Mem-Access	Area based Memory Access Control

**5.2 Security Objectives for the development and operational Environment**

The security objectives for the security IC embedded software development environment and the operational environment is defined in PP [11] section 4.2 and 4.3. The table below lists the security objectives.

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

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

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

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

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

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

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

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

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

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

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

## 5.3 Security Objectives Rationale

The security objectives rationale of the TOE are defined and described in PP [11] section 4.4. For organizational security policy P.Add-Functions, OE.Plat-Appl and OE.Resp-Appl the rationale is given in the following description.

Table 12: Security Objective Rationale

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

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

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

Compared to PP [11] clarification has been made for the security objective “Usage of Hardware Platform (OE.Plat-Appl)”: If required the Smartcard Embedded Software shall use these cryptographic services of the TOE and their interface as specified. In addition, the Smartcard Embedded Software must implement functions which perform operations on keys (if any) in such a manner that they do not disclose information about confidential data. The non-disclosure due to leakage A.Key-Function attacks is included in this objective OE.Plat-Appl. This addition ensures that the assumption A.Plat-Appl is still covered by the objective OE.Plat-Appl although additional functions are being supported according to O.Add-Functions.

Compared to the PP [11] a clarification has been made for the security objective “Treatment of User Data (OE.Resp-Appl)”: By definition cipher or plain text data and cryptographic keys are User Data. So, the Smartcard Embedded Software will protect such data if required and use keys and functions appropriately in order to ensure the strength of cryptographic operation. Quality and confidentiality must be maintained for keys that are imported and/or derived from other keys. This implies that appropriate key management has to be realized in the environment. That is expressed by the assumption A.Key—Function which is covered from OE.Resp—Appl. These measures make sure that the assumption A.Resp-Appl is still covered by the security objective OE.Resp-Appl although additional functions are being supported according to P.Add-Functions.

Compared to the PP [11] an enhancement regarding memory area protection has been established. The clear definition of privilege levels for operated software establishes the clear separation of different restricted memory areas for running the firmware, downloading and/or running the operating system and to establish a clear separation between different applications. Nevertheless, it is also possible to define a shared memory section where separated applications may exchange defined data. The privilege levels clearly define by using a hierarchical model the access right from one level to the other. These measures ensure that the threat T.Mem-Access is clearly covered by the security objective O.Mem-Access.

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

## 6 Extended Component Definition (ASE\_ECD)

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

- the family **FCS\_RNG** at the class FCS Cryptographic Support
- the family **FMT\_LIM** at the class FMT Security Management
- the family **FAU\_SAS** at the class FAU Security Audit
- the component **FPT\_TST.2** at the class FPT Protection of the TSF

The extended components FMT\_LIM and FAU\_SAS are defined and described in PP [11] section 5. The components FPT\_TST.2 and FCS\_RNG are defined in the following.

### 6.1 Component “Subset TOE security testing (FPT\_TST)”

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

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

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

### 6.2 Definition of FPT\_TST.2

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

This security functional component is used instead of the functional component FPT\_TST.1 from Common Criteria Part 2. For the user it is important to know which security functions or mechanisms can be tested. The functional component FPT\_TST.1 does not mandate to explicitly specify the security functions being tested. In addition, FPT\_TST.1 requires verifying the integrity of TSF data and stored TSF executable code which might violate the security policy. The functional component “Subset TOE testing (FPT\_TST.2)” is specified as given in the following chapter (Common Criteria Part 2 extended).

### 6.3 TSF self-test (FPT\_TST)

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

Component leveling



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

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

Management: FPT\_TST.2

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

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

Audit: FPT\_TST.2

There are no auditable events foreseen.

**FPT\_TST.2** Subset TOE testing

Hierarchical to: No other components.

Dependencies: No dependencies to other components.

**FPT\_TST.2.1** The TSF shall run a suite of self-tests [*selection: during initial start-up, periodically during normal operation, at the request of the authorized user, and/or at the conditions* [*assignment: conditions under which self-test should occur*] to demonstrate the correct operation of [*assignment: functions and/or mechanisms*].

## 6.4 Family “Generation of Random Numbers (FCS\_RNG)”

The family “Generation of Random Numbers (FCS\_RNG.1)” has to be newly created according the new version of the “Anwendungshinweise und Interpretationen zum Schema (AIS)” respectively “Functionality classes and evaluation methodology for physical random number generators”, AIS31, [15]. This security functional component is used instead of the functional component FCS\_RNG.1 defined in the protection profile [11].

The family “Generation of Random Numbers (FCS\_RNG.1)” is specified as follows (Common Criteria Part 2 extended.).

## 6.5 Definition of FCS\_RNG.1

This section describes the functional requirements for the generation of random numbers, which may be used as secrets for cryptographic purposes or authentication. The IT security functional requirements for the TOE are defined in an additional family (FCS\_RNG) of the Class FCS (Cryptographic support).

### FCS\_RNG Generation of random numbers

#### Family Behavior

This family defines quality requirements for the generation of random numbers that are intended to be used for cryptographic purposes.

#### Component leveling:



**FCS\_RNG.1:** Generation of random numbers requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.

Management FCS\_RNG.1

**FCS\_RNG.1:** There are no management activities foreseen.

Audit **FCS\_RNG.1:** FCS\_RNG.1

There are no actions defined to be auditable.

**FCS\_RNG.1** Random number generation

Hierarchical to: No other components.

Dependencies: No dependencies.

**FCS\_RNG.1.1:** The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].

**FCS\_RNG.1.2:** The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].

Note 8: The functional requirement FCS\_RNG.1 is a refinement of the FCS\_RNG.1 defined in the Protection Profile [11] according to “Anwendungshinweise und Interpretationen zum Schema (AIS)” respectively “Functionality classes and evaluation methodology for physical random number generators”, AIS31 [15].

## 7 Security Requirements (ASE\_REQ)

For this section the PP [11] 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 [11] section 6.1 and in the following description.

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

*Table 13: Security functional requirements defined in PP [11]*

Security Functional Requirement		Refined in PP [11]
FRU_FLT.2	“Limited fault tolerance“	Yes
FPT_FLS.1	“Failure with preservation of secure state“	Yes
FMT_LIM.1	“Limited capabilities“	No
FMT_LIM.2	“Limited availability“	No
FAU_SAS.1	“Audit storage“	No
FPT_PHP.3	“Resistance to physical attack“	Yes
FDP_ITT.1	“Basic internal transfer protection“	Yes
FPT_ITT.1	“Basic internal TSF data transfer protection“	Yes
FDP_IFC.1	“Subset information flow control“	No

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

Table 14: Augmented security functional requirements

Security Functional Requirement	
FPT_TST.2	“Subset TOE security testing“
FDP_ACC.1	“Subset access control“
FDP_ACF.1	“Security attribute based access control“
FMT_MSA.1	“Management of security attributes“
FMT_MSA.3	“Static attribute initialisation“
FMT_SMF.1	“Specification of Management functions“
FCS_COP.1	“Cryptographic support“
FCS_CKM.1	“Cryptographic key management“
FDP_SDI.1	“Stored data integrity monitoring“
FDP_SDI.2	“Stored data integrity monitoring and action“
FCS_RNG.1	“Quality metric for random numbers“

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

The above marked extended components FMT\_LIM.1 and FMT\_LIM.2 are introduced in PP [11] to define the IT security functional requirements of the TOE as an additional family (FMT\_LIM) of the Class FMT (Security Management). This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF.

The additional component FAU.SAS is introduced to define the security functional requirements of the TOE of the Class FAU (Security Audit). This family describes the functional requirements for the storage of audit data and is described in the next chapter.

The requirement FPT\_TST.2 is the subset of TOE testing and originated in [13]. This requirement is given as the correct operation of the security functions is essential. The TOE provides mechanisms to cover this requirement by the smartcard embedded software and/or by the TOE itself.

## 7.1.1 Extended Components FCS\_RNG.1 and FAU\_SAS.1

### 7.1.1.1 FCS\_RNG

To define the IT security functional requirements of the TOE an additional family (FCS\_RNG) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes.

**FCS\_RNG.1** Random Number Generation

Hierarchical to: No other components

Dependencies: No dependencies

**FCS\_RNG.1** Random numbers generation Class PTG.2 according to [15]

**FCS\_RNG.1.1** The TSF shall provide a *physical* random number generator that implements:

*PTG.2.1 A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.*

*PTG.2.2 If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.*

*PTG.2.3 The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.*

*PTG.2.4 The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.*

*PTG.2.5 The online test procedure checks the quality of the raw random number sequence. It is triggered continuously. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.*

**FCS\_RNG.1.2** The TSF shall provide *numbers in the format 8- or 16-bit* that meet

*PTG.2.6 Test procedure A, as defined in [15] does not distinguish the internal random numbers from output sequences of an ideal RNG.*

*PTG.2.7 The average Shannon entropy per internal random bit exceeds 0.997.*

Note 9: The functional requirement FCS\_RNG.1 is a refinement of the FCS\_RNG.1 defined in the Protection Profile [11] according to “Anwendungshinweise und Interpretationen zum Schema (AIS)” respectively “A proposal for: Functionality classes for random number generators” [15].

Note 10: The physical random number generator implements total failure test of the random source and a continuous RNG test according to:  
National Institute of Standards and Technology, Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication (FIPS) 140-2, 2002-03-12, chapter 4.9.2.

### 7.1.1.2 FAU\_SAS

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

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

**FAU\_SAS.1** Audit Storage

Hierarchical to: No dependencies

Dependencies: No dependencies.

**FAU\_SAS.1.1** The TSF shall provide the test process *before TOE Delivery* with the capability to store *the Initialization Data and/or Pre-personalization Data and/or supplements of the Security IC Embedded Software* in the *not changeable configuration page area and non-volatile memory*.

### 7.1.2 Subset of TOE testing

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

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

**FPT\_TST.2**                      Subset TOE testing

Hierarchical to:                No other components.

Dependencies:                 No dependencies to other components.

**FPT\_TST.2.1**                 The TSF shall run a suite of self tests *at the request of the authorized user* to demonstrate the correct operation of the *alarm lines and/or following environmental sensor mechanisms*:

- *The information is given in the confidential Security Target [10].*

### 7.1.3 Memory access control

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

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

The security functional requirement “**Static attribute initialisation (FMT\_MSA.3)**” ensures that the default values of security attributes are appropriately either permissive or restrictive in nature. Alternative values can be specified by any subject provided that the **Memory Access Control Policy** allows that. This is described by the security functional requirement “**Management of security attributes (FMT\_MSA.1)**”. The attributes are determined during TOE manufacturing (FMT\_MSA.3) or set at run-time (FMT\_MSA.1).

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

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

#### **Memory Access Control Policy**

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

The memory model provides distinct, independent privilege levels separated from each other in the virtual address space. The access rights to these levels are controlled by the MMU. Further details are given in the confidential Security Target [10]

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

**FDP\_ACC.1**                    Subset access control

Hierarchical to:    No other components.

Dependencies:    FDP\_ACF.1 Security attribute based access control

**FDP\_ACC.1.1**                The TSF shall enforce the *Memory Access Control Policy on all subjects (software running at the defined and assigned privilege levels), all objects (data including code stored in memories) and all the operations defined in the Memory Access Control Policy, i.e. privilege levels.*

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

**FDP\_ACF.1**                    Security attribute based access control

Hierarchical to:    No other components.

Dependencies:    FDP\_ACC.1 Subset access control  
                          FMT\_MSA.3 Static attribute initialisation

**FDP\_ACF.1.1**                The TSF shall enforce the Memory Access Control Policy to objects based on the following:

Subject:

- software running at the IFX, OS1 and OS2 privilege levels required to securely operate the chip. This includes also privilege levels running interrupt routines.
- software running at the privilege levels containing the application software

Object:

- data including code stored in memories

Attributes:

- the memory area where the access is performed to and/or the operation to be performed.

**FDP\_ACF.1.2** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:  
*evaluate the corresponding permission control information of the relevant memory range before, during or after the access so that accesses to be denied cannot be utilized by the subject attempting to perform the operation.*

**FDP\_ACF.1.3** The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none*.

**FDP\_ACF.1.4** The TSF shall explicitly deny access of subjects to objects based on the *following additional rules: none*.

The TOE shall meet the requirement “Static attribute initialisation (FMT\_MSA.3)” as specified below.

**FMT\_MSA.3** Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT\_MSA.1 Management of security attributes  
FMT\_SMR.1 Security roles

**FMT\_MSA.3.1** The TSF shall enforce the *Memory Access Control Policy* to provide *well defined*<sup>7</sup> default values for security attributes that are used to enforce the SFP.

<sup>7</sup> The static definition of the access rules is documented in the hardware reference manual as listed in Table 1: Identification

**FMT\_MSA.3.2** The TSF shall allow *any subject, provided that the Memory Access Control Policy is enforced and the necessary access is therefore allowed*<sup>8</sup>, to specify alternative initial values to override the default values when an object or information is created.

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

**FMT\_MSA.1** Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP\_ACC.1 Subset access control or  
FDP\_IFC.1 Subset information flow control]  
FMT\_SMF.1 Specification of management functions  
FMT\_SMR.1 Security roles

**FMT\_MSA.1.1** The TSF shall enforce the *Memory Access Control Policy* to restrict the ability to *change default, modify or delete* the security attributes *permission control information to the software running on the privilege levels*.

The TOE shall meet the requirement “Specification of management functions (FMT\_SMF.1)” as specified below:

**FMT\_SMF.1** Specification of management functions

Hierarchical to: No other components

Dependencies: No dependencies

**FMT\_SMF.1.1** The TSF shall be capable of performing the following security management functions: *access the configuration registers of the MMU*.

---

<sup>8</sup> The Smartcard Embedded Software is intended to set the memory access control policy

### 7.1.4 Support of Cipher Schemes

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

FCS\_COP.1 Cryptographic operation requires a cryptographic operation to be performed in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard; dependencies are discussed in 7.3.1.1.

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

- Advanced Encryption Standard (AES)
- Triple Data Encryption Standard (3DES)
- Elliptic Curve Cryptography (EC)
- Rivest-Shamir-Adleman (RSA)<sup>9</sup>
- Secure Hash Algorithm by software (SHA-2)
- Secure Hash Algorithm by hardware (Hash)

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

#### 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 [24] 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](http://www.bsi.bund.de). Any cryptographic functionality that is marked in the column “Security level above 100 Bits” of the following table with a “no” achieves a security level of lower than 100 Bits (in general context).

---

<sup>9</sup> For the case the TOE comes without RSA and/or EC library, the TOE provides basic HW-related routines for RSA and/or EC calculations. For a secure library implementation the user has to implement additional countermeasures himself.

Table 15: Cryptographic TOE functionality

Cryptographic Function	Implemented Standard	Key Size in Bits	Security Level above 100 Bits
<b>Key Agreement</b>			
ECDH	[23]	Key sizes corresponding to the used elliptic curves P-192, K-163 [17] and brainpoolP{160, 192}r1, brainpoolP{160, 192}t1 [18]	No
ECDH	[23]	Key sizes corresponding to the used elliptic curves P-{224, 256, 384, 521}, K-{233, 409}, B-{233, 283, 409} [17], brainpoolP{224,256,320,384,512}r1, brainpoolP{224,256,320,384,512}t1 [18]	Yes
<b>Cryptographic Primitive</b>			
Triple DES	[19]	k  = 112 in operating modes ECB, CBC, BLD CBC-MAC, CBC-MAC-ELB	No
	Proprietary	k  = 112 Recrypt Mode	No
Triple DES	[19]	k  = 168 in operating modes: CBC, BLD, CBC-MAC, CBC-MAC-ELB	Yes
	[19]	k  = 168 in operating mode ECB	No
	Proprietary	k  = 168 Recrypt Mode	Yes
AES	[20]	k  = 128, 192, 256	Yes
RSA encryption / decryption / signature generation / verification (only modular exponentiation part)	[21]	Modulus length = 1976 - 4096	Yes
ECDSA signature generation / verification	[22]	Key sizes corresponding to the used elliptic curves P-192, K-163 [17] and brainpoolP{160, 192}r1, brainpoolP{160, 192}t1 [18]	No
ECDSA signature generation / verification	[22]	Key sizes corresponding to the used elliptic curves P-{224, 256, 384, 521}, K-{233, 409}, B-{233, 283, 409} [17], brainpoolP{224,256,320,384,512}r1,	Yes

Cryptographic Function	Implemented Standard	Key Size in Bits	Security Level above 100 Bits
		brainpoolP{224,256,320,384,512}t1 [18]	
Physical True RNG PTG.2	[15]	N/A	N/A
SHA 256 and SHA 512	[25]	None	Yes
SHA 256	[25]	None	Yes

#### 7.1.4.2 Triple-DES Operation

The DES Operation of the TOE shall meet the requirement “Cryptographic operation (FCS\_COP.1)” as specified below.

**FCS\_COP.1/DES** 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/DES** The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm TDES in the *Electronic Codebook Mode (ECB)*, in the *Cipher Block Chaining Mode (CBC)*, in the *Blinding Feedback Mode (BLD)*, in the *Cipher Block Chaining Mode (CBC-MAC)*, in the *CBC-MAC- encrypt-last-block (CBC-MAC-ELB)* and in the *Recrypt Mode* and cryptographic key sizes of *112 bit and 168 bit* that meet the following standards:

- *ECB, CBC, BLD:*  
*National Institute of Standards and Technology (NIST) SP 800-67 Rev. 1 [26]*
- *ECB, CBC, BLD:*  
*National Institute of Standards and Technology (NIST) SP 800-38A [27]*
- *CBC-MAC, CBC-MAC-ELB:*  
*ISO/IEC 9797-1 Mac Algorithm 1 [28]*
- *Recrypt Mode*  
*Proprietary, description given in the hardware reference manual HRM [1]*

Note 11:

The TOE implements the following alternative block cipher modes for the user: the Electronic Codebook Mode (ECB), the Cipher Block Chaining Mode (CBC), the Blinding Feedback Mode (BLD) and the Cipher Feedback Mode (CFB)<sup>10</sup> The BLD is described in the hardware reference manual HRM [1] while the implementations of ECB, CBC and CFB follow the standard:

National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Data Encryption Standard (DES), NIST Special Publication 800-38A, 2001 Edition.

This TOE can come with both crypto co-processors accessible, or with a blocked SCP or with a blocked Crypto2304T, or with both crypto co-processors blocked. The blocking depends on the customer demands prior to the production of the hardware. In case the SCP is blocked, no AES and DES computation supported by hardware is possible. In case the Crypto2304T is blocked, no RSA and EC computation supported by hardware is possible. In case of a blocked Crypto2304T the optionally delivered cryptographic and the supporting Toolbox and Base Library cannot be used in that TOE product. The use of the SHA-2 library is also possible with both crypto coprocessors blocked. No accessibility of the deselected cryptographic co-processors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic co-processors.

End of note.

#### 7.1.4.3 AES Operation

The AES Operation of the TOE shall meet the requirement “Cryptographic operation (FCS\_COP.1)” 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 *encryption and decryption* in accordance with a specified cryptographic algorithm *Advanced Encryption Standard (AES)* and cryptographic key sizes of *128 bit or 192 bit or 256 bit* that meet the following standards:

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

<sup>10</sup> The CFB is also called Recrypt Mode.

Note 12:

This TOE can come with both crypto co-processors accessible, or with a blocked SCP or with a blocked Crypto2304T, or with both crypto co-processors blocked. The blocking depends on the customer demands prior to the production of the hardware. In case the SCP is blocked, no AES and DES computation supported by hardware is possible. In case the Crypto2304T is blocked, no RSA and EC computation supported by hardware is possible. In case of a blocked Crypto2304T the optionally delivered cryptographic and the supporting Toolbox and Base Library cannot be used in that TOE product. The use of the SHA-2 library is also possible with both crypto coprocessors blocked. No accessibility of the deselected cryptographic co-processors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic co-processors. Please consider also the statement of chapter 7.1.4.1.

End of note.

#### 7.1.4.4 Rivest-Shamir-Adleman (RSA) operation

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

**FCS\_COP.1/RSA** Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP\_ITC.1 Import of user data without security attributes, or FDP\_ITC.2 Import of user data with security attributes, or FCS\_CKM.1 Cryptographic key generation] FCS\_CKM.4 Cryptographic key destruction

**FCS\_COP.1.1/RSA** The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *Rivest-Shamir-Adleman (RSA)* and cryptographic key sizes 1976 - 4096 bits that meet the following *standards*

*Encryption:*

*According to section 5.1.1 RSAEP in PKCS v2.1 RFC3447, without 5.1.1.1.*

*Decryption (with or without CRT):*

*According to section 5.1.2 RSADP in PKCS v2.1 RFC3447*

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

*therefore without 5.1.2.2.b (ii)&(v), without 5.1.2.1.*

*5.1.2.2.a, only supported up to  $n < 2^{2048}$*

*Signature Generation (with or without CRT)::*

*According to section 5.2.1 RSASP1 in PKCS v2.1 RFC3447  
for  $u = 2$ , i.e., without any  $(r_i, d_i, t_i)$ ,  $i > 2$ ,  
therefore without 5.2.1.2.b (ii)&(v), without 5.2.1.1.  
5.2.1.2.a, only supported up to  $n < 2^{2048}$*

*Signature Verification:*

*According to section 5.2.2 RSAVP1 in PKCS v2.1 RFC3447,  
without 5.2.2.1.*

Please consider also the statement of chapter 7.1.4.1.

#### 7.1.4.5 Rivest-Shamir-Adleman (RSA) key generation

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

**FCS\_CKM.1/RSA** Cryptographic key generation

Hierarchical to: No other components.

Dependencies: FCS\_CKM.2 Cryptographic key distribution, or  
FCS\_COP.1 Cryptographic operation]  
FCS\_CKM.4 Cryptographic key destruction  
FMT\_MSA.2 Secure security attributes

**FCS\_CKM.1.1/RSA** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *rsagen1* (PKCS v2.1 RFC3447) and specified cryptographic key sizes of 1976 – 4096 bits that meet the following standard:

*According to section 3.2(2) in PKCS v2.1 RFC3447,  
for  $u=2$ , i.e., without any  $(r_i, d_i, t_i)$ ,  $i > 2$ .  
For  $p \times q < 2^{2048}$  additionally according to section 3.2(1).*

Note 13:

For easy integration of RSA functions into the user’s operating system and/or application, the library contains single cryptographic functions respectively primitives which are compliant to the standard. The primitives are referenced above. Therefore, the library supports the user to develop an application representing the standard if required. Please consider also the statement of chapter 7.1.4.1.

End of note.

Note 14:

The TOE can be delivered with or without the RSA library. If the TOE comes with, automatically the Base Library is part

of the shipment. In the case of coming without the RSA library the TOE does not provide the Additional Specific Security Functionality Rivest-Shamir-Adleman Cryptography (RSA) realized with the security functional requirements FCS\_COP.1/RSA and FCS\_CKM.1/RSA. In case of a blocked Crypto2304T the optionally delivered cryptographic and the supporting Toolbox and Base Library cannot be used in that TOE product.

End of note.

#### 7.1.4.6 General Preface regarding Elliptic Curve Cryptography

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

#### 7.1.4.7 Elliptic Curve DSA (ECDSA) operation

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

**FCS\_COP.1/ECDSA** 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** 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*:

*Signature Generation:*

*1. According to section 7.3 in ANSI X9.62 - 2005*

*Not implemented is step d) and e) thereof.*

*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 6.2 (6.2.2. + 6.2.3) in ISO/IEC 15946-2:2002

*Not implemented is section 6.2.1:*

*The output of 5.4.2 has to be provided by the caller as input to the function.*

*Signature Verification:*

1. According to section 7.4.1 in ANSI X9.62–2005

*Not implemented is step b) and c) thereof.*

*The output of step c) has to be provided as input to our function by the caller.*

*Deviation of step d):*

*Beside noted calculation, our algorithm adds a random multiple of BasepointerOrder  $n$  to the calculated values  $u1$  and  $u2$ .*

2. According to sections 6.4 (6.4.1. + 6.4.3 + 6.4.4) in ISO/IEC 15946-2:2002

*Not implemented is section 6.4.2:*

*The output of 5.4.2 has to be provided by the caller as input to the function.*

Note 15:

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

End of note.

#### 7.1.4.8 Elliptic Curve (EC) key generation

The key generation for the EC shall meet the requirement “Cryptographic key generation (FCS\_CKM.1)”

**FCS\_CKM.1/EC** Cryptographic key generation

Hierarchical to: No other components.

Dependencies: FCS\_CKM.2 Cryptographic key distribution, or FCS\_COP.1 Cryptographic operation]  
FCS\_CKM.4 Cryptographic key destruction

**FCS\_CKM.1.1/EC** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Elliptic Curve EC specified in ANSI X9.62-2005 and ISO/IEC 15946-1:2002* and specified cryptographic key sizes *160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or*

521 bits that meet the following *standard*:

ECDSA Key Generation:

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

Note 16:

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

End of note.

#### 7.1.4.9 Elliptic Curve Diffie-Hellman (ECDH) key agreement

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

**FCS\_COP.1/ECDH** Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP\_ITC.1 Import of user data without security attributes, or FDP\_ITC.2 Import of user data with security attributes, or FCS\_CKM.1 Cryptographic key generation] FCS\_CKM.4 Cryptographic key destruction

**FCS\_COP.1.1/ECDH** The TSF shall perform *elliptic curve Diffie-Hellman key agreement* in accordance with a specified cryptographic algorithm *ECDH* and cryptographic key sizes 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits that meet the following *standard*:

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

Note 17:

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 18:

The TOE can be delivered with or without the EC library. If the TOE comes with, automatically the Base Library is part of the shipment. In the case the TOE comes without, it does not provide the Additional Specific Security Functionality Elliptic Curve Cryptography realized with the security functional requirements FCS\_COP.1/ECSA, FCS\_COP.1/ECDH and FCS\_CKM.1/EC. In case of a blocked Crypto2304T, the RSA and EC cryptographic library cannot be used. In case of a blocked Crypto2304T the optionally delivered cryptographic RSA and EC, as well as the supporting Toolbox and Base Library cannot be used in that TOE product.

End of note.

Note 19:

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 SHA-2 Operation with Cryptographic Software Library

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

##### **FCS\_COP.1/SHA-SW 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/SHA-SW** The TSF shall perform *hash-value calculation of user chosen data* in accordance with a specified cryptographic algorithm *SHA-2* and with cryptographic key sizes of *none* that meet the following *standards*:

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

In case of a blocked Crypto2304T, the cryptographic libraries RSA, EC and Toolbox are not delivered, but the SHA library still can be part of the TOE.

Note 20:

The TOE can be delivered without the SHA-2 library. In this case the TOE does not provide the Additional Specific Security Functionality SHA-2 library, realized with the security functional requirements FCS\_COP.1/SHA.

End of note.

Note 21:

The secure hash-algorithm SHA-2 is intended to be used for signature generation, verification and generic data integrity checks. Further essential information is given in the confidential user guidance.

#### 7.1.4.11 Hash Operation with Hardware Module

The Hash operation of the TOE shall meet the requirement “Cryptographic operation (FCS\_COP.1)” as specified below.

#### **FCS\_COP.1/**                    **Cryptographic operation** **SHA-2-HW**

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

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

Note that the hash cryptographic operation is a keyless operation.

Note 22:

This Hash module is intended to be used for signature generation, verification and generic data integrity checks. Following the BSI recommendations the algorithms MD-5 and SHA-1 are not covered by this evaluation. Further essential information about the usage is given in the confidential user guidance.

End of note.

### 7.1.5 Data Integrity

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

**FDP\_SDI.1**                    Stored data integrity monitoring

Hierarchical to: No other components

Dependencies: No dependencies

**FDP\_SDI.1.1**                The TSF shall monitor user data stored in containers controlled by the TSF for *inconsistencies between stored data and corresponding EDC* on all objects, based on the following attributes: *EDC values for certain memories.*

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

**FDP\_SDI.2**                    Stored data integrity monitoring and action

Hierarchical to: FDP\_SDI.1 stored data integrity monitoring

Dependencies: No dependencies

**FDP\_SDI.2.1**                The TSF shall monitor user data stored in containers controlled by the TSF for *data integrity and one- and/or more-bit-errors* on all objects, based on the following attributes: *corresponding EDC value for the memories and error correction for the SOLID FLASH™ NVM.*

**FDP\_SDI.2.2**                Upon detection of a data integrity error, the TSF shall correct 1 bit errors in the SOLID FLASH™ NVM automatically and inform the user about more bit errors.

## 7.2 TOE Security Assurance Requirements

The evaluation assurance level is EAL6 augmented with ALC\_FLR.1.

In the following table, the security assurance requirements are given. The augmentation of the assurance components compared to the Protection Profile [11] is expressed with bold letters.

Table 16: Assurance components

Aspect	Acronym	Description	Refinement
Development	ADV_ARC.1	Security Architecture Description	In PP [11]
	ADV_FSP.5	<b>Complete semi-formal functional specification with additional error information</b>	in ST
	ADV_IMP.2	<b>Complete mapping of the implementation representation of the TSF</b>	In ST
	ADV_INT.3	<b>Minimally complex internals</b>	
	ADV_TDS.5	<b>Complete semi-formal modular design</b>	
	ADV_SPM.1	<b>Formal TOE security policy model</b>	
Guidance Documents	AGD_OPE.1	Operational user guidance	in PP [11]
	AGD_PRE.1	Preparative procedures	in PP [11]
Life-Cycle Support	ALC_CMC.5	<b>Advanced support</b>	in ST
	ALC_CMS.5	<b>Development tools CM coverage</b>	in ST
	ALC_DEL.1	Delivery procedures	in PP [11]
	ALC_DVS.2	Sufficiency of security measures	in PP [11]
	ALC_LCD.1	Developer defined life-cycle model	
	ALC_TAT.3	<b>Compliance with implementation standards – all parts</b>	
	ALC_FLR.1	<b>Basic Flaw Remediation</b>	
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	<b>Rigorous analysis of coverage</b>	in ST
	ATE_DPT.3	<b>Testing: modular design</b>	
	ATE_FUN.2	<b>Ordered functional testing</b>	
	ATE_IND.2	Independent testing - sample	
Vulnerability Assessment	AVA_VAN.5	Advanced methodical vulnerability analysis	in PP [11]

## 7.2.1 Refinements

Some refinements are taken unchanged from the PP [11]. In some cases a clarification is necessary. In the table above an overview is given where the refinement is done.

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

### 7.2.1.1 Development (ADV)

#### **ADV\_IMP Implementation Representation:**

The refined assurance 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\_INT TSF Internals:**

The assurance package ADV\_INT.2 well-structured internals is extended to ADV\_INT.3 minimally complex internals requiring the documentation to minimally complex internals with the intension that the entire TSF has been designed and implemented using sound engineering principles. The ADV\_INT.2 aspect remains applicable as well structured internals are fundamental for achieving sound engineering principles. ADV\_INT.2 and its refinements in the PP [1] remain therefore valid. The assurance and evidence was provided accordingly.

#### **ADV\_FSP Functional Specification:**

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

These aspects from ADV\_FSP.5 are independent from the ADV\_FSP.4 refinements from the PP [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.

**ADV\_SPM Formal Security Policy Model:**

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

**ADV\_SPM.1** Formal TOE security policy model

Hierarchical to: No other components

Dependencies: ADV\_FSP.4 Complete function description

**ADV\_SPM.1.1D** The developer shall provide a formal security policy model for the

*Memory Access Control Policy and the corresponding SFRs*

- *FDP\_ACC.1 Subset Access Control*
- *FDP\_ACF.1 Security attribute based access control*
- *FMT\_MSA.1 Management of Security Attributes*
- *FMT\_MSA.3 Static Attribute initialisation.*

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

- *FDP\_SDI.1 Stored data integrity monitoring*
- *FDP\_SDI.2 Stored data integrity monitoring and action*
- *FDP\_ITT.1 Basic Internal Transfer Protection*
- *FDP\_IFC.1 Information Flow Control*
- *FPT\_ITT.1 Basic internal TSF data transfer protection*
- *FPT\_PHP.3 Resistance to physical attack*
- *FPT\_FLS.1 Failure with preservation of secure state*
- *FRU\_FLT.2 Limited fault tolerance*
- *FMT\_LIM.1 Limited capabilities*
- *FMT\_LIM.2 Limited availability*
- *FAU\_SAS.1 Audit storage*

*FMT\_SMF.1 Specification of Management Functions*

**ADV\_SPM.1.2D** For each policy covered by the formal security policy model, the model shall identify the relevant portions of the statement of SFRs that make up that policy.

**ADV\_SPM.1.3D** The developer shall provide a formal proof of correspondence between the model and any formal functional specification.

**ADV\_SPM.1.4D** The developer shall provide a demonstration of correspondence between the model and the functional specification.

#### **ADV\_TDS TOE Design:**

The assurance package ADV\_TDS.4 Semiformal modular design is extended to ADV\_TDS.5 Complete semiformal modular design requires the complete semiformal design description. As the package ADV\_TDS.5 is an enhancement of ADV\_TDS.4 the package and its refinements in the PP [1] remain valid. 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 ACL\_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 automatism configuration management systems, acceptance and documentation procedures of changes, role separation with regard to functional roles of personnel, automatism for tracking and version controlling in those systems, and includes also production control systems. The additional aspects of ADV\_CMC.5 constitute an

enhancement of ACL\_CMC.4 and therefore the aspects and ACL\_CMC.4 refinements in the PP [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 [1] remain valid. The assurance and evidence was provided accordingly.

#### **ALC\_TAT Tools and Techniques:**

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

#### **7.2.1.3 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 [11].

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.

##### **ATE\_FUN Functional Tests:**

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

#### **7.2.1.4 AVA\_VAN Vulnerability Analysis:**

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

### 7.3 Security Requirements Rationale

#### 7.3.1 Rationale for the Security Functional Requirements

The security functional requirements rationale of the TOE are defined and described in PP [11] section 6.3 for the following security functional requirements: FDP\_ITT.1, FDP\_IFC.1, FPT\_ITT.1, FPT\_PHP.3, FPT\_FLS.1, FRU\_FLT.2, FMT\_LIM.1, FMT\_LIM.2, FCS\_RNG.1, and FAU\_SAS.1.

The security functional requirements FPT\_TST.2, FDP\_ACC.1, FDP\_ACF.1, FMT\_MSA.1, FMT\_MSA.3, FMT\_SMF.1, FCS\_COP.1, FCS\_CKM.1, FDP\_SDI.1 and FDP\_SDI.2 are defined in the following description:

*Table 17: Rational for additional SFR in the ST*

Objective	TOE Security Functional Requirements
O.Add-Functions	<ul style="list-style-type: none"> <li>- FCS_COP.1/DES „Cryptographic operation“</li> <li>- FCS_COP.1/AES „Cryptographic operation“</li> <li>- FCS_COP.1/SHA-SW „Cryptographic operation“</li> <li>- FCS_COP.1/SHA-2-HW “Cryptographic operation”</li> <li>- FCS_COP.1/RSA „Cryptographic operation“</li> <li>- FCS_COP.1/ECDSA „Cryptographic operation“</li> <li>- FCS_COP.1/ECDH „Cryptographic operation“</li> <li>- FCS_CKM.1/RSA „Cryptographic key generation “</li> <li>- FCS_CKM.1/EC „Cryptographic key generation“</li> </ul>
O.Phys-Manipulation	<ul style="list-style-type: none"> <li>- FPT_TST.2 „ Subset TOE security testing “</li> </ul>
O.Mem-Access	<ul style="list-style-type: none"> <li>- FDP_ACC.1 “Subset access control”</li> <li>- FDP_ACF.1 “Security attribute based access control”</li> <li>- FMT_MSA.3 “Static attribute initialisation”</li> <li>- FMT_MSA.1 “Management of security attributes”</li> <li>- FMT_SMF.1 “Specification of Management Functions”</li> </ul>
O.Malfunction	<ul style="list-style-type: none"> <li>- FDP_SDI.1 „Stored data integrity monitoring“</li> <li>- FDP_SDI.2 „Stored data integrity monitoring and action“</li> </ul>

The table above gives an overview, how the security functional requirements are combined to meet the security objectives. The detailed justification is given in the following:

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

The security functional requirement(s) “Cryptographic operation (FCS\_COP.1)” exactly requires those functions to be implemented which are demanded by O.Add-Functions. FCS\_CKM.1/RSA supports the generation of RSA keys, the FCS\_CKM.1/EC supports the generation of EC keys needed for this cryptographic operations. Therefore, FCS\_COP.1/RSA, FCS\_COP.1/ECDSA, FCS\_COP.1/ECDH and FCS\_CKM.1/RSA and FCS\_CKM/EC are suitable to meet the security objective. . The FCS\_COP.1/SHA-SW and FCS\_COP.1/SHA-HW are keyless algorithms and have no dependencies to FCS\_CKM.1.

Nevertheless, the developer of the Smartcard Embedded Software must ensure that the additional functions are used as specified and that the User Data processed by these functions are protected as defined for the application context.

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/DES (DES algorithm) and for FCS\_COP.1/AES (AES algorithm). For the FCS\_COP.1/RSA (RSA algorithm) and FCS\_COP.1/ECDSA and FCS\_COP.1/ECDH (both EC algorithms) the FCS\_CKM.1/RSA and FCS\_CKM.1/EC are optional, since they are fulfilled by the TOE or may be fulfilled by the environment as the user can generate keys externally additionally.

The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced define how to implement the specific security functionality. However, key-dependent functions could be implemented in the Smartcard Embedded Software.

The usage of cryptographic algorithms requires the use of appropriate keys. Otherwise these cryptographic functions do not provide security. The keys have to be unique with a very high probability, and must have a certain cryptographic strength etc. In case of a key import into the TOE (which is usually after TOE delivery) it has to be ensured that quality and confidentiality are maintained. Keys for DES and AES are provided by the environment. Keys for RSA and EC algorithms can be provided either by the TOE or the environment.

In this ST the objectives for the environment OE.Plat-Appl and OE.Resp-Appl have been clarified. The Smartcard Embedded Software defines the use of the cryptographic functions FCS\_COP.1 provided by the TOE. The requirements for the environment FDP\_ITC.1, FDP\_ITC.2, FCS\_CKM.1 and FCS\_CKM.4 support an appropriate key management. These security requirements are suitable to meet OE.Resp-Appl.

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

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

The tested security enforcing functions are SF\_DPM Device Phase Management, SF\_CS Cryptographic Support and SF\_PMA Protection against modifying attacks.

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

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

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

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

The justification related to the security objective "Protection against Malfunction due to Environmental Stress (O.Malfunction)" is as follows:

The security functional requirement "Stored data integrity monitoring (FDP\_SDI.1)" requires the implementation of an Error Detection (EDC) algorithm which detects integrity errors of the data stored in all memories. By this the malfunction of the TOE using corrupt data is prevented. Therefore FDP\_SDI.1 is suitable to meet the security objective.

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

The CC part 2 defines the component FIA\_SOS.2, which is similar to FCS\_RNG.1, as follows:

**FIA\_SOS.2**                    TSF Generation of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

**FIA\_SOS.2.1**                The TSF shall provide a mechanism to generate secrets that meet [assignment: *a defined quality metric*].

**FIA\_SOS.2.2**                The TSF shall be able to enforce the use of TSF generated secrets for [assignment: *list of TSF functions*].

The CC part 2, annex G.3, [13], states: “This family defines requirements for mechanisms that enforce defined quality metrics on provided secrets, and generate secrets to satisfy the defined metric“. Even the operation in the element FIA\_SOS.2.2 allows listing the TSF functions using the generated secrets. Because all applications discussed in annex G.3 are related to authentication, the component FIA\_SOS.2 is also intended for authentication purposes while the term “secret” is not limited to authentication data (cf. CC part 2, paragraphs 39-42).

Paragraph 685 in the CC part 2, [13], recommends the use of the component FCS\_CKM.1 to address random number generation. However, this may hide the nature of the secrets used for key generation and does not allow describing random number generation for other cryptographic methods (e.g., challenges, padding), authentication (e.g., password seeds), or other purposes (e.g., blinding as a countermeasure against side channel attacks).

The component FCS\_RNG addresses general RNG including the use of but no limitation to cryptographic mechanisms. FCS\_RNG allows specifying requirements for the generation of random numbers including necessary information for the intended use. These details describe the quality of the generated data where other security services rely on. Thus by using FCS\_RNG a ST or PP author is able to express a coherent set of SFRs that include or use the generation of random numbers as a security service.

#### **7.3.1.1 Dependencies of Security Functional Requirements**

The dependence of security functional requirements are defined and described in PP [11] section 6.3.2 for the following security functional requirements: FDP\_ITT.1, FDP\_IFC.1, FPT\_ITT.1, FPT\_PHP.3, FPT\_FLS.1, FRU\_FLT.2, FMT\_LIM.1, FMT\_LIM.2, FCS\_RNG.1 and FAU\_SAS.1.

The dependence of security functional requirements for the security functional requirements FDP\_ACC.1, FDP\_ACF.1, FMT\_MSA.1, FMT\_MSA.3, FMT\_SMF.1, FCS\_COP.1, FCS\_CKM.1, FDP\_SDI.1 and FDP\_SDI.2 are defined in the following description.

Table 18: Dependency for cryptographic operation requirement

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FCS_COP.1/DES	FCS_CKM.1	Yes, see comment 3
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) FCS_CKM.4	Yes, see comment 3
FCS_COP.1/AES	FCS_CKM.1	Yes, see comment 3
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) FCS_CKM.4	Yes, see comment 3
FCS_COP.1/RSA	FCS_CKM.1	Yes, see comment 3
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) FCS_CKM.4	Yes, see comment 3
FCS_CKM.1/RSA	FCS_CKM.2 or FCS_COP.1	Yes
	FCS_CKM.4	Yes, see comment 3
FCS_COP.1/ECDSA	FCS_CKM.1	Yes, see comment 3
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) FCS_CKM.4	Yes, see comment 3
FCS_CKM.1/EC	FCS_CKM.2 or FCS_COP.1	Yes
	FCS_CKM.4	Yes, see comment 3
FCS_COP.1/ECDH	FCS_CKM.1	Yes, see comment 3
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) FCS_CKM.4	Yes, see comment 3
FCS_COP.1/SHA-SW	No dependencies, see comment 4	Yes, see comment 4
FCS_COP.1/SHA-2-HW	No dependencies, see comment 4	Yes
FPT_TST.2	No dependencies, see comment 1	Yes, see comment 1
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1	Yes
	FMT_MSA.3	Yes
FMT_MSA.3	FMT_MSA.1	Yes
	FMT_SMR.1	Not required, see comment 2

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes see comment 2 Yes
FMT_SMF.1	None	N/A
FDP_SDI.1	None	N/A
FDP_SDI.2	None	N/A

**Comment 1:**

The TOE is already a platform representing the lowest level in a Smartcard. There is no lower or »underlying abstract machine« used by the TOE which can be tested. Therefore, the former dependency to FPT\_AMT.1 is fulfilled without further and by that dispensable. CC in the Revision 3 considered this and dropped this dependency. The requirement FPT\_TST.2 is satisfied.

End of comment.

**Comment 2:**

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

End of comment.

**Comment 3:**

The security functional requirement “Cryptographic operation (FCS\_COP.1)” met by the TOE, has the following 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.

The security functional requirement “Cryptographic key management (FCS\_CKM)” met by TOE, has the following dependencies:

- [FCS\_CKM.2 Cryptographic key distribution, or
- FCS\_COP.1 Cryptographic operation]
- FCS\_CKM.4 Cryptographic key destruction.

These requirements all address the appropriate management of cryptographic keys used by the specified cryptographic function and are not part of the PP [11]. Most requirements concerning key management shall be fulfilled by the environment since the Smartcard Embedded Software is designed for a specific application context and uses the cryptographic functions provided by the TOE.

For the security functional requirement FCS\_COP.1/DES and FCS\_COP.1/AES the respective dependencies FCS\_CKM.1, FCS\_CKM.4 and FDP\_ITC.1 or FDP\_ITC.2 have to be fulfilled by the environment. That mean, that the environment shall meet the requirements FCS\_CKM.1 and FCS\_CKM.4 as defined in [13], section 10.1 and shall meet the requirements FDP\_ITC.1 or FDP\_ITC.2 as defined in [13], section 11.7.

For the security functional requirement FCS\_COP.1/RSA, FCS\_COP.1/ECDSA and FCS\_COP.1/ECDH the respective dependencies FCS\_CKM.4 and FDP\_ITC.1 or FDP\_ITC.2 have to be fulfilled by the environment. That mean, that the environment shall meet the requirements FDP\_ITC.1 or FDP\_ITC.2 as defined in [13], section 11.7. The respective dependency FCS\_CKM.1 has to be fulfilled by the TOE with the security functional requirement FCS\_CKM.1/RSA (for FCS\_COP.1/RSA) and FCS\_CKM.1/EC (for FCS\_COP.1/ECDSA and FCS\_COP.1/ECDH) as defined in section 7.1.4. Additionally the requirement FCS\_CKM.1 can be fulfilled by the environment as defined in [13], section 10.1.

For the security functional requirement FCS\_CKM.1/RSA and FCS\_CKM.1/EC the respective dependency FCS\_COP.1 is fulfilled by the TOE. The environment covers the respective dependency FCS\_CKM.4. That mean, that the environment shall meet the requirement FCS\_CKM.4 as defined in [13], section 10.1.

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

In case of a blocked Crypto2304T the optionally delivered cryptographic and the supporting Toolbox and Base Library cannot be used in that TOE product. The SHA-2 library is computed in the CPUs. Therefore the IT environment has to fulfill the requirements of this chapter depending if the TOE comes with or without a/the library/ies. In case of a blocked Crypto2304T no cryptographic libraries are delivered.

End of comment.

#### **Comment 4**

The dependencies FCS\_CKM.1 and FMT\_CKM.4 are not required for the SHA-2 algorithm respectively library and for the algorithms of the hardware Hash module, because the algorithms are keyless operations. So the environment is not obligated to meet certain requirements for key management.

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 the chapter 7.2 the different assurance levels are shown as well as the augmentations. The augmentations are in compliance with the Protection Profile.

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

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

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

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

This evaluation assurance package was selected to permit a developer gaining maximum assurance from positive security engineering based on good commercial practices as well as the assurance that the TOE is maintained during its targeted life time. The evaluation assurance package follows the EAL6 assurance classes as given in [14].

#### 7.3.2.1 ALC\_FLR.1 Basic Flaw Remediation

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

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

Flaws are prioritized and assigned to a responsibility.

The assurance class ALC\_FLR.1 has no dependencies.

## 8 TOE Summary Specification (ASE\_TSS)

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

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

- SF\_DPM Device Phase Management
- SF\_PS Protection against Snooping
- SF\_PMA Protection against Modification Attacks
- SF\_PLA Protection against Logical Attacks
- SF\_CS Cryptographic Support

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

### 8.1 SF\_DPM: Device Phase Management

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

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

The covered security functional requirement is FAU\_SAS.1 "Audit storage".

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

The covered security functional requirements are FMT\_LIM.1 and FMT\_LIM.2.

During the production phase (phase 3 and 4) or after the delivery to the customer (phase 5 or phase 6), the TOE provides the possibility to download user code and data into the empty (erased) SOLID FLASH™ NVM flash memory area. More information is given in the confidential Security Target [10]. These procedures are defined as phase operation limitation.

The covered security functional requirement is FPT\_LIM.2 "Limited availability".

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

The covered security functional requirements are FDP\_ACC.1, FDP\_ACF.1 and FMT\_MSA.1.

In addition, during each start-up of the TOE the address ranges and access rights are initialized by the STS with predefined values. The covered security functional requirement is FMT\_MSA.3.

The TOE clearly defines and assigns access rights and privilege levels. By this clearly defined management functions are implemented, enforced by the MMU, and the covered security functional requirement is FMT\_SMF.1.

During the testing phase in production within the secure environment the entire SOLID FLASH™ NVM is deleted. The covered security functional requirement is FPT\_PHP.3.

Each operation phase is protected by means of authentication and encryption. The covered security functional requirements are FDP\_ITT.1 and FPT\_ITT.1.

The **SF\_DPM** “Device Phase Management” covers the security functional requirements FAU\_SAS.1, FMT\_LIM.1, FMT\_LIM.2, FDP\_ACC.1, FDP\_ACF.1, FMT\_MSA.1, FMT\_MSA.3, FMT\_SMF.1, FPT\_PHP.3, FDP\_ITT.1 and FPT\_ITT.1.

## 8.2 SF\_PS: Protection against Snooping

All contents of all memories of the TOE are encrypted on chip to protect against data analysis on stored data as well as on internally transmitted data. There is no plain data on the chip.

In addition the data transferred over the memory bus to and from the core, cryptographic coprocessors, certain SFRs and peripheral devices are automatically encrypted.

The memory content and bus encryption is done by the MED using a complex key management. All security relevant transfer of addresses or data via the peripheral bus is protected against readout and analysis. No plain data are handled anywhere on the TOE and thus also the two CPUs compute entirely masked, as well as the symmetric cryptographic co-processor.

The encryption means covers the data processing policy and FDP\_IFC.1 “Subset information flow control”. The covered security functional requirements are FPT\_PHP.3, FDP\_IFC.1, FPT\_ITT.1 and FDP\_ITT.1.

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

The covered security functional requirements are FPT\_PHP.3, FDP\_IFC.1, FPT\_ITT.1, and FDP\_ITT.1.

The proprietary implementation of the CPU has no standard command set and discloses therefore no possibility for deeper analysis. The covered security functional requirement is FPT\_PHP.3.

The entire design is kept in a nonstandard way to prevent attacks using standard analysis methods. A smartcard dedicated CPU operating in non-standard way renders analysis very complicated and time consuming. Important parts of the chip are especially designed to counter leakage or side channel attacks like DPA/SPA or EMA/DEMA. Therefore, even the physical data gaining is difficult to perform, since timing and current consumption is independent of the dynamically encrypted, masked and randomized processed data.

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

A further topological design method is used during the definition of the layout. The result is called implicit shielding or short I<sup>2</sup>-shielding.

The covered security functional requirements are FPT\_PHP.3, FPT\_ITT.1 and FDP\_ITT.1.

In addition, the storage of code and data in the SOLID FLASH™ NVM is protected against side channel attacks too: Even if users operate with direct and static addressing for storing their secrets, the addresses are always translated to virtual addresses.

The covered security functional requirements are FPT\_PHP.3, FPT\_ITT.1 and FDP\_ITT.1.

A low system frequency sensor FSE is implemented to prevent the TOE from single stepping.

Further protective means are described in the confidential Security Target [10]. The covered security functional requirements are FPT\_PHP.3 and FPT\_FLS.1.

An induced error which cannot be corrected will be recognized by the Integrity Guard and leads to an alarm. In case of security critical detections a security alarm and reset is generated. The covered security functional requirement is FPT\_FLS.1.

The **SF\_PS** “Protection against Snooping” covers the security functional requirements FPT\_PHP.3, FDP\_IFC.1, FPT\_ITT.1, FDP\_ITT.1 and FPT\_FLS.1.

### 8.3 SF\_PMA: Protection against Modifying Attacks

First of all we can say that all security mechanisms effective against snooping **SF\_PS** apply also here since a reasonable modification of data is almost impossible on dynamically encrypted, masked, scrambled, transparently relocated, randomized and topologically protected hardware. Due to this the covered security functional requirements are FPT\_PHP.3, FDP\_IFC.1, FPT\_ITT.1, FDP\_ITT.1 and FPT\_FLS.1.

The TOE is equipped with an error detection code (EDC) which covers the memory system of RAM, ROM and SOLID FLASH™ NVM and includes also the MED and MMU. Thus introduced failures could be detected and in terms of single bit errors in the SOLID FLASH™ NVM also automatically corrected (FDP\_SDI.2).

In order to prevent accidental bit faults during production in the ROM, over the data stored in ROM an EDC value is calculated (FDP\_SDI.1).

The covered security functional requirements are FRU\_FLT.2, FPT\_PHP.3, FDP\_SDI.1 and FDP\_SDI.2.

If a user tears the card resulting in a power off situation during an SOLID FLASH™ NVM programming operation or if other perturbation is applied, no data or content loss occurs and the TOE restarts power on. The SOLID FLASH™ NVM tearing save write functionality covers FPT\_FLS.1 “Failure with preservation of secure state” since if the programming was not successful, the old data are still present and valid, which ensures a secure state although a programming failure occurred. This action includes also FDP\_SDI.1 “Stored data integrity monitoring” as the new data to be programmed are checked for integrity and correct programming before the page with the old data becomes the new

physical page for the next new data.

The covered security functional requirement is also FPT\_PHP.3 “Resistance to physical attack“, since these measures make it difficult to manipulate the write process of the SOLID FLASH™ NVM. The covered security functional requirements are FPT\_FLS.1, FPT\_PHP.3 and FDP\_SDI.1.

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

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

During start up, the STS performs various configurations and subsystem tests. After the STS has finished, the operating system or application can call the User Mode Security Life Control (UMSLC) test. The UMSLC checks the alarm lines and/or certain functions and sensors for correct operation. More information is given in the confidential Security Target [10].

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, FPT\_PHP.3 and FPT\_TST.2.

As physical effects or manipulative attacks may also address the program flow of the user software, dedicated countermeasures are implemented. These features allow the user to check the correct processing his software. By this induced errors are discovered. More information is given in the confidential Security Target [10].

The covered security functional requirements are FPT\_FLS.1, FDP\_IFC.1, FPT\_ITT.1, FDP\_ITT.1 and FPT\_PHP.3.

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

All communication via the busses is in addition protected. If an error occurs an alarm is generated.

The covered security functional requirements are FPT\_FLS.1 and FPT\_PHP.3.

The virtual memory system and privilege level model are enforced by the MMU. This controls the access rights throughout the TOE. There is a clear differentiation within the privilege levels defined. The covered security functional requirements are FDP\_ACC.1, FDP\_ACF.1, FMT\_MSA.1, FMT\_MSA.3 and FMT\_SMF1.

The **SF\_PMA** “Protection against Modifying Attacks” covers the security functional requirements FPT\_PHP.3, FDP\_IFC.1, FPT\_ITT.1, FDP\_ITT.1, FMT\_MSA.1, FMT\_MSA.3, FMT\_SMF.1, FDP\_ACC.1, FDP\_ACF.1, FRU\_FLT.2, FPT\_TST.2, FDP\_SDI.1, FDP\_SDI.2 and FPT\_FLS.1.

## 8.4 SF\_PLA: Protection against Logical Attacks

The memory access control of the TOE uses a memory management unit (MMU) to control the access to the available physical memory by using virtual memory addresses and to segregate the code and data to a privilege level model. The MMU controls the address permissions of the privileged levels. In case of an access violation the MMU will trigger a reset. The policy of setting up the MMU is defined from the user software (OS).

As the TOE provides support for separation of memory areas the covered security functional requirements are FDP\_ACC.1 "Subset access control", FDP\_ACF.1 "Security attribute based access control", FMT\_MSA.3 "Static attribute initialisation", FMT\_MSA.1 "Management of security attributes" and FMT\_SMF.1 "Specification of Management functions".

The TOE provides the possibility to protect the property rights of user code and data by the encryption of the SOLID FLASH™ NVM areas with a specific key defined by the user. Due to this key management FDP\_ACF.1 is fulfilled. In addition, each memory present on the TOE is encrypted using either mask specific or chip individual or even session keys, assigned by a complex key management. All data are protected by means of encryption or masking also during transportation via the busses. Induced errors are to be recognized by the Integrity Guard concept and lead to an alarm. In case of security critical errors a security alarm is generated and the TOE ends up in a secure state. The covered security functional requirements are FPT\_PHP.3, FDP\_ITT.1, FDP\_IFC.1 and FPT\_FLS.1.

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

The **SF\_PLA** "Protection against Logical Attacks" covers the security functional requirements FDP\_ACC.1, FDP\_ACF.1, FMT\_MSA.1, FMT\_MSA.3, FPT\_PHP.3, FDP\_ITT.1, FDP\_IFC.1, FPT\_FLS.1 and FMT\_SMF.1.

## 8.5 SF\_CS: Cryptographic Support

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

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

### 8.5.1 Triple DES

The TOE supports the encryption and decryption in accordance with the specified cryptographic algorithm Triple Data Encryption Standard (3DES) with cryptographic key sizes of 112 bit or 168 bit meeting the standard:

*National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Data Encryption Standard (DES), NIST Special Publication 800-67, Version 1.1.*

The TOE implements the following alternative block cipher modes for the user: the Electronic Codebook Mode (ECB), the Cipher Block Chaining Mode (CBC), the Blinding Feedback Mode (BLD) and the Cipher Feedback Mode (CFB). The BLD is described in the hardware reference manual [1] while the implementations of ECB, CBC and CFB follow the standard:

*National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Data Encryption Standard (DES), NIST Special Publication 800-38A, 2001 Edition.*

Please consider also the statement of chapter 7.1.4.1

The covered security functional requirements are FCS\_COP.1/DES.

### 8.5.2 AES

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

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

Please consider also the statement of chapter 7.1.4.1.

The covered security functional requirement is FCS\_COP.1/AES.

### 8.5.3 RSA

#### Encryption, Decryption, Signature Generation and Verification

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

*Encryption:*

*According to section 5.1.1 RSAEP in PKCS v2.1 RFC3447,  
without 5.1.1.1.*

*Decryption (with or without CRT):*

*According to section 5.1.2 RSADP in PKCS v2.1 RFC3447  
for  $u = 2$ , i.e., without any  $(r_i, d_i, t_i)$ ,  $i > 2$ ,*

therefore without 5.1.2.2.b (ii)&(v), without 5.1.2.1.

5.1.2.2.a, only supported up to  $n < 2^{2048}$

*Signature Generation (with or without CRT)::*

According to section 5.2.1 RSASP1 in PKCS v2.1 RFC3447

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

therefore without 5.2.1.2.b (ii)&(v), without 5.2.1.1.

5.2.1.2.a, only supported up to  $n < 2^{2048}$

*Signature Verification:*

According to section 5.2.2 RSAVP1 in PKCS v2.1 RFC3447,

without 5.2.2.1.

Please consider also the statement of chapter 7.1.4.1.

### Asymmetric Key Generation

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *RSA specified in PKCS#1 v2.1* and specified cryptographic key sizes of 1976 – 4096 bits that meet the following *standard*:

According to section 3.2(2) in PKCS v2.1 RFC3447,

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

For  $p \times q < 2^{2048}$  additionally according to section 3.2(1).

Note 23:

For easy integration of RSA functions into the user's operating system and/or application, the library contains single cryptographic functions respectively primitives which are compliant to the standard. The primitives are referenced above. Therefore, the library supports the user to develop an application representing the standard if required. Please consider also the statement of chapter 7.1.4.1.

End of note.

The covered security functional requirement is FCS\_COP.1/RSA and FCS\_CKM.1/RSA.

### 8.5.4 Elliptic Curves EC

The EC library is used to provide a high level interface to Elliptic Curve cryptography implemented on the hardware component Crypto2304T 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.

The EC library is delivered as object code and in this way integrated in the user software. The certification covers the

standard NIST [17] and Brainpool [18] Elliptic Curves with key lengths of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 Bits, due to national AIS32 regulations by the BSI. 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.

### Signature Generation and Verification

The TSF shall perform signature generation and signature verification in accordance with a specified cryptographic algorithm ECDSA and cryptographic key sizes 192 - 521 bits that meet the following standard:

#### *Signature Generation:*

1. According to section 7.3 in ANSI X9.62 - 2005

*Not implemented is step d) and e) thereof.*

*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 6.2 (6.2.2. + 6.2.3) in ISO/IEC 15946-2:2002

*Not implemented is section 6.2.1:*

*The output of 5.4.2 has to be provided by the caller as input to the function.*

#### **Signature Verification:**

1. According to section 7.4.1 in ANSI X9.62-2005

*Not implemented is step b) and c) thereof.*

*The output of step c) has to be provided as input to our function by the caller.*

*Deviation of step d):*

*Beside noted calculation, our algorithm adds a random multiple of BasepointerOrder  $n$  to the calculated values  $u_1$  and  $u_2$ .*

2. According to sections 6.4 (6.4.1. + 6.4.3 + 6.4.4) in ISO/IEC 15946-2:2002

*Not implemented is section 6.4.2:*

*The output of 5.4.2 has to be provided by the caller as input to the function.*

### Asymmetric Key Generation

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Elliptic Curve EC specified in ANSI X9.62-1998 and ISO/IEC 15946-1:2002 and specified cryptographic key sizes 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits that meet the following standard:

ECDSA Key Generation:

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

### 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:

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

Note 24:

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

End of note.

The covered security functional requirements are FCS\_COP.1/ECDSA, FCS\_CKM.1/EC and FCS\_COP.1/ECDH.

### 8.5.5 SHA-2 Operation with Cryptographic Software Library

The TOE comes optionally with the SHA-2 library for hash value calculation. Regarding the SHA-2 library it has to be noted that the secure hash-algorithm SHA-2 is intended to be used for signature generation, verification and generic data integrity checks. Further essential information is given in the confidential user guidance.

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

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

The covered security functional requirement is FCS\_COP.1/SHA-SW.

### 8.5.6 Hash Operation with Hardware Module

The SHA module provides the calculation of a hash value of freely chosen data input in the CPU and is intended to be used for signature generation, verification and generic data integrity checks. Further essential information is given in the confidential user guidance.

The TOE provides the Hash module to compute extremely fast hash values within just some dozens of clock cycles. Following hashing algorithms can be performed using this module:

- MD-5
- SHA-1
- SHA-256.

Following the BSI recommendations the algorithms MD-5 and SHA-1 are not covered by this evaluation.

The TSF shall perform *Hash-value calculation of user chosen data* in accordance with a specified cryptographic algorithm SHA-2, SHA-1 and MD5 with cryptographic key sizes of *none* that meet the following standards:

*U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Information Technology Laboratory (ITL), Secure Hash Standard (SHS), FIPS PUB 180-4, 2012-March, section 6.2 SHA-256.*

The covered security functional requirement is FCS\_COP.1/SHA-2-HW.

### 8.5.7 Toolbox Library

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

The toolbox does not cover security functional requirements.

### 8.5.8 Base Library

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

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

### 8.5.9 PTRNG respectively TRNG

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

The covered security functional requirement is FCS\_RNG.1, FPT\_PHP.3, FDP\_ITT.1, FPT\_ITT.1, FPT\_TST.2 and FPT\_FLS.1.

The **SF\_CS** "Cryptographic Support" covers the security functional requirements FCS\_COP.1/DES, FCS\_COP.1/AES, FCS\_COP.1/RSA, FCS\_CKM.1/RSA, FCS\_COP.1/ECDSA, FCS\_CKM.1/EC, FCS\_COP.1/ECDH, FCS\_COP.1/SHA, FPT\_PHP.3, FDP\_ITT.1, FPT\_ITT.1, FPT\_TST.2, FPT\_FLS.1 and FCS\_RNG.1.

Note 25:

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

End of note.

Note 26:

This TOE can come with both crypto co-processors accessible, or with a blocked SCP or with a blocked Crypto2304T, or with both crypto co-processors blocked. The blocking depends on the customer demands prior to the production of the hardware. In case the SCP is blocked, no AES and DES computation supported by hardware is possible. In case the Crypto2304T is blocked, no RSA and EC computation supported by hardware is possible. The use of the SHA-2 library is also possible with both crypto coprocessors blocked. No accessibility of the deselected cryptographic co-processors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic co-processors.

End of note.

Note 27:

The TOE can come with the Secure Hash Algorithm by Hardware (optional HW Hash) being available or not. If the Hash module is blocked the hardware implemented Hash Algorithms are not available. The use of the Hash module is independent from the optional SHA-2 library software and also independent of the availability of the cryptographic coprocessors. No accessibility of the Hash module 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 Hash module.

End of note.

## 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 following table. 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 following table:

Table 19: Mapping of SFR and SF

Security Functional Requirement	SF_DPM	SF_PS	SF_PMA	SF_PLA	SF_CS
FAU_SAS.1	X				
FMT_LIM.1	X				
FMT_LIM.2	X				
FDP_ACC.1	X		X	X	
FDP_ACF.1	X		X	X	
FPT_PHP.3	X	X	X	X	X
FDP_ITT.1	X	X	X	X	X
FDP_SDI.1			X		
FDP_SDI.2			X		
FDP_IFC.1		X	X	X	
FMT_MSA.1	X		X	X	
FMT_MSA.3	X		X	X	
FMT_SMF.1	X		X	X	
FRU_FLT.2			X		
FPT_ITT.1	X	X	X		X
FPT_TST.2			X		X
FPT_FLS.1		X	X	X	X
FCS_RNG.1					X
FCS_COP.1/DES					X
FCS_COP.1/AES					X

Security Functional Requirement	SF_DPM	SF_PS	SF_PMA	SF_PLA	SF_CS
FCS_COP.1/RSA					X
FCS_COP.1/ECDSA					X
FCS_COP.1/ECDH					X
FCS_COP.1/SHA-SW					X
FCS_COP.1/SHA-2-HW					X
FCS_CKM.1/RSA					X
FCS_CKM.1/EC					X

### 8.7 Security Requirements are internally consistent

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

In addition to the discussion in section 6.3 of PP [11] the security functional requirement FCS\_COP.1 is introduced. The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the cryptographic algorithms implemented according to the security functional requirement FCS\_COP.1. Therefore, these security functional requirements support the secure implementation and operation of FCS\_COP.1.

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

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

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

requirements support the secure implementation and operation of FDP\_ACF.1 with its dependent security functional requirements.

The requirement FDP\_SDI.2.1 allows detection of integrity errors of data stored in memory. FDP\_SDI.2.2 in addition allows correction of one bit errors or taking further action. Both meet the security objective O.Malfunction. The requirements FRU\_FLT.2, FPT\_FLS.1, and FDP\_ACC.1 which also meet this objective are independent from FDP\_SDI.2 since they deal with the observation of the correct operation of the TOE and not with the memory content directly.

## 9 Literature

Ref	Version	As off	Titel
[1]	v2.3	2013-06-06	M7893 Controller Family for Security Applications, Family Hardware Reference Manual, called HRM
[2]		2015-04-01	SLx 70 Family Production and Personalization User's Manual
[3]	v8.4	2015-05-06	16-bit Controller Family, SLE 70, Programmer's Reference Manual
[4]	v1.03.006	2012-08-16	SLE70 Asymmetric Crypto Library Crypto@2304T, RSA / ECC / Toolbox, Users Interface
[5]		2009-11	Chipcard and Security ICs, SLx70 Family, Secure Hash Algorithm SHA-2, (SHA 256/224, SHA 512/384) (optional)
[6]		2010-03-23	SLE70 Crypto@2304T User Manual,
[7]		2015-08-17	M7893 SOLID FLASH™ Controller for Security Applications, 16-bit Security Controller Family, 90nm Technology, Security Guidelines
[8]	1.4	2014-11-25	M7893 Controller Family for Security Applications, Errata Sheet
[9]	1.0	2013-02-19	AMM Advanced Mode for Mifare-Compatible Technology, Addendum to M7893 Hardware Reference Manual
[10]	0.2	2015-08-31	The confidential Security Target for this TOE
[11]	1.0	2007-06-15	Security IC Platform Protection Profile PP0035
[12]	V3.1 Rev 4	2012-09	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model; Version 3.1 Revision 4 September 2012, CCMB-2012-09-001
[13]	V3.1 Rev 4	2012-09	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements; Version 3.1 Revision 4 September 2012, CCMB-2012-09-002
[14]	V3.1 Rev 4	2012-09	Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements; Version 3.1 Revision 4 September 2012, CCMB-2012-09-003
[15]	3.0	2013-05-15	Functionality classes and evaluation methodology for physical random number generators AIS31, Version 3.0, 2013-05-15, Bundesamt für Sicherheit in der Informationstechnik and belonging "A proposal for: Functionality classes for random number generators", Version 2.0, 2011-09-18, Wolfgang Killmann, T-Systems GEI GmbH, Werner Schindler, Bundesamt für Sicherheit in der Informationstechnik
[16]	2.9	2013-01	Application of Attack Potential to Smartcard, mandatory technical document, CCDB-2013-05-002, <a href="http://www.commoncriteriaportal.org">http://www.commoncriteriaportal.org</a>

The table continues on the next page.

Ref	Version	As off	Titel
17	186-4	2013-09-05	NIST: FIPS publication 186-4: Digital Signature Standard (DSS), 2013-09-05
18	RFC 5639	2010-03	IETF: RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010, <a href="http://www.ietf.org/rfc/rfc5639.txt">http://www.ietf.org/rfc/rfc5639.txt</a>
19	Rev. 1	2012-01	National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce, NIST Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
20	PUB 197	2001-11-26	U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), Advanced Encryption Standard (AES), FIPS PUB 197
21	v2.1	2002-06-14	PKCS #1: RSA Cryptography Standard, RSA Laboratories
22	X.9.62	2005-11-16	American National Standard for Financial Services ANS X9.62-2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standards Institute
23	X.9.63	2001-11-20	American National Standard for Financial Services X9.63-2001, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, American National Standards Institute
24	I	2009-08-14	Act on the Federal Office for Information Security (BSI-Gesetz - BSIg), Bundesgesetzblatt I p. 2821.
25	180-4	2015-08	Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8900, Federal Information Processing Standards Publication, Secure Hash Standard (SHS)
26	SP 800-67 Rev. 1	2012-01	National Institute of Standards and Technology (NIST), Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Revised January 2012, Technology Administration, U.S. Department of Commerce
27	SP 800-38A	2001-12	National Institute of Standards and Technology(NIST), Technology Administration, US Department of Commerce, NIST Special Publication SP 800-38A (for AES and DES)
28	ISO/IEC 9797-1	2011-03-01	International Standard ISO/IEC 9797-1, Information Technology - Security Techniques - Message Authentication Codes (MACs)

Note that the versions of these documents will be defined at the end of the evaluation and listed in the certification report.

## 10 Appendix

In Table 21 the hash signatures of the respective CL70 Crypto Library file are documented. For convenience purpose several hash values are referenced.

*Table 20: Reference hash values of the Cryptographic Libraries*

### Optional Cryptographic Library v1.03.006 Hash Values

CI70-LIB-base-XSMALL-HUGE.lib:

MD5=d41da6598a5fde96c090120a757c0f51

SHA1=b5ad2456aa5a13b21428986a2e34f71452152d48

SHA256=93a19624b2d76453abc5c37352e672e614c8e1eec7bf55d1db16385b5609aea0

CI70-LIB-ecc-XSMALL-HUGE.lib:

MD5=66956fba12b2126fe7228f0f939aced5

SHA1=aa13bb47ef66ed7f2dbf2e540edc118bf4669733

SHA256=7f403d7797a6c6b53914fd43a6dad80c35c55f152ffeb267079bea257be116cb

CI70-LIB-2k-XSMALL-HUGE.lib:

MD5=64fdfa83b754d2c6461dc720d2fc5de7

SHA1=4e85a3760084c68cf989c006bb3f287894a58a29

SHA256=5d93de6e609ea4f2316f0bd83c4fa1de9d4024b609b88831c507829c0bd30b2d

CI70-LIB-4k-XSMALL-HUGE.lib:

MD5=511cd1f3bb1c5ae58db064904f9018e0

SHA1=f2458477c94bd0fba8e8dde1b10aaa61cf2cb89d

SHA256=10c04adaff39b38372469c6a80f74a60c88c023eca2d1a760ca29038bff82d66

CI70-LIB-toolbox-XSMALL-HUGE.lib:

MD5=8fa281387c9cfc16942b8e704290598f

SHA1=1363e820486902d56b36ec365b49ef0767cdf411

SHA256=b4554607af89dd003f8ac34a771505ed0b097263fa8f61962395964f1a42ec79

CI70-ROM-XSMALL-HUGE.lib:

MD5=4e4334c65e795cb940b2a09665ddaf35

SHA1=8f0f0a4f86326430fe4bf8d9f33fc35ac21a8fbf

SHA256=1c31f50a1d24be9ef6ba8e368d617da34c7764a4b25564cb0a04c29e9157168a

**SHA-2 Library Version 1.01:**

MD5=70d2df490185b419fb820d597d82d117

SHA1= df15ff79b5f5ab70bbad0ee031953e1877cabd47

SHA256=765fc5d47cf8274833476406b24010a56ebcfd4b0972704ddd27e2d3e3e086f8

## 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
BSI	German: Bundesamt für Sicherheit in der Informationstechnik English: Federal Office for Information Security <a href="https://www.bsi.bund.de">https://www.bsi.bund.de</a>
CC	Common Criteria
GCIM	Generic Chip Identification Mode
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
Crypto2304T	Asymmetric Cryptographic Processor
CRT	Chinese Remainder Theorem
DPA	Differential Power Analysis
DFA	Differential Failure Analysis
DRNG	Deterministic Random Number Generator
EC	Elliptic Curve
ECC	Error Correction Code
EDC	Error Detection Code
EDU	Error Detection Unit
EMA	Electromagnetic analysis
GPIO	General Purpose Input/Output
HW	Hardware
IC	Integrated Circuit
ICO	Internal Clock Oscillator
ID	Identification
IMM	Interface Management Module
ITP	Interrupt and Peripheral Event Channel Controller
I/O	Input/Output
ITSEC	Information Technology Security Evaluation Criteria
M	Mechanism

---

MED	Memory Encryption and Decryption
MMU	Memory Management Unit
NVM	Non Volatile Memory
O	Object
OS	Operating system
PEC	Peripheral Event Channel
PRNG	Pseudo Random Number Generator, see also DRNG
PROM	Programmable Read Only Memory
PTRNG	Physical True Random Number Generator
RAM	Random Access Memory
RMS	Resource Management System
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest-Shamir-Adleman Algorithm
SA	Service Algorithm
SSC	Synchronous Serial Controller
SPI	Serial Peripheral Interface
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
SOLID FLASH™ NVM	Electrically Erasable and Programmable Read Only Memory
SPA	Simple power analysis
STS	Self-Test Software
SW	Software
SO	Security objective
T	Threat
TM	Test Mode
TOE	Target of Evaluation
TSC	TOE Security Functions Control
TSF	TOE Security Functionality
TRNG	True Random Number Generator, see also PTRNG

UART	Universal Asynchronous Receiver/Transmitter
UM	User Mode
UMSLC	User mode Security Life Control
USB	Universal Serial Bus
WDT	Watch Dog Timer
XRAM	eXtended Random Access Memory
3DES	Triple DES Encryption Standard

## 12 Glossary

Application Program/Data	Software which implements the actual TOE functionality provided for the user or the data required for that purpose
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
SOLID FLASH™ NVM	The Non Volatile Memory enables for reading and writing data and keeps information also in power-off state. The module implements the Unified Channel Programming UCP concept.
End User	Person in contact with a TOE who makes use of its operational capability
Firmware	Part of the software implemented as hardware
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 for operation
Programmable Read Only Memory	Non-volatile memory which can be written once and then only permits read operations

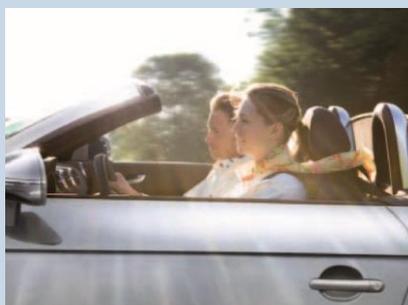
---

Random Access Memory	Volatile memory which permits write and read operations
Random Number Generator	Hardware part for generating random numbers
Read Only Memory	Non-volatile memory which permits read operations only
Resource Management System	Part of the firmware containing SOLID FLASH™ NVM programming routines, AIS31 testbench etc.
SCP	Symmetric cryptographic coprocessor for symmetric cryptographic operations (3DES, AES).
Self-Test Software	Part of the firmware with routines for controlling the operating state, performing the chip setup during its startup 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
Software	Information (non-physical part of the system) which is required to implement functionality in conjunction with the hardware (program code)
Subject	Entity, generally in the form of a person, who performs actions
Target of Evaluation	Product or system which is being subjected to an evaluation
Test Mode	Operational status phase of the TOE in which actions to test the TOE hardware take place
Threat	Action or event that might prejudice security
User Mode	Operational status phase of the TOE in which actions intended for the user takes place

Infineon Technologies – innovative semiconductor solutions for energy efficiency, mobility and security.



[www.infineon.com](http://www.infineon.com)



Published by Infineon Technologies AG