M5074 G11

M5074 G11
Including optional software library SCL

Security Target Lite

v1.9, 2016-01-21

Chip Card & Security

Edition 2016-01-21

Published by Infineon Technologies AG,

81726 Munich, Germany.

© 2016 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**).

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.

PUBLIC

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

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.

Last Trademarks Update 2015-01

Revision History

Version	Change Description
0.1	Initial version
1.9	Final Version

Table of Contents

1 Security Target Introduction (ASE_INT)

1.1 Security Target and Target of Evaluation Reference

The title of this document is Security Target (ST). The Security Target comprises the Infineon Technologies Security Controller M5074 G11 with optional SCL and with specific IC-dedicated firmware.

The target of evaluation (TOE) M5074 G11 is described in the following sections. The Security Target has the revision v1.9 and is dated 2016-01-21.

The Target of Evaluation (TOE) is an Infineon Technologies Security Controller M5074 G11 with optional SCL version 1.05.001 and with specific IC-dedicated firmware.

The Security Target is based on the Protection Profile “Smartcard IC Platform Protection Profile” [1].

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

The ST takes into account all relevant current final interpretations.

The targeted certificate is EAL5+.

Table 1 Identification

	Version	Date	Registration
Security Target	this version	see cover page	M5074 G11
Target of Evaluation	G11		M5074 G11
			with Flash Loader V3.96.013
			and Flash Loader patch version V0.00.000
			and RMS V7790b0174
			and STS V77042306
			and STS Patch V7240
			and SAM V25b01
			and Overall Patch V7000
			and optional SW:
			SCL V1.05.001
			and guidance documentation
Guidance Documentation	Edition	2015-08	M5074 SOLID FLASH™ Controller for Security Applications, Hardware Reference Manual
		2015-04	SLx 70 Family Production and Personalization User's Manual
		2015-09	SLE 70 Programmer’s Reference Manual
		2015-03	M5074 Security Guidelines User's manual
		2015-12	SLE77P Symmetric Crypto Library for µSCP version 2 DES/AES
		2015-06	SLE77 Controller Family, Solid Flash™ Controller for Security Applications, Errata Sheet

A customer can identify the TOE and its configuration (for details see chapter 2.2.7) using the Non-ISO ATR in combination with firmware functions. The TOE answers the Non-ISO-ATR with a Chip Identification Mode (CIM). This CIM outputs a STS version identifier (which is also used to identify the M5074) and design step. The RMS base version and configuration of the TOE (memory size and available peripherals) can be obtained by dedicated RMS functions. The Flash Loader offers a function to extract its version.

1.2 Target of Evaluation Overview

The TOE comprises the Infineon Technologies SmartCard IC (Security Controller) M5074 G11 with specific IC-dedicated software and optional SCL.

This Security Target (ST) describes the TOE known as the Infineon Technologies AG security controller group as listed in Table 1 and gives a summary product description.

The TOE is a member of the Security Controller family SLE70 and meets high requirements in terms of performance and security.

The TOE provides a 16-bit CPU-architecture and is compatible to the Intel 80251 architecture. The major components of the core system are the non-standard CPU, the MMU (Memory Management Unit) and MED (Memory Encryption/Decryption Unit). The TOE implements a 16-MByte linear addressable memory space, a simple scaleable Memory Management concept and a scaleable stack size. The flexible memory concept consists SOLID FLASH™[1] 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-safe writing to the SOLID FLASH™ NVM. The STS firmware is used for test purposes during startup and the Flash Loader allows downloading of user software to the SOLID FLASH™ NVM during the manufacturing process. The STS resides in a dedicated test ROM area, that is part of the TOE.

The µSCP in combination with the optional SCL provides a TDES and AES implementation and includes countermeasures against SPA, DPA and DFA attacks.

The TRNG (True Random Number Generator) is a physical random number generator and meets the requirements of the functionality class PTG.2 of [6].

The TOE can be delivered with or without the SCL. If the user decides not to use the SCL, the accompanying packages ”AES” and “TDES” are not provided by the TOE.

The TOE is equipped with signal protection implemented by Infineon-specific secure wiring of security-critical signals.

[1] SOLID FLASH™ is an Infineon Trade Mark.

2 Target of Evaluation Description

The TOE description helps the reader 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.

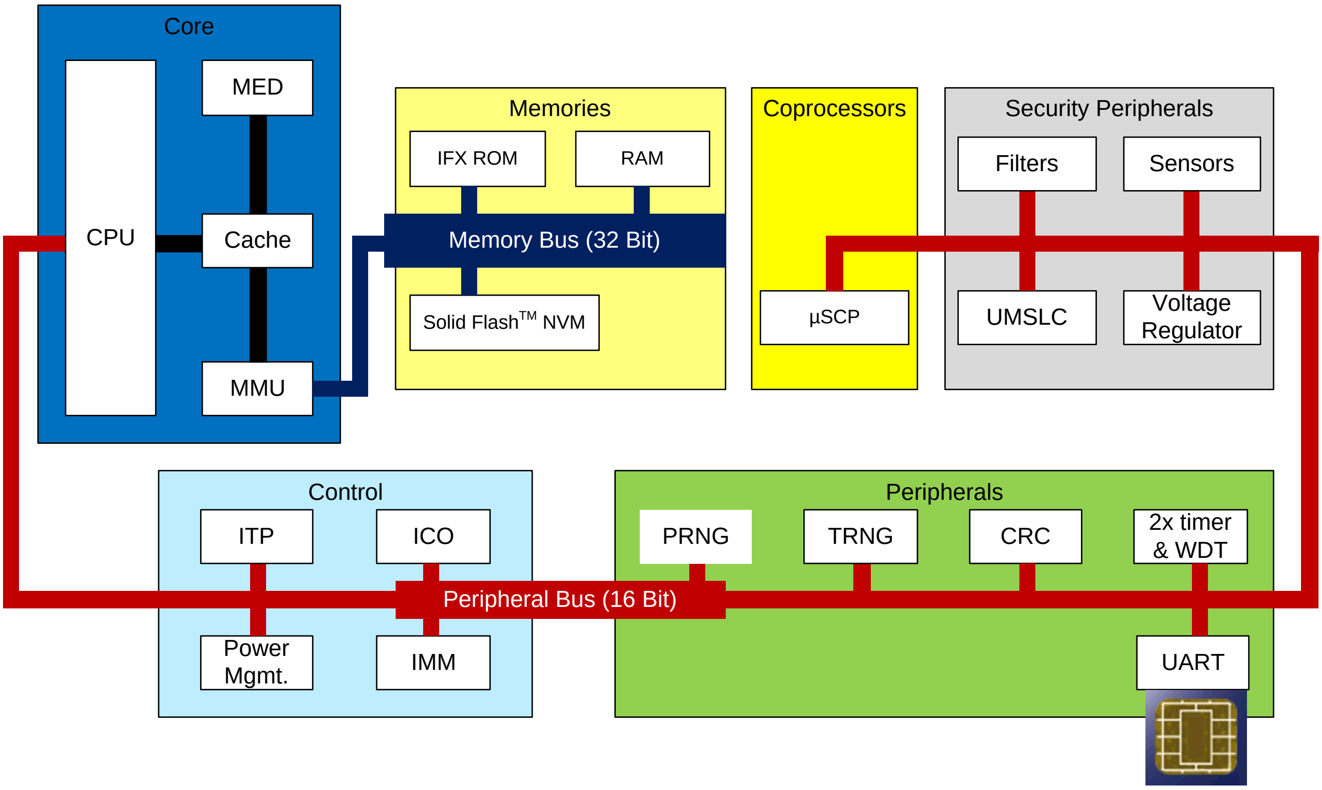
2.1 TOE Definition

The TOE is a member of the SLE77 family consists of smartcard ICs (Security Controllers) meeting the highest requirements in terms of performance and security. They are manufactured by Infineon Technologies in a 90 nm CMOS technology (L90FL). This TOE is intended to be used in smartcards and for its previous use as a development platform for smartcard operating systems according to the lifecycle model from [1]

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

Figure 1 shows a block diagram of the M5074:

Figure 1 Block diagram of the TOE



The TOE consists of a core system, memories, coprocessor, peripherals, security modules and control peripherals.

The major components of the core system are the non-standard CPU, the MMU (Memory Management Unit) and MED (Memory Encryption/Decryption Unit).

The CPU accesses memory via the integrated Memory Encryption and Decryption unit (MED). All data of the memory block is encrypted. The access rights of the application to the memories can be controlled with the memory management unit (MMU). Errors in RAM and ROM are automatically detected (EDC, Error Detection Code) in terms of the SOLID FLASH™ memory 1-Bit-errors are also corrected (ECC, Error Correction Code).

The controller of this TOE stores 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 cache is a high-speed memory buffer located between the CPU and (external) main memories holding a copy of some of the memory contents to enable fast access.

The power management module supports different halt and sleep modes (low activity modes consuming little power) as well as data transmissions using peripheral event channels. Moreover, the current limitation function can be used for power balancing.

The Clock Unit (ICO) supplies the clocks for all components of the TOE. The Clock Unit can work in an internal and external clock mode. When operating in the internal clock mode the system frequency is derived from an internal oscillator, whereas in external clock mode, the system clock is derived from an externally supplied interface clock according to a defined dependency.

The Interrupt and Peripheral Event Channel Controller (ITP) can process interrupt requests from different sources, each with its own subnodes, to determine whether a corresponding interrupt service routine (ISR) is to run or whether data is to be transferred in up to four peripheral event channels.

The Interface Management Module (IMM) monitors the status of all connected interfaces, detects changes in the status of an interface, receives reset requests from an interface, and provides a clock selection and automatic clock switching mechanism for the external clock of the clock unit. Reset, clock and power supply behaviour is managed here.

The controller provides a pseudo RNG (PRNG) for fast random number generation times.

The TRNG (True Random Number Generator) is specially designed for smartcard applications. The TRNG fulfils the requirements of the functionality class PTG.2 of [6] and produces genuine random numbers which then can be used directly or as seed for the PRNG (Pseudo Random Number generator). The PRNG is not in the scope of the evaluation.

The Cyclic Redundancy Check logic (CRC) allows easy generation of checksums according to ISO/IEC 3309 (16-bit CRC).

The UART-controlled I/O interface allows the smartcard controller and the terminal interface to be operated independently.

The timer/counter unit has 2 timers. The unit is used for timer operation when clocked by the oscillator/system clock or counter operation depending on the clock source configured.

The watchdog timer is a circuit that monitors controller operation by automatically initiating a reset if a specified period without an adequate response elapses after occurrence of a hardware or software irregularity.

The security peripherals consist of sophisticated modules, including a UMSLC (user mode security life control), a set of sensors, regulators and filters along with security-optimized wiring to detect faults as well as electrical and physical conditions, and initiate alarms to indicate security breaches. The UMSLC enables the user software to check the activity and proper function of the system’s security features.

The micro Symmetric Cryptographic Processor (µSCP) supports calculation of dual-key or triple-key triple-DES and AES. The µSCP in combination with the optional SCL compute the complete TDES and AES algorithm and are designed to counter attacks like DPA, EMA and DFA.

The STS (self-test software), RMS (Resource Management System), Service Algorithm Minimal (SAM) and Flash Loader together compose the TOE firmware stored in the ROM. All mandatory functions for internal testing, production usage and start-up behavior (STS), and also the RMS and SAM functions are grouped together in a common privilege level. These privilege levels are protected by a hardwired Memory Management Unit (MMU) setting.

The TOE uses Special Function Registers (SFRs). These SFRs are used for general purposes and chip configuration; they are located in SOLID FLASH™ memory in a configuration area page.

The bus system comprises two separate bus entities: a memory bus and a peripheral bus for high-speed communication with the peripherals.

Security optimized wiring protect certain critical signals.

The following is a list of features provided by the TOE:

- 24-bit linear addressing
- Up to 16 Mbytes of addressable memory
- Register-based architecture (registers can be accessed as bytes, words (2 bytes), and doublewords (4 bytes))
- 2-stage instruction pipeline
- Extensive set of powerful instructions, including 16- and 32-bit arithmetic and logic instructions
- Cache with single-cycle access searching
- 16-bit ALU

2.2 Scope of the TOE

The TOE comprises three parts:

1. Hardware of the smartcard security controller
2. Associated firmware and software
3. Documents

The hardware configuration options and configuration methods are described in Section 2.2.7

The second part of this TOE includes the associated firmware and software required for operation and cryptographic support.

The documents as described in Section 2.2.4 and listed in Table 1 are supplied for user guidance. In the following description, the term “manufacturer” stands for Infineon Technologies, the manufacturer of the TOE. The Smartcard Embedded Software or user software is not part of the TOE.

2.2.1 Hardware of the TOE

The hardware part of the TOE (see Figure 1) as defined in [1] comprises the following:

Core System

- Proprietary CPU implementation of the Intel^{TM} MCS251 standard architecture from a functional perspective
- Memory Encryption/Decryption Unit (MED)
- Memory Management Unit (MMU)
- Cache

Memories

- Read-Only Memory (ROM): not available to the user
- Random Access Memory (RAM)
- SOLID FLASH™memory

Peripherals

- True Random Number Generator (TRNG)
- Pseudo Random Number Generator (PRNG)
- Watchdog and timers
- Universal Asynchronous Receiver/Transmitter (UART)
- Checksum module (CRC)

Control

- Power Management
- Clock unit including Internal Clock Oscillator (ICO)
- Interrupt and Peripheral Event Channel Controller (ITP)
- Interface Management Module (IMM)

Coprocessors

- Micro Symmetric Crypto Coprocessor supporting AES and TDES Standard

Security Peripherals

- Filters

- Sensors
- Voltage regulator
- User mode Security Life Control (UmSLC)

Buses

- Memory Bus
- Peripheral Bus

2.2.2 Firmware and Software of the TOE

The entire firmware of the TOE consists of different parts, as described below:

One part comprises the RMS and SAM routines for SOLID FLASH™ memory programming, security functions test, and random number online testing (Resource Management System, IC Dedicated Support Software in PP [1]). The RMS and SAM routines are stored by Infineon Technologies in ROM.

The second part is the STS, consisting of test and initialization routines (Self Test Software, IC Dedicated Test Software in PP [1]). The STS routines are stored in a specially protected test ROM and are not accessible by user software.

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

The optional software part of the TOE is the SCL.

The SCL is used to provide a high level interface to the TDES and AES cryptography, which is partly implemented on the hardware component µSCP and includes countermeasures against SPA, DPA and DFA attacks. The SCL is delivered as object code and in this way integrated into the user software.

Note: The TOE can be delivered with or without the SCL. If the user decides not to use the SCL, the accompanying packages ”AES” and “TDES” are not provided by the TOE.

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 includes the pads of the chip, particularly the contacted RES, I/O, CLK lines and supply lines VCC and GND. The communication meets ISO 7816/ETSI/EMV standards.
- The data-oriented I/O interface of the TOE is represented by the I/O pad.
- The interface to the firmware consists of special registers used for hardware configuration and control (Special Function Registers, SFR).
- The interface of the TOE to the operating system is covered by the RMS routines and 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 SCL calculations is defined by the SCL

Note that the interfaces of the SCL are optional, as these depend on the procurement order.

2.2.4 Guidance Documentation

The guidance documentation consists of:

- M5074 SOLID FLASH™ Controller for Security Applications, Hardware Reference Manual
- SLx 70 Family Production and Personalization User's Manual
- SLE 70 Family Programmer’s Reference User’s Manual

- SLE77 Controller Family, Solid Flash™ Controller for Security Applications, Errata Sheet

These documents contain the description of all interfaces of the software to the hardware relevant for programming the TOE.

- M5074 Security Guidelines User's manual: This document provides secure coding guidance to the application writer.
- SLE77P Symmetric Crypto Library for µSCP version 2 DES/AES (optional): User Interface, contains all interfaces of the SCL. This document is only delivered to the user in case the SCL is part of the delivered TOE.

The “SLE77 Controller Family, Solid Flash™ Controller for Security Applications, Errata Sheet” may be changed during the life cycle of the TOE. Changes are reported in a monthly updated list [5] provided by Infineon Technologies to the user.

Finally the certification report may contain an overview of recommendations to a software developer regarding the secure use of the TOE.

2.2.5 Forms of Delivery

The TOE can be delivered in the form of complete modules, as plain wafers in an IC case (e.g. DSO20) or in bare dies. The delivery can therefore be at the end of phase 3 or at the end of phase 4 which may also include pre-personalization steps according to [1]. In any case the testing of the TOE is finished and the extended test features are removed. From a security policy point of view the different forms of delivery do not have any impact.

The delivery to the software developer (phase 2 ➔ phase 1) contains the development package, which is delivered in electronic form. It contains the documents as described above, the development and debugging tools.
Part of the software delivery is the Flash Loader program, provided by Infineon Technologies AG, running on the TOE and controlling the download of user software onto the TOE via the UART interface. The download is only possible after successful authentication. The user software can also be downloaded in an encrypted way. In addition, the user can permanently block further use of the Flash Loader.

2.2.6 Production sites

The TOE may be handled at different production sites but the silicon is produced in TSMC only.

The delivery measures are described in the ALC_DVS aspect.

2.2.7 TOE Configuration

This TOE is represented by various configurations called products.

All products based on the M5074 representing this TOE are identical from hardware perspective and produced with the same masks.

Depending on the blocking configuration an M5074 product can have different user available SOLID FLASH™[1] memory sizes. The size can vary up to 120 kBytes. The RAM size is 4kBytes. The user can order the TOE with Hot Spot Distribution (HSD) in SOLID FLASH™ NVM on or off.

The entire configuration is done during the manufacturing process of the TOE according to the choice of the user. All differences between the products of this TOE are realized by means of blocking without changing the hardware. Therefore, all products of this TOE are equivalent from hardware perspective.

The blocking of the SOLID FLASH™ is done by setting the according value in the chip configuration page, which is not available to the user.

The memory settings are done during the production process by programming the physical start- and end-address of the user available memory areas. The entire configuration page cannot be changed by the user and is protected against manipulation.

For the user’s clear identification of the TOE´s configuration, the RMS contains a function, which allows to extract the user available size of the SOLID FLASH™ memory.

[1] SOLID FLASH™ is a Trade Mark of Infineon Technologies AG.

2.2.8 TOE initialization with Customer Software

This TOE is equipped with Flash Loader software (FL) to download user software, i.e. an operating system and applications. Various options can be chosen by the user to store software onto the SOLID FLASH™:

Table 2 Options to initialize the TOE with customer software

1	The user or/and a subcontractor downloads the software into the SOLID FLASH™ memory. Infineon Technologies does not receive any user software.	The Flash Loader can be activated or reactivated by the user or subcontractor to download software into the SOLID FLASH™ memory.
2	The user provides software to download into the SOLID FLASH™ memory to Infineon Technologies AG. The software is loaded into the SOLID FLASH™ memory during chip production.	There is no Flash Loader present.
3	The user provides software to download into the SOLID FLASH™ memory to Infineon Technologies AG. The software is loaded into the NVM memory during chip production.	The Flash Loader is blocked by Infineon but can be activated or reactivated by the user or subcontractor to download software into the SOLID FLASH™ memory. The user is required to provide a reactivation procedure as part of the software to Infineon Technologies AG.

3 Conformance Claims (ASE_CCL)

3.1 CC Conformance Claim

This Security Target (ST) and the TOE claim conformance to Common Criteria version v3.1 part 1 [2], part 2 [3] and part 3 [4].

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 claims strict conformance to [1].

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

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

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

The augmentations of the PP [1] are listed below.

Table 3 Augmentations of the assurance level of the TOE

Assurance Class	Assurance components	Description
Life-cycle support	ALC_DVS.2	Sufficiency of security measures
Vulnerability assessment	AVA_VAN.5	Advanced methodical vulnerability analysis

3.3 Package Claim

This Security Target claims conformance to following functional packages from [1]:

- Packages “TDES” and “AES”; sections 7.4.1 and 7.4.2
- Package Loader dedicated for usage in secured environment only; section 7.3.1

The assurance level for the TOE is EAL5 augmented with the components ALC_DVS.2 and AVA_VAN.5.

[1] 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 to [1].

The Target of Evaluation (TOE) is a typical security IC as defined in [1] chapter 1.2.2 comprising:

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

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

3.4.1 Security Problem Definition:

The security problem definition of [1] is enhanced by adding a 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 [1], as the security target claims strict conformance to [1].

3.4.2 Conformance Rationale:

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 [2] and PP [1], with following rational:

The security target remains conformant to CC [2], claim 482 as the possibility to introduce additional restrictions is given.

3.4.3 Adding Objective

Due to an additional security functionality regarding memory access control - O.Mem-Access, an additional security objective has been introduced. This add-on has no impact on the conformance statements regarding CC [2] and PP [1], with following rational:

The security target remains conformant to CC [2], claim 482 as the possibility to introduce additional restrictions is given.

3.4.4 AES and TDES

[1] implements the optional policy cryptographic services P.Crypto_Service with its packages “TDES” and “AES”. This TOE claims conformance to these optional packages requiring secure hardware based cryptographic services for the IC Embedded Software as outlined in chapter 7.1.6.

3.4.5 Loader

The PP [12] implements the optional policy for applying a Loader. The Loader is used to load data into the SOLID FLASH™ NVM. The Loader policy defines the Package 1 P.LIM_Block_Loader where the Loader is dedicated for usage in secure environment only. This TOE provides a Loader complying with this optional package 1 as outlined in chapter 7.2. Due to these optional additional security functionalities the security objectives O.Cap_Avail_Loader, Capability and availability of the Loader, and for the environment OE.Lim_Block_Loader, Limitation of capability and blocking the Loader, have been introduced. These add-ons have no impact on the conformance statements regarding CC [14] and PP [12], with following rational:

The security target fulfills the strict conformance claim of the PP [12] due to the application notes 5 applying here. By this note the addition of further security functions and security services are covered, even without deriving particular security functionality from a threat or a policy

3.4.6 Summary

Due to the above rational, the security objectives of this security target are consistent with the statement of the security objectives in [1], as the security target claims package-augmentation to [1].

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

The following security functional requirements are taken from [3] in addition to the SFRs defined in [1]:

- FMT_MSA.1 “Management of security attributes”
- FMT_MSA.3 “Static attribute initialization”
- FMT_SMF.1 “Specification of Management functions”

The security functional requirements as follows are included and completely defined in this ST, section 6:

- FPT_TST.2 “Subset TOE security testing“ (Requirement from [12])

The security functional requirements as follows are added:

- FDP_ACC.1 “Subset access control”
- FDP_ACF.1 “Security attribute based access control”

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

3.5 Application Notes

The functional requirement FCS_RNG.1 is a refinement of the FCS_RNG.1 defined in the Protection Profile [1] according to “Anwendungshinweise und Interpretationen zum Schema (AIS)” [6].

4 Security Problem Definition (ASE_SPD)

The content of [1] applies to this chapter completely.

4.1 Threats

The threats are directed against the assets and/or the security functions of the TOE. For example, certain attacks are only one step towards a disclosure of assets while others may directly lead to a compromise of the application security. The more detailed description of specific attacks is given later on in the process of evaluation and certification. An overview on attacks is given in PP [1] section 3.2.

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

Table 4 Threats according to [1]

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

4.1.1 Additional Threat due to TOE specific Functionality

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

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

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

T.Mem-Access Memory Access Violation

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

Table 5 Additional threats due to TOE specific functions and augmentations

T.Mem-Access	Memory Access Violation

4.1.2 Assets regarding the Threats

The asset description from PP [1] section 3.1 applies.

4.2 Organizational Security Policies

The organizational policy from [1] section 3.3 and section 7.3.1 is applicable.

Table 6 Organizational Security Policies according PP [1]

P.Process-TOE	Protection during TOE Development and Production
P.Lim_Block_Loader	Limiting and Blocking the Loader Functionality
P.Crypto-Service	Cryptographic services of the TOE

Note: The TOE can be delivered with or without the SCL. If the user decides not to use the SCL, P.Crypto-Service is not an organizational policy of this TOE.

4.3 Assumptions

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

Table 7 Table 1: Assumption according PP [1]

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

5 Security objectives (ASE_OBJ)

This section shows the security objectives, which are relevant to the TOE.

5.1 Security objectives of the TOE

The security objectives of the TOE are defined and described in PP [1] sections 4.1, 7.3.1, 7.4.1 and 7.4.2.

Table 8 Objectives for the TOE according to PP [1]

O.Phys-Manipulation	Protection against Physical Manipulation
O.Phys-Probing	Protection against Physical Probing
O.Malfunction	Protection against Malfunction
O.Leak-Inherent	Protection against Inherent Information Leakage
O.Leak-Forced	Protection against Forced Information Leakage
O.Abuse-Func	Protection against Abuse of Functionality
O.Identification	TOE Identification
O.RND	Random Numbers
O.Cap_Avail_Loader	Capability and availability of the Loader
O.TDES	Cryptographic service Triple-DES
O.AES	Cryptographic service AES

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.

Note: The TOE can be delivered with or without the SCL. If the user decides not to use the SCL, O.TDES and O.AES are no objectives of the TOE.

Table 9 Additional objectives due to TOE specific functions and augmentations

O.Mem-Access	Area based Memory Access Control

5.2 Security Objectives for the development and operational Environment

The security objectives from [1] section 4.2, 4.3 and 7.3.1 are applicable for this TOE.

The table below lists the environmental security objectives.

Table 10 Security objectives for the environment according to [1]

OE.Resp-Appl	Treatment of User Data
OE.Process-Sec-IC	Protection during composite product manufacturing
OE.Lim_Block_Loader	Limitation of capability and blocking the Loader

5.3 Security Objectives Rationale

The security objectives rationale of the TOE is defined and described in PP [1] section 4.4, 7.3.1, 7.4.1 and section 7.4.2

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

The objective O.Cap_Avail_Loader and the organizational policy P.Lim_Block_Loader as described in [1] chapter 7.3.1 apply only to TOE products with Flash Loader enabled for software or data download by the user. In other cases the Flash Loader is not available anymore and the user software or data download is completed.

6 Extended Component Definition (ASE_ECD)

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

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

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

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.

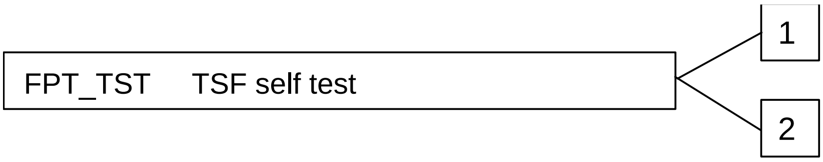
This security functional component is used instead of the functional component FPT_TST.1 from Common Criteria Part 2. For the user it is important to know which security functions or mechanisms can be tested. The functional component FPT_TST.1 does not mandate to explicitly specify the security functions 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 follows (Common Criteria Part 2 extended).

6.3 TSF self test (FPT_TST)

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

Component levelling



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

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

Management: FPT_TST.2

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

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

Audit: FPT_TST.2

There are no auditable events foreseen.

FPT_TST.2 Subset TOE testing

Hierarchical to: No other components.

Dependencies: No dependencies

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

7 Security Requirements (ASE_REQ)

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

7.1 TOE Security Functional Requirements

The security functional requirements (SFR) for the TOE are defined and described in [1] section 6.1 and in the following description.

Table 11 provides an overview of the functional security requirements of the TOE, defined in [1] section 6.1.

Table 11 Security functional requirements of the TOE defined in PP [1]

Security Functional Requirement	
FRU_FLT.2	“Limited fault tolerance“
FPT_FLS.1	“Failure with preservation of secure state”
FMT_LIM.1	“Limited capabilities”
FMT_LIM.2	“Limited availability”
FAU_SAS.1	“Audit storage”
FDP_SDC.1	“Stored data confidentiality
FDP_SDI.2	“Stored data integrity monitoring and action”
FPT_PHP.3	“Resistance to physical attack”
FDP_ITT.1	“Basic internal transfer protection”
FPT_ITT.1	“Basic internal TSF data transfer protection
FDP_IFC.1	“Subset information flow control”
FCS_RNG.1	“Random number generation”
FCS_COP.1/TDES	“Cryptographic operation - TDES”
FCS_CKM.4/TDES	“Cryptographic key desctruction”
FCS_COP.1/AES	“Cryptographic operation - AES”
FCS_CKM.4/AES	“Cryptographic key desctruction”
FMT_LIM.1/Loader	“Limited capabilities”
FMT_LIM.2/Loader	“Limited availability”

Note: The TOE can be delivered with or without the SCL. If the user decides not to use the SCL, the TOE does not claim the SFRs FCS_COP.1/TDES, FCS_CKM.4/TDES FCS_COP.1/AES and FCS_CKM.4/AES.

Table 12 provides an overview about security functional requirements, which are added to the TOE. All requirements are taken from [3] Part 2, with the exception of requirement FPT_TST.2, which is defined in this ST completely.

Table 12 Additional security functional requirements of the TOE

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”

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

The above marked extended components FMT_LIM.1 and FMT_LIM.2 are introduced in [1] 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 [3]. 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 Definition required by [1]

According to [1] Application Note 14 the term “secure state” used by FPT_FLS.1 shall be described and a definition should be provided.

Definition of secure state:

Secure state describes three different conditions of the TOE:

1. the controller ceases operation. This condition can only be resolved by a cold or warm start of the controller. It is triggered by a security reset.
2. the controller enters a security trap. The trap handler can be defined by the user. In case no trap handler is provided the first condition is entered.
3. in case of a sudden power loss of the TOE during EEPROM programming (tearing): the TOE is in a condition to either restore the old EEPROM content or to start with the new programmed value.

Note: a security reset invalidates the RAM content.

According to [1] Application Note 15, *“The Common Criteria suggest that the TOE generates audit data for the security functional requirements Limited fault tolerance (FRU_FLT.2) and Failure with preservation of secure state (FPT_FLS.1).”* In case of the first two conditions no Audit data are collected, because the effect entering the secure state is immediately visible. For the third condition indirect audit data is available, i.e. the user can check, whether new or old NVM data is available.

7.1.2 Extended Components FCS_RNG.1 and FAU_SAS.1

7.1.2.1 FCS_RNG

To define the IT security functional requirements of the TOE an additional family (FCS_RNG) of the Class FCS (cryptographic support) is defined in [1]. 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 [6]
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 [6] does not distinguish the internal random numbers from output sequences of an ideal RNG.

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

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

7.1.2.2 FAU_SAS

The PP [12] defines additional security functional requirements with the family FAU_SAS of the class FAU (Security Audit). This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

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

FAU_SAS.1 Audit Storage

Hierarchical to: No 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.*

7.1.3 Subset of TOE testing

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

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

FPT_TST.2 Subset TOE testing

Hierarchical to: No other components.

Dependencies: No dependencies

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

- *CORE – CPU related alarms*
- *Temperature alarm*
- *Memory Bus*

- *NVM_MISS – SOLID FLASH™ memory illegal addressing alarm*
- *FSE – Internal Frequency Sensor alarm*
- *Light – Light sensitive alarm*
- *WDT - Watch Dog Timer related alarms*
- *SW – Software triggered alarm*
- *TRNG – True Random Number Generator*
- *Glitch sensor alarm*
- *Backside light detection (BLD) - alarm*
- *RAM/ROM EDC or SOLID FLASH™ memory ECC*

7.1.4 Memory access control

Usage of multiple applications in one Smartcard often requires code and data separation in order to prevent one application from accessing 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 [7].

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

The security functional requirement "Static attribute 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.

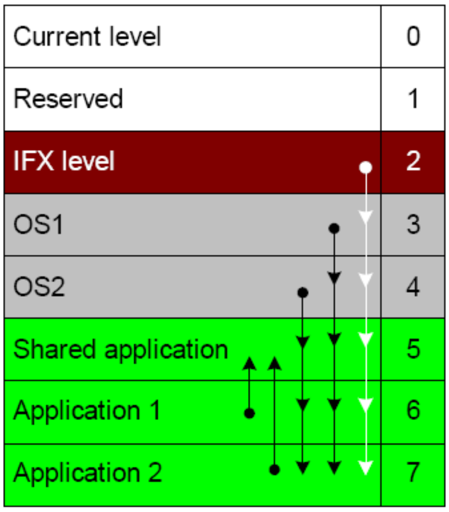
The following Security Function Policy (SFP) Memory Access Control Policy is defined for the requirement "Security attribute based access control (FDP_ACF.1)":

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. These levels are referred to as the Infineon Technologies (IFX) level, operating system 1 and 2 levels (OS1, OS2), shared application level, and application 1 and 2 levels. A pseudo-level is the "current" level, which is simply the level on which code is currently being executed. The access rights are controlled by the MMU and related to the privilege level as depicted in following diagram:

Figure 2 Privilege Levels of the TOE



Current level	0
Reserved	1
IFX level	2
OS1	3
OS2	4
Shared application	5
Application 1	6
Application 2	7

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 utilised by the subject attempting to perform the operation.

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

none.

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

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the *Memory Access Control Policy* to provide *well defined*[1] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow *any subject, provided that the Memory Access Control Policy is enforced and the necessary access is therefore allowed2,* to specify alternative initial values to override the default values when an object or information is created.

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

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

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

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

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components

Dependencies: No dependencies

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

[1] The static definition of the access rules is documented in [7]

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

7.1.6 Support of Cipher Schemes

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

FCS_COP.1 Cryptographic operation requires a cryptographic operation to be performed in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard; dependencies are discussed in Section 7.4.1.1.

The TOE implements the packages "TDES" and "AES" from [1].

Preface regarding Security Level related to Cryptography

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 functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102', **www.bsi.bund.de**.

Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context).

Table 13 TOE cryptographic functionality

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
Cryptographic Primitive	TDES	[19]	|k| = 112 in operating modes ECB, CBC, CBC-MAC	No
	TDES	[19]	|k| = 168 in operating modes: CBC, CBC-MAC	Yes
	TDES	[19]	|k| = 168 in operating mode ECB	No
	AES	[20]	|k| = 128, 192, 256 in operating modes CBC, CBC-MAC	Yes
	AES	[20]	|k| = 128, 192, 256 in operating mode ECB	No
	Physical True RNG PTG.2	[6]	N/A	N/A

Triple-DES Operation:

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

FCS_COP.1/TDES Cryptographic operation

Hierarchical to: No other components.

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

FCS_COP.1.1/TDES The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm *TDES* in *the Electronic Codebook Mode (ECB), Cipher Block Chaining Mode (CBC), Cipher Block Chaining Mode (CBC-MAC)*, and cryptographic key sizes of *112 bit and 168 bit* that meet the following standards:

- *TDES:*
  National Institute of Standards and Technology (NIST) SP 800-67 Rev. 1 [19]
- *ECB, CBC:*
  National Institute of Standards and Technology (NIST) SP 800-38A [20]
- *CBC-MAC:*
  ISO/IEC 9797-1 Mac Algorithm 1 [22]

The TDES cryptographic key destruction of the TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below.

FCS_CKM.4/TDES Cryptographic key destruction

Hierarchical to: No other components.

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

FCS_CKM.4.1/TDES The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *Invalidation of RAM encryption key during cold reset* that meets the following:

None

Application Note: This is the same effect as erasing the key with random values

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 to a specified cryptographic algorithm *Advanced Encryption Standard (AES)* in *Electronic Codebook Mode (ECB), Cipher Block Chaining Mode (CBC), Cipher Block Chaining Mode (CBC-MAC)*, and cryptographic key sizes of 128 bit, 192 bit and 256 bit that meet the following standards:

- *AES:*
  NIST FIPS PUB 197 [21]
- *ECB, CBC:*
  National Institute of Standards and Technology (NIST) SP 800-38A [20]
- *CBC-MAC:*
  ISO/IEC 9797-1 Mac Algorithm 1 [22]

The AES cryptographic key destruction of the TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below.

FCS_CKM.4/AES Cryptographic key destruction

Hierarchical to: No other components.

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

FCS_CKM.4.1/AES The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction *method Invalidation of RAM encryption key during cold reset* that meets the following:

None

Application Note: This is the same effect as erasing the key with random values

7.1.7 Data Integrity

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

FDP_SDI.2 **Stored data integrity monitoring and action**

Hierarchical to: FDP_SDI.1 stored data integrity monitoring

Dependencies: No dependencies

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for *data integrity and one-and/or more-bit-errors* on all objects, based on the following attributes: *corresponding EDC value for ROM and RAM, smart parity for Cache and error correction ECC for the SOLID FLASH™ NVM.*

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

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

FDP_SDC.1 **Stored data confidentiality**

Hierarchical to: No other components

Dependencies: No dependencies

FDP_SDC.1 The TSF shall ensure the confidentiality of the information of the user data while it is stored in the *RAM and SOLID FLASH™ NVM*

7.2 Support of the Flash Loader

The usage of the Flash Loader is only allowed in secured environment during the production phase. For this reason the TOE shall meet the requirements “Limited capabilities (FMT_LIM.1/Loader)” as specified below:

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

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

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

The security functional requirements FMT_LIM.1/Loader and FMT_LIM.2/Loader apply only to TOE products with Flash Loader enabled for software or data download by the user. In other cases the Flash Loader is not available anymore and the user software or data download is completed.

7.3 TOE Security Assurance Requirements

The evaluation assurance level is EAL 5 augmented with ALC_DVS.2 and AVA_VAN.5. In the following table, the security assurance requirements are given. The augmentation of the assurance components compared to [1] is expressed with bold letters.

Table 14 Assurance components

Aspect	Acronym	Description	Refinement
Development	ADV_ARC.1	Security Architecture Description	[1]
	ADV_FSP.5	Complete semi-formal functional specification with additional error information	[1]
	ADV_IMP.1	Implementation representation of the TSF	[1]
	ADV_INT.2	Well-structured internals	
	ADV_TDS.4	Semi-formal modular design	
Guidance Documents	AGD_OPE.1	Operational user guidance	[1]
	AGD_PRE.1	Preparative procedures	[1]
Life-Cycle Support	ALC_CMC.4	Production support, acceptance procedures and automation	[1]
	ALC_CMS.5	Development tools CM coverage	[1]
	ALC_DEL.1	Delivery procedures	[1]
	ALC_DVS.2	Sufficiency of security measures	[1]
	ALC_LCD.1	Developer defined life-cycle model	

Aspect	Acronym	Description	Refinement
	ALC_TAT.2	Compliance with implementation standards	
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.2	Analysis of coverage	[1]
	ATE_DPT.3	Testing: modular design	
	ATE_FUN.1	Functional testing	
	ATE_IND.2	Independent testing - sample	
Vulnerability Assessment	AVA_VAN.5	Advanced methodical vulnerability analysis	[1]

7.3.1 Refinements

Some refinements are taken unchanged from [1]. Table 14 provides an overview.

Two refinements from [1] have to be discussed here in the Security Target, as the assurance level is increased.

7.3.1.1 Life cycle support (ALC_CMS)

The refinement from [1] can also be applied to the assurance level EAL 5 augmented with ALC_CMS.5. The assurance package ALC_CMS.4 is extended to ALC_CMS.5 with aspects regarding the configuration control system for the TOE. The refinement is still valid.

7.3.1.2 Functional Specification (ADV_FSP)

The refinement from [1] can also be applied to the assurance level EAL 5 augmented with ADV_FSP.5. The assurance package ADV_FSP.4 is extended to ADV_FSP.5 with aspects regarding the level of description. ADV_FSP.5 requires a semi-formal description in addition. The refinement is still valid.

For refinement details see [1].

7.4 Security Requirements Rationale

7.4.1 Rationale for the Security Functional Requirements

While the security functional requirements rationale of the TOE are defined and described in PP [12] section 6.3.1, section 7.3.1, section 7.4.1 and section 7.4.2, the additional introduced SFRs are discussed below:

Table 15 Rational for additional SFR in the ST

Objective	TOE Security Functional Requirements
O.Phys-Manipulation	- FPT_TST.2 „ Subset TOE security testing “
O.Mem-Access	- FDP_ACC.1 “Subset access control” - FDP_ACF.1 “Security attribute based access control” - FMT_MSA.3 “Static attribute initialisation” - FMT_MSA.1 “Management of security attributes”

Objective	TOE Security Functional Requirements
	- FMT_SMF.1 “Specification of Management Functions”

The table above gives an overview, how the security functional requirements are combined to meet the security objectives (this table has to be read in addition to [1] table 2 “Security Requirements versus Security Objectives”. The detailed justification is given in the following:

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 security functional requirement FPT_TST.2 detects attempts to conduce a physical manipulation on the monitoring functions of the TOE. The objective of FPT_TST.2 is O.Phys-Manipulation.

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

The justification of the security objective and the additional requirements show that they do not contradict the rationale already given in [1] for the assumptions, policy and threats defined there. Moreover, these additional security functional requirements cover the requirements by [3] user data protection of chapter 11 which are not refined by [1].

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

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

7.4.1.1 Dependencies of Security Functional Requirements

The dependencies of security functional requirements are defined and described in [1] section 6.3.2, section 7.4.1 and section 7.4.2 for the following security functional requirements: FDP_SDC.1, FDP_SDI.2, FDP_ITT.1, FDP_IFC.1, FPT_ITT.1, FPT_PHP.3, FPT_FLS.1, FRU_FLT.2, FMT_LIM.1, FMT_LIM.2, FCS_RNG.1. FAU_SAS.1,FMT_LIM.1/Loader and FMT_LIM.2/Loader.

The dependencies of the additional security functional requirements (the functional requirements in addition to the ones defined in [1]) are analysed in the following description.

Table 16 Dependency for cryptographic operation requirement

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FPT_TST.2	None	n.a.
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Yes Yes
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes Not required, see comment 1
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes see comment 1 Yes
FMT_SMF.1	None	N/A
FCS_COP.1/TDES and FCS_COP/AES	FCS_CKM.4	Fulfilled by [1]

Security Functional Requirement	Dependencies	Fulfilled by security requirements
	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	No, see comment 2
FCS_CKM.4/TDES and FCS_CKM.4/AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	No, see comment 2

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

Comment 2:
The security functional requirement "Cryptographic operation (FCS_COP.1/TDES and FCS_COP.1/AES)" 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.

For the security functional requirement FCS_COP.1/TDES and FCS_COP.1/AES the respective dependencies FCS_CKM.1 and FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.4 have to be fulfilled by the environment. That means, that the environment shall meet the requirement FCS_CKM.1 as defined in [3], section 10.1 and shall additionally meet the requirements FDP_ITC.1 or FDP_ITC.2 as defined in [3], section 11.7.

7.4.2 Rationale of the Assurance Requirements

The chosen assurance level EAL5 and the augmentation with the requirements ALC_DVS.2 and AVA_VAN.5 were chosen in order to meet the assurance expectations explained in the following paragraphs. In Table 14 the different assurance levels are shown as well as the augmentations. The augmentations are in compliance with the Protection Profile.

An assurance level EAL5 with the augmentations ALC_DVS.2 and AVA_VAN.5 are required for this type of TOE since it is intended to defend against highly sophisticated attacks without protective environment. This evaluation assurance package was selected to permit a developer to gain maximum assurance from positive security engineering based on good commercial practices. In order to provide a meaningful level of assurance that the TOE provides an adequate level of defence against such attacks, the evaluators should 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 [11] shall be taken as a basis for the vulnerability analysis of the TOE.

ALC_DVS.2 Sufficiency of security measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE.

In the particular case of a Security IC the TOE is developed and produced within a complex and distributed industrial process which must especially be protected. Details about the implementation, (e.g. from design, test and development tools as well as Initialization Data) may make such attacks easier. Therefore, in the case of a Security IC, maintaining the confidentiality of the design is very important.

This assurance component is a higher hierarchical component to EAL5 (which only requires ALC_DVS.1). ALC_DVS.2 has no dependencies.

AVA_VAN.5 Advanced methodical vulnerability analysis

Due to the intended use of the TOE, it must be shown to be highly resistant to penetration attacks. This assurance requirement is achieved by AVA_VAN.5.

Independent vulnerability analysis is based on highly detailed technical information. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing high attack potential.

AVA_VAN.5 has dependencies to ADV_ARC.1 “Security architecture description”, ADV_FSP.2 “Security enforcing functional specification”, ADV_TDS.3 “Basic modular design”, ADV_IMP.1 “Implementation representation of the TSF”, AGD_OPE.1 “Operational user guidance”, and AGD_PRE.1 “Preparative procedures”.

All these dependencies are satisfied by EAL5.

It has to be assumed that attackers with high attack potential try to attack Security ICs like smartcards used for digital signature applications or payment systems. Therefore, specifically AVA_VAN.5 was chosen in order to assure that even these attackers cannot successfully attack the TOE.

8 TOE Summary Specification (ASE_TSS)

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

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

Table 17 TOE Security Features

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 into several phases. Different operation modes help to protect the TOE during each phase of its lifecycle.

8.2 SF_PS: Protection against Snooping

The TOE uses various means to protect from snooping of memories and busses and prevents single stepping.

8.3 SF_PMA: Protection against Modifying Attacks

This TOE implements protection against modifying attacks of memories, alarm lines and sensors.

8.4 SF_PLA: Protection against Logical Attacks

Memory access of the TOE is controlled by a Memory Management Unit (MMU), which implements different priviledge levels. The MMU decides, whether access to a physical memory location is allowed based on the access rights of the privilege levels.

8.5 SF_CS: Cryptographic Support

The TOE is equipped with a hardware accelerator and symmetric cryptographic library (SCL) to support the standard symmetric cryptographic operations TDES and AES. Key destruction is performed during cold reset by invalidation of the RAM encryption key. It further provides random numbers to meet FCS_RNG.1

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 the sections above. The results are shown in Table 18. The security functional requirements are addressed by at least one related security feature.

Table 18 Mapping of SFR and SF

SFR	SF_DPM	SF_PS	SF_PMA	SF_PLA	SF_CS
FAU_SAS.1	X				
FMT_LIM.1/Loader	X				
FMT_LIM.2/Loader	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.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
FDP_SDC.1		X			
FPT_TST.2			X		X
FPT_FLS.1		X	X	X	X
FCS_RNG.1					X
FCS_COP.1/TDES					X
FCS_CKM.4/TDES					X
FCS_COP.1/AES					X
FCS_CKM.4/AES					X

8.7 Security Requirements are internally Consistent

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

The functional requirement FPT_TST.2 requires further protection to prevent manipulation of test results, while checking the security functions of the TOE. An attacker could aim to switch off or disturb certain sensors or filters and prevent the detection of distortion 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.

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

9 References

9.1 Literature

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

[2] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model; Version 3.1 Revision 4 September 2012, CCMB-2012-09-001

[3] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements; Version 3.1 Revision 4 September 2012, CCMB-2012-09-002

[4] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements; Version 3.1 Revision 4 September 2012, CCMB-2012-09-003

[5] Status report, List of all available user guidance

[6] Functionality classes and evaluation methodology for physical random number generators AIS31, Version 3.0, 05.15.2013

[7] M5074 SOLID FLASH™ Controller Family for Security Applications, Hardware Reference Manual

[11] Joint Interpretation Library, Application of Attack Potential to Smartcards, Version 2.9, January 2013

[12] SLE77 Controller Family, Solid Flash™ Controller for Security Applications, Errata Sheet

[13] SLE 70 Controller Family Programmer’s Reference Manual

[18] SLx 70 Family Production and Personalization User's Manual

[19] NIST SP 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, revised January 2012, National Institute of Standards and Technology

[20] NIST SP 800-38A Recommendation for Block Cipher Modes of Operation, 2001, with Addendum Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode, October 2010

[21] Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001

[22] International Standard ISO/IEC 9797-1, Information Technology – Security Techniques – Message Authentication Codes (MACs), 2011-03-01

Note that the versions of these documents are listed in the certification report.

10 Appendix: hash signatures of the SCL

```
Scl77P-uSCP-v2-LIB-base-XSMALL-HUGE.lib:
MD5=3ae3a6389d39fcfd4b90f93c0d6eaf66
SHA1=079a990ed2618eaac540f157f633a8449d879d7a
SHA256=4876ceaceb2061871419a062e389ce57b5b9f5d7a701ed9515d59c4d2b43f55a

Scl77P-uSCP-v2-LIB-des-XSMALL-HUGE.lib:
MD5=fe9351112867e50bcde36aca75dc79dc
SHA1=76e5cdda578a5f9351c72cfc5c59a8a4bab28bf0
SHA256=758bac50c7a28924a894b52910dc67560fc7896825a137d77ce56eb2909e24a6

Scl77P-uSCP-v2-LIB-aes-XSMALL-HUGE.lib:
MD5=0719593879f718f5782cc1ce20dbaa72
SHA1=c08965506f8d964dd516c75e108d6a92ba4ee233
SHA256=c562f9f42569fbb9d3e61683903ebe45be44b124720e5f95a0f3539731daab48
```

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
ATR	Answer to Reset
CC	Common Criteria
CI	Chip Identification Mode (STS-CI)
GCIM	Generic Chip Identification Mode
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
Crypto2304T	Asymmetric Cryptographic Processor
DPA	Differential Power Analysis
DFA	Differential Failure Analysis
ECC	Error Correction Code
EDC	Error Detection Code
EMA	Electro magnetic analysis
Flash	Flash Memory
HSD	Hot Spot Distribution
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
MED	Memory Encryption and Decryption
MMU	Memory Management Unit
O	Object
OS	Operating system
PEC	Peripheral Event Channel
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
RMS	Resource Management System
RNG	Random Number Generator
ROM	Read Only Memory
SAM	Service Algorithm Minimal
SCP	Symmetric Cryptographic Processor
TSC	TOE Security Functions Control
TSF	TOE Security Functionality
UART	Universal Asynchronous Receiver/Transmitter
UM	User Mode (STS)
UMSLC	User mode Security Life Control
WDT	Watch Dog Timer

TDES	Triple DES Encryption Standard

12 Glossary

Application Program/Data	Software which implements the actual TOE functionality provided for the user or the data required for that purpose
Central Processing Unit	Logic circuitry for digital information processing
Chip Identification Data	Data to identify the TOE
Generic 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
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 NVM programming routines, AIS31 testbench etc.
Self Test Software	Part of the firmware with routines for controlling the operating state and testing the TOE hardware
Security Function	Part(s) of the TOE used to implement part(s) of the security objectives
Security Target	Description of the intended state for countering threats
SmartCard	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

www.infineon.com

Published by Infineon Technologies AG