Security Target Lite

M9905 with optional ACL Software Libraries

According to Common Criteria CCEAL5 augmented (EAL5+)

Version: 6.2

Date: 2025-07-18

Table of Content

1 Security Target Introduction (ASE_INT)

1.1 Security Target and Target of Evaluation Reference

The title of this document is: Security Target Lite M9905 with optional ACL Software Libraries

The name of the TOE on the CC certificate is:
“Infineon Technologies Security Controller M9905 A11 with optional ACL v2.07.003 and v2.09.002”

The Target of Evaluation (TOE) comprises the Infineon Technologies Smart Card IC (Security Controller) M9905 A11 with optional ACL v2.07.003 and v2.09.002

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

The ST built in compliance to CC:2022.

Table 1 Identification

Type	Version	Date	Title/Registration/Explainantion
Security Target Method of identification is done by version, date and title			
Security Target	6.2	2025-07-18	Security Target Lite M9905 with optional ACL Software Libraries
TOE Hardware Method of identification is done by reading of GCIM			
M9905	A11		M9905 with Firmware Identifier 80001151
Libraries (optional) Method of identification is done by hash values			
NRG Management	01.03.0927		Management of NRG cards
NRG Reader	01.02.0800		NRG reader mode support
ACL	2.07.003		Cl97-LIB-base.lib Cl97-LIB-ecc.lib
	2.09.002		ACL97-Crypto2304T-L90-base.lib ACL97-Crypto2304T-L90-ecc.lib
Hardware Guidance Documentation Method of identification is done by version, date and title			
General Guidance	Revision 3.0	2019-08-28	32-bit Security Controller M9900 Hardware Reference Manual
	Edition 2020-04-15 Update 2025-06-06	2020-04-15	M9900 Security Guidelines User´s Manual

Type	Version	Date	Title/Registration/Explainantion
	DDI 0403E.e	2021	ARMv7-M Architecture Reference Manual, ARM DDI ARM DDI 0403E.e N (ID021621), ARM Limited, 2021
	5.9	2024-11-25	SLE97 security controllers Programmer's Reference Manual SLCx7_DFP Document release reference: Z8F80731571-A
	Edition 2014-08-10a	2014-08-10	SLE97 / SLC14 Family Production and Personalization User´s Manual
M9905 Guidance	3.1	2019-09-05	M9905 M9906 Errata Sheet
Library Guidance Documentation (optional) Method of identification is done by version, date and title			
ACL Guidance	2.07.003	2024-08-26	CL97 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox, User Interface
	2.09.002	2024-06-27	ACL97-Crypto2304T-L90 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox, User interface manual
CC documents Method of indentification is done by version, date and title			
PP	1.0	2007-06-15	Security IC Platform Protection Profile BSI-PP-0035 The cert-id BSI-CC-PP-0035-2007 refers to the corresponding certification report.
CC	CC:2022 Revision 1	2022-11	Security Evaluation Part 1: CCMB-2022-11-001 Part 2: CCMB-2022-11-002 Part 3: CCMB-2022-11-003 Part 4: CCMB-2022-11-004 Part 5: CCMB-2022-11-005

The TOE can be identified with the Generic Chip Identification Mode (GCIM). The M-number hardware is identified by the bytes 05 and 06, which are the first two bytes of the chip identification number, having for the M9905 the value 0x0010. The design step, firmware identifier, mask identifier, temperature range and system frequency are also included in the GCIM. Additionally the customer can read the configuration area as defined in the SLE97 Programmer´s Reference Manual [11].

1.2 Target of Evaluation overview

The TOE comprises the Infineon Technologies AG security controller M9905 with optional ACL Software Libraries .

The Toolbox libraries are additionally supporting software which is out of scope of this certification.

The Toolbox libraries do not provide cryptographic support or additional security functionality as they provide 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 TOE is a member of the Infineon Technologies AG security controller family SLE97 meeting high requirements in terms of performance and security. The SLE97 family has been developed with a modular concept and different memory configurations, sets of peripherals and interfaces as well as different security features to satisfy market requirements. A summary product description is given in this Security Target (ST).

The TOE offers all functions that are both required and useful in security systems, and integrated peripherals that are typically needed in chipcard applications, such as information security, identification, access control, GSM and UMTS projects, electronic banking, digital signature and multi-application cards, ID cards, transportation and e-purse applications.

The TOE implements a dedicated security 32-bit RISC CPU designed on the basis of the ARMv7M architecture designed in 90 nm CMOS technology. The integrated peripherals combine enhanced performance and optimized power consumption for a minimized die size to make the SLE97 controllers ideal for chipcard applications. The TOE offers a wide range of peripherals, including a UART (using the ISO interface), four timers, two watchdogs, a CRC module, a true RNG (TRNG), coprocessors for symmetric (e.g. DES, AES) and asymmetric (e.g. EC) cryptographic algorithms. Additionally, a range of communication interfaces, such as GPIO, I2C, SWP, USB, SSC/SPI and NRG interface are offered to provide maximum flexibility in terms of simultaneous communication ability.

The TOE provides a real 32-bit CPU-architecture and is compatible to the ARMv7-M instruction set architecture. The major components of the core system are the 32-bit CPU as a variant of the ARM Secure Core SC300, the Cache system, the Memory Protection Unit and the Memory Encryption/Decryption Unit. The TOE implements a full 32-bit addressing with up to 4 GByte linear addressable memory space, a simple scalable memory management concept and a scalable stack size. The flexible memory concept is built on the non volatile memory, respectively SOLID FLASH™ NVM[1]. For the SOLID FLASH™ NVM the Unified Channel Programming (UCP) memory technology is used.

The TOE provides the low-level firmware components Boot Software (BOS) and Resource Management System (RMS) and the high-level firmware Flash Loader (FL) and NRG software.

The NRG software includes the NRG operating system and additionally the optional library Management of NRG cards (version 01.03.0927) and the optional library NRG Reader Mode Support (01.02.0800). The Management of NRG cards provides an API for the management and generation of NRG cards. The optional NRG reader mode support library (01.02.0800) enables an access to external NRG cards.

NRG software is not part of the TSF and does not implement any Security Functional Requirement.

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

The RMS firmware providing some functionality via an API to the Smartcard Embedded Software contains for example SOLID FLASH™ NVM service routines and functionality for the tearing save write into the SOLID FLASH™ NVM. The BOS firmware is used for test purposes during start-up and the FL allows downloading of user software to the NVM during the manufacturing process. The BOS is implemented in a separate Test-ROM being part of the TOE. The BOS executes the UMSLC test during the startup phase. It also includes the features "hardening" and the "Burn-In Test". The feature "hardening" analyzing a random SOLID FLASH™ NVM page after every regular program operation for written bits that are losing their charge, and, in this very unlikely case, the page is rewritten. The "Burn-In Test" during production is used to stress the chip in a high temperature, high internal voltage and active operation for a certain time and filtering out defect parts to get a low failure rate. The M9905 is qualified for an extended temperature range from -40°C to +105°C.

The two cryptographic co-processors serve the need of modern cryptography: The symmetric co-processor (SCP) combines both AES and Triple-DES with dual-key or triple-key hardware acceleration. The Asymmetric Crypto Co-processor, called Crypto2304T in the following, supports Elliptic Curve (EC) cryptography with high performance.

A True Random Number Generator (TRNG) specially designed for smart card applications is implemented. The TRNG fulfils the requirements from the functionality class PTG.2 of the AIS31 and produces genuine random numbers which then can be used internally or by the user software.

The software part of the TOE consists of the cryptographic libraries for EC and asymmetric the Base libraries. If an EC library is part of the shipment, the corresponding asymmetric Base library is automatically included.

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 cerification, ECDSA key generation and Elliptic Curve Diffie-Hellman key agreement. The EC library is delivered as object code. The certification covers the standard NIST [DSS] and Brainpool [ECC] Elliptic Curves with key lengths of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 Bits. 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.

The asymmetric Base library provides the low-level interface to the asymmetric cryptographic coprocessor and has no user available interface. The asymmetric Base library does not provide any security functionality, implements no security mechanisms and does not contribute to a security functional requirement.

To fulfill the high security standards for smartcards today and also in the future, this TOE utilizes an integral security concept comprising countermeasure mechanisms specially designed against possible attack scenarios. The TOE provides a robust set of sensors for the purpose of monitoring proper chip operating conditions and detecting fault attack scenarios. The sensors are complemented with digital error detection mechanisms such as parities, error detection codes and instruction stream signatures. Probing and forcing attacks will be counteracted by the security optimized wiring approach, implemented by an Infineon-specific shielding combined with secure wiring of security critical signals, partly masking of security critical signals and by encryption of all memories inside the chip (RAM, ROM, NVM). A decentralized alarm propagation and system deactivation principle is implemented, further decreasing the risk of manipulating and tampering. Additionally, an online check of the security mechanisms is available by using the User Mode Security Life Control (UMSLC). Side-channel attacks (e.g. Timing Attack, SPA, DPA, EMA) are typically defeated using a combination of hardware and software mechanisms, for this the TOE provides several supporting features e.g. trash register writes and instruction interrupt prevention. The Instruction Stream Signature Checking (ISS) is a powerful countermeasure against fault attacks that try to manipulate the execution sequence of the instruction stream. All executed instructions are hashed in the CPUs signature register and the hardware automatically checks the fitting of the values.

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

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

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

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.
A shielding algorithm finishes the upper layers above security critical signals and wires, finally providing the so called “security optimized wiring”.
The TOE with its integrated security features meets the requirements of all smart card applications such as information integrity, access control, mobile telephone and identification, as well as uses in electronic funds transfer and healthcare systems.
To sum up, the TOE is a powerful smart card IC with a large amount of memory and special peripheral devices with improved performance, optimized power consumption, at minimal chip size while implementing high security.

2 Target of Evaluation Introduction

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 [PP] as it belongs to the specific TOE.

2.1 Definition of the TOE

The TOE comprises three parts:

- Hardware of the smart card security controller including all configurations and derivatives
- Associated firmware, software and optional software
- Guidance Documents.

The hardware configuration options and configuration methods are described in the chapters 1.1 and 2.9. The second part of this TOE includes the associated firmware and software required for operation. The TOE can be delivered in various configurations, achieved by means of blocking and depending on the customer order.

The documents as described in section 2.6 and listed in Table 1, are supplied as user guidance. 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. The Smartcard Embedded Software respectively user software is not part of the TOE. 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 blocking of the involved firmware respectively software parts, used at Infineon Technologies AG 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.
One or more additional metal layer may be added on top of one of the TOE mask sets. These additional metal layer(s) just reroute the pads. Therefore, this last rerouting on top does not change the function of the TOE itself; it depends on the package only, and is not relevant for the security of the TOE. For these reasons, the metal layers are out of the scope of the certification and do not belong to the TOE. Of course, in all cases passivation and isolation coating is applied on top of the last layers carrying wires.

A shielding algorithm finishes the upper layers above security critical signals and wires, finally providing the so called “security optimized wiring”.

The firmware used for the TOE internal testing and TOE operation and the cryptographic EC and base libraries are part of the TOE and therefore part of the certification. The documents as described in chapter 2.6 are supplied as user guidance. BPU functionality is part of the TOE but is not in the certification scope.

The term Smartcard Embedded Software is used in the following for all operating systems and applications stored and executed on the TOE. The TOE is the platform for the Smartcard Embedded Software. The Smartcard Embedded Software itself is not part of the TOE. The TOE does not require any non-TOE hardware/software/firmware.

2.1.1 Major security functions of the TOE

The major security functions of the TOE are:

- Memory Protection Unit
- Memory Encryption/Decryption Unit
- Sensors for the purpose of monitoring proper chip operating conditions and detecting fault attack scenarios complemented with digital error detection mechanisms such as parities, error detection codes and instruction stream signatures
- Security optimized wiring for protection of security critical signals
- Instruction Stream Signature Checking (ISS) as a countermeasure against fault attacks that try to manipulate the execution sequence of the instruction stream
- Symmetric cryptographic coprocessor supporting AES and 3DES
- Crypto2304T, an asymmetric crypto coprocessor together with the libraries supporting EC (optional)
- Cryptographic libraries for EC computations (optional)
- A true random number generator, which can be used as a security service to the user and for internal purposes
-

2.1.2 Not part of the TOE Security Functionality

Not part of the certification are

- the Smartcard Embedded Software respectively user software (not part of the TOE),
- the piece of software running at user premises and collecting the BPU receipts coming from the TOE. This BPU software part is the commercially deemed part of the BPU software, not running on the TOE, but allowing refunding the customer, based on the collected user blocking information. The receipt from each blocked TOE is collected by this software – chip by chip.

Not part of the TSF are

- The NRG software
- The CRC module
- The parts Toolbox and RSA of the ACL libraries
- All other delivered libraries which do not have a security claim in this ST.

2.2 Hardware of the TOE

The hardware part of the TOE (see Figure 2) as defined in [PP] is comprised of:

Core System

- 32-bit CPU implementation of ARM Secure Core SC300 based on ARMv7-M Instruction set architecture including the Instruction Stream Signature Checking (ISS)
- CACHE for code and data buffering
- Memory Encryption/Decryption Unit (MED) and Error Detection Unit
- Memory Protection Unit (MPU)
- Nested Vectored Interrupt Controller (NVIC)

Interfaces

- Universal Asynchronous Receiver/Transmitter (UART)

- Single-Wire Protocol (SWP) with NRG interface
- Inter Integrated Circuit (I2C) interface
- General Purpose Input Output (GPIO)
- Synchronous Serial Communication (SSC) which provides the Serial Peripheral Interface (SPI)
- Universal Serial Bus (USB) interface
- Standard ISO Interface (PAD)

Memories

- Read-Only Memory (ROM, for internal firmware)
- Random Access Memory (RAM)
- SOLID FLASH™ NVM memory (NVM)

Note that the TOE has implemented a SOLID FLASH™ NVM memory module. Parts of this memory module are configured to work as an EEPROM.

Peripherals

- True Random Number Generator (TRNG)
- System Module (SYS)
- Clock Unit (CLK)

Coprocessors

- Crypto2304T co-processor for asymmetric algorithms (Crypto, optional)
- Symmetric Crypto co-processor for 3DES and AES
-

Analog Module (ANA)

- Glitch Sensor
- Temperature Sensor
- Backside Light Detector
- User Mode Security Life Control (UMSLC)

Buses

- Memory Bus
- Peripheral Bus

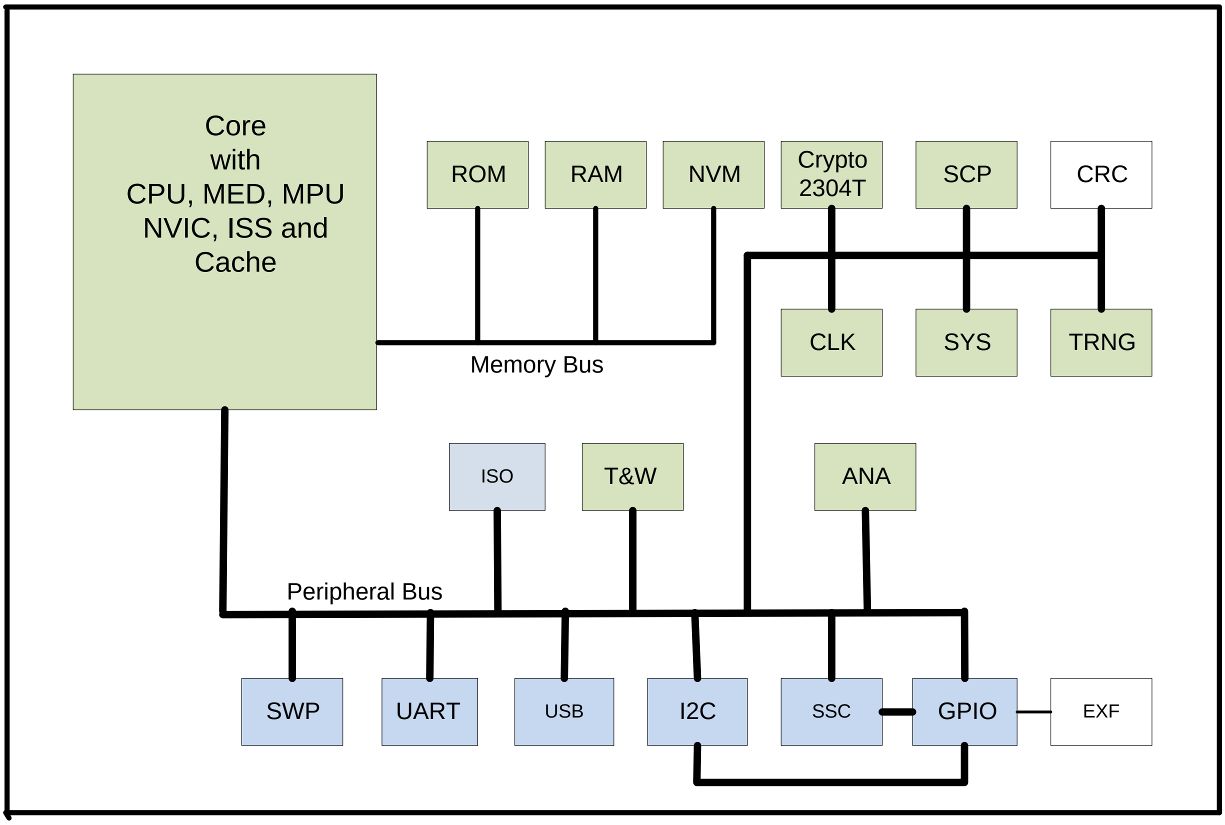


Figure 1

Core	Core System	ROM	Read Only Memory
NVM	SOLID FLASH™ NVM	RAM	Random Access Memory
CLK	Clock Unit	SYS	System Module
Crypto	Crypto2304T	SCP	Symmetric Crypto Processor
CRC	Cyclic Redundancy Check	TRNG	True Random Number Generator
T&W	Timer and Watchdog	UART	UART
I2C	Inter Integrated Circuit	GPIO	General Purpose IO
SSC	Synchronous Serial Communication	SWP	Single Wire Protocol
USB	Universal Serial Bus	ANA	Analog Units
ISO	Standard Interface	ISO	Standard ISO Interface
EXF	External Flash-memory (not available)		

Figure 2 Block diagram of the M9905 products (TOE parts are filled with light green, interface parts are filled in light blue)

The TOE consists of smart card ICs (Security Controllers) meeting high requirements in terms of performance and security. They are manufactured by Infineon Technologies AG in a 90 nm CMOS-technology (L90). This TOE is intended to be used in smart cards for particularly security-relevant applications and for its previous use as developing platform for smart card operating systems according to the lifecycle model from [PP]

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

The TOE consists of a core system, memories, co-processors, security peripherals, control logic and peripherals. The major components of the core system are the 32-bit CPU (Central Processing Unit), the MPU (Memory Protection Unit), the MED (Memory Encryption/Decryption Unit), the Nested Vectored Interrupt Controller (NVIC), the Instruction Stream Signature Checking (ISS) and the Cache system. The TOE contains the co-processors for EC (Crypto2304T) and DES/AES (SCP) processing, a CRC module and the true random number generator, four timers and two watchdog timers and several external interface services. All data of the memory block is encrypted, RAM and ROM are equipped with an error detection code (EDC) and the SOLID FLASH™ NVM is equipped in addition with an error correction code (ECC).
The memories are connected to the Core with the Memory Bus and the peripherals are connected with the Peripheral Bus.

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

The CPU is compatible with the instruction set of the ARMv7_M architecture. Despite its compatibility the CPU implementation is entirely proprietary and not standard.

The CPU accesses the memory via the integrated Memory Encryption and Decryption unit (MED). The memory model of the TOE provides two distinct, independent levels. Additionally, up to eight regions can be defined with different access rights controlled by the Memory Protection Unit (MPU). Errors in RAM and ROM are automatically detected (EDC, Error Detection Code), in terms of the SOLID FLASH™ NVM errors are detected and 1-Bit-errors are also corrected (ECC, Error Correction Code).

The controller of this TOE stores both code and data in a linear 4-GByte memory space, allowing direct access without the need to swap memory segments in and out of memory using a memory protection unit.
The CACHE is a high-speed memory-buffer located between the CPU and the main memories holding a copy of some of the memory contents to enable access, which is considerably faster than retrieving the information from the main memory. In addition to its fast access speed, the CACHE also consumes less power than the main memories. The CACHE is equipped with an integrity check to verify the contents of the cache memories.

A True Random Number Generator (TRNG) specially designed for smart card applications is implemented. The TRNG fulfils the requirements from the functionality class PTG.2 of the AIS31 and produces genuine random numbers which then can be used internally or by the user software.

The implemented sleep mode logic (clock stop mode per ISO/IEC 7816-3) is used to reduce the overall power consumption. The timers permit easy implementation of communication protocols such as T=1 and all other time-critical operations. The UART-controlled I/O interface allows the smart card controller and the terminal interface to be operated independently.

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

Two co-processors for cryptographic operations are implemented on the TOE. The Crypto2304T for calculation of asymmetric algorithms and the Symmetric Cryptographic Processor (SCP) for dual-key or triple-key triple-DES and AES calculations. 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. The Crypto2304T module provides basic functions for the implementation of EC cryptographic libraries.

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

The cyclic redundancy check (CRC) module is a 16-bit checksum generator, which is not part of the TSF and therefore shall not be used for security-critical data. The TOE includes two timer modules each with two 16-bit general purpose timers. The timer module can be used also as watchdog timer to monitor system operation for possible timeouts and to check the correct order of operation.

An Interface Management module, located in the System Module (SYS), provides the TOE with the possibility to maintain two or more data interfaces simultaneously. The TOE is provided with, dependent on the configuration, different peripherals and interfaces as the Universal Serial Bus (USB), the SWP Slave Peripheral (SWP), the Synchronous Serial Communication (SSC), which provides the serial Peripheral Interface (SPI), the GPIO module (GPIO), the Inter-Integrated Cirquit Module (I2C) and the Standard ISO Interface (PAD) to satisfy the different market requirements.

2.3 Firmware of the TOE

The entire firmware of the TOE consists of different parts:

The BOS (Boot Software) and the RMS (Resource Management System) compose the TOE firmware stored in the ROM and the patches hereof in the SOLID FLASH™ NVM. All mandatory functions for start-up and internal testing (BOS) are protected by a dedicated hardware firewall. Additionally two levels are provided, the privileged level and the non-privilege level, both are protected by a hardwired Memory Protection Unit (MPU) setting.

The firmware executes the UMSLC test during the startup phase and includes the features “hardening” and the “Burn-In Test”. The feature “hardening” analyzing a random SOLID FLASH™ NVM page after every regular program operation for written bits that are losing their charge, and, in this very unlikely case, the page is rewritten. The “Burn-In Test” during production is used to stress the chip in a high temperature, high internal voltage and active operation for a certain time and filtering out defect parts to get a low failure rate. The TOE is qualified for an extended temperature range from -40°C to +105°C.
The RMS is accessible in privileged level only. The FL (Flash Loader) allows downloading of user software to the NVM during the manufacturing process and can be completely deactivated.

2.4 Optional software of the TOE

The optional software part of the TOE consists of the cryptographic libraries EC and asymmetric Base libreries.
The EC library is used to provide a high level interface to Elliptic Curve cryptography and includes countermeasures against SPA, DPA and DFA attacks. The routines are used for ECDSA signature generation, ECDSA key generation and Elliptic Curve Diffie-Hellman key agreement. The EC library

is delivered as object code and integrated in this way into the user software. The certification covers the standard NIST [DSS] and Brainpool [ECC] Elliptic Curves with key lengths of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 Bits. 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.
The Asymmetric Base library provides the low level interface to the asymmetric cryptographic coprocessor for the ECC cryptographic libraries and has no user available interface. It does not support any security relevant policy or function. The Base and ECC library can optionally be delivered in the alternative versions:

- The version v2.07.003
- The version v2.09.002

2.5 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 five ISO 7816 pads consist particularly of the contacted RES, I/O, CLK lines and supply lines VCC and GND. The contact based communication is according to ISO 7816/ETSI/EMV. The I2C communication can be driven via the ISO 7816 pads. In this case no other communication using the ISO 7816 pads is possible.
  - The GPIO interface consists of 4 pads which can be individually configured and combined.
  - Also the I2C and the SSC/SPI communication can be exclusively driven via the GPIO pads. In this case no other communication using the GPIO pads is possible.
  - The USB interface is built out of two dedicated pads for data communication and two pads used from the ISO 7816 interface supplying power and ground.
  - The SWP interface is built out of one pad to support the SWP slave functionality.
- The data-oriented I/O interface to the TOE is formed by the I/O pad.
- The interface to the firmware is constituted by special registers used for hardware configuration and control (Special Function Registers, SFR).
- The interface of the TOE to the operating system is constituted 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 BOS test routine call, i.e. entry to test mode (OS-TM entry).
- The interface to the EC calculations is defined by the EC library (optionally).

2.6 Guidance documentation

The guidance documentation is listed in Table 1

2.7 Forms of delivery

The TOE can be delivered in form of bare dies, in form of plain wafers, in form of complete modules (wire bond module M4.x, provided as single chip wire bond or as stacked wire bond), or in one of the following an IC cases: MFC5.8 (FCOS), PG-VQFN-8-1, PG-VQFN-32-13 (SMD) and P-M2M4.7-8-1. 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 can therefore be at the end of phase 3 or at the end of phase 4 which can also include pre-personalization steps according to PP [PP].

The delivery to the software developer (phase 2 ➔ phase 1) is handled by downloading via SecureX portal. It contains the documentation as described above and the development and debugging tools.
Part of the software delivery could also be the Flash Loader program, provided by Infineon Technologies, 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 memory. The download is only possible after successful authentication. In addition, the user can permanently block further use of the Flash Loader. Whether the Flash Loader program is present or not depends on the procurement order.

Table 2 TOE deliveries: forms and methods

TOE Component	Delivered Format	Delivery Method	Comment
M9905 A11	See text above	Customer chooses delivery method. This ST describes under which circumstances transport protection is provided by the TOE.	
All Firmware	–	–	Stored on the delivered hardware.
All software libraries	ARM Library File (object code)	Secured download[1]	–
All User Guidance documents	Personalized PDF	Secured download	–

The TOE is identified by the components as described in the physical scope in chapter 2.2.

- The Hardware version, design step and Firmware version shall be read out form the chip by the Generic Chip Identification Mode (GCIM) and compared against the correct versions. The procedure how to read that data is described in the Programmers Reference Manual. The correct versions are listed in chapter 2.3
- The correct library versions shall be verified by the corresponding hash values as defined in chapter 10.
- The user guidance documents shall be compared to the versions listed in chapter 2.6

2.8 Production sites

The silicon of the design is produced in Dresden.
The delivery measures are described in the ALC_DVS aspect.

Table 3 Production site in chip identification

Production Site	Chip Identification
Dresden, Germany	byte number 13 (Fab number): 02_H

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

2.9 TOE Configuration

The TOE hardware offers different configuration options, which a customer can choose. The mechanism to choose a configuration can be done by the following methods:

1. by product selection or dialog-based in Tools,
2. via Bill-per-Use (BpU) and Flash Loader (FL),

The degree of freedom for configuring the TOE is predefined by Infineon Technologies AG. The list of TOE configurations is given in the confidential ST.
Besides fix TOE configurations, which can be ordered as usual, this TOE implements optionally the so called Bill-Per-Use (BPU) ability. This solution enables the customer to tailor the product on his own to the required configuration by blocking parts of the chip on demand into the final configuration at his own premises, without further delivery or involving support by Infineon Technology AG. Customers, who are intended to use this feature receive the TOE in a predefined configuration including the Flash Loader software, enhanced with the BPU blocking software. The blocking information is part of a chip configuration area and can be modified by customers using specific APDUs. Once a final blocking is done, further modifications are disabled.
The BPU software part is only present on the products which have been ordered with the BPU option. In all other cases this software is not present on the product.
Additionally the user can choose between different optional software libraries.
The user can choose the management of NRG libraries (version 01.03.0927) and/or the NRG reader mode support library (01.02.0800). Please note that the NRG libreries are not part of this certification.

The hardware of this TOE can be delivered with the following configuration options:

- both crypto co-processors accessible
- with a blocked Crypto2304T

In the case the Crypto2304T is blocked, no EC computation supported by hardware is possible. No accessibility of the deselected cryptographic co-processors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic co-processors.
The TOE can be delivered with the following optional libraries

- ECC
- Asymmetric Base library for ECC

In case of deselecting one or several of these libraries the TOE does not provide the respective functionality.

2.10 TOE initialization with Customer Software

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

Table 4 Options to implement user software at Infineon production premises

1	The user or/and a subcontractor downloads the software into the SOLID FLASH™ NVM memory 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 or reactivated by the user or subcontractor to download his software in the SOLID FLASH™ NVM memory.
2	The user provides software for the download into the SOLID FLASH™ NVM memory to	The Flash Loader is deactivated.

	Infineon Technologies AG. The software is downloaded to the SOLID FLASH™ NVM memory during chip production. There are no user data in the ROM.	
3	The user provides software for the download into the SOLID FLASH™ NVM memory to Infineon Technologies AG. The software is downloaded to the SOLID FLASH™ NVM memory during chip production. 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 memory. Precondition is that the user has provided an own reactivation procedure in software prior to chip production to Infineon Technologies AG.

The Generic Chip Identification Mode (GCIM) data of the TOE allows a unique identification of each TOE and provides several detailed production information. The Chip Identification Mode data is accessible by a non-ISO reset or can be read directly from the configuration area located at the NVM by the user operating system. The SLE97 Hardware Reference Manual [HRM] gives a detailed description of the GCIM data.

3 Conformance Claims (ASE_CCL)

3.1 CC Conformance Claim

This Security Target (ST) and the TOE claim conformance to Common Criteria version CC:2022, part 1 [CC-1], part 2 [CC-2], part 3 [CC-3] part 4 [CC-4]and part 5 [CC-5].

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 [PP].

The Security IC Platform Protection Profile is registered and certified by the Bundesamt für Sicherheit in der Informationstechnik[1] (BSI) under the reference BSI-PP-0035, Version 1.0, dated 15.06.2007.

The security assurance requirements of the TOE are according to the Security IC Platform Protection Profile [PP]. They are all drawn from [CC-3].

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

Table 5 Augmentations of the assurance level of the TOE

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

3.3 Package Claim

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

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 only to one PP, the PP [PP].

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, 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.

Security Problem Definition:

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

Conformance Rationale:

The augmented organizational security policy P.Add-Functions, coming from the additional security functionality of the cryptographic libraries, the augmented assumption A.Key-Function, related to the usage of key-depending function, the threat T-Masquerade.TOE and the threat memory access violation, due to specific TOE memory access control functionality, have been added. These add-ons have no impact on the conformance statements regarding CC [CC-1] and PP [PP], with following rationale:

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

The security target fulfils the strict conformance claim of the PP [PP] 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, the memory access control - O.Mem-Access, and the hash additional security objectives have been introduced. These add-ons have no impact on the conformance statements regarding CC [CC-1] and PP [PP], with following rational:

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

The security target fulfils the strict conformance of the PP [PP] 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 [PP], as the security target claimed strict conformance to the PP [PP].

All security functional requirements defined in the PP [PP] are included and completely defined in this ST. The security functional requirements listed in the following are all taken from Common Criteria part 2 [CC-2] 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 [CC-2])

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

All assignments and selections of the security functional requirements are done in the PP [PP] and in this security target in section 7.8.

The Assurance Requirements of the TOE obtain the Evaluation Assurance Level 5 augmented with the assurance components ALC_DVS.2 and AVA_VAN.5 for the TOE.

-
- With CC:2022 several SFR changes are introduced. Due to this ST claiming conformance to CC:2022 and PP0035 [PP], rationales are provided that these changes do not affect the conformance claim to PP0035:
- FCS_COP.1: for this SFR dependencies are changed in CC:2022. FCS_CKM.4 is removed and instead FCS_CKM.6 added. Further FCS_CKM.5 is added for key derivation as an alternative.
- FCS_CKM.1: for this SFR dependencies are changed in CC:2022. Additionally, to FCS_CKM.2 and FCS_COP.1, one further SFR is introduced as alternative: FCS_CKM.5. This SFR targets key derivation, subsequent to FCS_CKM.1. In CC:2022 key derivation would have been part of FCS_CKM.1 and thus conformancy to [PP] can still be claimed. FCS_CKM.4 is removed and instead FCS_CKM.6 added. All other dependencies (i.e. FCS_RNG.1 or FCS_RBG.1) are in addition to the already existing ones, i.e. add stricter requirements.
- FCS_CKM.6 replaces FCS_CKM.4 and adds further requirements on the timing of key destruction. As an alternative dependency to FCS_CKM.1, FCS_CKM.5 (key derivation) can be used. As FCS_CKM.5 is neither used within [PP] nor within this ST, it has no relevance in this context.
- FCS_RNG.1: this SFR is taken from [CC-2] rather than [PP].
- FMT_LIM.1 and FMT_LIM.2 are taken from [CC-2] rather than [PP]. There is a slightly different phrasing (i.e. removing redundancy from FMT_LIM.1) and availability and capability policy mentioned in both SFR’s. The meaning though is the same and therefore conformancy can still be claimed.

Further with CC:2022 some SAR changes were introduced. Rationales are provided that these changes do not affect the conformance claim to [PP]:

- ASE_CCL.1: for CC:2022 several extensions were introduced (e.g. exact conformance to PP), which add to the already existing assurance requirements. No relaxation was introduced.
- ASE_INT.1: introduction of multi-assurance in combination with PP-configuration: not relevant for [PP]
- ASE_REQ.2: extended for multi assurance: not relevant for [PP]
- AVA_VAN.5: extension about third party components introduced. No relaxation was introduced.

- ALC_TAT.1: extension with guidance on the minimum content for an implementation standards description and rules with ADV_COMP.1. No relaxation was introduced.

4 Security Problem Definition (ASE_SPD)

The content of the PP [PP] 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 [PP] section 3.2.

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

Table 6 Threats according PP [PP]

Threat	Description
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.

T.Masquerade_TOE Masquerade of the TOE

An attacker may threaten the property being a genuine TOE by producing a chip which is not a genuine TOE but wrongly identifying itself as genuine TOE sample. This threat has been additionally introduced because the chip can be delivered without an User OS doing the identification.

Table 7 Additional threats due to TOE specific functions and augmentations

T.Mem-Access	Memory Access Violation
T.Masquerade_TOE	Masquerade of the TOE

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 true random number or a deterministic random number generator or by both, when a true random number is used as seed for the deterministic random number generator. Note that the generation of random numbers is a requirement of the PP [PP].

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
- Initialisation Data and Pre-personalisation Data, specific development aids, test and characterisation 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-personalisation Data,
- specific development aids,
- test and characterisation 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 [PP] 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 [PP] section 3.3. Due to the augmentations of PP [PP] an additional policy is introduced and described in the next chapter.

Table 8 Organizational Security Policies according PP [PP]

P.Process-TOE	Protection during TOE Development and Production

4.2.1 Augmented Organizational Security Policy

Due to the augmentations of the PP [PP] 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)
- Elliptic Curve Cryptography (EC)

Note: This TOE can be delivered with the Crypto2304T coprocessor accessible or blocked. In case the Crypto2304T is blocked, no ECC computation supported by hardware is possible. The ECC functionality has then to be removed from this policy.

Note: The TOE can also be delivered with the optional ECC library. The optional ECC library needs an accessible Crypto2304T. If the optional ECC library is not delivered then ECC functionality has to be removed from this policy.

4.3 Assumptions

The TOE assumptions on the operational environment are defined and described in PP [PP] 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 unauthorised 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 9 Assumption according PP [PP]

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 [PP] 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 [PP] section 4.1.

Table 10 Objectives for the TOE according to PP [PP]

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)
- Elliptic Curve Cryptography (EC) (optional)

The hardware of this TOE can be delivered with the following configuration options:

- both crypto co-processors accessible
- with a blocked Crypto2304T

In the case the Crypto2304T is blocked, no EC computations supported by hardware are possible.

The optional security relevant software part of the TOE consists of the following optional libraries:

- EC Cryptographic Library

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

Table 12 Objectives for the TOE according to PP [PP]

OE.Plat-Appl	Usage of Hardware Platform
OE.Resp-Appl	Treatment of User Data
OE.Process-Sec-IC	Protection during composite product manufacturing

This ST further defines the objectives for the environment OE.Secure_Delivery as specified below.

OE.Secure_Delivery:
The TOE does not provide transport protection. Therefore, technical and / or organisational security procedures (e.g. a custom mutual authentication mechanism or a security transport) should be put in place by the customer to secure the personalized TOE during delivery as required by the security needs of the loaded IC Embedded Software.

The table below lists the security objectives for the environment in the life cycle phases.

Table 13 Security objectives for the environment

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
Phase 3, 4	OE.Secure_Delivery OE.Prevent-Masquerade	The TOE does not provide transport protection. Therefore, technical and / or organisational security procedures (e.g. a custom mutual authentication mechanism or a security transport) should be put in place by the customer to secure the personalized TOE during delivery as required by the security needs of the loaded IC Embedded Software.

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 [PP] section 4.4. For organizational security policy P.Add-Functions, OE.Plat-Appl and OE.Resp-Appl the rationale is given in the following description.

Table 14 Security Objective Rationale

Assumption, Threat or Organisational 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
T.Masquerade_TOE	OE.Secure_Delivery

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 [PP] 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 [PP] 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 [PP] 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.

The objective OE.Secure_Delivery is defined to require transport protection by the environment ias the TOE does not provide this objective.

6 Extended Component Definition (ASE_ECD)

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

- 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 component FAU_SAS is defined and described in PP [PP] section 5. The component FPT_TST.2 is defined in the following sections.

6.1 "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

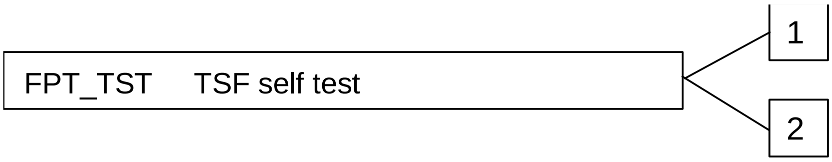
The functional component "Subset TOE security testing (FPT_TST.2)" has been newly created (Common Criteria Part 2 extended). This component allows that particular parts of the security mechanisms and functions provided by the TOE can be tested after TOE Delivery or are tested automatically and continuously 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 [CC-2] section 15.17.1

Component leveling



FPT_TST.1 The component FPT_TST.1 is defined in [CC-2] section 15.17.1.

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

Management: FPT_TST.2
The following actions could be considered for the management functions in FMT: management of the conditions under which subset TSF self testing occurs, such as during initial start-up, regular interval or under specified conditions management of the time of the interval appropriate.

Audit: FPT_TST.2
There are no auditable events foreseen.

FPT_TST.2 Subset TOE testing

Hierarchical to: No other components.

Dependencies: No dependencies

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

7 Security Requirements (ASE_REQ)

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

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

The Table 15 provides an overview of the functional security requirements of the TOE, defined in PP [PP] section 6.1. In the last column it is marked if the requirement is refined. The refinements are also valid for this ST.

Table 15 Security functional requirements defined in PP [PP]

Security Functional Requirement		Refined in PP [PP]
FRU_FLT.2	Limited fault tolerance	Yes
FPT_FLS.1	Failure with preservation of secure state	Yes
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

Table 16 provides an overview of all SFRs which are taken from the CC standard [CC-2]. They replace the corresponding SFRs from PP [PP].

Table 16 Security functional requirements defined in CC [CC-2]

Security Functional Requirement	
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FCS_RNG.1	Rndom number generation

The Table 17 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 [CC-2], with the exception of the requirement FPT_TST.2, which is defined in this ST completely.

Table 17 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 initialization
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

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

The above marked extended components FMT_LIM.1 and FMT_LIM.2 are introduced in PP [PP] 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 [CC-2]. 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 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 other components

Dependencies: No dependencies.

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

7.2 FPT_TST.2

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

FPT_TST.2 Subset TOE testing

Hierarchical to: No other components

Dependencies: No dependencies

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

7.3 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 [CC-2].

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 [CC-2]

FCS_RNG.1.1 The TSF shall provide a physical[1] 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 rawrandom 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 num ber 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.[2]

FCS_RNG.1.2 The TSF shall provide numbers in the format 8- or 16-bit[3] that meet

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

[1] [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]

[2] [assignment: list of security capabilities]

[3] [selection: bits, octets of bits, numbers [assignment: format of the numbers]]

PTG.2.7: The average Shannon entropy per internal random bit exceeds 0.997.[1]

7.4 Limited Capabilities and Limited Availability

The SFR's FMT_LIM.1 and FMT_LIM.2 from [PP] are adapted due to CC:2022.

FMT_LIM.1	**Limited Capabilities**
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2: Limited availability
FMT_LIM.1.1	The TSF shall limit its capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: Deploying Test Features after TOE Delivery does not allow user data of the Composite TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks[2].

FMT_LIM.2	**Limited availability**
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities.
FMT_LIM.2.1	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: Deploying Test Features after TOE Delivery does not allow user data of the Composite TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks[3].

7.5 Memory access control

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

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.

[1] [assignment: a defined quality metric]

[2] [assignment: Limited capability and availability policy]

[3] [assignment: Limited capability and availability policy]

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 support the standard ARMv7 Protected Memory System Architecture model. The MPU provides full support for:

- Protection regions.
- Overlapping protection regions, with ascending region priority:
  - Region 7 = highest priority.
  - Region 0 = lowest priority.
- Access permissions.
- MPU mismatches and permission violations invoke the programmable-priority MemManage fault handler.

The MPU can be used to:

- Enforce privilege rules, preventing user applications from corrupting operating system data.
- Separate processes, blocking the active task from accessing other tasks’ data.
- Enforce access rules, allowing memory regions to be defined as read-only or detecting unexpected memory accesses.

Subjects, Objects and Operations of the policy

- Subjects: privilege or non-privilege level of the ARM processor
- Objects: memory/code addresses
- Operations: Read a/o write a/o execute access

Attributes of the policy:

- MPU enable/disable bit.
- 8 regions with the following attributes
  - A unique priority
  - The enable bit
  - the start address and size
  - an access matrix which defines if an Operation of a Subject to an Object lying in the region is allowed or denied
- The default region with the following security attribute:
  - A bit which defines if an Operation for the Subject (privilege level) is allowed or if no Operation is allowed for any Subject.

Roles of the policy:

The roles correspond 1-1 to the subjects.

Properties of the policy:

- If an address is contained in multiple enabled regions, then the region with the highest priority defines the access rights.
- If an address is contained in no region then the default region defines the access rights.
- The region defining the access rights checks in the access matrix if the Subject has access to the Object with respect to the desired Operation. In case the access is denied the MPU throws an access violation exception.

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, all Objects and all Operations.

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

FDP_ACF.1.1 The TSF shall enforce the Memory Access Control Policy to objects based on the following: As specified in the definition of the memory access control policy.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
As specified in the definition of the memory access control policy.

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 initialization

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 restrictive[1] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the privilege level 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 modify[2] the security attributes which are defined in the Memory Access Control Policy[3] to the privilege level[4].

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: The privilege level shall be able to access the configuration registers of the MPU.

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

[2] [selection: change_default, query, modify, delete, [assignment: other operations]]

[3] [assignment: list of security attributes]

[4] [assignment: list of security attributes]

7.6 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 7.9.1.1.

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

- Advanced Encryption Standard (AES)
- Triple Data Encryption Standard (3DES)
- Elliptic Curve Cryptography (EC)[1]

General statements with regard to Elliptic Curves:

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

7.6.1 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 generation, or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1/DES The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm Triple Data Encryption Standard (3DES) in Electronic Codebook Mode (ECB) and in the Cipher Block Chaining Mode (CBC) and cryptographic key sizes of 2 x 56 or 3 x 56 bit that meet the following: [N38A], [N867]

7.6.2 AES Operation

The AES Operation of the TOE shall meet the requirement “Cryptographic operation (FCS_COP.1)” as specified below.

[1] In case a user deselects the EC library, the TOE provides basic HW-related routines for EC calculations. For a secure library implementation the user has to implement additional countermeasures.

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 or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of 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) in Electronic Codebook Mode (ECB) and in the Cipher Block Chaining Mode (CBC) and cryptographic key sizes of 128 bit or 192 bit or 256 bit that meet the following: [N197], [N38A]

7.6.3 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 or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1/ECDSA The TSF shall perform signature generation 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:
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.

Note: This TOE can be delivered with the Crypto2304T coprocessor accessible or blocked. In case the Crypto2304T is blocked, no ECC computation supported by hardware is possible and this SFR is not applicable.

Note: The TOE can be delivered with an optional ECC library. Any optional ECC library contains the ECC algorithms stated above. If no optional ECC library is available then this SFR is not applicable.

7.6.4 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_CKM.5 Cryptographic key derivation, or
FCS_COP.1 Cryptographic operation]
[FCS_RBG.1 Random bit generation, or
FCS_RNG.1 Generation of random numbers]
FCS_CKM.6 Timing and event of 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 specified cryptographic key sizes 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits that meet the following:

ECDSA Key Generation:
According to the appendix A4.3 in ANSI X9.62-2005
the cofactor h is not supported.

Note: This TOE can be delivered with the Crypto2304T coprocessor accessible or blocked. In case the Crypto2304T is blocked, no ECC computation supported by hardware is possible and this SFR is not applicable.

Note: The TOE can be delivered with an optional ECC library. Any optional ECC library contains the ECC algorithms stated above. If no optional ECC library is available then this SFR is not applicable.

7.6.5 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, or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of 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 of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 bits that meet the following: 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.

Note: The certification covers the standard NIST [DSS] and Brainpool [ECC] Elliptic Curves with key lengths of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 Bits. Other types of elliptic curves can be added by the user during a composite certification process.

Note: This TOE can be delivered with the Crypto2304T coprocessor accessible or blocked. In case the Crypto2304T is blocked, no ECC computation supported by hardware is possible and this SFR is not applicable.

Note: The TOE can be delivered with an optional ECC library. Any optional ECC library contains the ECC algorithms stated above. If no optional ECC library is available then this SFR is not applicable.

7.7 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 value for RAM and ROM and ECC value for the SOLID FLASH™ NVM and verification of stored data in the SOLID FLASH™ NVM.

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

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 stored data integrity monitoring

Dependencies: No dependencies

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

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

7.8 TOE Security Assurance Requirements

The evaluation assurance level is EAL5 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 the Protection Profile [PP] is expressed with bold letters.

Table 18 Assurance components

Aspect	Acronym	Description	Refinement
Development	ADV_ARC.1	Security Architecture Description	in PP [PP]
	ADV_FSP.5	**Complete semiformal functional specification with additional error information**	in ST
	ADV_IMP.1	Implementation representation of the TSF	in PP [PP]
	ADV_INT.2	**Well-structured internals**	in ST
	ADV_TDS.4	**Semi-formal modular design**	in ST
Guidance Documents	AGD_OPE.1	Operational user guidance	in PP [PP]
	AGD_PRE.1	Preparative procedures	in PP [PP]
Life-Cycle Support	ALC_CMC.4	Production support, acceptance procedures and automation	in PP [PP]
	ALC_CMS.5	**Development tools CM coverage**	in ST
	ALC_DEL.1	Delivery procedures	in PP [PP]
	ALC_DVS.2	Sufficiency of security controls	in PP [PP]
	ALC_LCD.1	Developer defined life-cycle process	in PP [PP]
	ALC_TAT.2	**Compliance with implementation standards**	in ST
Security Target Evaluation	ASE_CCL.1	Conformance claims	in PP [PP]
	ASE_ECD.1	Extended components definition	in PP [PP]
	ASE_INT.1	ST introduction	in PP [PP]
	ASE_OBJ.2	Security objectives	in PP [PP]
	ASE_REQ.2	Derived security requirements	in PP [PP]

	ASE_SPD.1	Security problem definition	in PP [PP]
	ASE_TSS.1	TOE summary specification	in PP [PP]
Tests	ATE_COV.2	Analysis of coverage	in PP [PP]
	ATE_DPT.3	**Testing: modular design**	in ST
	ATE_FUN.1	Functional testing	in PP [PP]
	ATE_IND.2	Independent testing - sample	in PP [PP]
Vulnerability Assessment	AVA_VAN.5	Advanced methodical vulnerability analysis	in PP [PP]

7.8.1 Refinements

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

Refinements from the PP [PP] have to be discussed here in the Security Target, as the assurance level is increased.

Life cycle support (ALC_CMS, ALC_TAT)

The refinement from the PP [PP] can be applied even at the chosen assurance level EAL 5 augmented with ALC_CMS.5 and ALC_TAT.2. The assurance package ALC_CMS.4 is extended to ALC_CMS.5 with aspects regarding the configuration control system for the TOE. The assurance package ALC_TAT.1 is extended to ALC_TAT.2 with aspects regarding the implementation standards for the TOE.

Development (ADV_FSP)

The refinement from the PP [PP] can be applied even at the chosen assurance level EAL 5 augmented with ADV_FSP.5, ADV_TDS.4 and ADV_INT.2.

For details of the refinement see PP [PP].

Tests (ATE_DPT.3)

The refinement from the PP [PP] can be applied even at the chosen assurance level EAL 5 augmented with ATE_DPT.3. The assurance package ATE_DPT.2 is augmented to ATE_DPT.3 relating to the requirements of the assurance level EAL 5. The refinement is not touched.

7.9 Security Requirements Rationale

7.9.1 Rationale for the Security Functional Requirements

The security functional requirements rationale of the TOE are defined and described in PP [PP] 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 19 Rational for additional SFR in the ST

Objective	TOE Security Functional Requirements
O.Add-Functions	FCS_COP.1/DES FCS_COP.1/AES FCS_COP.1/ECDSA (optional) FCS_COP.1/ECDH (optional) FCS_CKM.1/EC (optional)
O.Phys-Manipulation	FPT_TST.2
O.Mem-Access	FDP_ACC.1 FDP_ACF.1 FMT_MSA.3 FMT_MSA.1 FMT_SMF.1
O.Malfunction	FDP_SDI.1 FDP_SDI.2

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/EC supports the generation of EC keys needed for these cryptographic operations. Therefore, FCS_COP.1/ECDSA, FCS_COP.1/ECDH and FCS_CKM/EC are suitable to meet the security objective. The use of the supporting Base library has no impact on any security functional requirement nor does its use generate additional requirements. 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 3DES and AES are provided by the environment, the keys for 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.6 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 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 and SF_PMA Protection against modifying attacks.

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

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 [CC-2] user data protection of chapter 11 which are not refined by the PP [PP].

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 RAM, ROM and SOLID FLASH™ NVM (in the SOLID FLASH™ NVM more bit errors are detected). 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 in RAM and ROM 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.

7.9.1.1 Dependencies of Security Functional Requirements

The dependencies of security functional requirements are defined and described in PP [PP] 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 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 20 Dependency for cryptographic operation requirement

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FCS_COP.1/DES	FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.5	See comment
	FCS_CKM.6	See comment
FCS_COP.1/AES	FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.5	See comment
	FCS_CKM.6	See comment
FCS_COP.1/ECDSA	FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.5	FCS_CKM.1/EC
	FCS_CKM.6	See comment
FCS_CKM.1/EC	FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1	FCS_COP.1/ECDH FCS_COP.1/ECDSA
	FCS_RBG.1 or FCS_RNG.1	FCS_RNG.1
	FCS_CKM.6	See comment
FCS_COP.1/ECDH	FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.5	FCS_CKM.1/EC
	FCS_CKM.6	See comment
FPT_TST.2	None	See comment
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
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes See comment Yes
FMT_SMF.1	None	N/A
FDP_SDI.1	None	N/A
FDP_SDI.2	None	N/A

Comment:

The security functional requirement “Cryptographic operation (FCS_COP.1)” met by the TOE, has the following dependencies:

- FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.5
- FCS_CKM.6

The security functional requirement “Cryptographic key management (FCS_CKM.1)” met by TOE, has the following dependencies:

- FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1
- FCS_RBG.1 or FCS_RNG.1
- FCS_CKM.6

These requirements all address the appropriate management of cryptographic keys used by the specified cryptographic function and are not part of the PP [PP]. 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, FCS_COP.1/AES, the respective dependencies FCS_CKM.6 and FCS_CKM.1, FCS_CKM.5 or FDP_ITC.1 or FDP_ITC.2 have to be fulfilled by the environment.

For the security functional requirement FCS_COP.1/ECDSA, and FCS_COP.1/ECDH, the respective dependency FCS_CKM.6 has to be fulfilled by the environment.

The security functional requirement FCS_CKM.6 has to be fulfilled by the environment.

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.

7.9.2 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 18 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 “Application of Attack Potential to Smartcards” [JIL] 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 the AVA_VAN.5 component.

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.4 “Complete functional specification”, ADV_TDS.3 “Basic modular design”, ADV_IMP.1 “Implementation representation of the TSF”, AGD_OPE.1 “Operational user guidance”, and ATE_DPT.1 “Testing: basic design.

All these dependencies are satisfied by EAL5.

It has to be assumed that attackers with high attack potential try to attack Security ICs like smart cards 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. In the following the Security Features are described 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:

- 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 operation modes is taken dependent on phase identifiers. The decision of accessing a certain mode is defined as phase entry protection. The phases follow also a defined and protected sequence. The sequence of the phases is protected by means of authentication.
The covered security functional requirements are FMT_LIM.1 “Limited capabilities” and FMT_LIM.2 “Limited availability”.

During the production phase (phase 3 and 4) or after the delivery to the customer (phase 5 or phase 6), the TOE provides the possibility to download a user specific encryption key and user code and data into the empty (erased) SOLID FLASH™ NVM memory area as specified by the associated control information of the Flash Loader software. After finishing the load operation, the Flash Loader can be permanently deactivated, so that no further load operation with the Flash Loader is possible. These procedures are defined as phase operation limitation.
The covered security functional requirement is FMT_LIM.2 “Limited availability”.

During operation within a phase the accesses to memories are granted by the MPU controlled access rights and related levels.
The covered security functional requirements are FDP_ACC.1 “Subset access control”, FDP_ACF.1 “Security attribute-based access control” and FMT_MSA.1 “Management of security attributes”.

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

The TOE clearly defines access rights and levels in conjunction with the appropriate key management in dependency of the firmware or software to be executed.
The covered security functional requirement is FMT_SMF.1 “Specification of Management functions”.

Each operation phase is protected by means of authentication and encryption.
The covered security functional requirements are FPT_ITT.1 “Basic internal TSF data transfer protection” and FDP_IFC.1 “Subset information flow control”. If any comparison of the authentication code fails a direct security reset is performed. The covered security functional requirements is FPT_FLS.1 (”Failure with preservation of secure state”).

The **SF_DPM** “Device Phase Management” covers the security functional requirements FPT_FLS.1, 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_ITT.1 and FDP_IFC.1.

8.2 SF_PS: Protection against Snooping

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

The entire design is kept in a non standard way to prevent attacks using standard analysis methods. Important parts of the chip are especially designed to counter leakage or side channel attacks like DPA/SPA or EMA/DEMA. Therefore, even the physical data gaining is difficult to perform, since timing and current consumption is independent of the processed data. In the design a number of components are automatically synthesized and mixed up to disguise an attacker and to make an analysis more difficult.
The covered security functional requirement is FPT_PHP.3 “Resistance to physical attack”.

A further protective design method used is secure wiring. All security critical wires have been identified and protected by special routing measures against probing. Additionally the wires are embedded into shield lines and used as normal signal lines for operation of the chip to prevent successful probing. This measurement is called “security optimized wiring”.
The covered security functional requirements are FPT_PHP.3 “Resistance to physical attack”, FPT_ITT.1 “Basic internal TSF data transfer protection”, FPT_FLS.1 “Failure with preservation of secure state” and FDP_ITT.1 “Basic internal transfer protection”.

All contents of the memories RAM, ROM and SOLID FLASH™ NVM of the TOE are encrypted on chip to protect them against data analysis. In addition the data transferred over the memory bus to and from (bi-directional encryption) the CPU, Co-processor (Crypto2304T and SCP), the special SFRs and the peripheral devices (RNG and Timer) are transported encrypted with an automatically dynamic key change.
The encryption of the memory content is done by the MED using a proprietary cryptographic algorithm and a complex key management providing protection against cryptographic analysis attacks. This means that the SOLID FLASH™ NVM, RAM, ROM and the bus are encrypted with module dedicated and dynamic keys. The only key remaining static over the product life cycle is the specific ROM key changing from mask to mask.
All security relevant transfer of addresses or data via the peripheral bus is dynamically masked and thus protected against readout and analysis.
The function Trash Register Writes can be activated by the user to hide the fact if a register has been written.
The covered security functional requirements are FDP_IFC.1 “Subset information flow control“, FPT_PHP.3 “Resistance to physical attack”, FPT_ITT.1 “Basic internal TSF data transfer protection, FPT_FLS.1 “Failure with preservation of secure state” and FDP_ITT.1 “Basic internal transfer protection”.

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

8.3 SF_PMA: Protection against Modifying Attacks

The TOE is equipped with an error detection code (EDC) for protecting RAM and ROM and an ECC, which is realized in the SOLID FLASH™ NVM. Thus introduced failures are securely detected and, in terms of single bit errors in the SOLID FLASH™ NVM also automatically corrected (FDP_SDI.2). For SOLID FLASH™ NVM in case of more than one bit errors and for RAM in case of any bit errors detected, a security alarm is triggered.
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 “Limited fault tolerance“, FDP_PHP.3 “Resistance to physical attack“, FDP_SDI.1 “Stored data integrity monitoring” and FDP_SDI.2 “Stored data integrity monitoring and action”.

If a user tears the card resulting in a power off situation during 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 NVM tearing save write functionality covers 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 valid.

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

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.

A shielding algorithm finishes the upper layers above security critical signals and wires, finally providing the so called “security optimized wiring”.

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

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

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

During start up, the TOE performs various configurations and subsystem tests. After the TOE startup has finished, the operating system or application can call the User Mode Security Life Control (UMSLC) test provided by the Resource Management System. The UMSLC checks the alarm lines and/or the different security functions and sensors for correct operation. The test can be triggered by user software during normal operation. As attempts to modify the security features will be detected from the test, the covered security functional requirement is FPT_TST.2 "Subset TOE security testing".

The correct function of the TOE is only given in the specified range of the environmental operating parameters. To prevent an attack exploiting that circumstance the TOE is equipped with a temperature sensor, glitch sensor and backside light detection. The TOE falls into the defined secure state in case of a specified range violation. The defined secure state causes the chip internal reset process. Note that the specified range checking can only work when the TOE is running and can not prevent reverse engineering.
The covered security functional requirements are FRU_FLT.2 "Limited fault tolerance" and FPT_FLS.1 "Failure with preservation of secure state".

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

8.4 SF_PLA: Protection against Logical Attacks

The memory model of the TOE provides two distinct, independent levels called the privileged and non-privilege level and the possibility to define up to eight memory regions with different access rights enforced by the Management Protection Unit (MPU). This gives the user software the possibility to define different access rights for the regions 0 to 7 for privilege or non-privilege level. In the case of an access violation the MPU will trigger a trap. The policy of setting up the MPU and specifying the memory ranges for the regions (0 to 7) is defined from the user software.
The covered security functional requirements are FDP_ACC.1 "Subset access control", FDP_ACF.1 "Security attribute based access control", FMT_MSA.1 "Management of security attributes", FMT_MSA.3 "Static attribute initialisation" and FMT_SMF.1 "Specification of Management functions".

All memories present on the TOE (NVM, ROM, RAM) are encrypted using individual keys assigned by complex key management. In case of security critical error a security alarm is generated and the TOE ends up in a secure state.
The covered security functional requirements are FDP_ACF.1 "Security attribute based access control" and FPT_FLS.1 "Failure with preservation of secure state".

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

8.5 SF_CS: Cryptographic Support

The TOE is equipped an asymmetric and a symmetric hardware accelerators 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. The components are a co-processor supporting the DES and AES algorithms and a co-processor and software modules to support EC signature generation, ECDH key agreement and EC public key calculation and testing. Additionally the TOE is equipped with a True Random Number Generator for the generation of random numbers.

8.5.1 3DES encryption

The TOE supports the encryption and decryption in accordance with the specified cryptographic algorithm Triple Data Encryption Standard (3DES) in the Electronic Codebook Mode (ECB), Cipher Block Chaining Mode (CBC) and with cryptographic key sizes of 112 and 168 bit meeting the standard: [N867], [N38A], [N38B].

The covered security functional requirements are FCS_COP.1/DES.

8.5.2 AES encryption

The TSF supports the encryption and decryption in accordance with the specified cryptographic algorithm Advanced Encryption Standard (AES)) in the Electronic Codebook Mode (ECB), Cipher Block Chaining Mode (CBC) and cryptographic key sizes of 128 bit or 192 bit or 256 bit according to the standard: [N197], [N38A], [N38B].

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

8.5.1 Elliptic Curves

The certification covers the standard NIST [DSS] and Brainpool [ECC] Elliptic Curves with key lengths of 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512 or 521 Bits. Note that there exist 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.

8.5.1.1 Signature Generation

The TSF shall perform signature generation 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:

- 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.

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

8.5.1.2 Asymmetric Key Generation

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Elliptic Curve EC specified in ANSI X9.62-1998 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:

- According to the appendix A4.3 in ANSI X9.62-2005 the cofactor h is not supported.

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

8.5.1.3 Asymmetric Key Agreement

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

- 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.

3.

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

8.5.2 Asymmetric Base Library

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

8.5.3 TRNG

Random data is essential for cryptography as well as for security mechanisms. The TOE is equipped with a physical True Random Number Generator (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 TRNG implements also self testing features. The TRNG fulfils the requirements from the functionality class PTG.2 of [6].
The covered security functional requirement is FCS_RNG.1 “Quality metric for random numbers”, 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“, FPT_TST.2 “Subset TOE security testing“ and FPT_FLS.1“Failure with preservation of secure state”.

The **SF_CS** “Cryptographic Support” covers the security functional requirements FCS_COP.1/DES, FCS_COP.1/AES, FCS_COP.1/ECDSA, FCS_COP.1/ECDH, FCS_CKM.1/EC, FPT_PHP.3, FDP_ITT.1, FPT_ITT.1, FPT_FLS.1 ,FCS_RNG.1 and FDP_IFC.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 sections the sections above. The results are shown in Table 21. 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 21 Mapping of SFR and SF

SFR	SF_DPM	SF_PS	SF_PMA	SF_PLA	SF_CS
FAU_SAS.1	X				
FMT_LIM.1	X				
FMT_LIM.2	X				
FDP_ACC.1	X			X	
FDP_ACF.1	X			X	
FPT_PHP.3		X	X		X
FDP_ITT.1		X	X		X
FDP_SDI.1			X		
FDP_SDI.2			X		
FDP_IFC.1	X	X	X		X
FMT_MSA.1	X			X	
FMT_MSA.3	X			X	
FMT_SMF.1	X			X	
FRU_FLT.2			X		
FPT_ITT.1	X	X	X		X
FPT_TST.2			X		
FPT_FLS.1	X	X	X	X	X
FCS_RNG.1					X
FCS_COP.1/DES					X
FCS_COP.1/AES					X
FCS_COP.1/ECDSA					X
FCS_COP.1/ECDH					X
FCS_CKM.1/EC					X

8.7 Security Requirements are internally Consistent

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

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

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

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

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

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.

1 9 References

[PP] Security IC Platform Protection Profile, Version 1.0, 15.06.2007, BSI-PP-0035

[CC-1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model; CC:2022 Revision 1, November 2022, CCMB-2022-11-001

[CC-2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements; CC:2022 Revision 1, November 2022, CCMB-2022-11-002

[CC-3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements; CC:2022 Revision 1, November 2022, CCMB-2022-11-003

[CC-4] Common Criteria for Information Technology Security Evaluation Part 4: Framework for the specification of evaluation methods and activities; CC:2022 Revision 1, November 2022, CCMB-2022-11-004

[CC-5] Common Criteria for Information Technology Security Evaluation Part 5: Pre-defined packages of security requirements; CC:2022 Revision 1, November 2022, CCMB-2022-11-005

[ARM] ARMv7-M Architecture Reference Manual, ARM DDI ARM DDI 0403E.e N (ID021621), ARM Limited, 2021

[RNG] A proposal for: Functionality classes for random number generators, Version 2.0, 18. September 2011

[HRM] SLE97 M9900 Hardware Reference Manual, Revision 3.0, 2019-08-28

[JIL] Joint Interpretation Library, Application of Attack Potential to Smartcards, Version 3.2.1, Fabruary 2024

[ERR] M9905 M9906 Errata Sheet, Rev.3.1, 2019-06-05

[AIS31] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS31, Version 3, 2013-05-15, Bundesamt für Sicherheit in der Informationstechnik

[DSS] NIST: FIPS publication 186-4: Digital Signature Standard (DSS), July 2013

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

[N867] 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, Revised January 2012, Revision 1

[N197] U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), Advanced Encryption Standard (AES), FIPS PUB 197

[N38A] National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Data Encryption Standard, NIST Special Publication 800-38A, Edition 2001

[X962] 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), November 16, 2005, American National Standards Institute

[X963] American National Standard for Financial Services X9.63-2001, Public Key Cryptograph for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, November 20, 2001, American National Standards Institute

10 Hash values

In the following tables, the hash signatures of the respective CL97 Crypto Library files are documented. For convenience purposes several hash values are referenced.

Library	Hash

ACL v2.07.003	Cl97-LIB-base.lib:
	SHA256=02009f6c7b84b6e3d148dfa761143052720361c14babccc265aa8ce5a22a947a
	Cl97-LIB-ecc.lib:
	SHA256=8f72c8ebdad3c99c59e9d115b284e6245122bb9ab38bd93da247c282c1526383

ACL v2.09.002	ACL97-Crypto2304T-L90-base.lib:
	SHA256=1b93e84247402e585683564ba42859e5f386e9fc4758300946797832300f95cd
	ACL97-Crypto2304T-L90-ecc.lib:
	SHA256=6354bada8cd0f395bf212bd56ade39675653a8c2d409673d377da5c150abc134

NRG	NRGManagement-01.03.0927-M9900.lib
	SHA256=95f2ed5f6a3001146c9fef36c539ac2844839af0bacb92e44a2da474e6d5aa8e
	NRGReader-01.02.0800-M9900.lib
	SHA256=16848631a68b3094e29790ee34bbb95af208a9985c8e111f46849fffc4ef3385

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
BOS	Boot Software
CC	Common Criteria
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
Crypto2304T	Asymmetric Cryptographic Processor
CRT	Chinese Reminder Theorem
DPA	Differential Power Analysis
DFA	Differential Failure Analysis
EC	Elliptic Curve
ECC	Error Correction Code
EDC	Error Detection Code
EDU	Error Detection Unit
GCIM	Generic Chip Identification Mode (BOS-CIM)
EEPROM	Electrically Erasable and Programmable Read Only Memory
EMA	Electro magnetic analysis
HW	Hardware
IC	Integrated Circuit
ID	Identification
IMM	Interface Management Module
I/O	Input/Output
MED	Memory Encryption and Decryption
MPU	Memory Protection Unit
NRG	ISO/IEC14443-3 Type A with CRYPTO1
O	Objective
OS	Operating system
RAM	Random Access Memory
RMS	Resource Management System
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rives-Shamir-Adleman Algorithm
SCL	Symmetric Crypto Library
SCP	Symmetric Cryptographic Processor

SF	Security Feature
SFR	Special Function Register, as well as Security Functional Requirement
SPA	Simple power analysis
SW	Software
T	Threat
TM	Test Mode (BOS)
TOE	Target of Evaluation
TRNG	True Random Number Generator
TSF	TOE Security Functionality
UART	Universal Asynchronous Receiver/Transmitter
UM	User Mode (BOS)
UMSLC	User Mode Security Life Control
3DES	Triple DES Encryption Standard

12 Glossary

Boot System	Part of the firmware with routines for controlling the operating state and testing the TOE hardware
Central Processing Unit	Logic circuitry for digital information processing
Chip	Integrated Circuit]
Chip Identification Mode 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 BOS version number
Chip Identification Mode	Operational status phase of the TOE, in which actions for identifying the individual chip by transmitting the Chip Identification Mode data take place
Controller	IC with integrated memory, CPU and peripheral devices
Crypto2304T	Cryptographic coprocessor for asymmetric cryptographic operations
Cyclic Redundancy Check	Process for calculating checksums for error detection
Electrically Erasable and Programmable Read Only Memory (SOLID FLASH™ NVM)	Non-volatile memory permitting electrical read and write operations
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
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
Non-privilege level	Restricted (non Supervisor) mode of the CPU
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
Privilege level	Supervisor mode of the CPU
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.
Security Mechanism	Logic or algorithm which implements a specific security function in hardware or software
SCP	Symmetric cryptographic coprocessor for symmetric cryptographic operations (3DES, AES).
Security Function	Part(s) of the TOE used to implement part(s) of the security objectives
Security Target	Description of the intended state for countering threats
Smart Card	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	Person in contact with a TOE who makes use of its operational capability
User Mode	Operational status phase of the TOE in which actions intended for the user takes place
WLB	Wafer Level Ballgrid Array
WLP	Wafer Level Package

Revision History

Major changes since the last revision

Page or Reference	Description
4.9	Version of last recertification
6.2	Final version

Other Trademarks
All referenced product or service names and trademarks are the property of their respective owners.

Edition 2025-07-18
Published by
Infineon Technologies AG
81726 Munich, Germany

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

IMPORTANT NOTICE
The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics (“Beschaffenheitsgarantie”).

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, 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.

In addition, any information given in this document is subject to customer’s compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer’s products and any use of the product of Infineon Technologies in customer’s applications.

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

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

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

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