SM4128(V3) LSI FOR USE IN NATIONAL IDS AND PASSPORTS WITH SHARP SOFTWARE

SECURITY TARGET

Version:	1.8.5
Date of Issue:	29 March 2005
Prepared by:	Shigeo Ohyama, Development Department IC Card Business Development center IC Group Sharp Corporation
Additional input by:	Dirk-Jan Out and Wouter Slegers TNO-ITSEF BV

Contents

ABOUT THIS VERSION

- This version is adapted for interim use with e-passport application. The cryptographic functionality is not used and therefore removed and the non-compliance to the PP is explicitly marked.

1. ST Introduction

1.1. ST Identification

Title: LSI Security Target for SM4128(V3) IC Card for use in national IDs and passports with Sharp software
Version: 1.8.5
Date of Issue: 29 March 2005
Prepared by: Shigeo Ohyama, Development Dept.
IC Card Business Development centre
IC Group, Sharp Corporation
Assisted by: Dirk-Jan Out and Wouter Slegers
TNO-ITSEF BV
The TOE SM4128(V3) A5-step

1.2. ST Overview

The Target of Evaluation (TOE) is the SM4128(V3) A5-step module (a packaged IC), hereafter called SM4128(V3). This SHARP dual interface type module has interfaces for contact and contact-less communications, physical and logical protection mechanisms, DES and RSA/ECC coprocessors.
This module is intended for exclusive use with the Sharp software in national ID cards and electronic passports. **It is not intended for general usage.**

The rest of this ST describes the TOE, the TOE security environment, security objectives and security requirements re-used from, but **not conformant** to, [EuroPP]. augmented with addition #4 from [EuroAug], and provides argumentation why the TOE covers these requirements.

1.3. CC Conformance Claim

- The criteria applied are described in CC version 2.1 parts 1, 2, and 3.
- The methodology applied is described in CEM version 1.0 part 2
- The SFRs are CC Part 2 extended.
- The SARs are CC Part 3 conformant and consist of EAL4 augmented with ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.**3**.
- The minimum strength of function claim for the TOE is SOF-high.
- This ST re-uses all SFRs, all but one SAR (AVA_VLA.**3** instead of AVA_VLA.**4**) and all interpretations of [EuroPP]. Because of the different SAR, this ST is **not conformant** to [EuroPP]. This ST was augmented with Addition #4 "Area Based Memory Access Control" (Chapter 5) taken from [EuroAug].

Note that in concordance with "Usage of this Document" (section 1.2.2.) from [EuroAug], the text from [EuroPP] is used by reference and text from the relevant numbered paragraphs from [EuroAug] is copied in the ST (shown in *italics*) as appropriate.
The text of [EuroPP] is part of this ST as Appendix A.
This ST should be read together with [EuroAug].

2. TOE Description, scope and boundaries

The Target of Evaluation (TOE) is the SM4128(V3) module (a packaged IC). This SHARP dual interface type module has interfaces for contact and contact-less communications, physical and logical protection mechanisms, DES and RSA/EC coprocessors.
This module is intended for exclusive use with the Sharp software in national ID cards and electronic passports. **It is not intended for general usage.**

The functional features include

1) CPU Sharp original 16 bit CPU
   - General purpose register construction, 16 bit x 16
   - 62 basic commands including bit manipulation command, bit transfer instruction and bit branch instruction suitable for controlling application.
   - High speed multiplication and division instructions (16 bit x 16 bit, 16 bit / 16 bit, 32 bit /16 bit)
   - 10 types of addressing mode
   - 16M bytes address space
   - Data automatic transfer function (DTS) for highly functional interrupt processing. It is possible to automatically transfer data using hardware instead of interrupt processing when generating the demand for interrupt. Continuous operation of each type of function block is possible using DTS and continuous storage of the results and data is possible.
   - CPU clock switching function.
     CONTACT Mode: Multiplication x 3 of the CLK PORT which is input from the CLK pin and x 3/8 can be selected.
     CONTACT-LESS Mode: Multiplication x 1 of the RF CLOCK and x 1/8 can be selected.

2) Memory
   - ROM 8k Byte
   - RAM 8k Byte
   - Coprocessor RAM 1664 Byte
   - Flash memory 1024k Byte

3) Terminal for IC card ISO/IEC 7816 base
   - Communications method
   - <Contact operation>
   - ISO/IEC 7816 base T=0 & T=1 protocol
   - Operating power voltage: 2.7 - 5.5V
   - Input clock frequency: 1.0 - 5.0 MHz

   - <Contact-less operation>
   - ISO14443-2 TypeB 106kbps - 424kbps
   - The anti-collision is compatible with the slot marker method

4) Interrupt
   - In addition to a total of 15 types of interrupt, software interrupt is also possible.
   - Mask capable interrupt 15 types (external 1: internal 14)
   - Non-maskable interrupt 6 types

5) Crypto Accelerator

- RSA/ECC Crypto Accelerator integrated containing an effective countermeasure for the SPA (Simple Power Analysis) attacks.
- DES Circuit integrated containing an effective countermeasure for the DFA (Differential Fault Analysis), the SPA (Simple Power Analysis) and the DPA (Dynamic Power Analysis) attacks.

6) Timer
   - 16 bit compare type timer 2
   - 8 bit watch dog timer 1

7) Serial interface Asynchronous simultaneous (UART) 1 channel

8) PLL Integrated PLL generates an operating clock for CPU and for Crypto Accelerator in contact operation.

9) Base Register By storing the start address of the applications in Base Register, multi applications are available easily.

10) Hardware seed generator for the software DRNG

11) Watchdog Timer The SM4128(V3) is reset when the time out occurs.

12) Odd Address Access The SM4128(V3) is reset when the violation of the odd address access occurs.

13) Illegal Instruction The SM4128(V3) is reset when the illegal instruction occurs.

14) Sensors The SM4128(V3) is reset when the sensors detect an out of the specified value.

15) Over-voltage Protector The SM4128(V3) limits the internal voltage VCC.

16) Voltage Regulator The SM4128(V3) generates four voltages such as VPPO, VFF, VDD and VAA from the VCC voltage.

17) Memory Protection The SM4128(V3) is reset when the violation of the memory protection occurs.

18) Bus Scramble The data bus between the CPU and the memory is scrambled as the countermeasure for the physical attacks such as the reading and the rewriting the data bus with the probing.

19) Module The chip is covered with a resin. The module prevents an attacker from looking at the circuits of the chip because it is difficult to scratch the resin off.

20) Passivation The surface of the chip is covered with a passivation. The passivation prevents an attacker from probing the circuits directly.

21) Shielding Layer (Wire Break Down Sensor) The shielding layer covers the circuits. The wire break down sensor responds and the SM4128(V3) is reset when the shielding layer is scratched off.

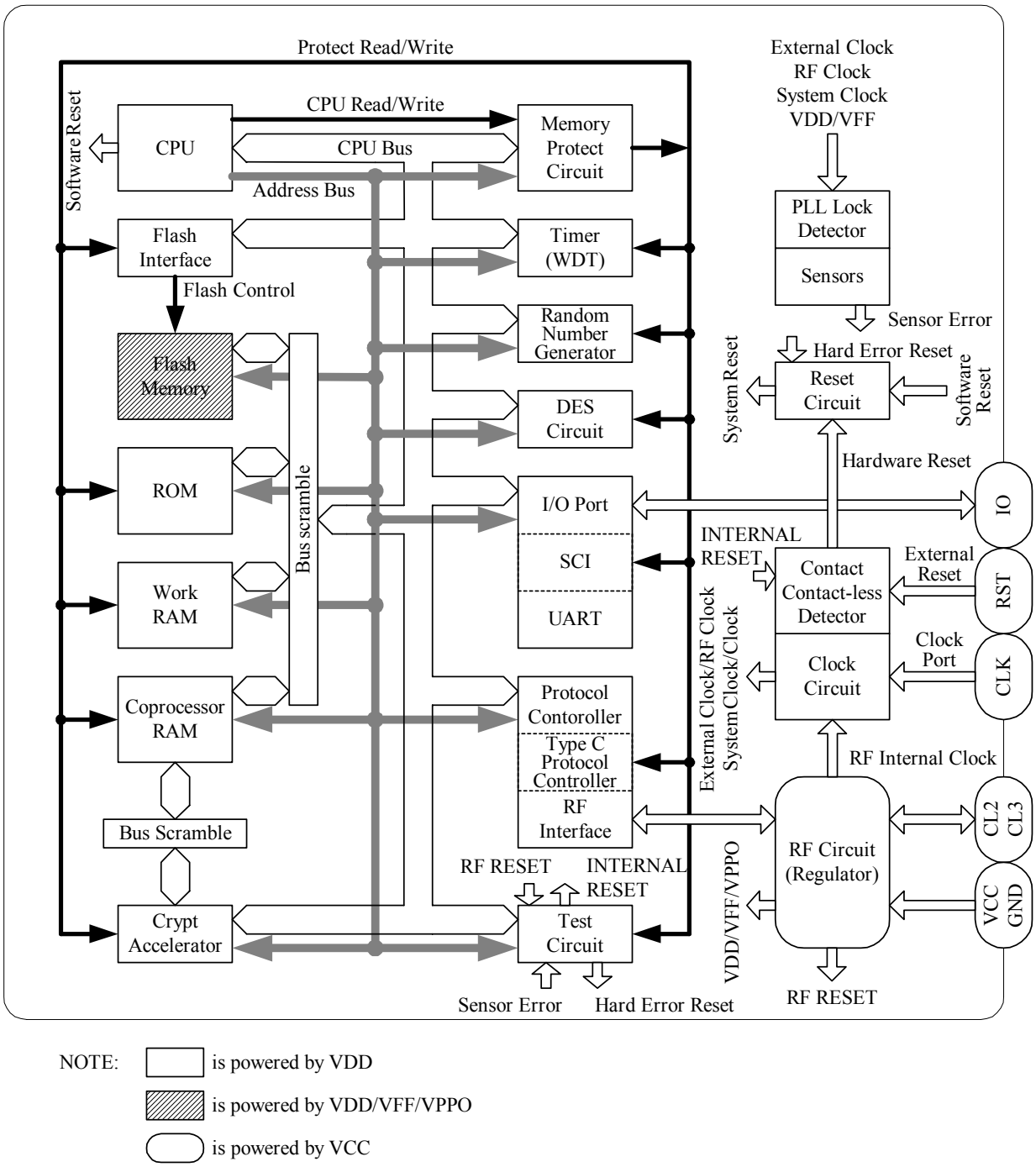

Figure 2-1: Block diagram of TOE

The TOE physically consists of a packaged module containing the following:

- The circuitry of an IC (hardware, including the physical memories RAM, ROM and Flash ROM (FROM))
- TSF data stored in the IC
- The following IC dedicated software:
    - BootROM (including DRNG function)

  - TestROM (test functionality is disabled before TOE delivery)
- The following guidance documents:
  - Technical Document of SM4128(V3)
  - Combination Type Smart Card LSI HERMES Bootstrap program Functional Specification

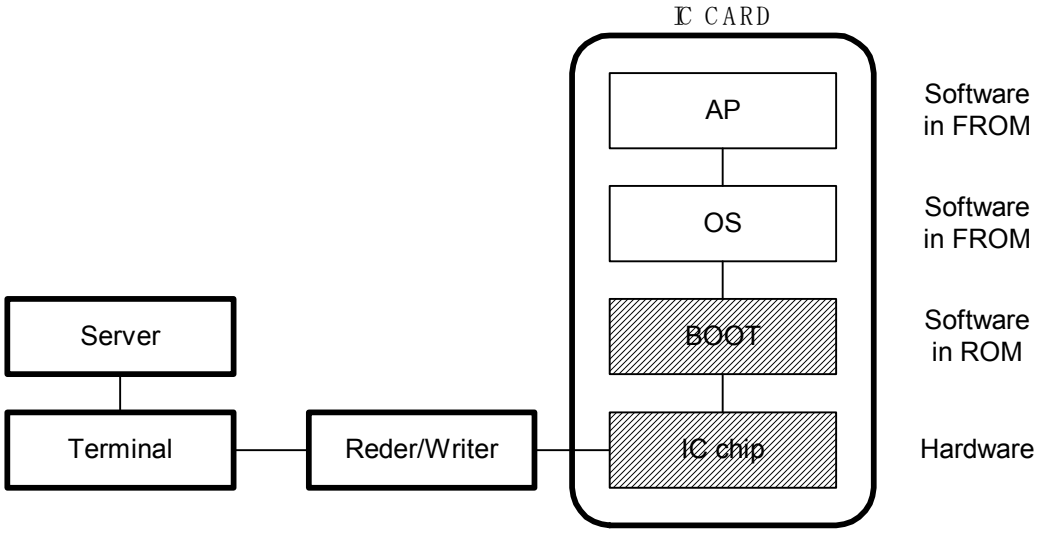

Figure 2-2 System Configuration (the shaded parts are the TOE)

The TOE logically consists of:

- Hardware, providing an execution environment for programs and the physical interaction with the reader/writer.
- BootROM, IC dedicated software for starting the OS (OS itself is outside of the TOE) and a DRNG function.
- TestROM, IC dedicated test software, disabled before TOE delivery.

Smartcard Embedded Software (outside of TOE) may be loaded in and executed from the FROM (logically outside the TOE). Only Sharp software dedicated to national ID and passport usage is allowed.

Interfaces of the TOE:

- The physical interface of the TOE to the environment is the entire surface of the module. The physical interface to an attacker consists of the entire surface of the module, the passivation layer, the shielding layer, the flat layout, the narrow wiring and the scrambled data bus.
- The environmental interface of the TOE is the temperature.
- The electrical interface of the TOE to the environment are the ISO7816 contacts (RST, CLK, and I/O), the ISO14443 contacts (CL2 and CL3), the backside pins (IOR0, IOR1, RFTEST, T_SO and MRGRD), the power pins (VCC, GND, VFF, VDD, VPPO, VPP and VNN), the covered and blocked pins (A[18:0], DQ[15:0], RPB, CEB, WEB, WPB, CK1IO, CK2IO, CPRCKIO and OEB) and the covered pins (RBB, REGDIS, T_DEMIN, T_CLK, T_RSTB, MRGRD and T_SI).
- The software interface of the TOE to the environment is via memory (including RAM, ROM, Flash and special function registers), the instruction set and DRNG function in

the BootROM.

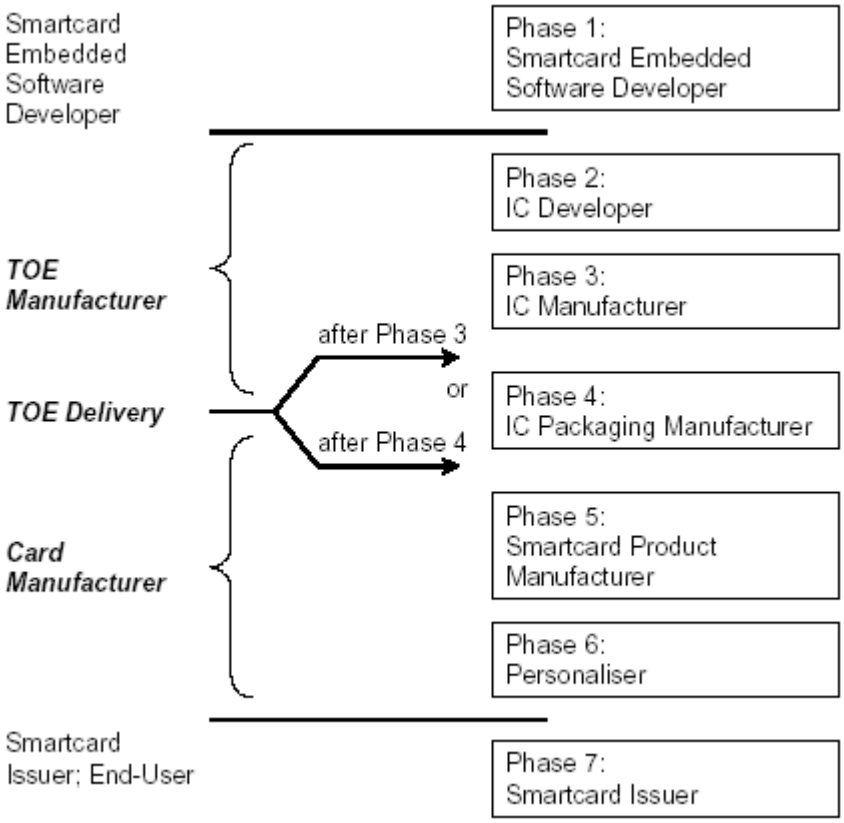

Figure 2-3 System Configuration (from [EuroPP])

The TOE is delivered in module form. This means that it is delivered at the end of Phase 4, therefore the relevant phases of the lifecycle model for this TOE are Phases 2, 3 and 4. For more information on this model, see [EuroPP], section 2.1

3. TOE Security Environment

3.1. Assumptions

The following assumptions were taken from section 3.2 of [EuroPP]:

- A.Process-Card
- A.Plat-Appl
- A.Resp-Appl

As part of Addition #4: Area based Memory Access Control, the on assumption was added.
The Smartcard Embedded Software is responsible for its User Data according to the assumption "Treatment of User Data (A.Resp-Appl)" in [3].

3.2. Threats

The following threats were taken from section 3.3 of [EuroPP]:

- T.Leak-Inherent
- T.Phys-Probing
- T.Malfunction
- T.Phys-Manipulation
- T.Leak-Forced
- T.Abuse-Func
- T.RND

As part of Addition #4: Area based Memory Access Control, the following threats were added from section 5.2.3 of [EuroAug]:
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.

- *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).

3.3. Organisational Security Policies

The following OSPs were taken from section 3.4 of [EuroPP].

- P.Process-TOE

4. Security Objectives

4.1. Security Objectives for the TOE

The following security objectives for the TOE were taken from section 4.1 of [EuroPP]:

- O.Phys-Manipulation
- O.Phys-Probing
- O.Malfunction
- O.Leak-Inherent
- O.Leak-Forced
- O.Abuse-Func
- O.Identification
- O.RND

As part of Addition #4: Area based Memory Access Control, the following objective was added from section 5.3.1 of [EuroAug]:

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 is controlled as required, for example, in a multi-application environment.

4.2. Security Objectives for the Environment

The following security objectives for the environment were taken from section 4.2 of [EuroPP]:

- OE.Plat-Appl
- OE.Resp-Appl
- OE.Process-TOE
- OE.Process-Card

As part of Addition #4: Area based Memory Access Control, no security objectives for the environment were added, but the following clarification was added:

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

The treatment of User Data is still 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. IT Security Requirements

5.1. TOE security functional requirements

The following SFRs are specified in [EuroPP]. Some are CC Part 2 extended and defined in [EuroPP].

SFR	Defined in
FAU_SAS.1	[EuroPP], Section 8.6
FCS_RND.1	[EuroPP], Section 8.4
FDP_IFC.1	CC Part 2
FDP_ITT.1	CC Part 2
FMT_LIM.1	[EuroPP], Section 8.5
FMT_LIM.2	[EuroPP], Section 8.5
FPT_FLS.1	CC Part 2
FPT_ITT.1	CC Part 2
FPT_PHP.3	CC Part 2
FPT_SEP.1	CC Part 2
FRU_FLT.2	CC Part 2

Except for FCS_RND.1, all operations on the SFRs are performed in [EuroPP].

FCS_RND.1 Quality Metric for random numbers

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet *AIS20 K3 requirements*[1].

Dependencies: No dependencies

With respect to Application Note 16 of [EuroPP], no additional generation of audit data is defined for FRU_FLT.2 and FPT_FLS.1.

With respect to Application Note 17 of [EuroPP], no additional requirement is defined for the TOE.

5.2. Additional TOE security functional requirements

The following SFRs are specified in [EuroAug]. These are drawn from CC Part 2.

5.2.1. Addition #4: "Area based Memory Access Control"

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

Memory Access Control Policy

The TOE shall control read, write accesses [2] of all subjects (software)[3] on all objects (data including code stored in memories).[4]

The TOE shall restrict the ability to define, to change or at least to finally accept the applied rules (as mentioned in FDP_ACF.1) to the Software running with the Memory Protect status Off[5].

Application Note 33: The term "at least to finally accept the applied rules" has been added to allow

---

1 [assignment: a defined quality metric]
2 [selection of operations: read, write, delete, execute accesses]
3 [assignment of subjects: software residing in memory areas]
4 [assignment of objects: data including code stored in memory areas].
5 [selection: none, [assignment of privileged subject: software with a specific attribute]]

that any software may define or change "rules" (the application of permission control information to attributes/properties). However, the TOE ensures that this is only a proposal which needs to be "finally accepted" and therefore made effective by the TSF.

Application Note 34: A Memory Management Unit may or may not perform a translation of logical to physical addresses and vice versa. If it does the terms "memory area" or "memory location" pertains to physical addresses because different software or data must have different attributes though perhaps being executed in the same logical address space. – If it does not (no address translation is performed), area or location may pertain to physical or logical addresses which are identical.

Application Note 35: For "memory areas" above specify whether this pertains to (i) types of memories or (ii) address ranges or (iii) a combination of both.

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

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the *Memory Access Control Policy*[6] on *all subjects (software), all objects (data including code stored in memories) and all the operations defined in the Memory Access Control Policy*[7]*.*

Dependencies: FDP_ACF.1 Security attribute based access control

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

FDP_ACF.1.1 The TSF shall enforce the *Memory Access Control Policy*[8] to objects based on the following: *the status of the Memory Protect (On/Off) and the memory area where the access is performed to*[9]*.*

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
If the Memory Protect is On:
access to the RAM is allowed except for:

- *the OS stack area*
- *the OS working area*
- *the co-processor shared RAM area (unless explicitly enabled)*

access to the remaining memory areas is denied, except for:

- *the application area*
- *the SCALL Protect Relief area*
- *the SRET Protect Relief area*

---

6 [assignment: access control SFP]

7 [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

8 [assignment: access control SFP]

9 [assignment: list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

- *the General Purpose Registers except the SYS register*[10].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:
If the Memory Protect is Off:
all access is allowed[11].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
none[12].

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

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

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the *Memory Access Control Policy*[13] to provide *permissive*[14] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow *any subject (provided Memory Protect is off)*[15] to specify alternative initial values to override the default values when an object or information is created.

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

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

FMT_MSA.1[On] Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the *Memory Access Control Policy*[16] to restrict the ability to *set*[17] the security attributes *Memory Protect*

[10] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[11] [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]
[12] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
[13] [assignment: access control SFP, information flow control SFP]
[14] [selection: choose one of: restrictive, permissive [assignment: other property]]
[15] [assignment: the authorised identified roles]
[16] [assignment: access control SFP, information flow control SFP]
[17] [selection: change_default, query, modify, delete, [assignment: other operations]]

status to On[18] to *the Software running with the Memory Protect status Off*[19]

Dependencies: FDP_ACC.1 Subset access control[20], FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles

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

FMT_MSA.1[Off] Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the *Memory Access Control Policy*[21] to restrict the ability to *set*[22] the security attributes *Memory Protect status to Off*[23] to *the Software running with the Memory Protect status On*[24] *only by returning control to the Software in the SCALL or SRET relief areas with the SCALL or SRET instruction respectively or to the interrupt handling Software by generating an interrupt*[25].

Dependencies: FDP_ACC.1 Subset access control[26], FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles

The TOE shall meet the requirement "Security Roles (FMT_SMR.1)" as specified below.

FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles *Software running with the Memory Protect status On and Software running with the Memory Protect status Off*[27].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: *No dependencies*[28]

The TOE shall meet the requirement "Specification of Management Functions (FMT_SMF.1)" as specified below.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

- *setting the Memory Protect status to Off, and*
- *setting the Memory Protect status to On*[29]

---

18 [assignment: list of security attributes]
19 [assignment: the authorised identified roles]
20 [selection: FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]
21 [assignment: access control SFP, information flow control SFP]
22 [selection: change_default, query, modify, delete, [assignment: other operations]]
23 [assignment: list of security attributes]
24 [assignment: the authorised identified roles]
25 refinement.
26 [selection: FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]
27 [assignment: the authorised identified roles]
28 [FIA_UID.1 Timing of identification] refined away, as there is no relevant concept of users in this TOE, only software running in roles.
29 [assignment: list of security management functions to be provided by the TSF]

Dependencies: No dependencies

5.3. Security Requirement for the IT Environment

No Security Requirements for the IT Environment are defined by [EuroPP].

No Security Requirements for the IT Environment are required by [EuroAug] for Addition #4: "Area based Memory Access Control".

5.4. Security Requirement for the Non-IT Environment

The following Security Requirements for the Non-IT Environment are defined by [EuroPP]:

- RE.Phase-1
- RE.Process-Card

No Security Requirements for the Non-IT Environment are required by [EuroAug] for Addition #4: "Area based Memory Access Control".

5.5. TOE Security Assurance Requirements

The TOE SARs consist of EAL4 augmented with ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.3, as defined by CC part 3 and as refined by [EuroPP] "Refinements of the TOE Assurance Requirements".

No TOE SARs are added or refined by [EuroAug] Addition #4: "Area based Memory Access Control".

6. TOE Summary Specification

6.1. IT Security Functions

To cover FPT_PHP.3, FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_SEP.1

SF.Passivation
The complete top layer of the IC, except for the bond pads, is covered with a passivation layer making physical attack difficult.

SF.Module
The IC (including the passivation layer) is covered with resin making physical attack difficult.

SF.Flat_Layout
The TOE's wiring rule for the logic circuits, which is called "Flat-layout", does not have hierarchies. This makes it difficult for an attacker to find the signals between the logical circuits (CPU, CPU Bus, Reset Circuit, Clock Circuit, I/O Port, Timer, UART, SCI, Memory Protect Circuit, Flash Interface, Protocol Controller, Type C Protocol Controller, Contact/Contact-less Detector, RF Interface, Crypto Accelerator, DES Circuit, PLL Lock Detector, Test Circuit).

SF.Narrow_Wiring
The wiring space of the IC is very narrow, making it difficult to change the IC or read data from it.

SF.Bus_Scrambling
The bus between the CPU and memories (Flash, ROM, RAM and coprocessor RAM) is scrambled, making it difficult to read data from it.

SF.Shielding_Layer
The two top layers of the IC (part of the TOE) are shielding layers, one passive and one active.If the active shield is broken, the TOE does not operate, making physical attacks difficult.

To cover FPT_FLS.1

SF.Watchdog_Timer
The TOE has a watchdog timer, which resets the TOE when it times out.

SF.Odd_Address
The TOE resets when it detects an odd address violation.

SF.Illegal_Instruction
The TOE resets when it detects an illegal instruction.

SF.Abnormal_Internal_Clock
The TOE resets when it detects that the period of the high level or low level of the internal clock is outside of the range FSYS_tmin specified in [FSP].

SF.Abnormal_RF_Clock
The TOE resets when, in contact-less mode, it detects that the period of the high level or low level of the RF clock outside of the range RFCS_tmin specified in [FSP].

SF.Abnormal_Temperature
The TOE resets when it detects a temperature higher than TMPS_Tmax or lower than TMPS_Tmin specified in [FSP].
SF.Abnormal_Voltage_Flash
Flash memory uses 2 power-sources. One is the internal voltage. The other is the internal program voltage.
The TOE resets when it detects the internal voltage for the flash component is less then VFFS_VL or more then VFFS_VH specified in [FSP]

SF.Abnormal_Voltage_Logic
The TOE resets when it detects an internal voltage for the logic components is less then VDDS_VL or more then VDDS_VH specified in [FSP]

To cover FRU_FLT.2

SF.Over-Voltage_Protector
Should the voltage of the internal supply power (VCC) become too high, then the TOE will absorb excess power up to a limit. If the absorbed power is too high, the TOE will disable itself permanently.

SF.Power_Regulator
The TOE regulates the internal power voltages VAA, VDD, VFF and VPPO from the internal supply power VCC.

SF.PLL
The TOE regulates the internal clock in contact operation.

To cover FMT_LIM.1, FMT_LIM.2

SF.Blocked_Test_Pins
The test pins, which are defined in [FSP], of the TOE are irreversibly blocked before the TOE is shipped to the customer

To cover FDP_ACC.1, FDP_ACF.1, FMT_MSA.3, FMT_MSA.1[On], FMT_MSA.1[Off], FMT_SMR.1, FMT_SMF.1

The following is shown as the list of security functions.

SF.Memory_Protect: The TOE enforces the following memory protection:
If the Memory Protect is On:
read/write access to the RAM is allowed except for:

- *Read/write access to the OS stack area*
- *Read/write access to the OS working area*
- *Read/write access to the co-processor shared RAM area unless explicitly enabled*

read/write access to all other memory areas is denied, except for:

- *Read access to the application area*
- *Read/write access the General Purpose Registers except the SYS register.*

SF.Memory_Protect_On: The TOE ensures that only Software running with the Memory Protect Off can turn the Memory Protect On.

SF.Memory_Protect_Off: The TOE ensures that Software running with the Memory Protect On can turn the Memory protect Off only by:

- returning control to the Software in the SCALL relief area with the SCALL instruction, or
- returning control to the Software in the SRET relief area with the SRET instruction, or
- to the interrupt handling Software by generating an interrupt.

To cover FAU_SAS.1

SF.FLASH: The TOE has flash memory capable of storing initialisation data and/or pre-personalisation data and/or supplements of the Smartcard Embedded Software.

To cover FCS_RNG.1

SF.RNG: The TOE has Deterministic Random Number Generator that meets the AIS20 K3 requirements.

6.2. Strength of Function Claim

The minimum strength of security functions for the TOE is SOF-high (Strength of Functions High). Note that this does not apply to the cryptographic functionality: the assessment of algorithmic strength is not part of the evaluation.

6.3. Assurance Measures

Assurance requirements of this TOE conform to the dependency of assurance components as well as functional components of EAL4 augmented with ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.3. Those assurance requirements are mainly to check correct implementation of IC chips through deliberate review on sources of evidence supplied by Sharp Corporation.

For definition of assurance measures necessary for compliance with security assurance requirements set forth in the Article 5.5, TOE offers correlation between assurance requirements and assurance measures intended to satisfy those requirement. As shown in Table 18, assurance measures will be provided in such a way as related documents may properly address to each of those requirements.

Table 18 List of Documents

Assurance Measures Component	Documents List
ACM_AUT.1 ACM_CAP.4 ACM_SCP.2	● SHARP QA templates ● Life Cycle v1.1 ● DesignFlow.xls ● IC Card QC Chart ● Overview of the relevant Department for SM4128 development and production version 6 ● Crushing process, document D200402008, data 20 February 2004 ● Flaw process, document D200402008, date 20 February 2004
ADO_DEL.2 ADO_IGS.1	● SHARP QA templates ● Overview of the relevant Department for SM4128 development and production version 6 ● Crushing process, document D200402008, data 20 February 2004 ● Flaw process, document D200402008, date 20 February 2004 ● Configuration Title List (Ver 6.0.1), document D200402010, date 23 February 2004
ADV_FSP.2	● Technical Document of SM4128(V3), version 1.0.0 ● Combination Type Smart Card LSI HERMES Bootstrap program Functional Specification, version 0.3.0 ● Security Correspondence of SM4128(V3), version 0.3.0
ADV_HLD.2	● Technical Document of SM4128(V3), version 1.0.0 ● Combination Type Smart Card LSI HERMES Bootstrap program Functional Specification, version 0.3.0 ● Security Correspondence of SM4128(V3), version 0.3.0 ● Hierarchy Map (Logic Part) ● HDL Source Code files
ADV_IMP.2	HDL Source Codes Layout Chart
ADV_LLD.1	SM4128 Hardware Manual
ADV_RCR.1	SM4128 Hardware Manual
ADV_SPM.1	SM4128 Hardware Manual
AGD_ADM.1 AGD_USR.1	● Technical Document of SM4128(V3), version 1.0.0 ● Combination Type Smart Card LSI HERMES Bootstrap program Functional Specification, version 0.3.0 ● SM4128(V3) Security Guidance, version 0.2

ALC_DVS.2 ALC_LCD.1 ALC_TAT.1	● SHARP QA templates ● Departments TOE development and production ● Life Cycle v1.1 ● DesignFlow.xls ● IC Card QC Chart ● Crushing process, document D200402008, data 20 February 2004
ATE_COV.2	SM4128 Test Manual
ATE_DPT.1	SM4128 Test Manual
ATE_FUN.1	SM4128 Test Manual
ATE_IND.2	SM4128 Test Manual
AVA_CCA.1	SM4128 Evaluation Report
AVA_MSU.3	SM4128 Evaluation Report
AVA_SOF.1	SM4128 Evaluation Report
AVA_VLA.3	SM4128 Evaluation Report

7. PP Claim

This ST does **not** claim conformance to any Protection Profile.

For historical reasons, this ST re-uses all SFRS, all but one SAR (AVA_VLA.**3** instead of AVA_VLA.4) and all interpretations of the "Smartcard IC Platform Protection Profile", version 1.0 of July 2001, certified by Bundesambt für Sicherheit in der Informationstechnik (BSI) under registration number BSI-PP-0002. The text of this PP is part of this ST, see Appendix A.

8. Rationale

The [EuroPP] rationales and validations are applicable for this ST because all SFRs, all but one SAR and all interpretations are re-used (by reference); the only difference is the use of SAR AVA_VLA.3 instead of SAR AVA_VLA.4. In this ST all dependencies are met just as in [EuroPP], and therefore the argumentation in the rational is equally applicable, except for the level of the attacker.
For the application area, of national IDs and passports, controlled modification of the data (i.e. counterfeiting) is the main threat. The threats described in [EuroPP], and therefore this ST, are the implementations of this main threat. The data stored on the TOE is digitally signed with a key outside of the TOE and verified outside of the TOE, or other countermeasures in the system exist to detect modification (such as verification against backend systems and physical tamper proofing). In either case, the system requires of the TOE protection against attackers with only moderate attack potential, hence the choice of AVA_VLA.3.
This TOE is therefore **not** intended for general use and in particular **not** intended for digital signature applications or payment systems.

8.1. Security Objectives Rationale

The correlation between security objectives from [EuroPP] and corresponding threats, organizational security policies or assumptions, and the adequacy is described in [EuroPP].

The correlation between security objectives from [EuroAug] addition #4 and corresponding threats, organizational security policies or assumptions, and the adequacy is described below (literal copy from [EuroAug] 5.6.1):

Application Note 38: Add the following entry to Table 1 in [3].

Assumption, Threat or Organisational Security Policy	*Security Objective*	*Note*
T.Mem-Access	*O.Mem-Access*	

The justification related to the threat "Memory Access Violation (T.Mem-Access)" is as follows:

According to O.Mem-Access the TOE must enforce the partitioning of memory areas so that access of software to memory areas is controlled. Any restrictions are to be defined by the Smartcard Embedded Software. Thereby security violations caused by accidental or deliberate access to restricted data (which may include code) can be prevented (refer to T.Mem-Access). The threat T.Mem-Access is therefore removed if the objective is met.

The clarification of "Usage of Hardware Platform (OE.Plat-Appl)" makes clear that it is up to the Smartcard Embedded Software to implement the memory management scheme by appropriately administrating the TSF. This is also expressed both in T.Mem-Access and O.Mem-Access. The TOE shall provide access control functions as a means to be used by the Smartcard Embedded Software. This is further emphasised by the clarification of "Treatment of User Data (OE.Resp-Appl)" which reminds that the Smartcard Embedded Software must not undermine the restrictions it defines. Therefore, the clarifications contribute to the coverage of the threat T.Mem-Access.

In addition to the rational from [EuroPP]:
The TOE is to be used with Sharp software for national IDs and passports.

For this usage, no confidential data is stored on the TOE: all User Data stored on the TOE is publicly readable via the software as part of its functionality, and no confidential TSF data is present for this application (there are no cryptographic keys for example). The absence of confidential data protects against the threats T.Leak-Inherent, T.Phys-Probing (i), T.Leak-Forced and T.Abuse-Func (i). This means that the objectives O.Leak-Inherent and O.Leak-Forced are completely met by not having confidential data. Of objective O.Phys-Probing, the part "disclosure of User Data" and of objective O.Abuse-Func the part "(i) to disclose critical User Data" are met also.

8.2. Security Requirements Rationale

8.2.1. Verification of Security Functional Requirements Adequacy

The correlation between security objectives from [EuroPP] and functional requirements from [EuroPP] is shown in [EuroPP], as is the adequacy.

The correlation between security objectives from [EuroAug] addition #4 and functional requirements, and the adequacy is described below (literal copy from [EuroAug] 5.6.2.1).

Application Note 39: Add the following entry to Table 2 in [3].

Objective	*TOE Security Functional Requirements*	*Security Requirements for the environment*
O.Mem-Access	• *FDP_ACC.1 "Subset access control"* • *FDP_ACF.1 "Security attribute based access control"* • *FMT_MSA.3 "Static attribute initialisation"* • *FMT_MSA.1 "Management of security attributes"*	*RE.Phase-1 "Design and Implementation of the Smartcard Embedded Software"*

The justification related to the security objective "Area based Memory Access Control (O.Mem-Access)" is as follows:

The security functional requirement "Subset access control (FDP_ACC.1)" with the related Security Function Policy (SFP) "Memory Access Control Policy" exactly require to implement an area based memory access control as demanded by O.Mem-Access. Therefore, FDP_ACC.1 with its SFP is suitable to meet the security objective.

Nevertheless, the developer of the Smartcard Embedded Software must ensure that the additional functions are used as specified and that the User Data processed by these functions are protected as defined for the application context. These issues are addressed by the requirement RE.Phase-1.

The security functional requirement "Static attribute initialisation (FMT_MSA.3)" requires that the TOE provides default values for security attributes. These default values can be overwritten by any subject (software) provided that the necessary access is allowed what is further detailed in the security functional requirement "Management of security attributes (FMT_MSA.1)": The ability to update the security attributes is restricted to privileged subject(s). These management functions ensure that the required access control can be realised using the functions provided by the TOE.

8.2.2. TOE Assurance Requirements Validation

See [EuroPP].

8.2.3. TOE SOF Validation

See [EuroPP].

8.2.4. The requirements are internally consistent

The requirements from [EuroPP] are evaluated to be internally consistent.
The requirements from [EuroAug] addition #4 applies to subjects, objects and operations unrelated to the subjects, objects and operations in [EuroPP] and therefore do not cause inconsistencies.
The requirements in [EuroAug] addition #4 handles the subjects, objects and operations consistently as the same access control policy applies for all subjects, objects and operations.

8.2.5. The requirements are mutually supportive

The requirements from [EuroPP] are evaluated to be mutually supportive.
The requirements [EuroAug] addition #4 apploes to subjects, objects and operations unrelated to the subjects, objects and operations in [EuroPP] and therefore do not undermine the mutual support of [EuroPP] requirements.
The requirements [EuroAug] addition #4 handles the subjects, objects and operations mutually supportively.

8.3. TOE Summary Specification Rationale

8.3.1. IT Security Functions Rationale

The correlation of security functions with functional requirements is shown in Table 24 and the adequacy in Table 25.

	FPT_PHP.3	FDP_IFC.1	FDP_ITT.1	FPT_ITT.1	FPT_SEP.1	FPT_FLS.1	FRU_FLT.2	FMT_LIM.1	FMT_LIM.2	FDP_ACC.1	FDP_ACF.1	FMT_MSA.3	FMT_MSA.1[On]	FMT_MSA.1[Off]	FMT_SMR.1	FMT_SMF.1	FAU_SAS.1	FCS_RND.1
SF.Passivation	×	×	×	×	×													
SF.Module	×	×	×	×	×													
SF.Flat_Layout	×	×	×	×	×													
SF.Narrow_Wiring	×	×	×	×	×													
SF.Bus_Scrambling	×	×	×	×	×													
SF.Shielding_layer	×	×	×	×	×													
SF.Watchdog_Timer						×												
SF.Odd_Address						×												
SF.Illegal_Instruction						×												
SF.Abnormal_Internal_Clock						×												
SF.Abnormal_RF_Clock						×												
SF.Abnormal_Temperature						×												
SF.Abnormal_Voltage_Flash						×												
SF.Abnormal_Voltage_Logic						×												
SF.Over-Voltage_Protector							×											
SF.Power_Regulator							×											
SF.PLL							×											
SF.Blocked_Test_Pins								×	×									
SF.Memory_Protect										×	×	×			×	×		
SF.Memory_Protect_On										×	×	×	×		×	×		
SF.Memory_Protect_Off										×	×	×		×	×	×		
SF.FLASH																	×	
SF.RNG																		×

Table 24 Correlation between IT Security Functions and Functional Requirements

Table 25 IT Security Functional Verification

#	Functional Requirements	IT Security Functions	Adequacy
1.	FPT_PHP.3, FDP_IFC.1, FDP_ITT.1, FPT_ITT.1 FPT_SEP.1	SF.Passivation SF.Module SF.Flat_Layout SF.Narrow_Wiring SF.Bus_Scrambling SF.Shielding_Layer	The following four security functions protect against physical attacks on the TOE, regardless whether the TOE is powered or not. This covers FPT_PHP.3 and FDP_IFC.1, FDP_ITT.1. FPT_ITT.1 and FPT_SEP.1 for physical attacks. **SF.Passivation** makes it hard for signals to be read out or for the module to be peeled off by covering the uppermost layer of the chip with a passivation layer. **SF.Module** makes it harder for signals to be read out or for the module to be peeled off by covering the chip with resin. **SF.Flat_Layout** makes it hard to find bus wiring on the chip as the layout is done without hierarchy in the components. **SF.Narrow_Wiring** makes it hard for signals to be read out or for the TOE to be modified by using very narrow wiring space. The following security function protects against physical attacks on the TOE when it is powered and operational. This covers FDP_IFC.1, FDP_ITT.1, FPT_ITT.1 and FPT_SEP.1 for physical attacks. **SF.Shielding_Layer** makes it hard to read signals from the TOE or modify the TOE as it contains a shielding layer. The following security function protects against eavesdropping attacks on the TOE when it is powered and operational. This covers FDP_IFC.1, FDP_ITT.1, FPT_ITT.1 and FPT_SEP.1 for eavesdropping attacks. **SF.Bus_Scrambling** makes it hard to recover the data sent between CPU and RAM by scrambling the bus.
2.	FPT_FLS.1	SF.Watchdog_Timer SF.Odd_Address SF.Illegal_Instruction SF.Abnormal_Internal_Clock SF.Abnormal_RF_Clock SF.Abnormal_Temperature SF.Abnormal_Voltage_Flash SF.Abnormal_Voltage_Logic	**SF.Watchdog_Timer** detects failure of the software to respond within a set timeframe and resets the TOE, making it harder to successfully exploit results from glitching attacks. **SF.Odd_Address** detects odd address violations and resets the TOE, making it harder to successfully exploit results from glitching attacks. **SF.Illegal_Instruction** detects illegal instructions and resets the TOE, making it harder to successfully exploit results from glitching attacks. **SF.Abnormal_Internal_Clock** detects an abnormal internal clock and resets the TOE. **SF.Abnormal_RF_Clock** detects an abnormal RF clock in contact-less mode and resets the TOE. **SF.Abnormal_Temperature** detects abnormal temperatures and resets the TOE, preventing temperature attacks.

			SF.Abnormal_Voltage_Flash detects abnormal internal flash voltage and resets the TOE. **SF.Abnormal_Voltage_Logic** detects abnormal internal logic voltage and resets the TOE. .
3.	FRU_FLT.2	SF.Over-Voltage_Protector SF.Power_Regulator SF.PLL	**SF.Over-Voltage_Protector** detects abnormal internal supply voltage and absorbs the excess power. If the absorbed excess power is too much, the TOE will be permanently disabled **SF.Power_Regulator** regulates the internal power voltages for from the internal supply power, keeping the internal power voltages constant. **SF.PLL** regulates the internal clock, suppressing fluctuations in the internal clock.
4.	FMT_LIM.1, FMT_LIM.2	SF.Blocked_Test_Pins	The following security functions protects against misuse of the test functionality by disabling all access to this test functionality prior to TOE delivery. With no access to the test functionality, the capabilities of the test functionality are not relevant. This covers FMT_LIM.1 and FMT_LIM.2. **SF.Blocked_Test_Pins** restricts logical access to the test pins by blocking them before TOE delivery.
5.	FDP_ACC.1 FDP_ACF.1 FMT_MSA.3 FMT_MSA.1[On] FMT_MSA.1[Off] FMT_SMR.1 FMT_SMF.1	SF.Memory_Protect SF.Memory_Protect_On SF.Memory_Protect_Off	**SF.Memory_Protect** enforces access control by state of the memory protect and area of the memory, covering FDP_ACC.1, FDP_ACF.1 and FMT_MSA.3. **SF.Memory_Protect_On** allows Software running with Memory Protect Off to turn Memory Protect On, covering FMT_MSA.1[On]. **SF.Memory_Protect_Off** allows Software running with Memory Protect On to turn Memory Protect Off but only by returning control to Software in the SCALL or SRET relief areas or the Software in the interrupt service routines, covering FMT_MSA.1[Off].
9.	FAU_SAS.1	SF.FLASH	**SF.FLASH** supports storage of initialisation data and/or pre-personalisation data and/or supplements of the Smartcard Embedded Software
10.	FCS_RND.1	SF.RNG	**SF.RNG** implements generation of Random Numbers with the required quality.

8.4. Assurance Requirements and Strength of Function Rationale

This ST follows the rationale given in Chap. 7.2.3 of [EuroPP] for the choice of EAL4, assurance augmentations and the strength of function SOF-high.

9. References

[AIS20] "Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators", Version 2.0, 2 December 1999.

[EuroAug] "Smartcard IC Platform Augmentations", version 1.00, March 2002"

[3] or [EuroPP] Text of the "Eurosmart Smartcard IC Platform PP", version 1.0, July 2001, see appendix A.

[FIPS46-3] National Institute of Standards and Technology (NIST), FIPS Publication 46-3: Data Encryption Standard (DES), 25 Oct 1999. Excluding Appendix 2 (TDES).

[JIL-AAPS 1.0] Joint Interpretation Library, Application of Attack Potential to Smartcards, version 1.0, March 2002

9.1. Glossary/List of abbreviations

CC	Common Criteria
DPA	Differential Power Analysis
DFA	Differential Fault Analysis
PLL	Phase Locked Loop
RAM	Random Access Memory
ROM	Read Only Memory

10. Appendix A

The literal text of "Eurosmart Smartcard IC Platform PP", version 1.0, July 2001 is reproduced below. This text is part of this ST for historical reasons. This ST is **not compliant** with the PP because it does not meet the AVA_VLA.**4**, instead it meets the AVA_VLA.3 requirement.