General Business Use

AT91SC464384RCU (Revision B)

Security Target Lite

Important notice to readers…

Atmel makes no warranty for the use of its products, other than those expressly contained in the Company's standard warranty which is detailed in Atmel's Terms and Conditions located on the Company's web site. The Company assumes no responsibility for any errors which may appear in this document, reserves the right to change devices or specifications detailed herein at any time without notice, and does not make any commitment to update the information contained herein. No licenses to patents or other intellectual property of Atmel are granted by the Company in connection with the sale of Atmel products, expressly or by implication. Atmel's products are not authorized for use as critical components in life support devices or systems.

The security of any system in which the product is used will depend on the system's security as a whole. Where security or cryptography features are mentioned in this document this refers to features which are intended to increase the security of the product under normal use and in normal circumstances.

All products are sold subject to Atmel's Terms & Conditions of Supply and the provisions of any agreements made between Atmel and the Customer. In ordering a product covered by this document the Customer agrees to be bound by those Terms & Conditions and agreements and nothing contained in this document constitutes or forms part of a contract (with the exception of the contents of this Notice). A copy of Atmel's Terms & Conditions of Supply is available on request.

Figures

AT91SC464384RCU Security Target Lite

1.1 Identification

1 Title: AT91SC464384RCU Security Target Lite

2 Version: TPG0172A_(07 Aug 08).

3 This Security Target has been constructed with Common Criteria (CC) Version 2.3.

1.2 Overview

Protection Profile Claims

4 This Security Target (ST) is conformant to the Protection Profile BSI-PP-002-2001, with additions taken from the Smartcard Integrated Circuit Augmentations BSI-AUG-2002:

Document	Title	Date
BSI-PP-002-2001	Smartcard IC Platform Protection Profile V1.0	July 2001
BSI-AUG-2002	Smartcard Integrated Circuit Platform Augmentations	March 2002

Project Derivation

5 It is for a microcontroller (MCU) device with security features. The device is a member of a family of single chip MCU devices which are intended for use within Smartcard products. The family codename is AT91SC.

Project Information:

Part Number	AT91SC464384RCU	Identifier
Product Identification Number	AT58U21	SN_0=0x43 *
Revision	B	SN_1 = 02x01 *
Atmel Toolbox Version	02.03.12.01 (outwith Scope)	0x02031201 *

Note

* As detailed in [TD] the TOE identified using serial number registers, SN_0 gives the identification of the chip ID for the TOE, SN_1 gives the revision identifier for the TOE

For the Atmel toolbox the version number is outputed by the TOE when the TBX self test function is executed [APP_TBX]

Assurance Level

6 The TOE is being evaluated against the CC Smartcard IC Platform Protection Profile (BSI-PP-002-2001) to Evaluation Assurance Level 4 (EAL4) augmented with AVA_VLA.4, ALC_DVS.2, ADV_IMP.2, and AVA_MSU.3 under the Common Criteria scheme.

Sponsor

7 Atmel Smart Card ICs, a division of ATMEL Corporation, is the developer and the sponsor for the AT90SC ASL4 evaluations.

Atmel Corporation
3235 Orchard Parkway
San Jose
CA95131
USA

Evaluation Scheme

8 The TOE is evaluated under the French CC Scheme

Centre De Certification
Direction centrale de la securite des systemes d'information
51 bouleverard de la Tour-maubourg
75700 Paris
France

Evaluator

9 The TOE is independently verified by the following Test facility (ITSEF), registered with the French CC Scheme.

Thales
BPI 1414
18 avenue Edouard Belin
Toulouse
France

Brief TOE Description

10 The devices in the AT91SC family are based on the SC100 32-bit family of single-chip microcontroller devices. The SC100 microcontroler is based on the ARM® enhanced RISC architecture. AT91SC devices are equipped with Flash, RAM, ROM and EEPROM, cryptographic coprocessors, and a host of security features to protect device assets, making them suitable for a wide range of smartcard applications.

1.3 Common Criteria Conformance Claim

11 This Security Target Lite is conformant to parts 2 and 3 of the Common Criteria, V2.3, as follows:

- Part 2 extended: the security functional requirements are based on those identified in part 2 of the Common Criteria, the additional security functional requirements are defined in BSI-PP-002-2001 Protection Profile.
- Part 3 conformant: the security assurance requirements are in the form of an EAL (assurance package) that is based upon assurance components in part 3 of the Common Criteria (CC).The augmentations used are also taken from part 3 of the Common Criteria.

1.4 Document Objective

12 The purpose of this document is to satisfy the Common Criteria (CC) requirements for a Security Target Lite; in particular, to specify the security requirements and functions, and the assurance requirements and measures, in accordance with Protection Profile BSI-PP-002-2001, Smartcard IC Platform Protection Profile, and including augmentations from, Smartcard Integrated Circuit Platform Augmentations.

1.5 Document Structure

Section 1 introduces the Security Target Lite, and includes sections on terminology, references and main actors.

Section 2 contains the product description and describes the TOE as an aid to the understanding of its security requirements and addresses the product type, the intended usage and the general features of the TOE.

Section 3 describes the TOE security environment.

Section 4 describes the required security objectives.

Section 5 describes the TOE security functional requirements.

Section 6 describes the TOE security functions.

Section 7 describes the Protection Profile (PP) claims.

Appendix A provides a glossary of the terms and abbreviations.

1.6 Scope and Terminology

13 Security objectives are defined herein with labels in the form O.xx_xx. These labels are used elsewhere for reference. Similarly, modes, assets, subjects, threats, assumptions

and organizational security policy are defined with labels of the form M.xx_xx, D.xx_xx, S.xx_xx, T.xx_xx, A.xx_xx, and P.xx_xx respectively.

14 Hexadecimal numbers are prefixed by 0x, e.g. 0xFF is 255 decimal. Binary numbers are prefixed by%, e.g.%0001 1011 is decimal 27. An integer value may be expressed as a hexadecimal, binary or decimal number, whichever form is the most convenient.

1.7 References

15 The AT91SC464384RCU Deliverables List (EDL) identifies the latest revision of the following documents, the EDL list details all the deliverables sent as evidence as part of the TOE evaluation.

- [ESOF] AT90SC Strength of Security Functions Analysis
- [STI] Standard Test Interface
- [TD] AT91SC464384RCU Technical Data (TPR0284)
- [APP_AdvX] AdvX for AT91SC Family (TPR0053)
- [APP_TBX] Using Toolbox version 02.03.12.xx (TPR0333)
- [APP_CRYPT] Efficient use of AdvX for Implementing Cryptographic Operations
- [WSR] Wafer Saw Recommendations (TPG0079)

Within this security target the above are referred to with the use of [ ] brackets, for example [WSR] refers to the document Wafer saw Recommendations, the ST user should refer to the this document for further information. Some documents listed above are only available to an ITSEF, the Composite product developer should refer to their ITSEF for guidance on what they require.

1.8 Revision History

Rev	Date	Description	Originator
A	07 Aug 08	Initial release	John Boggie

Section 2

Target of Evaluation Description

16 This part of the Security Target Lite (ST-lite) describes the Target of Evaluation (TOE) as an aid to the understanding of its security requirements and address the product type, the intended usage and the general features of the TOE.

2.1 Product Type

17 The TOE is the single chip microcontroller unit to be used in a smartcard product. Specifically, the TOE is the AT91SC464384RCU device from the AT91SC family of smartcard devices. Generally, a smartcard product may include other optional elements (such as specific hardware components, batteries, capacitors, antennae) but these are not in the scope of this Security Target.

18 The devices in the AT91SC family are based on the Low power 32-bit ARM SC100 enhanced RISC architecure. The SC100 core allows the protection and the linear addressing of up to 1M bytes of code data as well as a number of functional and security features.

19 The SC100 supports both ARM and Thumb® instruction sets. ARM instructions are 32 bits in length, they are suited to write high performance services. Thumb instructions have a single 16-bit word format, they are designed to write compact and efficient code.

20 The CPU controls 15 peripherals in a 8k-Byte space that can contain up to 32 256-byte peripherals. Each peripheral has a dedicated function such as Timer/Counters, serial pins, power control, exceptions, AdvX and other I/O functions.

21 Additional security features include power and frequency protection logic, logical scrambling on program data and addresses, Power Analysis countermeasures and memory access controlled by privileged modes.

22 The TOE requires engineering embedded software to test the device and demonstrate certain security characteristics during the development phase. In the end-usage phase there will be no engineering embedded test software in the TOE. Production test software will be downloaded into the device EEPROM and be fully erased before devices leave the test environment. This production test software is only used in the testing phase of the TOE life cycle and is fully erased before disabling Test Mode, therefore this test software is outwith the scope of the evaluation. Test Mode disable is achieved by sawing the wafer.

23 Any faulty devices returned by a customer can be put into package mode. This allows the test engineer to access the EEPROM to analyse the failure. On entering package mode the EEPROM is erased clearing any customer data, Package Mode only allows a limited set operations and inputs [PME].

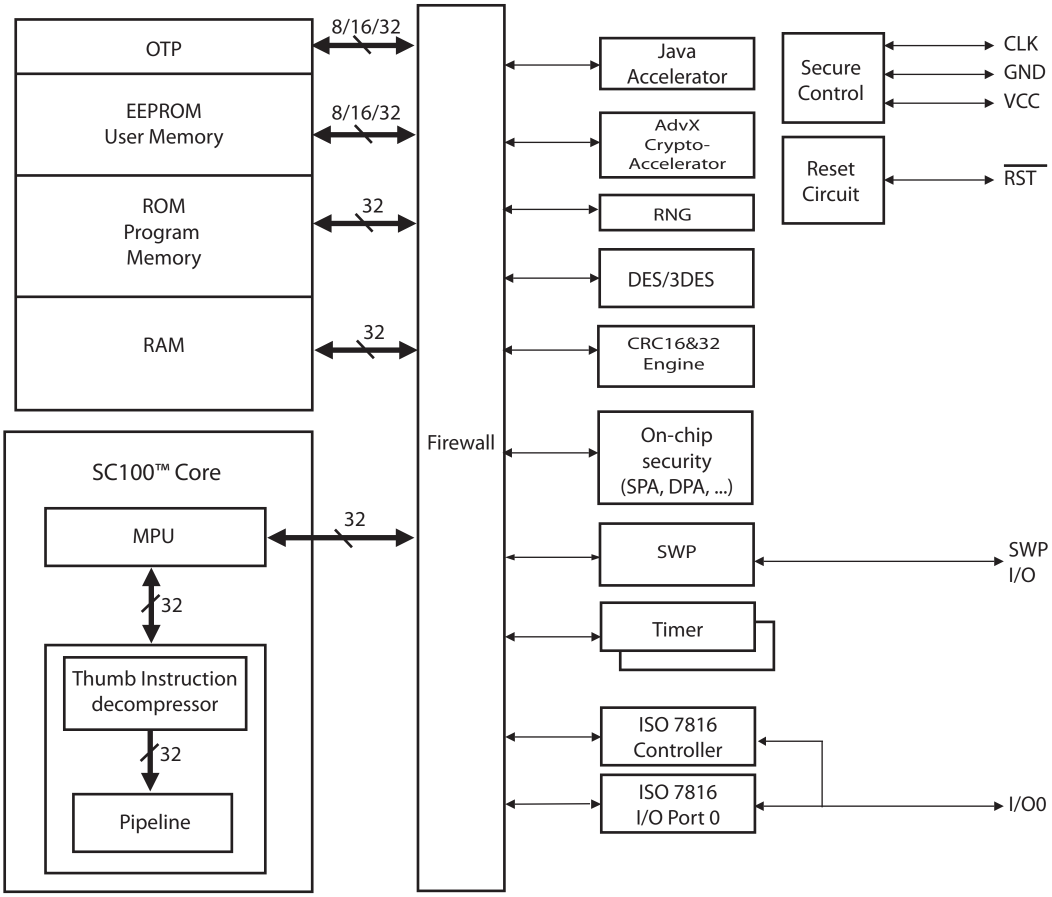


Figure 2-1 AT91SC464384RCU Block Diagram

24 Figure 2-1 shows the block diagram of the TOE, listed below is the features of the device.

General

- High performance, Low power 32-bit ARM SC100 Enhanced RISC Architecure
- Low power Idle and Power down Modes
- Bond Pad Locations Conforming to ISO 7816-2
- ESD Protection to ±6000V
- Operating Ranges: from 1.6V to 5.5V
- Compliant with GSM, 3GPP and EMV 2000 Specifications

Memory

- 464K bytes ROM Program Memory
- 384K bytes EEPROM, Including 128 OTP bytes and 384-byte Bit-addressable bytes
  - 1 to 128-byte Program/Erase
  - 1.25ms Program, 1,25ms Erase
  - Endurance: 500,000 Write/Erase Cycles at 25^{o}C
  - 10 Years Data Retention
- 16K bytes RAM memory + 2K Bytes of shared RAM

Perhiperals

- One I/O Port
- One ISO 7816 Controller
  - Up to 625 kbps at 5Mhz
  - Compliant with T=0 and T=1 Protocols
- Single Wire Protocol (SWP) Controller
- Programmable Internal Oscillator (Up to 35Mhz on ROM)
- Two 16-bit Timers with Watchdog capability
- Random Number Generator (RNG)
- 2-level, 15-Interrupt Controller
- Hardware DES and Triple DES (DPA/DEMA Resistant)
- CRC16 and 32 Engine (Compliant with ISO/IEC 3309)
- 32-bit Cryptographic Accelerator (AdvX for Public Key Operations)
  - To support RSA, DSA, Key Generation, ECC (**Outwith Scope of this evaluation**)

25 The TOE widely uses ATMEL high density non volatile memories.

26 The EEPROM includes a charge pump and its oscillator, security encoding bytes (scrambling keys, security configuration bytes), but also some chip traceability information and a transport code.

27 The TOE has a 32-bit Cryptographic Accelerator (AdvX) and a section of ROM can be loaded with either the ATMEL Toolbox library or it can be loaded with the Customer Proprietary crypto library.

02.03.12.01 Atmel Toolbox

28 The Atmel Toolbox [TBX] 02.03.12.01, software library allowing fast cryptographic algorithm implementations (RSA, SHA-1, Prime Generation,...) on the AdvX. The

cryptographic library is stored in ROM. A crypto library [TBX] with cryptographic primitives (such as modular exponentiation) is provided by ATMEL.

Note

Please note that within the scope of the evaluation is the TOE hardware. The algorithms listed above do not form part of the evaluation never the less the Atmel Toolbox must be considered as part of the evaluation, to prevent malicious interference with the security operation of the TOE.

Customer Toolbox

29 The customer may provide a proprietary cryptographic library to be implemented instead. If the customer wish to supply their own cryptographic library, Atmel give guidance on how to maintain the security level of the TOE through customer guidance notes [APP_AdvX] and [APP_CRYPT].

30 The TOE includes security logic comprising detectors which monitor voltage, frequency, temperature and light exposure.

Firewall/Memory Protection Unit

31 The memory space can be split into regions..

Note

The MPU (Memory Protection Unit) and the Firewall work together to define the memory regions that may be accesses by the various authenticated users.

32 The MPU/Firewall defines the possible modes of execution for the ARM SC100 program execution.

Java Accelerator

33 The TOE includes a Javacard Accelerator.

SWP Controller

34 The TOE includes a SWP module with the following characteristics:

- Compliant with the SWP specifications written by the SWP working group
- Full-duplex on 1 wire
- Data speed rate supported: 212Kb/s up to 1696Kb/s
- Majority filter for clock recovery
- Class B and C compliant
- Internally clocked by a 20MHz VFO
- Dedicated RAM
- Special registers to ease the code development

35 The Single Wire Protocol was designed to enable the communication between a USIM/SIM card and a Near Field Interface Component through a one line connection.

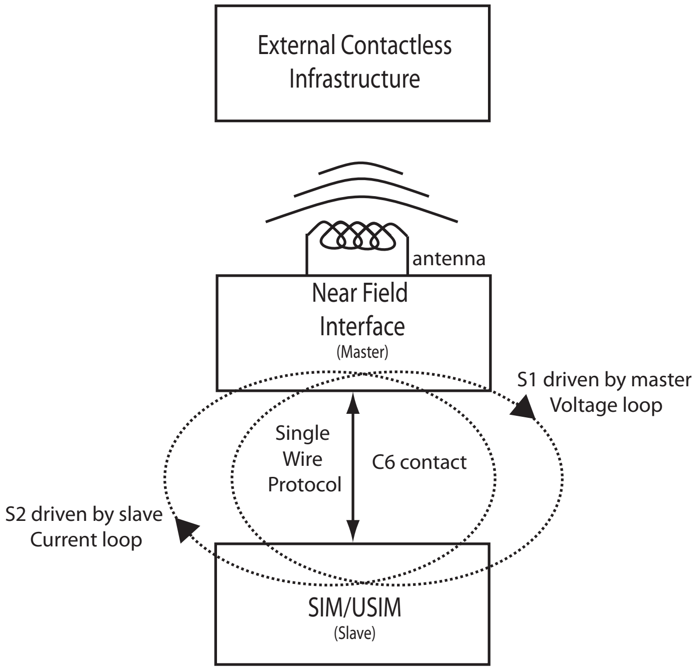


Figure 2-2 SWP Context Overview

36 Once test mode has been disabled by wafer saw the only other way to access the EEPROM test modes is to enter package mode, this is restricted mode and does not have all the features of test mode, Package mode is within the scope of the evaluation.

37 The smartcard embedded software delivered by the software developer for the device comprises ROM, EEPROM and OTP EEPROM. This smartcard embedded software is outwith the scope of the evaluation.

TOE Interfaces

38 The TOE interfaces consist of:

- The physical surface of the circuit
- The ISO7816-3 electrical contacts (VCC, GND, CLK, RST, I/O0)
- The Single Wire Protocol I/O
- The software interface to the hardware component through memories and registers

Customer Software Guidance Documents

39 The guidance documents applicable for the development of the smartcard embedded software for this TOE are:

- [TD] AT91SC464384RCU Technical Data (TPR0284)
- [ATM_CG] ARM Developer Suite Compilers and Libraries Guide
- [APP_SEC] Security Recommendations for the AT91SC464384RCU Product (TPR0267)
- [APP_DES] Secure Hardware DES/TDES on the AT91SC ASL4 Products
- [APP_RNG_ENT] Generating Random Numbers with a controlled entropy on the AT91SC464384RCU Product (TPR0331)
- [TBX] Toolbox 02.03.12.00 for AT91SCxxxxC Family with AdvX (TPR0333)
- [APP_SCRY] Securing Cryptographic Operations on AT90SC products with the Toolbox 3.10.x (TPR0260)
- [APP_CRYPT] Efficient use of AdvX for Implementing Cryptographic Operations
- [WSR] Wafer Saw Recommendations (TPG0079)

40 The software developer should refer to the Certification report issued by BSI for the correct revisions of the documents stated above.

2.1.1 Scope of Evaluation Summary

Within the Scope of the Evaluation

- AT91SC464384RCU Hardware device
- Package Mode
- Atmel Security User Guidance as detailed on page 20
- The TOE interfaces as detailed in Section 38
- Phases 2-3 of the Life Cycle
- The Atmel Toolbox 02.03.12.00

Outwith the Scope of the Evaluation

- Software loaded during Phase 2-3, used to test the TOE
- Atmel Toolbox Cryptographic functions
- Customer Toolbox code

- Strength of Cryptographic Functions
- Phases 1 and 4-7 of the Life Cycle

2.2 Smartcard Product Life-cycle

41 The smartcard product life-cycle consists of 7 phases where the following authorities are involved

.

Table 2-1 Smartcard Product Life-cycle

Phase 1	Smartcard software development	The smartcard software developer is in charge of the smartcard embedded software development and the specification of IC pre-personalization requirements,
Phase 2	IC Development	The IC designer designs the IC, develops IC dedicated software, provides information, software or tools to the smartcard software developer, and receives the software from the developer, through trusted delivery and verification procedures. From the IC design, IC dedicated software and smartcard embedded software, the IC designer constructs the smartcard IC database, necessary for the IC photomask fabrication.
Phase 3	IC manufacturing and testing	The IC manufacturer is responsible for producing the IC through three main steps: ▪ IC manufacturing ▪ IC testing ▪ IC pre-personalization
Phase 4	IC packaging and testing	The IC packaging manufacturer is responsible for the IC packaging and testing.
Phase 5	Smartcard product finishing process	The smartcard product manufacturer is responsible for the smartcard product finishing process and testing.
Phase 6	Smartcard personalization	The personalizer is responsible for the smartcard personalization and final tests. Other application software may be loaded onto the chip at the personalization process.
Phase 7	Smartcard end-usage	The smartcard issuer is responsible for the smartcard product delivery to the smartcard end-user, and the end of life process.

Life Cycle Definition

42 The limits of the evaluation correspond to phases 2 and 3, including the phase 1 delivery and verification procedures and the TOE delivery to the IC packaging manufacturer ; procedures corresponding to phases 4, 5, 6 and 7 are outside the scope of the Security Target.

43 Nevertheless, in certain cases, it would be of great interest to include the phase 4 (IC packaging and testing), within the limits of the TOE. However, for the time being, this option remains outside the scope of this Security Target.

44 Figure 2-3 describes the Smartcard product life-cycle.

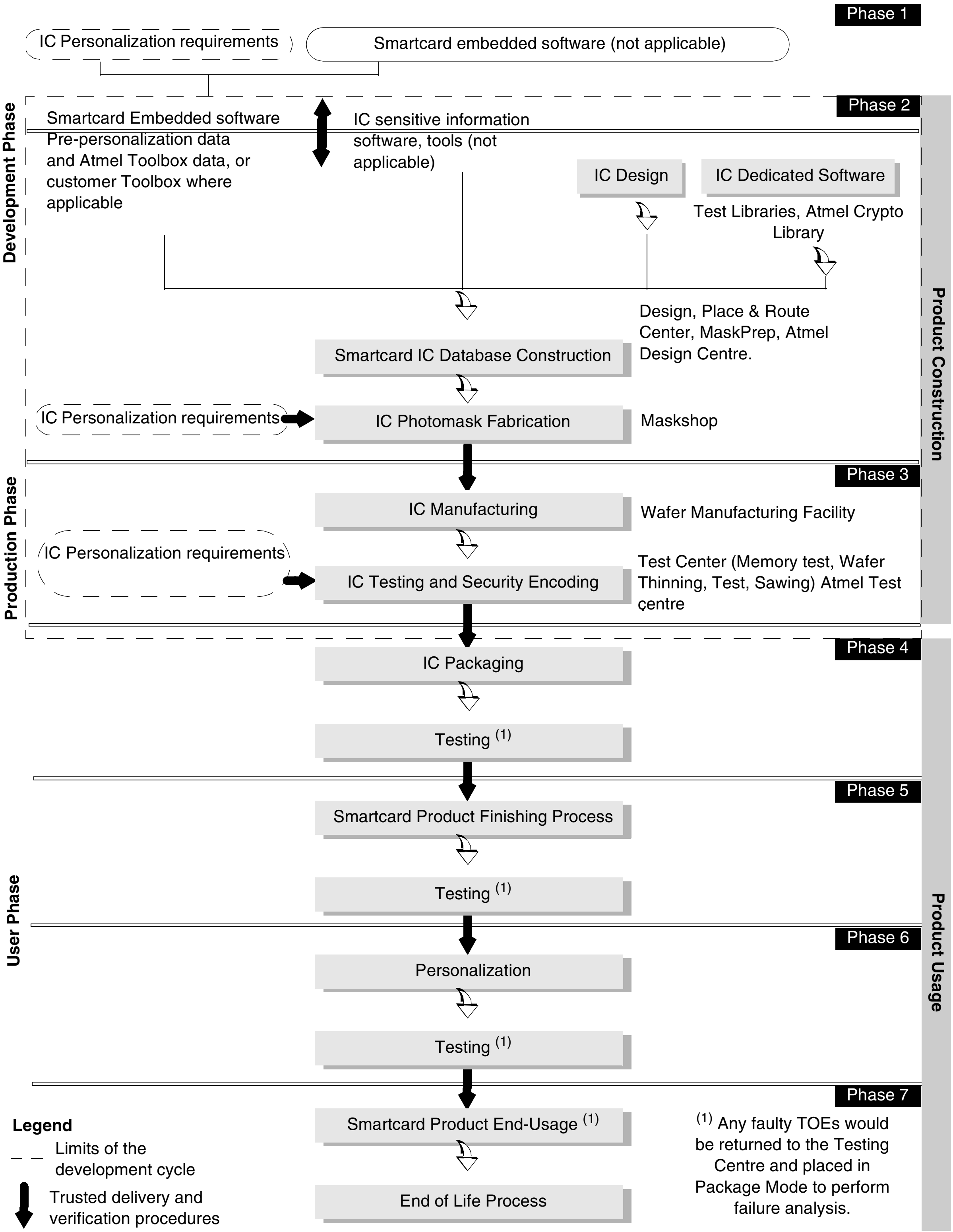

Phase 1
IC Personalization requirements
Smartcard embedded software (not applicable)
Phase 2
Development Phase
Smartcard Embedded software Pre-personalization data and Atmel Toolbox data, or customer Toolbox where applicable
IC sensitive information software, tools (not applicable)
IC Design
IC Dedicated Software
Test Libraries, Atmel Crypto Library
Design, Place & Route Center, MaskPrep, Atmel Design Centre.
Smartcard IC Database Construction
IC Personalization requirements
IC Photomask Fabrication
Maskshop
Phase 3
Production Phase
IC Manufacturing
Wafer Manufacturing Facility
IC Personalization requirements
IC Testing and Security Encoding
Test Center (Memory test, Wafer Thinning, Test, Sawing) Atmel Test çentre
Product Construction
Phase 4
IC Packaging
Testing (1)
Phase 5
Smartcard Product Finishing Process
Testing (1)
User Phase
Phase 6
Personalization
Testing (1)
Phase 7
Smartcard Product End-Usage (1)
End of Life Process
Product Usage
Legend
_ _ Limits of the development cycle
Trusted delivery and verification procedures
(1) Any faulty TOEs would be returned to the Testing Centre and placed in Package Mode to perform failure analysis.

Figure 2-3 Smartcard Product Life Cycle

Secure Delivery Between Phases

45 These different phases may be performed at different sites; procedures on the delivery process of the TOE shall exist and be applied for every delivery within a phase or between phases. This includes any kind of delivery performed from phase 1 to phase 7, including:

- Intermediate delivery of the TOE or the TOE under construction within a phase
- Delivery of the TOE or the TOE under construction from one phase to the next

46 These procedures shall be compliant with the assumptions [A_DLV] developed in Section 3.2.

47 Although the return of faulty TOEs is applicable to Phases 4-7 therefore outwith the scope of the evaluation, the fact that Package mode is controlled by hardware means that Package mode is within the scope of the evaluation.

2.3 TOE Environment

48 Considering the TOE, three types of environments are defined:

- Development environment corresponding to phase 2
- Production environment corresponding to phase 3
- User environment, from phase 4 to phase 7

2.3.1 TOE Development Environment

49 To assure security, the environment in which the development takes place is made secure with controllable accesses having traceability. Access to the development building is strictly monitored by a security person. Visitors must sign a log book and record the time of arrival and time of departure to the building. All visitors are escorted by authorized personnel at all times. All authorized personnel involved fully understand the importance and the rigid implementation of the defined security procedures.

50 The development begins with the TOE's specification. All parties in contact with sensitive information are required to abide by Non-Disclosure Agreements.

51 Design and development of the IC then follows. The design engineer uses appropriate software tools running on a UNIX operating system with the necessary password controls to make his schematic entry/RTL descriptions, design simulations, verifications and generation of the TOE's IC photomask databases. Sensitive documents, databases on tapes, diskettes, and circuit layout information are stored in appropriate locked cupboards and safes. Disposal of unwanted confidential data is carried out by shredding (paper documents) or complete electronic erasures (electronic documents, databases).

52 Reticles and photomasks are generated from the verified IC database. These are manufactured by Maskshop, for wafer fab processing undertaken as within the Atmel Manufacturing Facility. Data is transferred from the ATMEL design centre to the photomask manufacturer by means of an encrypted electronic link or handcarried tapes. The reticles and photomasks are then shipped in a secure manner to the wafer fab processing facilities.

2.3.2 TOE Production Environment

53 Production starts within the Wafer Fab; here the silicon wafers undergo diffusion processing in 25-wafer lots. Computer tracking at wafer level throughout the process is achieved by a based batch tracking system.

54 The tracking system is an on-line manufacturing system which monitors the progress of the wafers through the fabrication cycle. After fabrication the wafers are tested for memory wake-up, then, sent to Test Center where they are thinned to a pre-specified thickness and tested. The TOE is then tested to assure conformance with the device specification. During the IC testing, security encoding is performed where some of the EEPROM bytes are programmed with the unique traceability information, and the customer software is loaded in the EEPROM if required.

55 The wafers are inked to separate the functional ICs from the non-functional ICs. Finally, the wafers are thinned, sawn and then shipped to the customer. Unsawn wafers may be shipped to the customer if requested.

Note The TOE is thinned to a thickness of 150 µm. If the customer require a different thickness they have the option to specify this using their Purchase Order (PO)

2.3.3 TOE User Environment

56 The TOE user environment is the environment of phases 4 to 7.

57 At phases 4, 5, and 6, the TOE user environment is a controlled environment.

58 Following the sawing step, the wafers are split into individual dies. The good ICs are assembled into modules in a module assembly plant.

59 Further testing is carried out followed by the shipment of the modules to the smartcard product manufacturer (embedder) by means of a secure carrier.

60 Additional testing occurs followed by smartcard personalization, retesting and then delivery to the smartcard issuer.

End-user environment (Phase 7)

61 Smartcards are used in a wide range of applications to assure authorized conditional access. Examples of such are Pay-TV, Banking Cards, Portable communication SIM cards, Health cards, Transportation cards.

62 Therefore, the user environment covers a wide spectrum of very different functions, thus making it difficult to avoid or monitor any abuse of the TOE.

2.4 TOE Logical Phases

63 During its construction usage, the TOE may be under several life logical phases. These phases are sorted under a logical controlled sequence. The change from one phase to the next shall be under the TOE control.

2.5 TOE Intended Usage

64 The TOE can be incorporated in several applications such as:

- Banking and finance market for credit/debit cards, electronic purse (stored value cards) and electronic commerce.
- Network based transaction processing such as mobile phones (GSM SIM cards), pay-TV (subscriber and pay-per-view cards), communication highways (Internet access and transaction processing).
- Transport and ticketing market (access control cards).
- Governmental cards (ID-cards, healthcards, driver license etc).
- Multimedia commerce and Intellectual Property Rights protection.

65 During the phases 1, 2, 3, the product is being developed and produced. The administrators are the following:

- The smartcard embedded software developer
- The smartcard IC designer

  The Atmel toolbox [TBX] is developed during Phase 2 of the product life cycle.
- The IC manufacturer

66 Table 2-2 lists the users of the product during phases 4 to 7.

Table 2-2 Phases 4 to 7 Product Users

Phase 4	■ Packaging manufacturer (administrator) ■ Smartcard embedded software developer ■ System integrator, such as the terminal software developer
Phase 5	■ Smartcard product manufacturer (administrator) ■ Smartcard embedded software developer ■ System integrator, such as the terminal software developer
Phase 6	■ Personalizer (administrator) ■ Customers who, before manufacture, determine the MCU's mask options and the initial memory contents (i.e. the application program), and who, after manufacture, incorporate the MCU into devices. Customers are trusted and privileged users. ■ Smartcard issuer (administrator). ■ Smartcard embedded software developer. ■ System integrator, such as the terminal software developer.
Phase 7	■ Smartcard issuer (administrator) ■ Smartcard end-user, who use devices incorporating the MCU. End-users are not trusted and may attempt to attack the MCU. ■ Smartcard software developer. ■ System integrator, such as the terminal software developer. **Note** The IC manufacturer and the smartcard product manufacturer may also receive ICs for analysis, should problems occur during the smartcard usage.

67 The product may be used in the following modes:

a) Test Mode, in which the product runs under the control of dedicated test software After testing, Test Mode is permanently disabled by sawing off the test pads, and the product is set to User Mode.Test Mode is permanently disabled by sawing the wafer.

b) Package Mode is a mode similar to Test Mode for testing returns from Phases 4-7. Package Mode runs a limited subset of test commands. This mode is intended to be used solely by authorized staff.

c) User Mode, in which the product runs under control of the Product Embedded Software. It is intended that customers and end-users will always use the product in User Mode. This mode is reserved for Phases 4 to 7. If a faulty TOE is returned from the field then analysis can be done either in User Mode, or Package Mode by an authorized test engineer.

68 The only modes of operation are those stated in paragraph 67 a), b) and c).

2.6 General IT Features of the TOE

69 The TOE IT functionalities consist of tamper resistant data storage and processing such as:

- Arithmetic functions (e.g. incrementing counters in electronic purses, calculating currency conversion in electronic purses)
- Data communication
- Cryptographic operations (e.g. random number generation, data encryption, digital signature verification)

TOE Security Environment

70 This section describes the security aspects of the environment in which the TOE is intended to be used, and addresses the description of the assets to be protected, the assumptions, the threats, and the organizational security policies.

71 The environment elements are derived from BSI-PP-002-2001 and adapted to the AT91SC464384RCU TOE to cover all the phases of the TOE life cycle, and also the delivery from one phase to another.

3.1 Assets

3.1.1 Assets regarding the Threats

72 Assets are security relevant elements of the TOE that include the Primary and Secondary assets.

Primary Assets

- User application data (D.xxx_DATA) of the TOE comprising the IC pre-personalization requirements, located in:
  - CPU ROM (D.CPU_ROM_DATA),
  - Crypto ROM (D.CRYPTO_ROM_DATA),
  - EEPROM (D.EEPROM_DATA),
  - CPU RAM (D.CPU_RAM_DATA),
  - Crypto RAM (D.ADVX_RAM_DATA),
  - Peripherals (D.PERIPH_DATA),

The User data can be subject to manipulation and disclosure while being stored or processed by the TOE.

- Smartcard embedded software (D.xxx_SOFT) located in:
  - CPU ROM (D.CPU_ROM_SOFT),
  - Crypto ROM (D.CRYPTO_ROM_SOFT),
  - EEPROM (D.EEPROM_SOFT),

Smartcard Embedded software needs to be protected to prevent manipulation and disclosure.

- IC dedicated software (D.xxx_DSOFT) located in:

  - CPU ROM (D.CPU_ROM_DSOFT),
  - Crypto ROM (D.CRYPTO_ROM_DSOFT),
  - CPU EEPROM (D.EEPROM_DSOFT),
- IC dedicated support software:
  - Random numbers generated by the TOE (D.RNG_DATA)

73 Therefore, the TOE itself is an asset.

Secondary Assets

74 There are many ways to manipulate or disclose the User Data:

1. An attacker may manipulate the smartcard Embedded Software or the TOE (Primary assets)
2. An attacker may cause malfunctions of the TOE or abuse Test Features provided by the TOE.

Such attacks usually require design information of the TOE to be obtained. Therefore, the design information is a secondary asset.

- IC specification (D.IC_SPEC)
- Design (D.DESIGN)
- Development tools (D.DEV_TOOLS)
- Technology (D.TECHNO)
- Photomasks (D.MASK)

75 The above secondary assets disclose the following information to an attacker and therefore need to be protected.

1. The circuitry of the IC (hardware including the physical memories)
2. The IC dedicated Software with the parts IC Dedicated Test software, and IC dedicated support software
3. The TSF data

76 Assets must be protected in terms of confidentiality and integrity.

Grouping of Assets / Object Definition

77 These assets can be grouped to define objects that must be protected, which is useful for the following sections of this document.

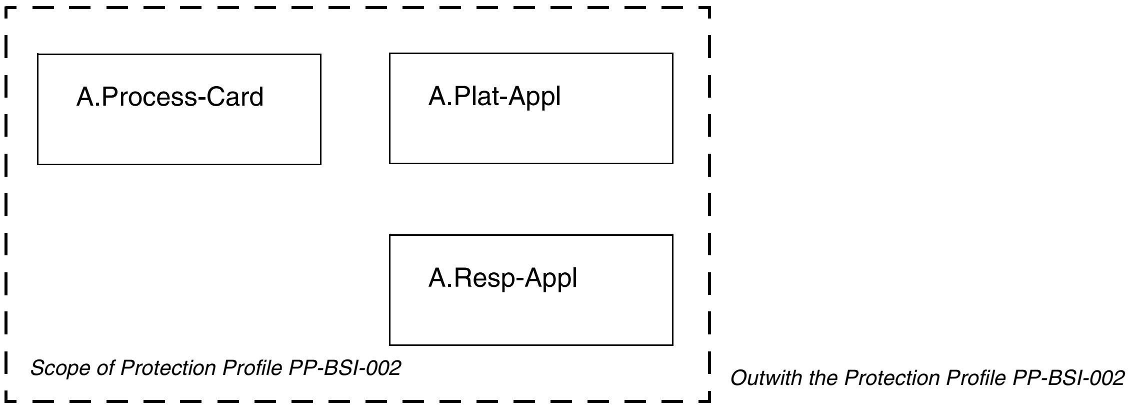
- O1: CPU ROM: covering D.CPU_ROM_DATA, D.CPU_ROM_SOFT, D.CPU_ROM_DSOFT,
- O2: EEPROM: covering D.EEPROM_DATA, D.EEPROM_SOFT, D.EEPROM_DSOFT,

- O3: Crypto ROM: covering D.CRYPTO_ROM_DATA, D.CRYPTO_ROM_SOFT, D.CRYPTO_ROM_DSOFT,
- O4: CPU RAM: covering D.CPU_RAM_DATA,
- O5: CRYPTO RAM: covering D.CRYPTO_RAM_DATA,
- O6: Peripherals and IO Registers: covering D.PERIPH_DATA, D.RNG_DATA,

3.2 Assumptions

78 This Security Target claims conformance to the BSI-PP-002-2001 “Smartcard IC Platform Protection Profile”, the assumptions defined in section 3.2 of the PP are valid for this security target and are listed below.

Figure 3-1 Assumptions


A.Process-Card
A.Plat-Appl
A.Resp-Appl
Scope of Protection Profile PP-BSI-002
Outwith the Protection Profile PP-BSI-002

A.Plat-Appl

Usage of Hardware Platform

The Smartcard Embedded Software shall be designed according to the latest TOE user guidance as stated in Section 2.1 on page 20. The Smartcard Embedded Software designer should also take into account the findings of the TOE evaluation report.

Applies to Phase 1

A.Resp-Appl

Treatment of User Data

User data is owned by the Smartcard Embedded Software. Therefore, is assumed that security relevant User Data for example Cryptographic keys, are treated by the Smartcard Embedded Software according to the requirements of the specific end application.

Applies to Phase 1

A.Process-Card

Protection during Packaging, Finishing and Personalisation

It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-user to maintain confidentiality and integrity of the TOE. These procedures shall prevent any possible copy, modification, retention, theft or unauthorised use of the TOE or the system

In the case where unsawn wafers are delivered, it is assumed that the wafer saw guidance is known and used by the customer [WSR].

Applies to Phase 4-6

3.3 Threats

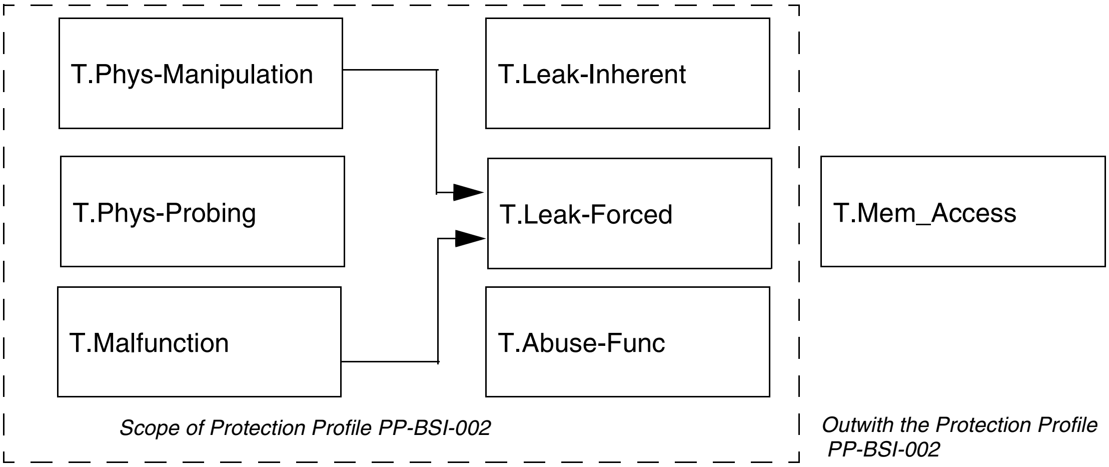
79 This Security Target claims conformance to the BSI-PP-002-2001 “Smartcard IC Platform Protection Profile”, the threats defined in section 3.3 of the PP are valid for this security target and are listed below.

According to BSI-PP-002-2001, there are the following standard high-level security concerns

SC1	Manipulation of User Data and of the Smartcard Embedded Software (while being executed/processed and while being stored in the TOE’s memories)
SC2	Disclosure of User Data and of the Smartcard Embedded Software (while being processed and while being stored in the TOE’s memories)
SC3	Deficiency of random numbers

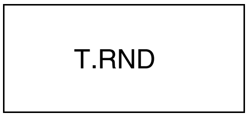
80 The security concerns 1 and 2 give rise to the following threats:

Figure 3-2 Standard Threats



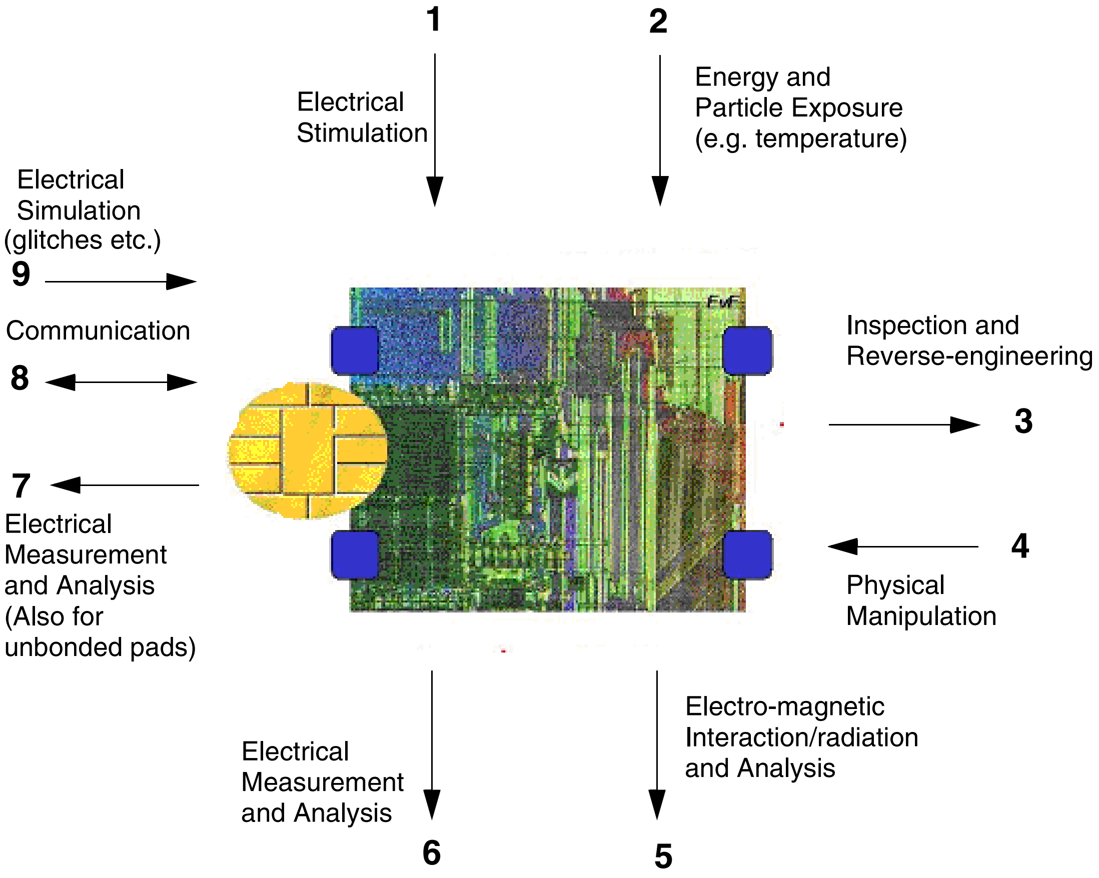
81 The security concern 3 gives rise to the following threat:

Figure 3-3 Specific Threat



82 The TOE is exposed to different types of influences or interactions with it's outside world. Some of them may result from just using the TOE, others may also indicate an attack. The different types of influences or interactions are shown in Figure 3-4.

Figure 3-4 Attack Model for the TOE


1
Electrical Stimulation
2
Energy and Particle Exposure (e.g. temperature)
Electrical Simulation (glitches etc.)
9
Communication
8
Inspection and Reverse-engineering
3
7
Electrical Measurement and Analysis (Also for unbonded pads)
4
Physical Manipulation
Electrical Measurement and Analysis
6
Electro-magnetic Interaction/radiation and Analysis
5

83 An interaction with the TOE can be done through the ISO interfaces (number 7-9 in Figure 3-4) which are realized using contacts. Influences or interactions with the TOE also occurs through the chip surface (number 1-6 in Figure 3-4). In number 1and 6 galvanic contacts are used. In number 2 and 5 the influence (arrow directed to the chip) does not require a contact. Number 3 and 4 refer to specific situations where the TOE and it's functional behaviour is not only influenced but definite changes are made by applying mechanical, chemical and other methods (such as 1 and 2). Many attacks require a prior inspection and some reverse-engineering (number 3).

84 The Smartcard Embedded Software must contribute to averting the threats: At least it must not undermine the security provided by the TOE. For details refer to the assumptions regarding the Smartcard Embedded Software, specified in Section 3.2.

Standard Threats (referring to SC1 and SC2).

85 The TOE shall avert the threats listed below:

T.Leak-Inherent **Inherent Information Leakage**

An attacker may exploit information which is leaked from the TOE during usage of the smartcard in order to disclose confidential data (User Data or TSF data).

No direct contact with the smartcard internal is required here. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. One example is the Differential Power Analysis (DPA). This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from direct (contact) measurements (numbers 6 and 7 Figure 3-4) or measurement of emanations (number 5) and can be related to the specific operation being performed.

T.Phys-Probing

Physical Probing

An attacker may perform physical probing of the TOE in order to:

- Disclose User Data
- Disclose/reconstruct the Smartcard Embedded Software
- Disclose other critical operational information especially TSF data

Physical probing requires direct interaction with the Smartcard Integrated Circuit internals (numbers 5 and 6 Figure 3-4). Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before hardware security mechanisms and layout characteristics need to be identified (number 3). Determination of software design including treatment of User Data may also be a perquisite.

This pertains to “measurements” using galvanic contacts or any type of charge interaction whereas manipulations are considered under the threat “Physical Manipulation” (T.Phys-Manipulation). The threats “inherent Information Leakage” (T.Leak-Inherent) and “Forced Information Leakage” (T.Leak-Forced) may use physical probing but require complex signal processing in addition.

T.Malfunction

Malfunction due to Environmental Stress

An attacker may cause a malfunction of TSF or of the Smartcard Embedded Software by applying environmental stress in order to:

- Deactivate or modify security features or functions of the TOE
- Deactivate or modify security functions of the Smartcard Embedded Software

This may be achieved by operating the smartcard outside the normal operating conditions (numbers 1, 2 and 9 Figure 3-4).

To exploit this the attacker needs information about the functional operation.

T.Phys-Manipulation **Physical Manipulation**

An attacker may physically modify the smartcard in order to:

- Modify security features or functions of the TOE
- Modify security functions of the Smartcard Embedded Software
- Modify User Data

The modification may be achieved through techniques commonly employed in IC failure analysis (Numbers 1, 2 and 4 in Figure 3-4) and IC reverse engineering efforts (Number 3 in Figure 3-4). The modification may result in the deactivation of a security function. Before that hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data may also be a pre-requisite. Changes of circuitry or data can be permanent or temporary.

In contrast to malfunctions (refer to T.Malfunction) the attacker requires to gather significant knowledge about the TOE's internal construction here (number 3 Figure 3-4).

T.Leak-Forced **Forced Information Leakage**

An attacker may exploit information which is leaked from the TOE during usage of the product in order to disclose confidential data (User Data, TSF data) even if the information leakage is not inherent but caused by the attacker.

This threat pertains to attacks where methods described in “Malfunction due to Environmental Stress” (refer to T.Malfunction) and/or “Physical Manipulation” (refer to T.Phys-Manipulation) are used to cause leakage from signals (numbers 5, 6, 7 and 8 Figure 3-4) which normally do not contain significant information about secrets.

T.Abuse-Function **Abuse of Functionality**

An attacker may use functions of the TOE which may not be used after TOE delivery in order to:

- Disclose or manipulate User Data
- Manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or of the Smartcard Embedded Software
- Enable an attack

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). Any restrictions are defined by the security policy of the specific application context.

Threats Related to Specific Functionality (referring to SC3)

86 The TOE shall avert the threat below

T.RND **Deficiency of Random Numbers**

An attacker may predict or obtain information about random numbers generated by the TOE for instance because of a lack of entropy of the random numbers provided.

An attacker may gather information about the reduced random numbers which might be a problem because they may be used for instance to generate cryptographic keys.

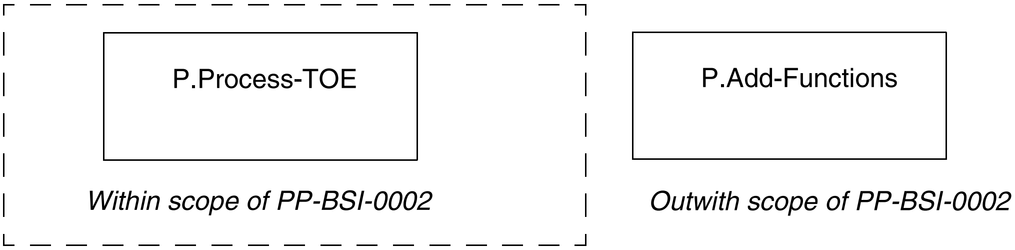
Here the attacker is expected to take advantage of statistical properties of the random numbers generated by the TOE without specific knowledge about the TOE's generator. Malfunctions or premature ageing are also considered which may assist in getting information about random numbers.

3.4 Organizational Security Policies

87 This Security Target claims conformance to the BSI-PP-002-2001 "Smartcard IC Platform Protection Profile", the Security Policy defined in section 3.2 of the PP is valid for this security target and is listed below.

88 The TOE may provide specific security functionality which can be used by the Smartcard Embedded Software. Particular specific security functionality may not necessarily be 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. Therefore, the necessity of some specific functionality may not derived from a threat. The Security organizational policies are shown in Figure 3-5.

Figure 3-5 Organizational Security Policies



89 The TOE developer must apply the policy “Protection during TOE Development and Production” (P.Process-TOE) as specified below.

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

The TOE Manufacturer must ensure that the development and production of the Smartcard Integrated Circuit (Phase 2 up to TOE Delivery, refer to Section 2.2) is secure so that no information is unintentionally made available for the operational phase of the TOE. For example, the confidentiality and integrity of design information and test data shall be guaranteed; access to samples, development tools and other material shall be restricted to authorised persons only; scrap will be destroyed etc. This not only pertains to the TOE but also to all information and material exchanged with the developer of the Smartcard Embedded Software and therefore especially to the Smartcard Embedded Software itself. This includes the delivery (exchange) procedures for Phase 1 and the Phases after TOE Delivery as far as they can be controlled by the TOE Manufacturer.

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

For a list of assets refer to Section 3.1.1.

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

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

The TOE must provide the following specific security functionality to the Smartcard Embedded Software, according to accepted international standard:

- Triple Data Encryption Standard (TDES)

Security Objectives

91 The security objectives of the TOE contains the following sections:

- Security Objectives for the TOE
- Security Objectives for the Environment

4.1 Security Objectives for the TOE

According to this Security Target, there are the following standard high level security goals:

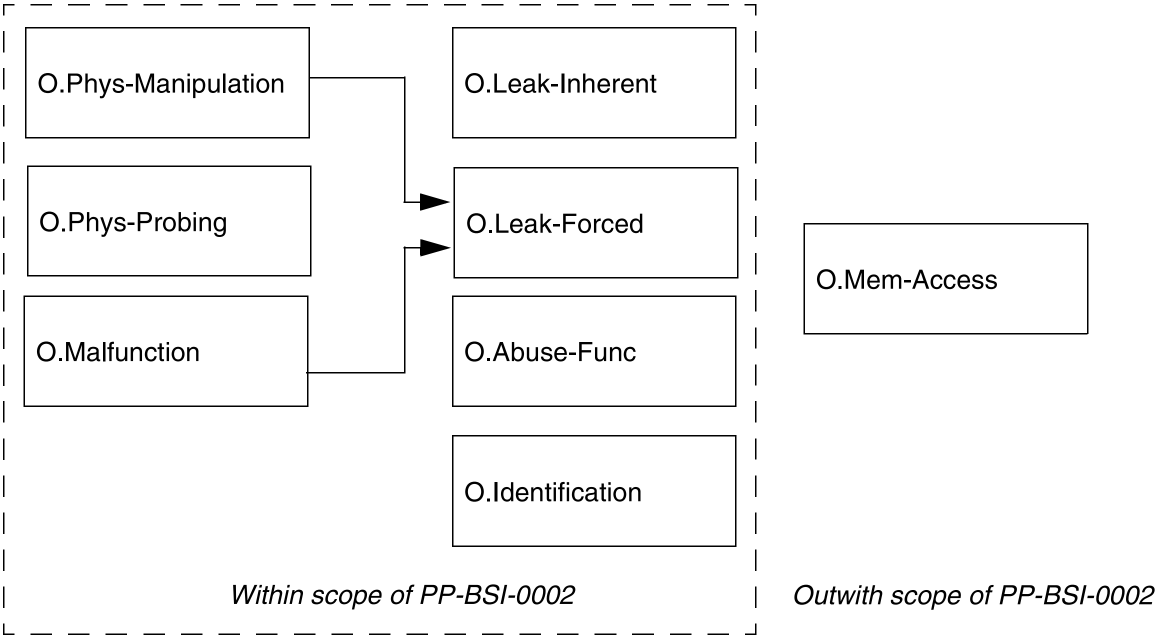
SG1 Maintain the integrity of User Data and of the Smartcard Embedded Software (when being executed/processed and when being stored in the TOE's memories).

SG2 maintain the confidentiality of User Data and of the Smartcard Embedded Software (when being processed and when being stored in the TOE's memories).

92 Though the Smartcard Embedded Software stored in ROM, will in many cases not contain secret data or algorithms, it must be protected from being disclosed, since for instance knowledge of specific implementation details may assist an attacker. In many cases critical User Data will be stored in the EEPROM.

93 These standard high-level security goals are refined below by defining security objectives as required by the Common Criteria (Figure 4-1). Note that the integrity of the TOE is a means to reach these objectives.

Figure 4-1 Standard Security Objectives

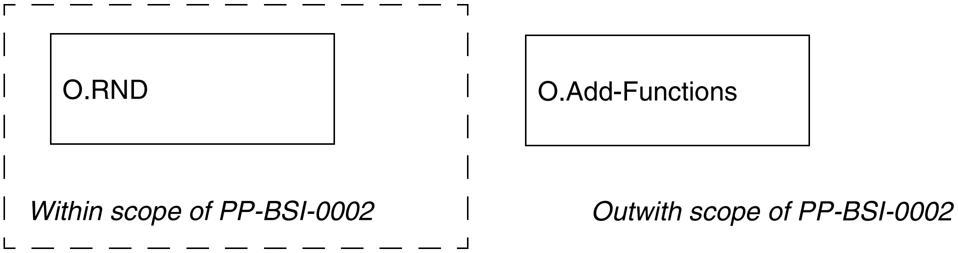


94 According to the security this security target there are the following high level security goals related to specific functionality:

SG3	Provide Random Numbers.
SG4	Provide additional security functionality.

95 The additional high level security considerations are refined below by defining security objectives as required by the Common Criteria.

Figure 4-2 Security Objectives Related to Specific Functionality



Standard Security Objectives (referring to SG1 and SG2)

96 The TOE shall provide protection on each of the Standard Security Objectives as listed below:

O.Leak-Inherent **Protection Against Inherent Information Leakage**

The TOE must provide protection against disclosure of confidential data (User Data or TSF data) stored and/or processed in the smartcard IC

- By measurement and analysis of the shape and amplitude of signals (for example on the power, clock, or I/O lines) and
- By measurement and analysis of the time between events found by measuring signals (for instance on the power, clock, or I/O lines).

This objective pertains to measurements with subsequent complex signal processing whereas O.Phys-Probing is about direct measurements on elements on the chip surface. Details correspond to an analysis of attack scenarios which is not given here.

O.Phys-Probing **Protection against Physical Probing**

The TOE must provide protection against disclosure of User Data, against the disclosure/reconstruction of the Smartcard Embedded Software or against the disclosure of other critical operational information. This includes protection against:

- Measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current)
- Measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)

with a prior

- Reverse-engineering to understand the design and its properties and functions

The TOE must be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack.

O.Malfunction **Protection against Malfunctions**

The TOE must ensure its correct operation.

The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent errors. The environmental conditions may include voltage, clock frequency, temperature, or external energy fields.

Remark: A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective O.Phys-Manipulation) provided that detailed knowledge about the TOE´s internal construction is required and the attack is performed in a controlled manner.

O.Phys-Manipulation **Protection against Physical Manipulation**

The TOE must provide protection against manipulation of the TOE (including its software and TSF data), the Smartcard Embedded Software and the User Data. This includes protection against:

- Reverse-engineering (understanding the design and its properties and functions
- Manipulation of the hardware and any data
- controlled manipulation of memory contents (User Data)

The TOE must be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack.

O.Leak-Forced **Protection against Forced Information Leakage**

The Smartcard must be protected against disclosure of confidential data (User Data or TSF data) processed in the Card (using methods as described under O.Leak?Inherent) even if the information leakage is not inherent but caused by the attacker.

- By forcing a malfunction (refer to "Protection against Malfunction due to Environmental Stress" (O.Malfunction)
- By a physical manipulation (refer to "Protection against Physical Manipulation" (O.Phys-Manipulation)

If this is not the case, signals which normally do not contain significant information about secrets could become an information channel for a leakage attack.

O.Abuse-Func **Protection against Abuse of Functionality**

The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order:

- To disclose critical User Data
- To manipulate critical User Data of the Smartcard Embedded Software
- To manipulate Soft-coded Smartcard Embedded Software
- To bypass, deactivate, change or explore security features or functions of the TOE

Details depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

O.Identification **TOE Identification**

The TOE must provide means to store Initialisation Data and Pre-personalisation Data in its non-volatile memory. The Initialisation Data (or parts of them) are used for TOE identification.

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.

Security Objectives Relating to Specific Functionality (referring to SG3 and SG4)

97 The TOE shall provide protection on each of the Specific Functionality Security Objectives as listed below:

O.RND **Random Numbers**

The TOE will ensure the cryptographic quality of random number generation. For instance random numbers shall not be predictable and shall have a sufficient entropy.

The TOE will ensure that no information about the produced random numbers is available to an attacker since they might be used for instance to generate cryptographic keys.

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

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

- Triple Data Encryption Standard (TDES)

4.2 Security Objectives for the Environment

Phase 1

98 The Smartcard Embedded Software shall provide for each of the Security Objectives for the Environment as stated below.

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

To ensure that the TOE is used in a secure manner the Smartcard Embedded Software shall be designed so that the requirements from the following documents are met:

- Hardware data sheet for the TOE
- TOE application notes
- Findings of the TOE evaluation reports relevant for the Smartcard Embedded Software

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

Security relevant User Data (especially cryptographic keys) are treated by the Smartcard Embedded Software as required by the security needs of the specific application context.

For example the Smartcard Embedded Software will not disclose security relevant user data to unauthorised users or processes when communicating with a terminal.

Phase 2 up to TOE Delivery

99 The TOE manufacturer shall ensure that the Security Objective for the Environment is complied with as stated below.

OE.Process-TOE **Protection during TOE Development and Production**

The TOE Manufacturer must ensure that the development and production of the Smartcard Integrated Circuit (Phases 2 and 3 up to TOE Delivery, Figure 2-3) is secure so that no information is unintentionally made available for the operational phase of the TOE. For example, the confidentiality and integrity of design information and test data must be guaranteed, access to samples, development tools and other material must be restricted to authorised persons only, scrap must be destroyed. This not only pertains to the TOE but also to all information and material exchanged with the developer of the Smartcard Embedded Software and therefore especially to the Smartcard Embedded Software itself. This includes the delivery (exchange) procedures for Phase 1 and the Phases after TOE Delivery as far as they can be controlled by the TOE Manufacturer.

An accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries this unique identification. In order to make this practical, electronic identification shall be possible.

For a list of assets refer to Section 3.1.

TOE Delivery up to the end of Phase 6

100 Appropriate protection during packaging finishing and personalisation must be ensured after TOE Delivery up to the end of Phase 6, as well as during delivery to Phase 7 as specified below.

OE.Process-Card **Protection during Packaging, Finishing and Personalisation**

Security procedures shall be used after TOE Delivery up to delivery to the end user 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).

In the case where unsawn wafers are delivered,the wafer saw guidance is followed by the customer [WSR].

This means that Phases after TOE Delivery up to the end of Phase 6, Figure 2-3, must be protected appropriately. For a list of assets to be protected refer to Section 3.1.

Section 5

TOE Security Functional Requirements

101 The TOE security functional requirements define the functional requirements for the TOE using functional requirements components drawn from the Common Criteria part 2, and extended functional requirements defined in BSI-PP-002-2001.

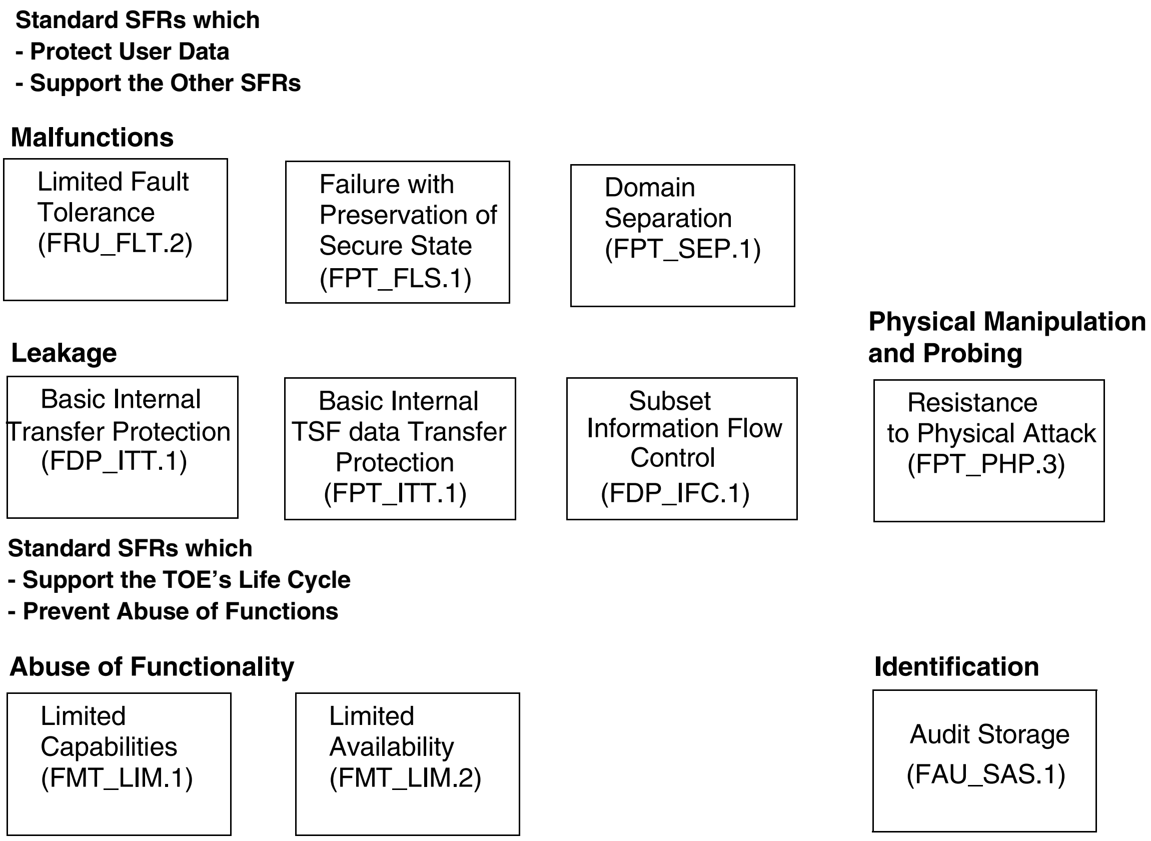
102 The minimum strength of function level for the TOE security requirements is SOF-high.

5.1 TOE Functional Requirements

Standard Security Functional Requirements

103 The Standard TOE Security Functional Requirements as listed within the BSI-PP-002-2001 are shown in Figure 5-1

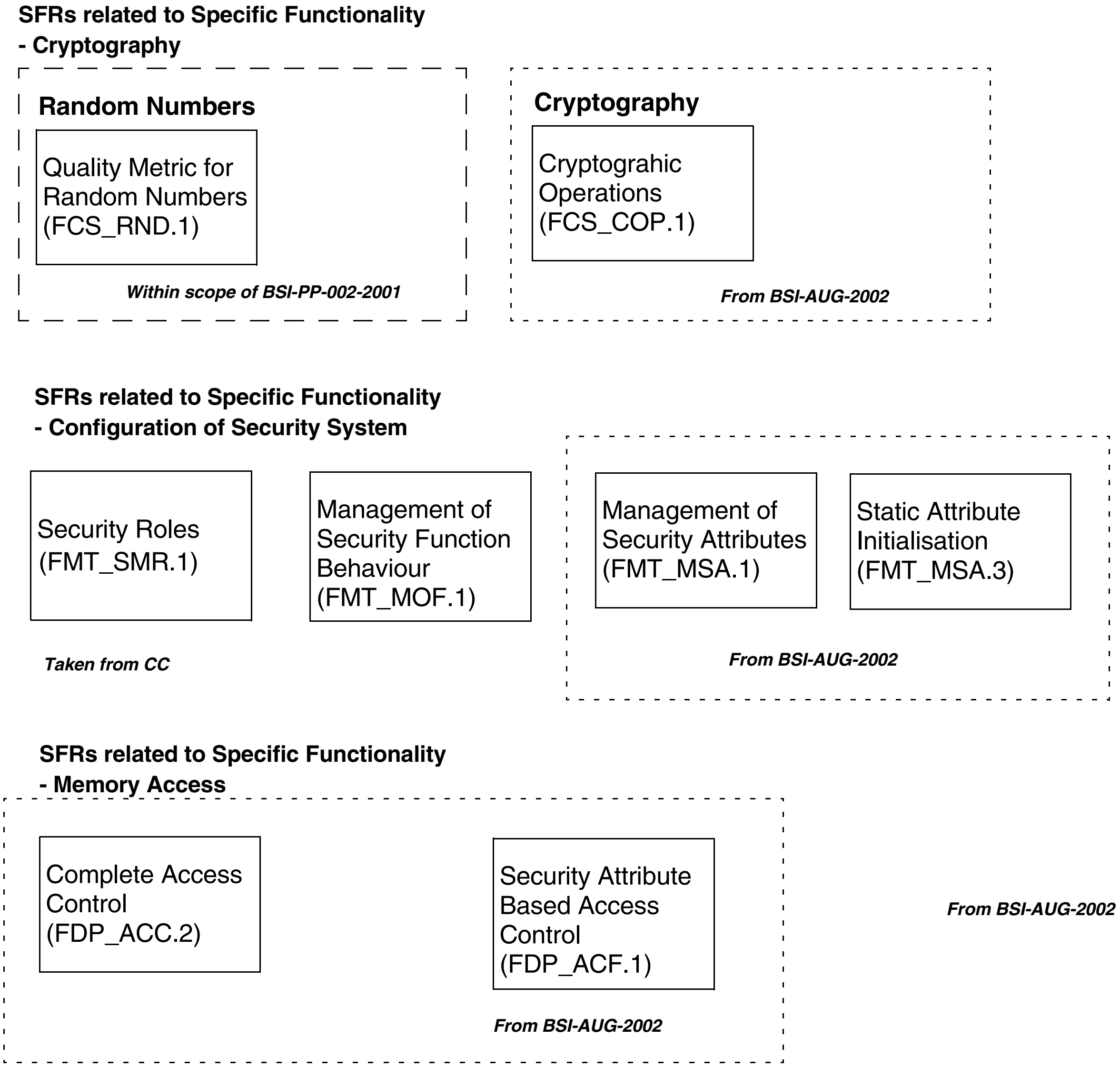
Figure 5-1 Standard Security Functional Requirements


Standard SFRs which
- Protect User Data
- Support the Other SFRs
Malfunctions
Limited Fault Tolerance (FRU_FLT.2)
Failure with Preservation of Secure State (FPT_FLS.1)
Domain Separation (FPT_SEP.1)
Leakage
Basic Internal Transfer Protection (FDP_ITT.1)
Basic Internal TSF data Transfer Protection (FPT_ITT.1)
Subset Information Flow Control (FDP_IFC.1)
Physical Manipulation and Probing
Resistance to Physical Attack (FPT_PHP.3)
Standard SFRs which
- Support the TOE's Life Cycle
- Prevent Abuse of Functions
Abuse of Functionality
Limited Capabilities (FMT_LIM.1)
Limited Availability (FMT_LIM.2)
Identification
Audit Storage (FAU_SAS.1)

104 The Security Functional Requirements related to specific Functionality are shown in Figure 5-2. The Security Functional Requirements are split into three:

- the SFRs as stated within the BSI-PP-002-2001 the SFRs as stated within this Security Target and taken from BSI-AUG-2002
- the SFR as stated within this Security Target and taken from the CC

Figure 5-2 Security Functional Requirements related to Specific Functionality


SFRs related to Specific Functionality
- Cryptography
Random Numbers
Quality Metric for Random Numbers (FCS_RND.1)
Within scope of BSI-PP-002-2001
Cryptography
Cryptograhic Operations (FCS_COP.1)
From BSI-AUG-2002
SFRs related to Specific Functionality
- Configuration of Security System
Security Roles (FMT_SMR.1)
Management of Security Function Behaviour (FMT_MOF.1)
Taken from CC
Management of Security Attributes (FMT_MSA.1)
Static Attribute Initialisation (FMT_MSA.3)
From BSI-AUG-2002
SFRs related to Specific Functionality
- Memory Access
Complete Access Control (FDP_ACC.2)
Security Attribute Based Access Control (FDP_ACF.1)
From BSI-AUG-2002
From BSI-AUG-2002

5.1.1 Functional Requirements Relating to Physical Malfunction

Limited Fault Tolerance (FRU_FLT.2)

105 The TOE **shall** meet the requirement "Limited Fault Tolerance" as specified below:

FRU_FLT.2	Limited fault tolerance
Hierarchical to	FRU_FLT.2
FRU_FLT.2.1	The TSF shall ensure the operation of **all the TOE's capabilities** when the following failure occur: **exposure to operating conditions which are not detected according to the requirement "Failure with preservation of secure state" (FPT_FLS.1).**
Dependencies	FPT_FLS.1 Failure with preservation of secure state
Refinement	The term "failure" above means "circumstances". The TOE prevents failures for "Circumstances" defined above.

Failure with Preservation of Secure State (FPT_FLS.1)

106 The TOE **shall** meet the requirement "Failure with Preservation of Secure State" as specified below:

FPT_FLS.1	Failure with preservation of secure state
Hierarchical to	No other components
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failure occur: **exposure to operating conditions which may not be tolerated according to the requirement "Limited fault tolerance" (FRU_FLT.2) and where therefore a malfunction could occur.**
Dependencies	ADV_SPM.1 Informal TOE security policy model
Refinement	The term "failure" above means "circumstances". The TOE prevents failures for "Circumstances" defined above.

TSF Domain Separation (FPT_SEP.1)

107 The TOE **shall** meet the requirement "TSF domain separation" as specified below:

FPT_SEP.1	TSF domain separation
Hierarchical to	No other components
FPT_SEP.1.1	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2	the TSF shall enforce separation between the security domains of subjects in the TSC.
Dependencies	No dependencies
Refinement	Those parts of the TOE which support the security functional requirements "Limited fault tolerance (FRU_FLT.2)" and "Failure with preservation of secure state (FPT_FLS.1)" shall be protected from interference of the Smartcard Embedded Software.

5.1.2 Functional Requirements Relating to Leakage

Basic Internal Transfer Protection (FDP_ITT.1)

108 The TOE **shall** meet the requirement “Basic internal transfer protection” as specified below:

FDP_ITT.1	Basic internal transfer protection
Hierarchical to	No other components
FDP_ITT.1.1	The TSF shall enforce the **Data Processing Policy** to prevent the **disclosure** of user data when it is transmitted between physically-separated parts of the TOE.
Dependencies	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control
Refinement	The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as physically-separated parts of the TOE.

Basic Internal TSF data transfer protection (FPT_ITT.1)

109 The TOE **shall** meet the requirement “Basic internal TSF data transfer protection” as specified below:

FPT_ITT.1	Basic internal TSF data transfer protection
Hierarchical to	No other components

FPT_ITT.1.1	The TSF shall protect TSF data from **disclosure** when it is transmitted between separate parts of the TOE.
Dependencies	No dependencies
Refinement	The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as separated parts of the TOE. This requirement is equivalent to FDP_ITT.1 above but refers to TSF data instead of User Data. Therefore, it should be understood as to refer to the same Data Processing Policy defined under FDP_IFC.1.

Subset Information Flow Control (FDP_IFC.1)

110 The TOE **shall** meet the requirement “Subset information flow control” as specified below:

FDP_IFC.1	Subset information flow control
Hierarchical to	No other components
FDP_IFC.1.1	The TSF shall enforce the **Data Processing Policy** on **all confidential data when they are processed or transferred by the TOE or by the Smartcard Embedded Software**.
Dependencies	FDP_IFF.1 Simple security attributes

111 The following Security Functional Policy (SFP) Data Processing Policy is defined for the requirement “Subset information flow control”:

- User Data and TSF data shall not be accessible from the TOE except when the Smartcard Embedded Software decides to communicate the User Data via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the Smartcard Embedded Software.

5.1.3 Functional Requirements Relating to Physical Probing and Manipulation

Resistance to Physical Attack (FPT_PHP.3)

112 The TOE **shall** meet the requirement “Resistance to physical attack” as specified below:

FPT_PHP.3	Resistance to physical attack
Hierarchical to	No other components
FPT_PHP.3.1	The TSF shall resist **physical manipulation and physical probing** to **the TSF** by responding automatically such that the TSP is not violated.
Dependencies	No dependencies
Refinement	The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, "automatic response" means here: ■ assuming that there might be an attack at any time ■ and countermeasures are provided at any time.

5.1.4 Functional Requirements Relating to Abuse of Functionality

Limited Capabilities (FMT_LIM.1)

113 The TOE **shall** meet the requirement “Limited capabilities” as specified below:

FMT_LIM.1	Limited capabilities
Hierarchical to	No other components
FMT_LIM.1.1	The TSF shall be designed in a manner that limits their 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 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**.
Dependencies	FMT_LIM.2 Limited availability

Limited Availability (FMT_LIM.2)

114 The TOE **shall** meet the requirement “Limited availability” as specified below:

FMT_LIM.2	Limited availability
Hierarchical to	No other components
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities" the following policy is enforced: **Deploying Test Features after TOE Delivery does not allow User Data 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**.
Dependencies	FMT_LIM.1 Limited capabilities

5.1.5 Functional Requirements Relating to Identification

Audit Storage (FAU_SAS.1)

115 The TOE **shall** meet the requirement “Audit storage” as specified below:

FAU_SAS.1	Audit storage
Hierarchical to	No other components
FAU_SAS.1.1	The TSF shall provide test personnel before TOE Delivery with the capability to store **the Initialisation Data and/or Pre-personalisation Data and/or supplements of the Smartcard Embedded Software** in the audit records.
Dependencies	No dependencies

5.1.6 Functional Requirements Relating to Cryptography

Quality Metric for Random Numbers (FCS_RND.1)

116 The TOE **shall** meet the requirement “Quality metric for random numbers” as specified below:

FCS_RND.1	Quality metric for random numbers

Hierarchical to	No other components
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet **FIPS140-2**.
Dependencies	No dependencies

Cryptographic operation (FCS_COP.1)

117 The TOE **shall** meet the requirement "Cryptographic operation" on cryptographic operations as specified below:

FCS_COP.1	Cryptographic operation
Hierarchical to	No other components
FCS_COP.1.1	The TSF shall perform **hardware TDES encryption and decryption** in accordance with a specified cryptographic algorithm: **triple Data Encryption Standard (TDES)** and cryptographic key sizes: **112-bit cryptographic key sizes** that meet the following **E-D-E two-key triple-encryption implementation of the Data Encryption Standard, FIPS PUB 46-3, 25th October, 1999.**
Dependencies	(FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation) FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

5.1.7 Functional Requirements Relating to Configuration of Security System

Security Roles (FMT_SMR.1)

118 The TOE **shall** meet the requirement "Security roles" as specified below:

FMT_SMR.1	Security roles
Hierarchical to	No other components
FMT_SMR.1.1	The TSF shall maintain the roles**: Not Disclosed in ST-Lite**
FMT_SMR.1.2	The TSF shall be able to associate users with roles
Dependencies	FIA_UID.1 Timing of Identification

Management of Security Function Behaviour (FMT_MOF.1)

119 The TOE **shall** meet the requirement “Management of security function behaviour” as specified below:

FMT_MOF.1	Management of security function behaviour
Hierarchical to	No other components
FMT_MOF.1.1	The TSF shall: **Not Disclosed in ST-Lite**
Dependencies	FMT_SMR.1 Security Roles FMT_SMF.1 Specification of Management Functions

Management of Security Attributes (FMT_MSA.1)

120 The TOE shall meet the requirement “Management of security attributes” as specified below:

FMT_MSA.1	Management of security attributes
Hierarchical to	No other components
FMT_MSA.1.1	The TOE security functions shall enforce **the ACSF_Policy (Access Control Security Functions Policy)** to restrict the ability to **grant/deny** the security attributes: **Not Disclosed in ST-Lite** to: **Not Disclosed in ST-Lite**
Dependencies	FDP_ACC.1 Subset access control or FDP_IFC.1 subset information flow control FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions

Static Attribute Initialisation (FMT_MSA.3)

121 The TOE **shall** meet the requirement “Static attribute initialisation” as specified below:

FMT_MSA.3	Static attribute initialisation
Hierarchical to	No other components

FMT_MSA.3.1 The TOE security functions shall enforce the **ACSF_Policy** to provide **restrictive** default values for security attributes that are used to enforce the security functions policy.

FMT_MSA.3.2 The TSF shall allow the: **Not Disclosed in ST-Lite** to specify alternate 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

5.1.8 Functional Requirements Relating to Memory Access

Complete Access Control (FDP_ACC.2)

122 The TOE **shall** meet the requirement “Complete access control” as specified below:

FDP_ACC.2 Complete access control

Hierarchical to FDP_ACC.1 Subset access control

FDP_ACC.2.1 The TOE security functions shall enforce the **Access Control SFP** on:

- **Subjects: Not Disclosed in ST-Lite**
- **Objects: (O1) CPU ROM, (O2) EEPROM, (O3) Crypto ROM, (O4) CPU RAM, (O5) Crypto RAM, (O6) peripherals**

and all operations among subjects and objects covered by the SFP

FDP_ACC.2.2 The TOE security function shall ensure that all operations between any subject in the TOE scope of control and any object within the TOE scope of control are covered by an access control SFP.

Dependencies FDP_AFC.1 Security attribute based access control

Security attribute based access control (FDP_ACF.1)

123 The TOE **shall** meet the requirement “Security attribute based access control” as specified below:

FDP_ACF.1	Security attribute based access control
Hierarchical to	No other components
FDP_ACF.1.1	The TOE security functions shall enforce the **ACSF_Policy** to objects based on the following: - **Subjects: Not Disclosed in ST-Lite** - **Objects: (O1) CPU ROM, (O2) EEPROM, (O3) Crypto ROM, (O4) CPU RAM, (O5) Crypto RAM, (O6) peripherals** - **Operations: Read, Write, Execute** - **Conditions**: **Not Disclosed in ST-Lite**
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed **see section** 5.1.9
FDP_ACF.1.3	The TSF shall explicitly authorise 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**: **Not Disclosed in ST-Lite**
Dependencies	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

5.1.9 ACFS-Policy

124 **Not Disclosed in ST-Lite**

5.2 Security Requirements for the NON-IT-Environment

125 In the following, security requirements for the Non-IT-Environment are defined. For the development of the Smartcard Embedded Software (in Phase 1) the requirement

"Design and implementation of the Smartcard Embedded Software (RE.Phase-1)" is valid.

RE.Phase-1 Design and Implementation of the Smartcard Embedded Software

The developers shall design and implement the Smartcard Embedded Software in such a way that it meets the requirements from the following documents (i) hardware data sheet for the TOE, (ii) TOE application notes, and (iii) findings of the TOE evaluation reports relevant for the Smartcard Embedded Software.

The developers shall implement the Smartcard Embedded Software in a way that it protects security relevant User Data (especially cryptographic keys) as required by the security needs of the specific application context.

126 The Smartcard Embedded Software shall meet the requirement "Cipher Schemas (RE.Cipher)" as specified below.

RE.Cipher Cipher Schemas

The developers of Smartcard Embedded Software must not implement routines in a way which may compromise keys when the routines are executed as part of the Smartcard Embedded Software. Performing functions which access cryptographic keys could allow an attacker to misuse these functions to gather information about the key which is used in the computation of the function.

Keys must be kept 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 not possible to derive the private key from a public key if asymmetric algorithms are used. This implies that an appropriate key management has to be realized in the environment.

127 The responsible parties for the Phases 4-6 are required to support the security of the TOE by appropriate measures.

RE.Process-Card Protection during Packaging, Finishing and Personalisation

The Card Manufacturer (after TOE Delivery up to the end of Phase 6) shall use adequate security measures 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).

5.3 TOE Security Assurance Requirements

128 The assurance requirement is EAL4 augmented of additional assurance components listed in Table 5-1.

129 Some of the augmentation components are hierarchical ones to the components specified in EAL4.

130 All the components are drawn from Common Criteria Part 3.

Table 5-1 EAL4 Package and Augmentation

Assurance Class	EAL4 Package	AT91SC464384RCU EAL4+ Package	Augmented From EAL4
ACM_AUT	1	1	No
ACM_CAP	4	4	No
ACM_SCP	2	2	No
ADO_DEL	2	2	No
ADO_IGS	1	1	No
ADV_FSP	2	2	No
ADV_HLD	2	2	No
ADV_IMP	1	2	Yes
ADV_LLD	1	1	No
ADV_RCR	1	1	No
ADV_SPM	1	1	No
AGD_ADM	1	1	No
AGD_USR	1	1	No
ALC_DVS	1	2	Yes
ALC_FLR	N/A	N/A	No
ALC_LCD	1	1	No
ALC_TAT	1	1	No
ATE_COV	2	2	No
ATE_DPT	1	1	No
ATE_FUN	1	1	No
ATE_IND	2	2	No
AVA_MSU	2	3	Yes
AVA_SOF	1	1	No
AVA_VLA	2	4	Yes

131 The refinements to the assurance requirements as stated within the Protection Profile BSI-PP002-2001 have been taken into account.

Section 6

TOE Summary Specification

132 This section defines the TOE security functions that implement the security functional requirements defined in Section 5.1, and the TOE assurance measures that implement the security assurance requirements defined in Section 5.3.

6.1 TOE Security Functions

6.1.1 Protected Test Access (SF1)

M1.1 Test Mode Entry

133 Test Mode is a special mode of operation that allows authenticated engineers access to the device to ren test operations.

134 SF1 shall ensure that only authorized users will be permitted to enter Test Mode. This is provided by M1.1 Test Mode Entry conditions that are required to enable the TOE to enter Test Mode. Failure to meet the M1.1 conditions will prevent entry into Test Mode.

M1.2 Test Mode Disable

135 M1.2 Test Mode Disable ensures that once activated the Entry into Test Mode is permanently disabled. The mechanism shall ensure that after wafer sawing none of the test features are available, not even to authenticated users in test mode. Only Package Mode limited test features will remain accessible to authenticated users.

M1.3 Package Mode Entry

136 Package Mode is a special mode of operation that allows authenticated engineers access to the device to run limited test operations for field return analysis.

137 SF1 shall ensure that only authorized users will be permitted to enter Package Mode. This is provided by M1.3 Package Mode Entry conditions that are required to be passed to enable the TOE to enter Package Mode. Failure to meet these conditions will prevent entry into Package Mode.

M1.4 Serial Number Register Write

138 SF1 shall provide the ability to store initialisation and pre-personalisation data and more specifically the means to uniquely identify the TOE. This is provided by M1.4 Serial Number Register Write [TD]. The ability to use M1.4 is restricted to M1.1 TME authenticated users, M1.2 Test Mode Disable prevents the usage of M1.4 as M1.1 is now disabled.

139 The Strength of Function for the Protected Test Access is high.

6.1.2 Protection against Disclosure (SF2)

140 SF2 shall ensure that users/third parties will have difficulty observing DPA or EMA leakage from the TOE.

141 The TOE has the following security features:

142 **Not Disclosed in ST-Lite**

143 The Strength of Function claimed for the Protection against Disclosure security function is high.

6.1.3 True RNG (SF3)

144 M3.1 the TSF shall provide a hardware Random Number Generator (RNG) to support security operations performed by cryptographic applications. This RNG noise source shall not be predictable, have sufficient entropy, and not leaking information related to the value of the generated random numbers as this leakage could be used to retrieve cryptographic keys for instance. The RNG noise source as a sufficient entropy to comply with the FIPS 140-2 standard.

145 The Strength of Function claimed for the RNG security function is high.

6.1.4 Memory Access Control (SF4)

146 SF4 shall enforce access control based on the Access Control rules as defined in the ACSF_Policy. **Not Disclosed in ST-Lite**

6.1.5 Violation Source (SF5)

147 The TOE shall provide an Event Audit security function (SF5) to enforce the following rules for monitoring audited events.

148 Accumulation or combination of the following auditable events would indicate a potential security violation.

Environmental/Physical type of violations

- M5.1 External supply monitor
- M5.2 Internal supply monitor
- M5.3 External frequency monitor
- M5.4 Internal frequency monitor
- M5.5 Temperature monitor
- M5.6 UV light detector
- M5.7 Light Scan Detector
- M5.8 Active Shield
- M5.9 Mirrored registers
- M5.10 E2PROM Protection Object

Software type of violations

- M5.11 MPU data access violations
- M5.12 MPU Alignment checking
- M5.13 MPU Overflow checking
- M5.14 Firewall data access violations
- M5.15 Pre-fetch access violations
- M5.16 Endianess checking
- M5.17 Undefined (Illegal) opcodes
- M5.18 Watchdog

149 The Strength of Function claimed for the Event audit security function is high.

6.1.6 Violation Action (SF6)

150 SF6 shall provide a Violation action when a violation source is triggered by the TOE. Detection of such occurrences will cause an information flag to be set, the Smartcard Embedded Software can then take one of the following Violation Actions: **Not Disclosed in ST-Lite**

151 Event Action depends on the type of Event (see [TD] for more information).

6.1.7 Cryptography (SF7)

152 The TSF shall provide a cryptographic algorithm to be able to transmit and receive objects in a manner protected from data retrieval or modification.

153 M7.1 the TSF shall provide hardware TDES data encryption/decryption capability.

154 These may be used by the smartcard embedded software to support data encryption and decryption for maintaining data integrity, and protect against sensitive data unauthorized disclosure.

155 The Strength of Function claimed for the SF7 Security Function is high.

156 An assessment of the strength of the following algorithms does not form part of the evaluation:

- TDES algorithm

6.1.8 Security Functions Based on Permutations/combinations

157 Security function SF1 is based on mechanisms using permutation and/or combination properties.

158 Therefore, the resistance of SF1 should be evaluated against attacks using brute force techniques.

159 Further details on these mechanisms and on the Strength of Function Analysis performed by ATMEL can be found in [ESOF].

6.2 TOE Assurance Measures

160 Table 6-1 specifies how they satisfy the TOE security assurance requirements.

Table 6-1 Relationship Between Assurance Requirements and Measures

		Security Target	Configuration Management	Delivery and Operation	Development Activity	Guidance	Life Cycle Support	Test Activity	Vulnerability assessment	Smartcard Devices	Development Site	Test Site	Manufacturing Site	Sub-contractor Site
Assurance Requirement		**SA1**	**SA2**	**SA3**	**SA4**	**SA5**	**SA6**	**SA7**	**SA8**	**SA9**	**SA10**	**SA11**	**SA12**	**SA13**
ASE_xxx		x												
ACM_AUT.1			x								x	x	x	x
ACM_CAP.4			x								x	x	x	x
ACM_SCP.2			x								x	x	x	x
ADO_DEL.2				x							x	x	x	x
ADO_IGS.1				x							x	x	x	x
ADV_FSP.2					x									

Table 6-1 Relationship Between Assurance Requirements and Measures

ADV_HLD.2					x									
ADV_IMP.2					x									
ADV_LLD.1					x									
ADV_RCR.2					x									
ADV_SPM.2					x									
AGD_ADM.1						x								
AGD_USR.1						x								
ALC_DVS.2							x				x	x	x	x
ALC_LCD.2							x				x	x	x	x
ALC_TAT.2							x				x	x	x	x
ATE_COV.2								x		x		x		
ATE_DPT.2								x		x		x		
ATE_FUN.1								x		x		x		
ATE_IND.2								x		x		x		
AVA_CCA.1									x	x				
AVA_MSU.3									x	x				
AVA_SOF.1									x	x				
AVA_VLA.4									x	x				

Security Target (SA1)

161 SA1 shall provide the “TOE Security Target” document plus its references.

Configuration Management (SA2)

162 SA2 shall provide the “CC Configuration Management (ACM)” interface document plus its references.

Delivery and Operation (SA3)

163 SA3 shall provide the “CC Delivery and Operation (ADO)” interface document plus its references.

Development Activity (SA4)

164 SA4 shall provide the “CC Development Activity (ADV)” interface document plus its references.

Guidance (SA5)

165 SA5 shall provide the “CC Guidance (AGD)” interface document plus its references.

Life Cycle Support (SA6)

166 SA6 shall provide the “CC Life Cycle Support (ALC)” interface document plus its references.

Test Activity (SA7)

167 SA7 shall provide the “CC Test Activity (ATE)” interface document plus its references, and undertaking of testing described therein.

Vulnerability Assessment (SA8)

168 SA8 shall provide the “CC Vulnerability Assessment (AVA)” interface document plus its references, and undertaking of vulnerability assessment described therein.

Smart Card Devices (SA9)

169 SA9 shall provide functional AT91SC464384RCU smart card devices.

Development Site (SA10)

170 SA10 shall provide access to the development site.

Test Site (SA11)

171 SA11 shall provide access to the test site.

Manufacturing Site (SA12)

172 SA12 shall provide access to the manufacturing site.

Sub-contractor Sites (SA13)

173 SA13 shall provide access to the sub-contractor sites.

Section 7

PP Claims

7.1 PP Reference

174 This Security Target is conformant to the Protection Profile “Smartcard IC Platform Protection Profile” V1.0 July 2001,and has been registered under the German Certification Scheme (BSI) under the reference BSI-PP-002-2001.

7.2 PP Refinements

175 For clarification of this Security Target, modes, assets, subjects, threats, assumptions and organizational security policy are defined with labels of the form M.xx_xx, D.xx_xx, S.xx_xx, T.xx_xx, A.xx_xx, and P.xx_xx respectively.

176 Refinements to assumption A.Process-Card and security objective for the environment OE.Process-Card, relate to the shipment of unsawn wafers and the guidance given to customers.

7.3 PP Additions

177 The PP additions fall into the following categories, the additions:

- from the “Smartcard Integrated Circuit Augmentations” registered under the German Certification Scheme (BSI) under the reference BSI-AUG-2002
- taken directly from Common Criteria V2.3
- assumption and security objective for environment, defined in Section 3.2 of this Security Target

7.3.1 Additions from BSI-AUG-2002

178 Additions include Threats, Organisational security Policies, Security Objectives and Security Functional Requirements.

7.3.1.1 Assumptions

179 None

7.3.1.2 Threats

180 This security target specifies the additional threat, T.Mem-Access this relates to the threat that the Smartcard Embedded Software may cause security violations by accessing restricted data.

7.3.1.3 Organizational Security Policies

181 This security target specifies the additional organizational security policies, P.Add-Functions this policy relates to the cryptographic functions provided by the TOE.

7.3.1.4 Security Objectives

182 This security target specifies the additional security objective, O.Add-Functions this objective relates to the cryptographic functions provided by the TOE.

183 This security target specifies the additional security objective, O.Mem-Access this objective relates to area based memory access control provided by the TOE.

7.3.1.5 Security Functional Requirements

184 This security target specifies the additional security functional requirements:

- FCS_COP.1 relating to the cryptographic functions provided by the TOE
- FMT_MSA.1 relating to the configuration of security functions
- FDP_ACC.2 relating to the memory access controls provided by the TOE
- FDP_ACF.1 relating to the memory access controls provided by the TOE

7.3.2 Additions from the Common Criteria

7.3.2.1 Security Functional Requirements

185 This security target specifies the additional security functional requirements:

- FMT_SMR.1 relating to the configuration of security functions
- FMT_MOF.1 relating to the configuration of security functions

Appendix A

Glossary

A.1 Terms

IC Dedicated Software IC Proprietary software which is required for testing purposes and to implement special functions. For AT91SC464384RCU this includes the embedded test software and additional test programmes which are run from outside of the IC.

The Crypto libraries also form part of the IC dedicated software.

IC Designer Institution (or its agent) responsible for the IC Development. Atmel is the institution in respect of the TOE.

IC Manufacturer Institution (or its agent) responsible for the IC manufacturing, testing and pre-personalization. Atmel is the institution in respect of the TOE.

IC Packaging Manufacturer Institution (or its agent) responsible for the IC packaging and testing.

IC Pre-personalization Data Required information to enable the smartcard IC to be configured by means of ROM options and to enable programming of the EEPROM with customer specified data.

Integrated Circuit (IC) Electronic component(s) designed to perform processing and/or memory functions.

Personalizer Institution (or its agent) responsible for the smartcard personalization and final testing.

Smartcard A credit sized plastic card which has a non volatile memory and a processing unit embedded within it.

Smartcard Embedded Software Software embedded in the smartcard application (smartcard application software). This software is provided by smartcard embedded software developer (customer). Embedded software may be in any part of User ROM or EEPROM.

Smartcard Embedded Software Developer Institution (or its agent) responsible for the smartcard embedded software development and the specification of pre-personalization requirements.

Smartcard Issuer Institution (or its agent) responsible for the smartcard product delivery to the smartcard end-user.

Smartcard Product Manufacturer Institution (or its agent) responsible for the smartcard product finishing process and testing.

A.2 Abbreviations

ACSF	Access Control Security Functions
AdvX	32-bit Crypto Accelerator developed and produced by Atmel
AVR	8-bit RISC processor developed and produced by Atmel
CC	Common Criteria
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
DPA	Differential Power Analysis
EEPROM	Electrically Erasable Programmable ROM
EKB	East Kilbride
FIB	Focussed Ion Beam
HCMOS	High Speed Complementary Metal Oxide Semiconductor
I/O	Input/Output
IC	Integrated Circuit
IFCSF	Information Flow Control Security Functions
ISO	International Standards Organization
LFSR	Linear Feedback Shift Register
MAC	Master Authentication Key
MCU	Microcontroller
MPU	Memory Protection Unit (Firewall)
NVM	Non Volatile Memory
OTP	One Time Programmable
PME	Package Mode Entry
PP	Protection Profile
RAM	Random-Access Memory
RFO	Rousset France Operations
RISC	Reduced Instruction Set Core
RNG	Random Number Generator
ROM	Read-Only Memory
SPA	Simple Power Analysis

TME	Test Mode Entry
TOE	Target of Evaluation
VFO	Variable Frequency Oscillator

Atmel Corporation

2325 Orchard Parkway
San Jose, CA 95131, USA
Tel: 1(408) 441-0311
Fax: 1(408) 487-2600

Regional Headquarters

Europe
Atmel Sarl
Route des Arsenaux 41
Case Postale 80
CH-1705 Fribourg
Switzerland
Tel: (41) 26-426-5555
Fax: (41) 26-426-5500

Asia
Room 1219
Chinachem Golden Plaza
77 Mody Road Tsimshatsui
East Kowloon
Hong Kong
Tel: (852) 2721-9778
Fax: (852) 2722-1369

Japan
9F, Tonetsu Shinkawa Bldg.
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033
Japan
Tel: (81) 3-3523-3551
Fax: (81) 3-3523-7581

Atmel Operations

Memory
2325 Orchard Parkway
San Jose, CA 95131, USA
Tel: 1(408) 441-0311
Fax: 1(408) 436-4314

Microcontrollers
2325 Orchard Parkway
San Jose, CA 95131, USA
Tel: 1(408) 441-0311
Fax: 1(408) 436-4314

La Chantrerie
BP 70602
44306 Nantes Cedex 3, France
Tel: (33) 2-40-18-18-18
Fax: (33) 2-40-18-19-60

ASIC/ASSP/Smart Cards
Zone Industrielle
13106 Rousset Cedex, France
Tel: (33) 4-42-53-60-00
Fax: (33) 4-42-53-60-01

1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906, USA
Tel: 1(719) 576-3300
Fax: 1(719) 540-1759

Scottish Enterprise Technology Park
Maxwell Building
East Kilbride G75 0QR, Scotland
Tel: (44) 1355-803-000
Fax: (44) 1355-242-743

RF/Automotive
Theresienstrasse 2
Postfach 3535
74025 Heilbronn, Germany
Tel: (49) 71-31-67-0
Fax: (49) 71-31-67-2340

1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906, USA
Tel: 1(719) 576-3300
Fax: 1(719) 540-1759

Biometrics/Imaging/Hi-Rel MPU/
High Speed Converters/RF Datacom
Avenue de Rochepleine
BP 123
38521 Saint-Egreve Cedex, France
Tel: (33) 4-76-58-30-00
Fax: (33) 4-76-58-34-80

Literature Requests
www.atmel.com/literature

Disclaimer: The information in this document is provided in connection with Atmel products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Atmel products. **EXCEPT AS SET FORTH IN ATMEL'S TERMS AND CONDITIONS OF SALE LOCATED ON ATMEL'S WEB SITE, ATMEL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ATMEL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ATMEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.** Atmel makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Atmel does not make any commitment to update the information contained herein. Unless specifically provided otherwise, Atmel products are not suitable for, and shall not be used in, automotive applications. Atmel's products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.

Printed on recycled paper.