General Business Use

AT90SC12818RCU

Security Target Lite

Important notice to readers…

AT90SC12818RCU Security Target Lite

1.1 Identification

1 Title: AT90SC12818RCU Security Target Lite

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

1.2 Overview

Protection Profile Claims

3 This Security Target Lite (ST-Lite) 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

4 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 AT90SC ASL4 and the 'parent' device of the family, the initial device in the family was the VEGA2 project, part number AT90SC19264RC, certified under the French CC scheme, Ref. 2002/04.

Project Information:

Part Number	AT90SC12818RCU
Product Identification Number	AT58U14
Revision	B
Atmel Toolbox Version[+]	00.03.01.07

Assurance Level

5 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

6 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

7 The TOE is evaluated under the French CC Scheme

DCSSI
Bureau Certification
51 boulevard de La Tour-Maubourg
75700 Paris 07 SP
FRANCE

Evaluator

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

Serma Technologoes

30 Avenue Gustave Eiffel

33608 PESSAC Cedex

FRANCE

Brief TOE Description

9 The devices in the AT90SC ASL4 family are based on the AVR RISC family of single-chip microcontroller devices. The AVR RISC family, with designed-in security features, is based on the industry-standard AVR low-power HCMOS core and gives access to the powerful instruction set of this widely used device. AT90SC ASL4 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

10 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

11 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

12 This document is based on the AT90SC12818RCU Technical Data Sheet [TD].

13 The term *Target of Evaluation* (TOE) is standard CC terminology and refers to the product being evaluated, the AT90SC12818RCU MCU device in this case.The stated toolbox commands are not part of the evaluation. Downloaded test software will be used for evaluation purposes but is outside the scope of the TOE. Description of how to use the security features can be found in [TD].

14 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.

15 Hexadecimal numbers are prefixed by $, e.g. $FF 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

16 The AT90SC12818RCU 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] AT90SC12818RCU Technical Data (TPR0249)
- [TestROMDD] Engineering Software Detailed Description
- [TestROMUG] Engineering Software User Guide
- [TMRE2] Production Test Software Detailed Description
- [TMR-User] Production Test Software User Guide
- [PME] Package Mode Test
- [TBX] Toolbox 3.x on AT90SCxxxxC Family with AdvX (TPR0133)
- [APP_AdvX] AdvX for AT90SC Family (TPR0116)

- [APP_SCRY] Securing Cryptographic Operations on AT90SC products with the Toolbox 3.x (TPR0141)
- [APP_CRYPT] Efficient use of AdvX for Implementing Cryptographic Operations (TPR0142)
- [WSR] Wafer Saw Recommendations (TPG0079)
- [DIGDES] AT90SC12818RCU Digital Modules Design

Within this security Target Lite 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	10 Mar 08	Initial release	Gordon Caffrey

Target of Evaluation Description

17 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

18 The TOE is the single chip microcontroller unit to be used in a smartcard product, independent of the physical interface and the way it is packaged. Specifically, the TOE is the Artemis AT90SC12818RCU device from the AT90SC ASL4 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.

19 The devices in the AT90SC ASL4 family are based on ATMEL's AVR RISC family of single-chip microcontroller devices. The AVR RISC family, with designed-in security features, is based on the industry-standard AVR RISC low-power HCMOS core and gives access to the powerful instruction set of this widely used device. Different AT90SC ASL4 family members offer various options. The AT90SC ASL4 family of devices are designed in accordance with the ISO standard for integrated circuit cards (ISO 7816), where appropriate.

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

21 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].

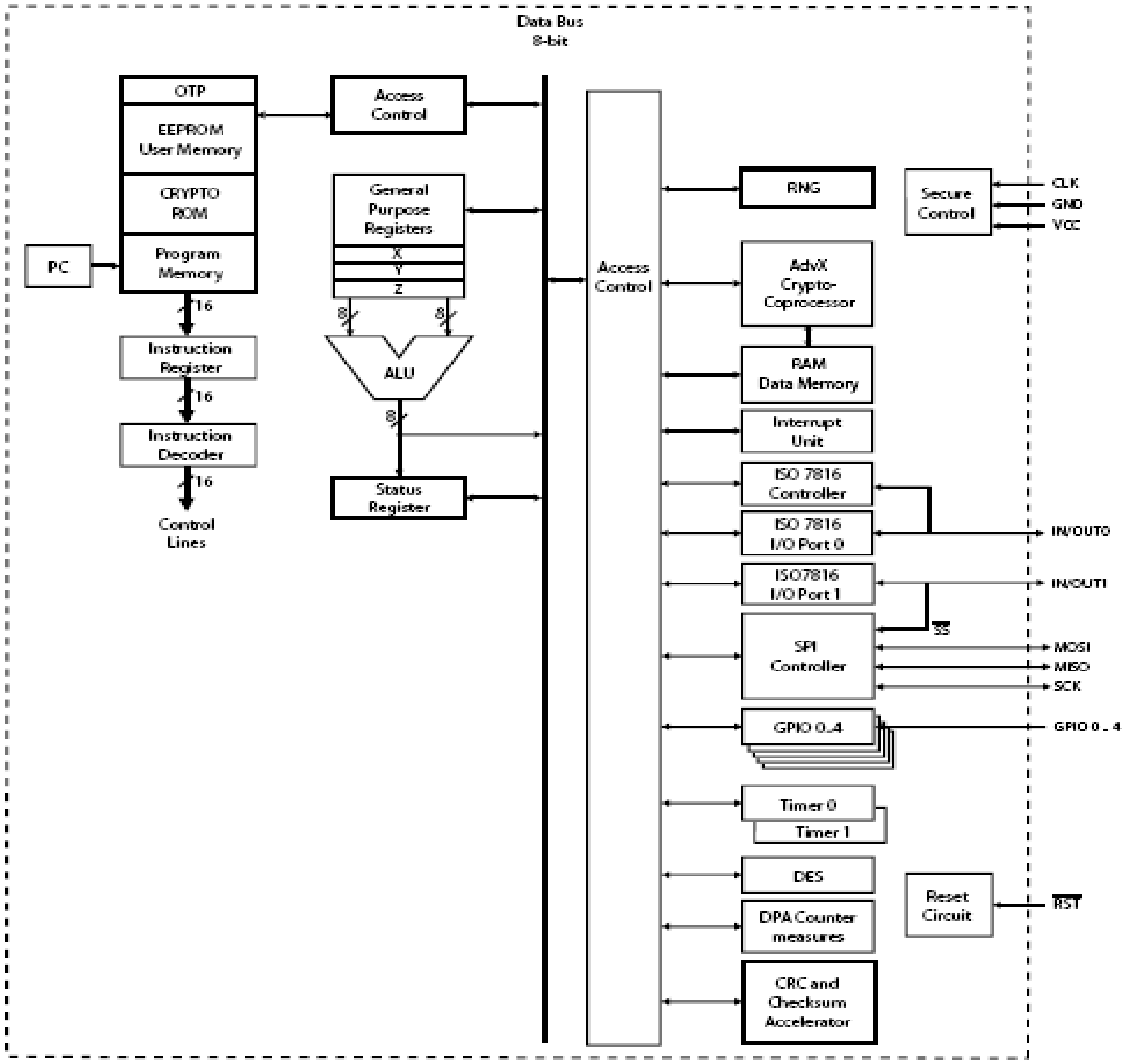


Figure 2-1 Artemis Block Diagram

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

General

- High performance, Low power secureAVR^{TM} Core Enhanced RISC Architecure
  - 137 Powerful Instructions (Most executed in a Single Clock Cycle)
- Low power Idle and Power down Modes
- Bond Pad Locations Conforming to ISO 7816-2
- ESD Protection to ±4000V
- Operating Ranges: from 1.62V to 5.5V

- Optional external clock. Can run using the internal Variable Frequency Oscillator only

Memory

- 96K bytes ROM Program Memory
- 18K bytes EEPROM, Including 128 OTP bytes and 384-byte Bit-addressable bytes
  - 1 to 64-byte Program/Erase
  - 1.25ms Program, 1,25ms Erase
  - Endurance: 500,000 Write/Erase Cycles at $25^{o}C$
  - 10 Years Data Retention
- 6K bytes RAM memory
- 32K bytes of the ROM is dedicated to Atmel’s Crypto Library
- Memory Protection Unit

Perhiperals

- One ISO 7816 Controller
  - Up to 625 kbps at 5Mhz
  - Compliant with T=0 and T=1 Protocols
- One SPI Controller (master and slave modes)
- General purpose Input and Output (0 to 4)
- Programmable Internal Oscillator (Up to 30Mhz for AdvX and 30Mhz for internal CPU Clock)
- Two 16-bit Timers
- Random Number Generator (RNG)
- 2-level Interrupt Controller
- Hardware DES and Triple DES (DPA/DEMA Resistant)
- Checksum Accelerator
- CRC16 and 32 Engine (Compliant with ISO/IEC 3309)
- 32-bit Cryptographic Accelerator (AdvX for Public Key Operations)
  - To support RSA, DSA, ECC, Diffie-Hellman (outwith the scope of this evaluation)

Security

- Dedicated hardware for protection against SPA/DPA/SEMA/DEMA attacks
- Advanced protection against physical attack including active shield
- Envirinmental protection systems
- Voltage Monitor
- Frequency Monitor
- Temperature Monitor

- Light protection
- Security Memory Management/Acces Protection (Supervisor Mode)

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

24 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.

25 The NVM can be operated in two ways Classic and XP operating mode. Classic System this is embedded in most AT90SC products. It features byte and page writing modes and uses BHS, IDLE or Polling modes [TD].

26 Expert (XP) System allows the NVM to be written by page and erase block, full page or partial page. A smart write feature is also available to avoid non-allowed actions [TD].

27 Table Table 2-1 gives a summary of the write modes for the two operating modes.

	Write Modes Classic	Write Modes XP
Standard EEPROM	Page mode with autoerase Page mode without autoerase Byte mode with autoerase Byte mode without autoerase Erase only	Erase + Write Write only Full page erase Partial page erase Block erase
Bit Addressable	Page mode with autoerase Page mode without autoerase Byte mode with autoerase Byte mode without autoerase Erase only Pseudo bit by page Pseudo bit by byte	Erase + Write Write only Full page erase Partial page erase Block erase Bit write
Byte Writable OTP	Pseudo bit by byte	Write only

Table 2-1 Classic and XP Write modes

28 The TOE has a 32-bit Cryptographic Accelerator (AdvX) with its 32K-byte Crypto ROM this can be loaded with either the ATMEL Toolbox library (ATMEL ROM or ATMEL crypto ROM), or it can be loaded with the Customer Proprietary crypto library.

29 The Atmel Toolbox [TBX] software library allowing fast cryptographic algorithm implementations (RSA, SHA-1, Prime Generation,...) on the AdvX. The cryptographic library is stored in an 32K byte ROM, this ROM is split into two regions Figure 2-3. A crypto library [TBX] with cryptographic primitives (such as modular exponentiation) is provided by ATMEL, but the customer can 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]. Therefore, part of this ROM memory can be considered as User ROM memory, the rest of the available memory is locked by Atmel, Table 5-1 explains the two regions access rights

Note

Note the Evaluation is Hardware only and there for the Toolbox is outwith theTOE

Customer Toolbox

30 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]. Therefore, part of this ROM memory can be considered as User ROM memory, the rest of the available memory is locked by Atmel, Table 5-1 explains the two regions access rights

31 The TOE shall also provide software cryptographic primitives to ease the customer proprietary software implementation of these algorithms (full multiply, square, partial multiply, division,...) as well as DSA and EC-DSA data signature in the CPU embedded software. The primitives listed as well as DSA and EC-DSA are not TSF portions of the TOE, they are covered in terms of CC compliance, but not covered in terms of penetration testing

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

33 The TOE includes a powerful Firewall (Memory protection Unit) that protects all memories, peripheral and IO register accesses. This Firewall defines the 5 user modes (Supervisor, and Non-Supervisor (User))

2.1.1 Scope of Evaluation Summary

Part of the TOE

- AT90SC12818RCU Hardware device
- Package Mode
- Atmel Security User Guidance as detailed on page 23
- The TOE interfaces as detailed in Section 46
- Phases 2-3 of the Life Cycle

Outwith the TOE

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

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

2.2 Smartcard Product Life-cycle

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

.

Table 2-2 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

35 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 Lite.

36 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 Lite.

37 Figure 2-2 describes the Smartcard product life-cycle. Appendix C contains the addresses of the relevant organizations.

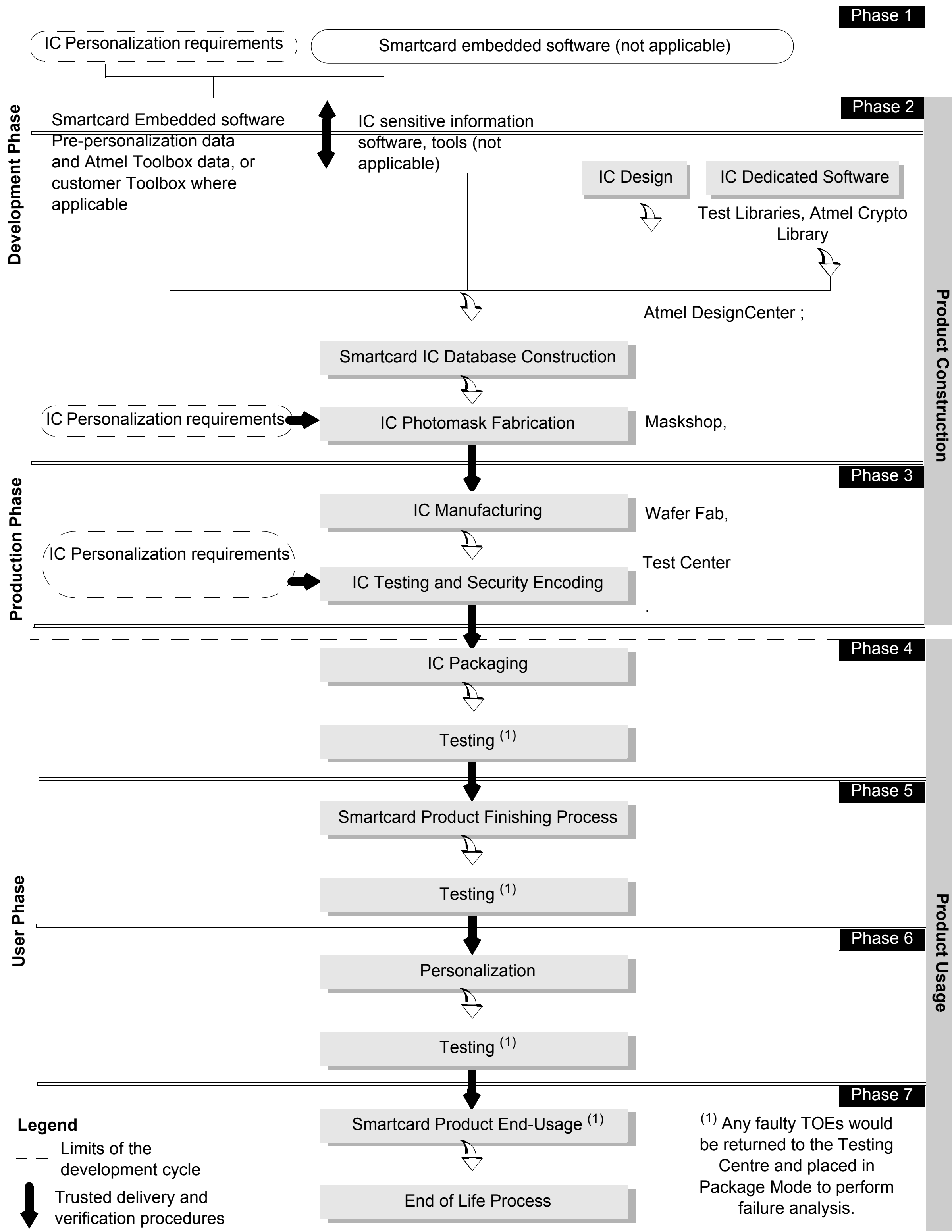


Figure 2-2 Smartcard Product Life Cycle

Secure Delivery Between Phases

38 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

39 These procedures shall be compliant with the assumptions [A_Process_Card] developed in Section 3.2.

40 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

41 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

42 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.

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

44 Reticles and photomasks are generated from the verified IC database. The reticles and photomasks are then shipped in a secure manner to the wafer fab processing facilities.

2.3.2 TOE Production Environment

45 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.

46 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.

47 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.

2.3.3 TOE User Environment

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

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

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

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

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

End-user environment (Phase 7)

53 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.

54 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

55 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

56 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.

57 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

58 Table 2-3 lists the users of the product during phases 4 to 7.

Table 2-3 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.

59 The MCU may be used in the following modes:

a) M.TEST_MODE: Test mode, in which the MCU runs under the control of dedicated test software written to EEPROM via a test interface, and in conjunction with stimulus provided by an external test system. This mode is intended to be used solely by authorized development staff.

b) M.USER_MODE: User mode, in which the MCU runs under control of the smartcard embedded software. It is intended that customers and end-users will always use the MCU in user mode.

60 During the initial part of the manufacturing process, the MCU is set to M.TEST_MODE mode. Authorized development staff then test the MCU. After testing, M.TEST_MODE mode is permanently disabled by sawing off the critical wires, and the MCU is set to M.USER_MODE mode.

61 M.PACKAGE_MODE: Package Mode is a mode similar to Test Mode for testing returns from Phases 4-7. M.PACKAGE_MODE runs a limited subset of test commands via a test interface, and in conjunction with stimulus provided by an external test system. This mode is intended to be used solely by authorized staff.

62 If a faulty TOE is returned from the field then analysis can be done either in M.USER_MODE, or M.PACKAGE_MODE by an authorized test engineer.

63 The only modes of operation are those stated in paragraph 58 and 60.

64 Once manufactured, the MCU operates by executing the smartcard embedded software, which is stored in MCU ROM. The contents of the MCU ROM cannot be modified, whereas the contents of the EEPROM can, in general, be written to or erased, under the control of the smartcard embedded software.

65 The FireWall (Memories and Peripherals Protection Unit) allows the smartcard embedded software to prevent read/write/execute access to (parts of) CPU ROM, EEPROM, RAM, Crypto ROM and peripherals from EEPROM.

66 The ISO7816 compliant I/O port can be used to pass data to or from the MCU. The application program determines how to interpret the data.

2.6 General IT Features of the TOE

67 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)

Section 3

TOE Security Environment

68 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.

69 The environment elements are derived from BSI-PP-002-2001 and adapted to the AT90SC12818RCU 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

70 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),
  - CPU EEPROM (D.CPU_EEPROM_DATA),
  - Crypto ROM (D.CRYPTO_ROM_DATA),
  - CPU RAM (D.CPU_RAM_DATA),
  - CRYPTO RAM (D.CRYPTO_RAM_DATA),
  - Peripherals/IO Registers (D.PERIPH_REG_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),
  - CPU EEPROM (D.CPU_EEPROM_SOFT),
  - Crypto ROM (D.CRYPTO_ROM_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),
  - CPU EEPROM (D.CPU_EEPROM_DSOFT),
  - Crypto ROM (D.CRYPTO_ROM_DSOFT)
- IC dedicated support software:
  - Random numbers generated by the TOE (D.RNG_DATA)

71 Therefore, the TOE itself is an asset.

Secondary Assets

72 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)

73 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

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

Grouping of Assets / Object Definition

75 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: CPU EEPROM: covering D.CPU_E2PROM_DATA, D.CPU_E2PROM_SOFT, D.CPU_E2PROM_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_REG_DATA, D.RNG_DATA,
- O7: Illegal address: unmapped memory space areas,
- O8: Illegal opcode: unmapped CPU opcode.

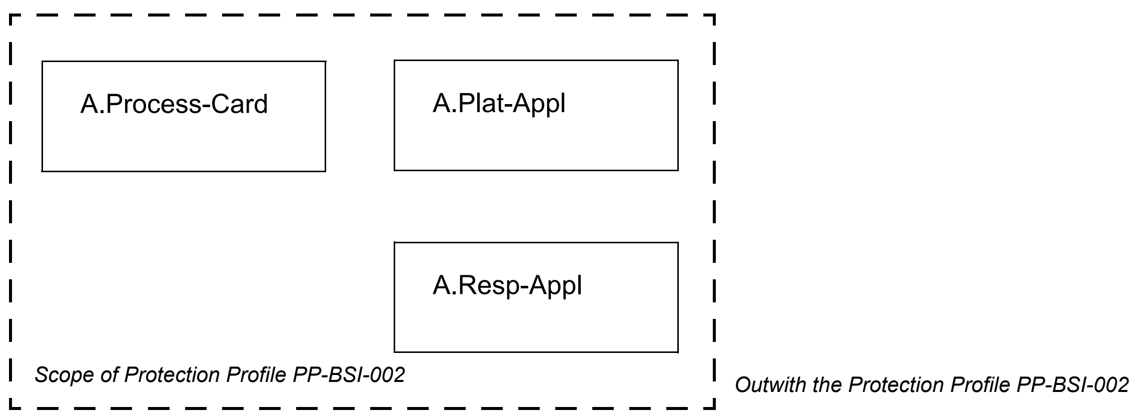
76 Illegal address is defined as unmapped regions in the memory map, as listed in [TD].

77 Illegal opcodes are defined as unmapped CPU opcodes, as listed in [AMIS].

3.2 Assumptions

78 This Security Target Lite 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 Lite and are listed below.

Figure 3-1 Assumptions



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 47. 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 Lite 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 Lite and are listed below.

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

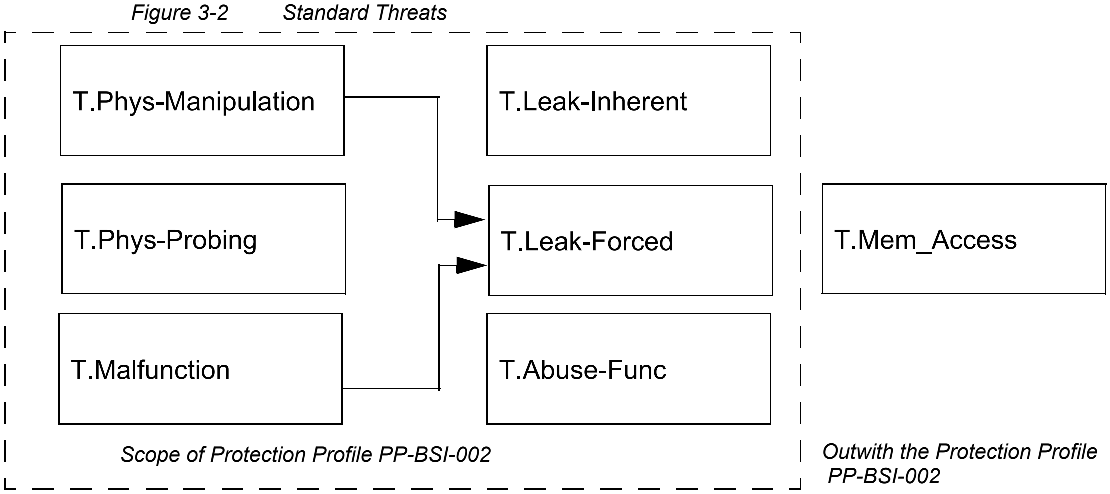
SC1 Manipulation of User Data and of the Smartcard Embedded Software (while being executed/processed and while being stored in the TOE’s memories)

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

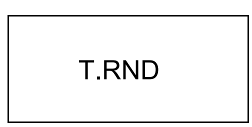
80 The security concerns 1 and 2 give rise to the following threats:

Figure 3-2 Standard Threats



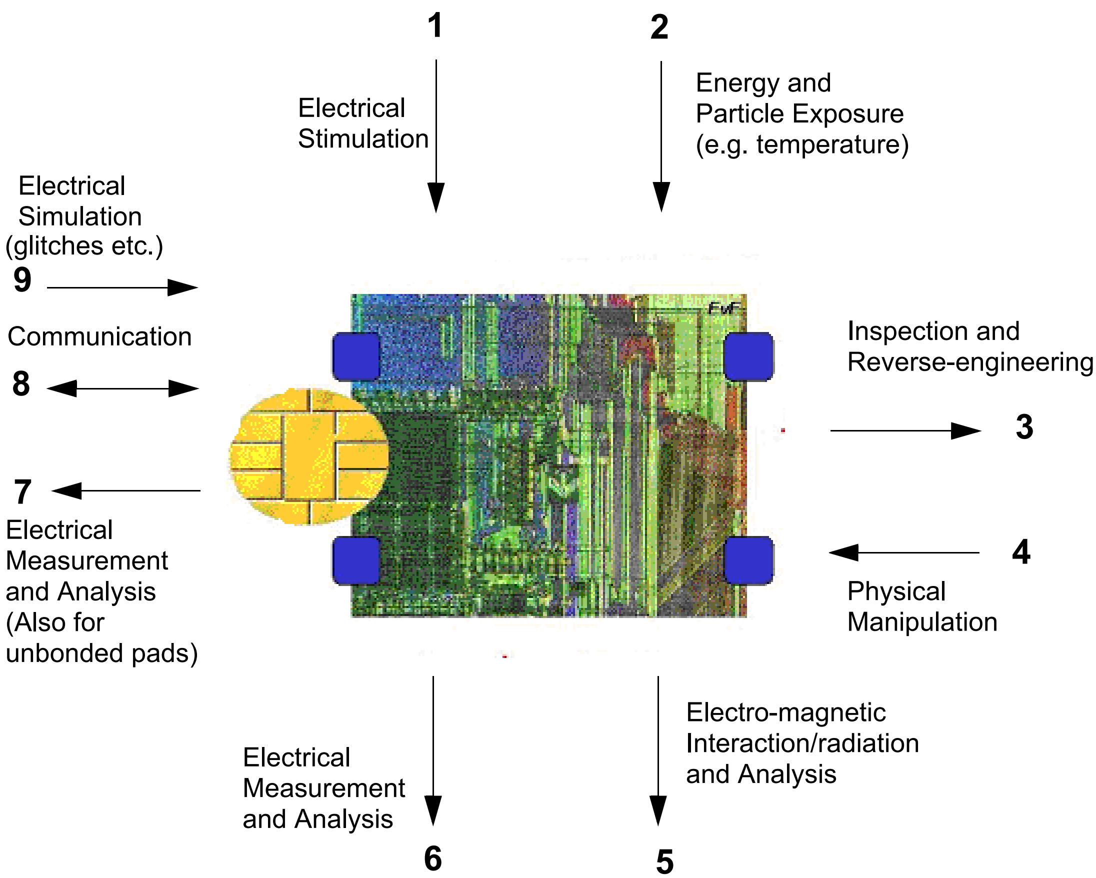
81 The security concern 3 gives rise to the following threat:

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



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 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

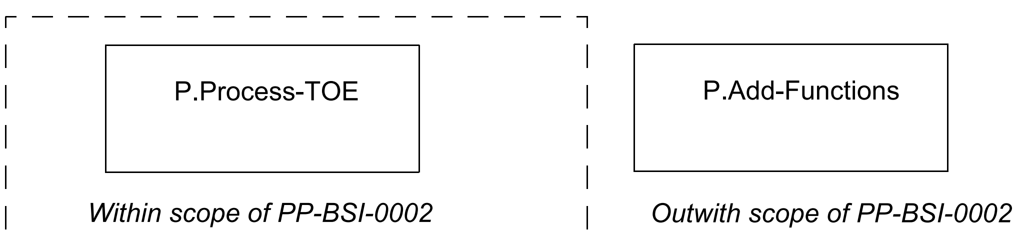
T.RND	**Deficiency of Random Numbers** An attacker may predict or obtain information about random numbers generated by the TOE for instance because of a lack of entropy of the random numbers provided. An attacker may gather information about the reduced random numbers which might be a problem because 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 Lite 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 Lite 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.

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)

Section 4

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 Lite, there are the following standard high level security goals:

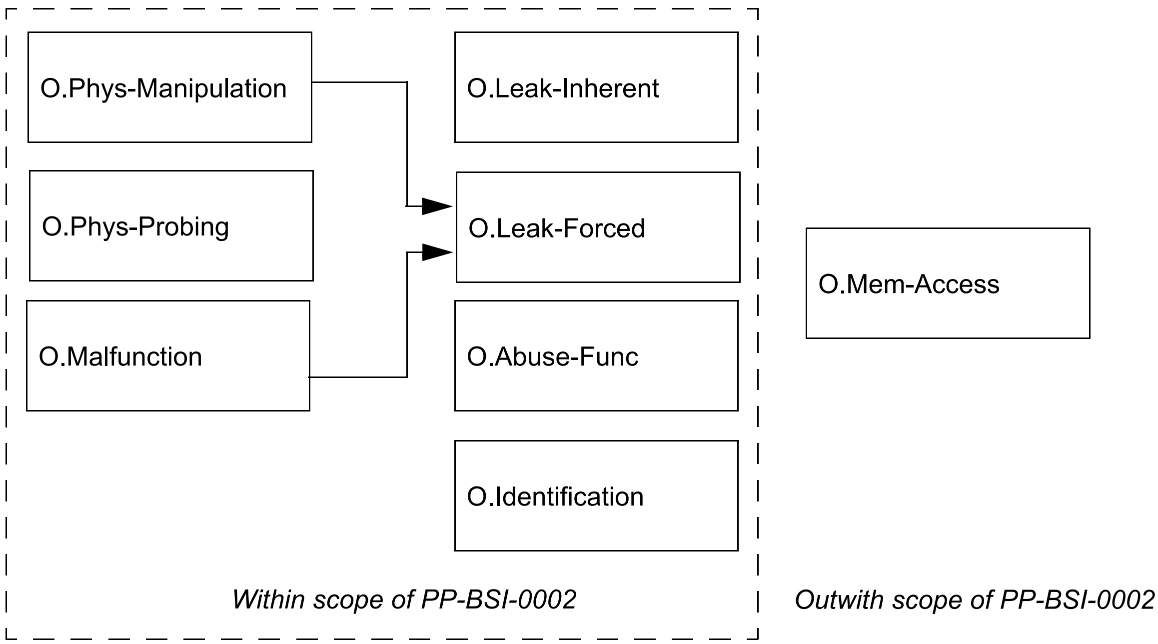
SG1 Maintain the integrity of User Data and of the Smartcard Embedded Software (when being executed/processed and when being stored in the TOE's memories).

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

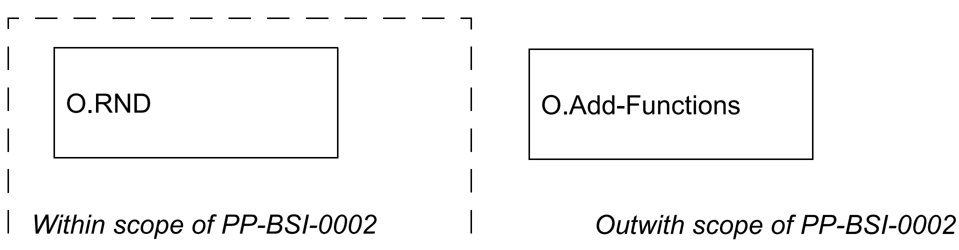


94 According to the security **OBJECTIVES IN** this security Target Lite there are the following high level security goals related to specific functionality:

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 2-2) 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 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 2-2, 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.

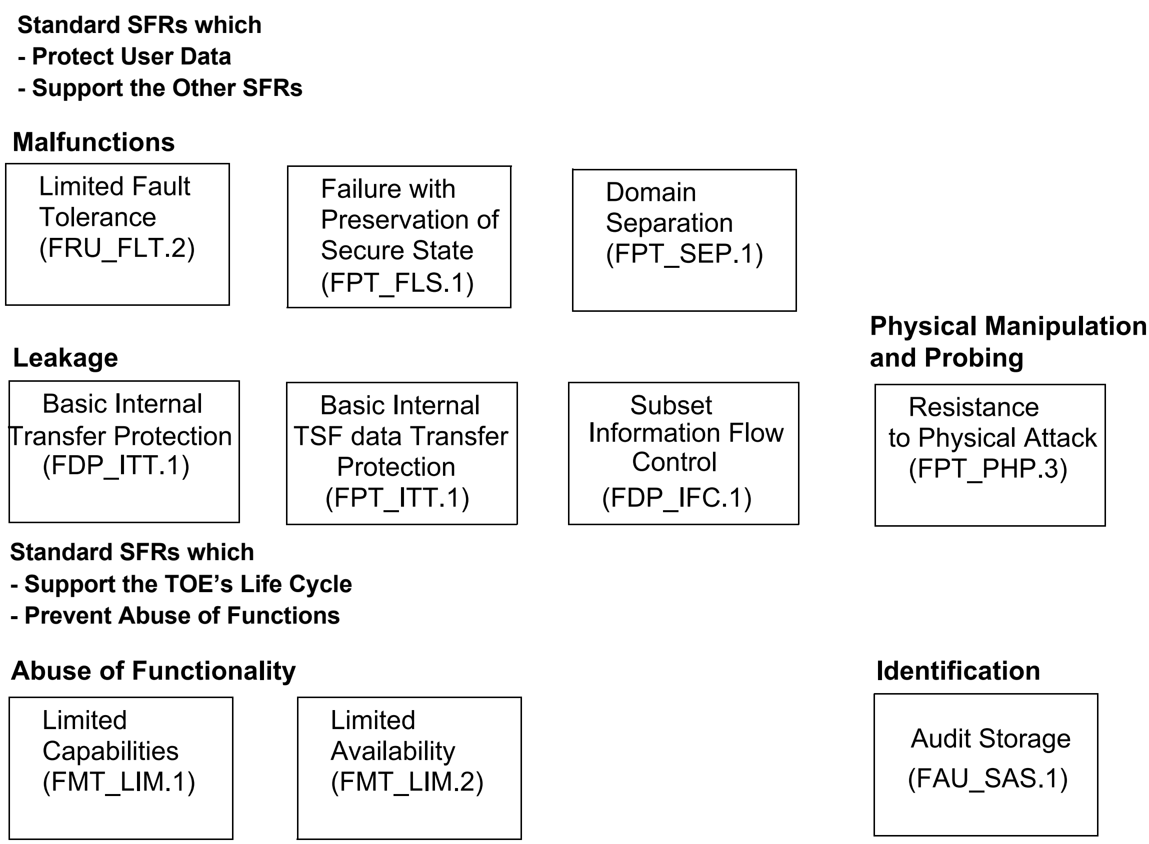
102 The minimum strength of function level for the TOE security requirements is SOF-high.

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

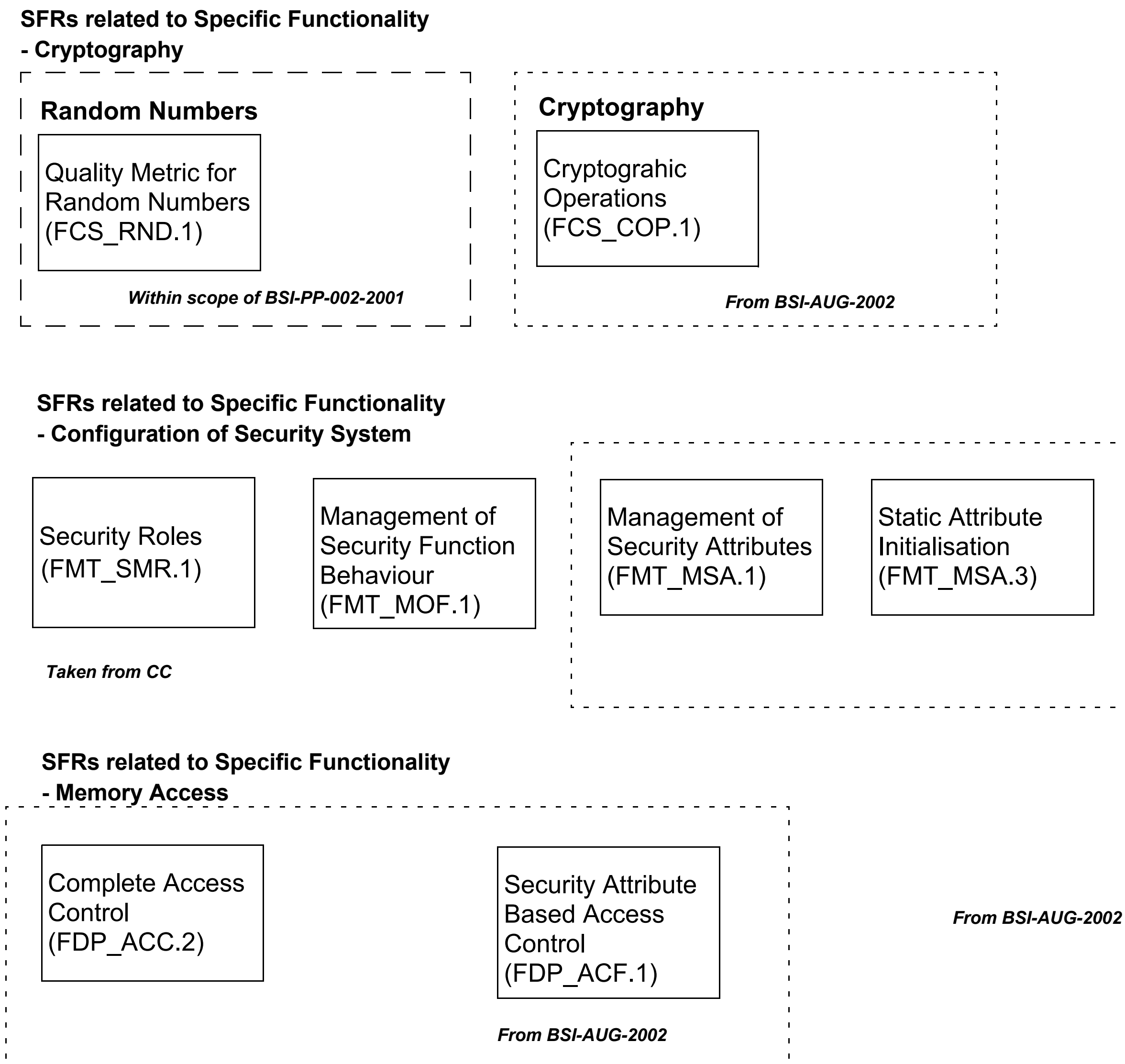
Figure 5-1 Standard Security Functional Requirements



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 Lite and taken from BSI-AUG-2002
- the SFR as stated within this Security Target Lite and taken from the CC

Figure 5-2 Security Functional Requirements related to Specific Functionality



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.1
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 Manipulation and Probing

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 **FIPS 140-2**.
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 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: ▪ **S.TME_ADMIN: Test mode entry (TME) administrator** ▪ **S.SUPER: supervisor** ▪ **S.NON_SUPER: Non-supervisor** ▪ **S.PME_ADMIN: Package mode entry (PME) administrator**
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: ■ restrict the ability to **F1 (Not disclosed in ST-Lite)**. ■ restrict the ability to **F2 (Not disclosed in ST-Lite)**. ■ restrict the ability to **F3 (Not disclosed in ST-Lite)**. ■ restrict the ability to **F4 (Not disclosed in ST-Lite)**. ■ restrict the ability to **F5 (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 (Not disclosed in ST-Lite)** to restrict the ability to **modify** the security attributes to **S.TME_ADMIN, S.SUPER**
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

121 Static Attribute Initialisation (FMT_MSA.3)

122 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(Not disclosed in ST-Lite)** 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 **S.TME_ADMIN** 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)

123 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: S.TME_ADMIN, S.SUPER, S.PME_ADMIN, S.NON_SUPER** ■ **Objects: (O1) CPU ROM, (O2) EEPROM, (O3) Crypto ROM, (O4) CPU RAM, (O5) Crypto RAM, (O6) peripheral and IO registers** 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)

124 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(Not disclosed in ST-Lite)** to objects based on the following: ▪ **Subjects: S.TME_ADMIN, S.SUPER, S.PME_ADMIN, S.NON_SUPER** ▪ **Objects: (O1) CPU ROM, (O2) EEPROM, (O3) Crypto ROM, (O4) CPU RAM, (O5) Crypto RAM, (O6) peripheral and IO registers** ▪ **Operations: Read, Write, Execute** ▪ **Conditions: the MPU configuration** ▪ **Conditions: the Firewall configuration** **For full list see note**
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed
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**
Dependencies	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

Note

- A1: Read CPU ROM (O1) access right
- A2: Write CPU ROM (O1) access right
- A3: Execute CPU ROM (O1) access right
- A4: Read EEPROM (O2) access right
- A5: Write EEPROM (O2) access right
- A6: Execute EEPROM (O2) access right
- A16: Read Crypto ROM (O3) access right
- A17: Write Crypto ROM (O3) access right
- A18: Execute Crypto ROM (O3) access right
- A19: Read CPU EEPROM (O2) access right
- A20: Write CPU EEPROM (O2) access right
- A21: Execute CPU EEPROM (O2) access right
- A22: Read CPU RAM (O4) access right
- A23: Write CPU RAM (O4) access right
- A24: Execute CPU RAM (O4) access right
- A25: Read Crypto RAM (O5) access right
- A26: Write Crypto RAM (O5) access right
- A27: Execute Crypto RAM (O5) access right
- A28: Read peripheral and IO registers (O6) access right
- A29: Write peripheral and IO registers (O6) access right
- A30: Execute peripheral and IO registers (O6) access right

5.2 TOE Security Assurance Requirements

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

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

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

Table 5-1 EAL4 Package and Augmentation

Assurance Class	EAL4 Package	AT90SC12818RCU 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_INT	N/A	N/A	No
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_CCA	N/A	N/A	No
AVA_MSU	2	3	Yes
AVA_SOF	1	1	No
AVA_VLA	2	4	Yes

128 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

129 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 5.2.

6.1 TOE Security Functions

6.1.1 Test Mode Entry (SF1)

130 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.

131 All test entry requirements occur while the TOE is held in reset and failure in any one will prevent Test Mode Entry. It is required that the TOE satisfies the test entry conditions during any internal reset condition.

132 It is not possible to move from User Mode to Test Mode. Any attempt to do this, for example, by forcing internal nodes will be detected and the security functions will disable the ability to enter Test Mode.

133 The Strength of Function claimed for the Test Mode Entry security function is high.

6.1.2 Protected Test Memory Access (SF2)

134 SF2 shall ensure that, although authenticated users can have access to memories using commands in test mode, they cannot access directly their contents.

135 Only authorized Test engineers running tests on the TOE have access to the TME conditions

136 Authorized Test Mode users also have access to other address regions which are not accessible in user mode.

137 The Strength of Function claimed for the Protected Test Memory Access security function is high.

6.1.3 Test Mode Disable (SF3)

138 SF3 shall make provision for:

- Wafer sawing which, once done, shall ensure that none of the test features are available, not even to authenticated users in test mode. Although Package Mode Entry (PME) is available.

6.1.4 TOE Testing (SF4)

139 SF4 shall provide embedded hardware test circuitry with high fault coverage to prevent faulty devices being released in the field. Devices with manufacturing problems (short circuits, open nets,...) could lead to a poor level of security by disabling some security functions.

140 To conform with ISO 7816 standards the TOE embedded software will always return an Answer-To-Reset command via the serial I/O port. This contains messages with information on the integrity and identification of the device. An ATR also verifies significant portions of device hardware (CPU, ROM, EEPROM and logic).

6.1.5 Data Error Detection (SF5)

141 SF5 shall provide means for performing data error detection.

142 Means of performing checksum error detection and parity error detection is provided. The 16/32-bit Checksum Accelerator or the CRC-16/32 hardware peripheral can be used by the smartcard embedded software to compute fast data error detection on the program and/or data memories before starting any operation.

143 To prevent data corruption of the CPU RAM, a Cstack Checker is provided. The Cstack checker protects the CPU RAM access using Y pointer against fault injection attacks, fault injection could change the RAM address during the CPU RAM read and write sequences with the intention of changing the device behaviour or extracting sensitive data. The Cstack checker checks the RAM address during RAM access, using Y

pointer, and is located in a RAM window, the window is defined through four registers. The registers are accessible in read/write operations, to be used by the smartcard embedded software to check the CPU RAM for data corruption.

6.1.6 FireWall (SF6)

144 SF6 shall enforce access control based on the FireWall rules as defined in the ACSF_Policy (Not disclosed in the ST-Lite).

Memory protection

145 The FireWall defines five user modes to execute embedded software:

- S.SUPER
- S.NON_SUPER mode (also named user mode).

146 The embedded software is split into two segments: a supervisor Operating System (located in S.SUPER region), and a user application (located in S.NON_SUPER region). The supervisor segment defines by software the limits of the S.NON_SUPER segment.

147 If a protected address is accessed by the S.NON_SUPER software, a security interrupt is invoked.

Illegal address

148 If an illegal address is accessed, a security interrupt is invoked.

Illegal opcode

149 If an attempt is made to execute any opcode that is not implemented in the instruction set, a security non maskable interrupt is invoked.

6.1.7 Event Audit (SF7)

150 The TOE shall provide an Event Audit security function (SF7) to enforce the following rules for monitoring audited events.

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

- The external voltage supply goes outside acceptable bounds:
- The external clock signal goes outside acceptable bounds:
- The ambient temperature goes outside acceptable bounds:
- Application program abnormal runaway:
- Attempts to physically probe the device:
- Attempts to gain illegal access to reserved RAM memory locations:

- Attempts to gain illegal access to reserved EEPROM (O2) memory locations:
- Attempts to gain illegal access to reserved peripheral, IO and AdvX register locations:
- Attempts to execute illegal instruction “LPM” to read the program memory from the S.NON_SUPER program location:
- Attempts to move the RAM stack to an illegal RAM memory location defined by SPHLC and SPLLC registers:
- Attempts to execute an CPU opcode that is not implemented:
- Attempts to illegally write access the device’s EEPROM (O2):
- Attempts to gain illegal access to Supervisor modes:
- Exposure to UV light goes outside acceptable bounds:

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

6.1.8 Event Action (SF8)

153 SF8 shall provide an Event Action security function to register occurrences of audited events and take appropriate action. Detection of such occurrences will cause an information flag to be set, and may cause one of the following to occur if warranted by the violation:

- Memory wiping actions
- Different levels of immediate reset
- Different levels of security interupts

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

6.1.9 Unobservability (SF9)

155 SF9 shall ensure that users/third parties will have difficulty observing the following operations on the TOE by the described means.

1. Extract information relating to any specific resource or service being used by:Monitoring power consumption.
2. Extract information relating to any specific resource or service being used by: Carrying out timing analysis on Crypto Functions.
3. Extract information relating to any specific resource or service being used by:Using mechanical, electrical or optical means.

156 The Strength of Function claimed for the Unobservability security function is high.

6.1.10 Cryptography (SF10)

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

158 the TSF shall provide hardware DES, TDES data encryption/decryption capability.

159 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. The RNG has a Digitized Analogue Source (DAS) bit that enables the smartcard embedded software to check that the RNG noise source maintains a sufficient entropy throughout the life of the TOE, this confirms to the FIPS 140-2 standard.

160 The Strength of Function claimed for the cryptography security function is high.

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

- DES algorithm
- TDES algorithm

6.1.11 Package Mode Entry (SF11)

162 SF11 shall ensure only authorized users will be permitted to enter Package Mode. This is provided by the Test Mode Entry conditions, and also the Package Mode Entry conditions. Both conditions must be met to enter Package Mode.

163 To enter Package mode the conditions must be met in SF1 first, then whilst the TOE is still held in reset the PME conditions must be met. Failure to meet these conditions will prevent entry into Package Mode.

164 The Strength of Function for the Package Mode Entry function is high.

6.1.12 Test Memory Access in Package Mode (SF12)

165 SF12 shall ensure that, although authenticated users can have access to memories using commands in package mode, they cannot access directly their contents.

166 When package mode is entered a full EEPROM (O2) erase is performed. Access to the device memories are limited by test algorithms.

167 Only authorized Test engineers running tests on the TOE have access to the TME conditions

168 The Strength of Function claimed for the Protected Test Memory Access in Package Mode is high.

6.1.13 Security Functions Based on Permutations/combinations

169 Not disclosed in the ST-Lite

6.2 TOE Assurance Measures

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

Table 6-1 Relationship Between Assurance Requirements and Measures

		Security Target Lite	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									
ADV_HLD.2					x									
ADV_IMP.2					x									
ADV_LLD.1					x									
ADV_RCR.1					x									
ADV_SPM.1					x									
AGD_ADM.1						x								
AGD_USR.1						x								
ALC_DVS.2							x				x	x	x	x
ALC_LCD.1							x				x	x	x	x
ALC_TAT.1							x				x	x	x	x
ATE_COV.2								x		x		x		
ATE_DPT.1								x		x		x		
ATE_FUN.1								x		x		x		
ATE_IND.2								x		x		x		
AVA_MSU.3									x	x				

Table 6-1 Relationship Between Assurance Requirements and Measures

AVA_SOF.1									x	x				
AVA_VLA.4									x	x				

Security Target (SA1)

171 SA1 shall provide the "TOE Security Target" document plus its references.

Configuration Management (SA2)

172 SA2 shall provide the "CC Configuration Management (ACM)" interface document plus its references.

Delivery and Operation (SA3)

173 SA3 shall provide the "CC Delivery and Operation (ADO)" interface document plus its references.

Development Activity (SA4)

174 SA4 shall provide the "CC Development Activity (ADV)" interface document plus its references.

Guidance (SA5)

175 SA5 shall provide the "CC Guidance (AGD)" interface document plus its references.

Life Cycle Support (SA6)

176 SA6 shall provide the "CC Life Cycle Support (ALC)" interface document plus its references.

Test Activity (SA7)

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

Vulnerability Assessment (SA8)

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

Smart Card Devices (SA9)

179 SA9 shall provide functional AT90SC12818RCU smart card devices.

Development Site (SA10)

180 SA10 shall provide access to the development site.

Test Site (SA11)

181 SA11 shall provide access to the test site.

Manufacturing Site (SA12)

182 SA12 shall provide access to the manufacturing site.

Sub-contractor Sites (SA13)

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

Section 7

PP Claims

7.1 PP Reference

184 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

185 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.

186 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

187 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

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

7.3.1.1 Assumptions

189 None

7.3.1.2 Threats

190 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

191 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

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

193 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

194 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
- FMT_MSA.3 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

195 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

0.1 Terms

Control Bytes	Reserved bytes of EEPROM which can be programmed with traceability information.
CRC-32	Algorithm used to compute powerful checksum on memory blocks
HASH	Transformation of a string of characters into a usually shorter fixed length value or key that represents the original string.
IC Dedicated Software	IC Proprietary software which is required for testing purposes and to implement special functions. For AT90SC12818RCU 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.
UNIX	Interactive Time Sharing Operating System.

0.2 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
PMT	Package Mode Test
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

TD	Technical Data
TME	Test Mode Entry
TMR	Test Mode Run
TOE	Target of Evaluation
USB	Universal Serial Bus
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