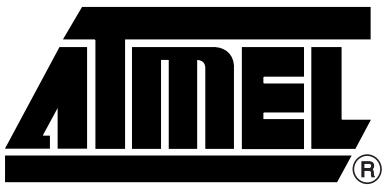
AT90SC6404RT

Security Target Lite

EAL5+



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.

Export of this Product outside of the EU may require an Export Licence.

1.1 Identification

1 Title: AT90SC6404RT Security Target Lite

2 This Security Target Lite has been constructed with Common Criteria (CC) Version 2.2.

1.2 Overview

3 This Security Target Lite (ST) 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 AVR ASL4 and the ‘parent’ device of the family, from which other family members will be derived, is the AT90SC19264RC.

4 The AT90SC6404RT MCU device

Product Identification Number	AT58884
Revision	B

5 is being evaluated against the Common Criteria CC Smartcard Integrated Circuit Protection Profile PP/9806 to Evaluation Assurance Level 5 (EAL5) augmented of AVA_VLA.4, ALC_DVS.2 and AVA_MSU.3 under the Common Criteria maintenance scheme. Atmel Smart Card ICs, a division of ATMEL Corporation, is the developer and the sponsor for the AVR ASL4 evaluations.

6 The devices in the AVR 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. AVR 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

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

- Part 2 conformant: the security functional requirements are based on those identified in part 2 of the Common Criteria.
- Part 3 conformant: the security assurance requirements, including those used in the augmentation, are based on those in part 3 of the Common Criteria.

1.4 Document Objective

8 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 PP/9806, Smartcard Integrated Circuit V2.0, against which the AVR ASL4 devices will be evaluated.

1.5 Document Structure

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

10 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.

11 Section 3 describes the TOE security environment.

12 Section 4 describes the required security objectives.

13 Section 5 describes the TOE security functional requirements and the security assurance requirements.

14 Section 6 describes the TOE security functions.

15 Section 7 describes the Protection Profile (PP) claims.

16 Appendix A provides a glossary of the terms and abbreviations.

1.6 Scope and Terminology

17 This document is based on the TOE Technical Data Sheet [TD].

18 The term *Target of Evaluation* (TOE) is standard CC terminology and refers to the product being evaluated, the AT90SC6404RT MCU device in this case. The TOE is subject to hardware evaluation only. 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].

19 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.

20 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

21 This document refers to the latest issues of the following Atmel documents:

- [STI] AT90SC6404RT Test Hardware Specification
- [ROMDD] AT90SC Engineering Software Detailed Description
- [ROMUG] AT90SC Engineering Software User Guide
- [TMRE2] AT90SC Production Test Software Detailed Description
- [TMRUSER] AT90SC Production Test Software User Guide
- [TD] AT90SC6404RT Technical Data (TPR0125)
- [ESOF] TOE Strength of Security Functions Analysis
- [PLC] Common Criteria PLC

1.8 Revision History

Rev	Date	Description	Originator
A	08 Aug 06	Initial release	Alexandre Croguennec, Atmel, RFO / John Boggie, Atmel, EKB
B	10 Jan 07	Updated PIN to AT58884 and changed Rev to B due to Fab change	John Boggie

Target of Evaluation Description

22 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

23 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 AT90SC6404RT device from the AVR 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 Lite.

24 The devices in the AVR 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 AVR ASL4 family members offer various options. The AVR ASL4 family of devices are designed in accordance with the ISO standard for integrated circuit cards (ISO 7816), where appropriate.

25 Although the TOE evaluation is hardware only, 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.

26 The TOE widely uses ATMEL high density non volatile memories: it features 64K bytes of CPU ROM program memory, 4K bytes of EEPROM program/data memory, 2K bytes of static RAM memory.

27 The EEPROM includes 64 bytes of One Time Programmable (OTP) memory (32 bytes are byte-addressable; 32 bytes are bit-addressable) and a 192-byte bit-addressable area.

28 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].

29 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].

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

Table 2-1 Classic and XP Write modes

31 The TOE also includes a 32bit Checksum Accelerator, a CRC-16 peripheral, a Random Number Generator (the RNG is outwith the scope of the evaluation), and a fast hardware DES/3DES peripheral.

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

33 The TOE is equipped with logic peripherals including 2 timers, 1 serial port, an ISO7816 interface and an ISO7816 controller.

34 The TOE includes a powerful Firewall that protects all memories, peripheral and IO register accesses. This Firewall defines the 2 user modes and many different address spaces.

35 The TOE interfaces consist of:

- The physical surface of the circuit,
- The ISO7816-3 electrical contacts (VCC, GND, CLK, RSTN, I/O0),
- The software interface to the hardware component through memories and registers,
- No other software interface (as there is no IC dedicated software in the TOE).

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

- [TD] AT90SC6404RT Technical Data (TPR0125)
- [AM_IS] AT90SC Addressing Modes and Instruction Set (1323)
- [APP_SEC] Security Recommendations AT90SC ASL4 Products (TPR0066)
- [APP_DES] Secure Hardware DES/TDES on the AT90SC ASL4 Products (TPR0063)
- [APP_FWL] Using the Supervisor and User Mode in the AT90SC ASL4 Products (TPR0095)
- [APP_RNG] Generating Unpredictable Random Numbers on the AT90SC Family Devices (1573)
- [APP_RNG_ENT] Generating Random Numbers with a controlled entropy on AT90SC family (TPR0166)

37 These guidance documents are constantly updated as the state-of-the-art of the attacks evolves. Software developer should always refer to the latest version of these documents.

2.2 Smartcard Product Life-cycle

38 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.

39 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.

40 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.

41 Figure 2-1 describes the Smartcard product life-cycle. [PLC] contains the addresses of the relevant organizations.

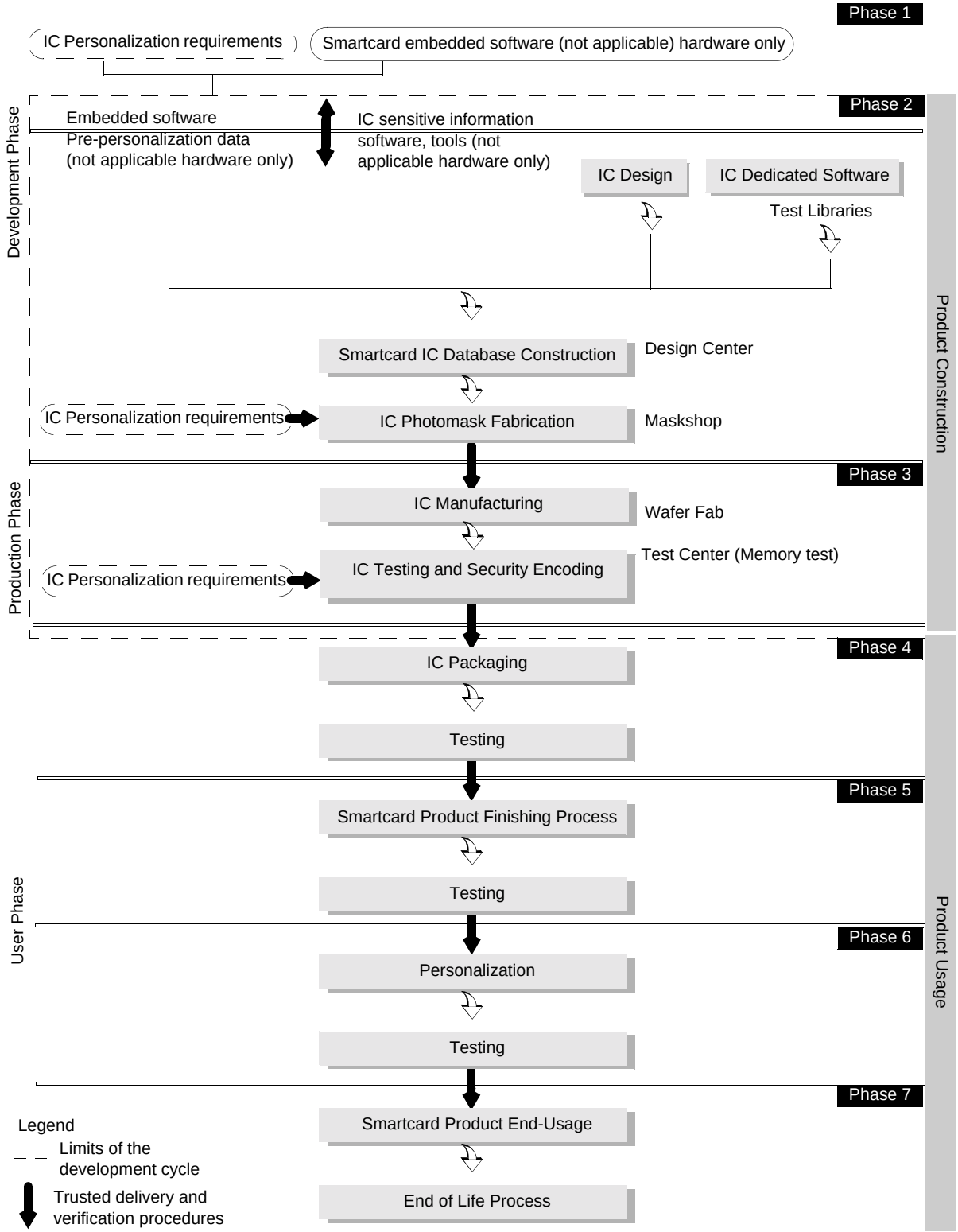


Figure 2-1 Smartcard Product Life Cycle

42 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

43 These procedures shall be compliant with the assumptions [A_DLV] developed in Section 3.2.2.

2.3 TOE Environment

44 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

45 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.

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

47 Reticles and photomasks are generated from the verified IC database. These are manufactured by Maskshop (see address in [PLC]), for wafer fab processing undertaken as per [PLC]. The reticles and photomasks are then shipped in a secure manner to the wafer fab processing facilities.

2.3.2 TOE Production Environment

48 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.

49 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, then sent to Test Center (see [PLC]) 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.

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

2.3.3 TOE User Environment

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

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

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

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

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

End-user environment (Phase 7)

56 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.

57 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

58 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

59 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.

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

- The IC designer:

  Authorized staff who work for the developer, and who design the MCU (such development staff are trusted and privileged users).

- The IC manufacturer:

  Authorized staff who work for the developer and who manufacture and test the MCU (such manufacturing staff are trusted and priviliged users).

- The smartcard dedicated software developer:

  Authorized staff who work for the developer and who develop the dedicated test software and crypto libraries (such development staff are trusted and priviliged users).

61 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.

62 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.

63 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.

64 If a faulty MCU is returned from the field then analysis can only be done in M.USER_MODE mode because M.TEST_MODE mode is inhibited by sawing off the critical wires, prior to devices going to the field.

65 There is no intermediate mode for fault analysis. The only modes of operation are those stated in paragraph 62.

66 Once manufactured, the MCU operates by executing the smartcard embedded software, which is stored in CPU ROM. The contents of the CPU 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.

67 The EEPROM includes One Time Programmable (OTP) bytes, which can be used by the embedded software to store security-related information such as cryptographic keys or life state software flags. Customer embedded software is outwith the scope of the evaluation.

68 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 and peripherals from EEPROM.

69 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

70 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)

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

3.1 Assets

72 Assets are security relevant elements of the TOE that include the:

- 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),
  - CPU RAM (D.CPU_RAM_DATA),
  - Peripherals/IO Registers (D.PERIPH_REG_DATA),
- Smartcard embedded software (D.xxx_SOFT) located in:
  - CPU ROM (D.CPU_ROM_SOFT),
  - CPU EEPROM (D.CPU_EEPROM_SOFT),
- IC dedicated software (D.xxx_DSOFT) located in:
  - CPU ROM (D.CPU_ROM_DSOFT),
  - CPU EEPROM (D.CPU_EEPROM_DSOFT),
- IC specification (D.IC_SPEC), design (D.DESIGN), development tools (D.DEV_TOOLS) and technology (D.TECHNO).

73 Therefore, the TOE itself is an asset.

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

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 : CPU RAM: covering D.CPU_ROM_DATA,
- O4 : Peripherals and IO Registers: covering D.PERIPH_REG_DATA,
- O5 : Illegal address: unmapped memory space areas,
- O6 : 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 It is assumed that this section concerns the following items:

- Due to the definition of the TOE limits, any assumption for the smartcard software development (phase 1 is outside the scope of the TOE)
- Any assumption from phases 4 to 7 for the secure usage of the TOE, including the TOE trusted delivery procedures

79 Security is always dependent on the whole system: the weakest element of the chain determines the total system security. Assumptions described hereafter must be considered for a secure system using smartcard products:

- Assumptions on phase 1
- Assumptions on the TOE delivery process (phases 4 to 7)
- Assumptions on phases 4-5-6
- Assumptions on phase 7

3.2.1 Assumptions on Phase 1

A.SOFT_ARCHI	The smartcard embedded software and data (D.SOFT_xxx and D.xxx_DATA) shall be designed in a secure manner, that is focusing on integrity of program and data.
A.DEV_ORG	Procedures dealing with physical, personnel, organizational, technical measures for the confidentiality and integrity of smartcard embedded software and data (e.g. source code and any associated documents related to D.xxx_SOFT and D.xxx_DATA) and IC designer proprietary information (tools D.DEV_TOOLS, software D.xxx_DSOFT, documentation D.IC_SPEC, D.DESIGN, D.TECHNO) shall exist and be applied in software development.

3.2.2 Assumptions on the TOE Delivery Process (Phases 4 to 7)

80 Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives as described in the following assumptions.

A.DLV_PROTECT	Procedures shall ensure protection of TOE material and information under delivery and storage. A procedure shall ensure protection of the TOE for unsawn wafer delivery.
A.DLV_AUDIT	Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.
A.DLV_RESP	Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

3.2.3 Assumptions on Phases 4 to 6

A.USE_TEST	It is assumed that appropriate functionality testing of the IC is used in phases 4, 5 and 6.
A.USE_PROD	It is assumed that security procedures are used during all manufacturing and test operations through phases 4, 5, 6 to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use). In the case when unsawn wafers are delivered, appropriate guidance on sawing will be known and used by the customer.

3.2.4 Assumptions on Phase 7

A.USE_DIAG	It is assumed that secure communication protocols and procedures are used between smartcard and terminal.
A.USE_SYS	It is assumed that the integrity and confidentiality of sensitive data stored/handled by the system (terminals, communications...) is maintained.

3.3 Threats

81 The TOE as defined in Section 2 is required to counter the threats described hereafter; a threat agent wishes to abuse the assets either by functional attacks, environmental manipulations, specific hardware manipulations or by any other types of attacks.

82 Threats have to be split in:

- Threats against which specific protection within the TOE is required (class I),
- Threats against which specific protection within the environment is required (class II).

3.3.1 Unauthorized Full or Partial Cloning of the TOE

T.CLON	Functional cloning of the TOE (full or partial) appears to be relevant to any phases of the TOE life-cycle, from phase 1 to phase 7. Generally, this threat is derived from specific threats combining unauthorized disclosure, modification or theft of assets at different phases.

3.3.2 Threats on Phase 1 (Delivery and Verification Procedures)

83 During phase 1, three types of threats have to be considered:

a) Threats on the smartcard's embedded software D.xxx_SOFT and its environment of development, such as:

- Unauthorized disclosure
- Modification or theft of the smartcard embedded software D.xxx_SOFT and any additional data D.xxx_DATA at phase 1.

Considering the limits of the TOE, these previous threats are outside the scope of this Security Target Lite.

b) Threats on the assets transmitted from the IC designer to the smartcard software developer during the smartcard development.

c) Threats on the smartcard embedded software D.xxx_SOFT and any additional application data D.xxx_DATA transmitted during the delivery process from the smartcard embedded software developer to the IC designer.

84 The previous types b and c threats are described hereafter.

T.DIS_INFO	Unauthorized disclosure of the assets delivered by the IC designer to the smartcard software developer such as sensitive information on IC specification D.IC_SPEC, design D_DESIGN and technology D.TECHNO, software and tools D.DEV_TOOLS if applicable.
T.DIS_DEL	Unauthorized disclosure of the smartcard embedded software D.xxx_SOFT and any additional application data D.xxx_DATA (such as IC pre-personalization requirements) during the delivery process to the IC designer.
T.MOD_DEL	Unauthorized modification of the smartcard embedded software D.xxx_SOFT and any additional application data D.xxx_DATA (such as IC pre-personalization requirements) during the delivery process to the IC designer.
T.T_DEL	Theft of the smartcard embedded software D.xxx_SOFT and any additional application data D.xxx_DATA (such as IC pre-personalization requirements) during the delivery process to the IC designer.

3.3.3 Threats on Phases 2 to 7

85 During these phases, the assumed threats could be described in three types:

- Unauthorized disclosure of assets
- Theft or unauthorized use of assets
- Unauthorized modification of assets

Unauthorized disclosure of assets

86 This type of threats covers unauthorized disclosure of assets by attackers who may possess a wide range of technical skills, resources and motivation. Such attackers may also have technical awareness of the product.

T.DIS_DESIGN	Unauthorized disclosure of IC design D.DESIGN. This threat covers the unauthorized disclosure of proprietary elements such as IC technology detailed information D.TECHNO, IC specification, IC design, IC hardware security mechanisms specifications D.DESIGN and D.IC_SPEC.
T.DIS_SOFT	Unauthorized disclosure of smartcard embedded software D.xxx_SOFT and data D.xxx_DATA such as access control, authentication system, data protection system, memory partitioning, cryptographic programs.

T.DIS_DSOFT	Unauthorized disclosure of IC dedicated software D.xxx_DSOFT. This threat covers the unauthorized disclosure of IC dedicated software D.xxx_DSOFT including security mechanisms specifications D.IC_SPEC and implementation D.DESIGN.
T.DIS_TEST	Unauthorized disclosure of test information such as full results of IC testing including interpretations.
T.DIS_TOOLS	Unauthorized disclosure of development tools D.DEV_TOOLS. This threat covers potential disclosure of IC development tools and testing tools (analysis tools, microprobing tools).
T.DIS_PHOTOMASK	Unauthorized disclosure of photomask information D.CPU_ROM_DATA, D.CPU_ROM_SOFT, D.CPU_ROM_DSOFT, D.DESIGN, used for photoengraving during the silicon fabrication process.

Theft or unauthorized use of assets

87 Potential attackers may gain access to the TOE and perform operations for which they are not authorized. For example, such attackers may personalize the product in an unauthorized manner, or try to gain fraudulous access to the smartcard system.

T.T_SAMPLE	Theft or unauthorized use of TOE silicon samples, for example, bond out chips.
T.T_PHOTOMASK	Theft or unauthorized use of TOE photomasks, D.CPU_ROM_DATA, D.CPU_ROM_SOFT, D.CPU_ROM_DSOFT, D.DESIGN.
T.T_PRODUCT	Theft or unauthorized use of smartcard products.

Unauthorized modification of assets

88 The TOE may be subjected to different types of logical or physical attacks which may compromise security. Due to the intended usage of the TOE (the TOE environment may be hostile), the TOE security parts may be bypassed or compromised reducing the

integrity of the TOE security mechanisms and disabling their ability to manage the TOE security. This type of threat includes the implementation of malicious trojan horses.

T.MOD_DESIGN	Unauthorized modification of IC design D.DESIGN. This threat covers the unauthorized modification of IC specification D.IC_SPEC, IC design including IC hardware security mechanisms specifications and realization D.DESIGN.
T.MOD_PHOTOMASK	Unauthorized modification of TOE photomasks, D.CPU_ROM_DATA, D.CPU_ROM_SOFT, D.CPU_ROM_DSOFT, D.DESIGN,.
T.MOD_DSOFT	Unauthorized modification of IC dedicated software D.xxx_DSOFT including modification of security mechanisms.
T.MOD_SOFT	Unauthorized modification of smartcard embedded software D.xxx_SOFT and data D.xxx_DATA.

89 Table 3-1 indicates the relationships between the smartcard phases and the threats.

Table 3-1 Threats and Phases

Threats	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Phase 6	Phase 7
Functional cloning							
T.CLON	Class II	Class II	Class I/II	Class I	Class I	Class I	Class I
Unauthorized disclosure of assets							
T.DIS_INFO	Class II						
T.DIS_DEL	Class II						
T.DIS_SOFT		Class II	Class I/II	Class I	Class I	Class I	Class I
T.DIS_DSOFT		Class II	Class I/II	Class I	Class I	Class I	Class I
T.DIS_DESIGN		Class II	Class I/II	Class I	Class I	Class I	Class I
T.DIS_TOOLS		Class II	Class II				
T.DIS_PHOTOMASK		Class II	Class II				
T.DIS_TEST			Class I/II	Class I	Class I	Class I	
Theft or unauthorized use of assets							
T.T_DEL	Class II						
T.T_SAMPLE		Class II	Class I/II	Class I	Class I		
T.T_PHOTOMASK		Class II	Class II				
T.T_PRODUCT			Class I/II	Class I	Class I	Class I	Class I
Unauthorized modification threats							
T.MOD_DEL	Class II						
T.MOD_SOFT		Class II	Class I/II	Class I	Class I	Class I	Class I
T.MOD_DSOFT		Class II	Class I/II	Class I	Class I	Class I	Class I
T.MOD_DESIGN		Class II	Class I/II	Class I	Class I	Class I	Class I
T.MOD_PHOTOMASK		Class II	Class II				

3.4 Organizational Security Policies

90 An organizational security policy is mandatory for the smartcard product usage. The specifications of organizational security policies essentially depend on the applications in which the TOE is incorporated.

91 However, it was found relevant to address the following organizational security policy with the TOE because most of the actual Smart Card secure applications make use of cryptographic standards.

P.CRYPTO	**Cryptographic entities, data authentication, and approval functions must be in accordance with ISO, associated industry, or organizational standards or requirements.** Various cryptographic algorithms and mechanisms, such as triple DES, AES, RSA, MACs, and Digital Signatures, are accepted international standards. These, or others in accordance with industry or organizational standards of similar maturity and definition, should be used for all cryptographic operations in the TOE. These cryptographic operations are used for instance to support establishment and control of a trusted channel between the TOE and the outside environment.

92 The security objectives of the TOE cover principally the following aspects:

- Integrity and confidentiality of assets
- Protection of the TOE and associated documentation during development and production phases

4.1 Security Objectives for the TOE

93 The TOE shall use state of art technology to achieve the following IT security objectives:

O.TAMPER **The TOE must prevent physical tampering with its security critical parts.**

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

This includes protection against direct micro-probing of signals not connected to bonding pads, but also other contact or contactless probing techniques such as laser probing or electromagnetic sensing. Most of these techniques require a prior reverse engineering of parts of the device to understand its architecture and its security functions.

This also includes protection against inherent information leakage (for example shape of signals, power consumption) on the device external interfaces (for example clock, supply, I/O lines) that could be used to disclose confidential data, as well as forced information leakage caused by induced malfunction or physical manipulation

O.CLON	**The TOE functionality needs to be protected from cloning.** The TOE must include means to prevent an attacker from reproducing the smartcard functionality. Most of these techniques require a prior reverse engineering of parts of the device to understand its architecture and its security functions.
O.OPERATE	**The TOE must ensure the continued correct operation of its security functions**. The TOE must include protection against the use of stolen silicon samples or products that would ease an attacker gaining fraudulous access to the smartcard system. The TOE must also provide mechanisms to avoid the unauthorized modification of the security functions or software and data, by using the device test commands for instance, or by using uncontrolled/unauthenticated software access to memories. 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
O.FLAW	**The TOE must not contain flaws in design, implementation or operation.** The TOE design must include protection against modification of its security mechanisms (for example detectors or memory protections) that would lead to bypass or reduce their integrity, and therefore open security holes that could be used to access embedded software and data. The TOE design must also provide protection against modification of its embedded software that would lead to bypass or reduce the integrity of some software controlled security mechanisms (for example memory areas definition), and therefore open security holes that could be used to access embedded software and data.
O.DIS_MECHANISM	**The TOE shall ensure that the hardware security mechanisms are protected against unauthorized disclosure.** The TOE must be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill and time to derive detailed designed information or other information which could be used to compromise security through physical attacks.

O.DIS_MEMORY	**The TOE shall ensure that sensitive information stored in memories is protected against unauthorized access.** The TOE must provide protection against unauthorized access to embedded software and data stored in memories, either using test commands, or by some embedded software (for instance a non-supervisor user application) that would try to dump the memories protected by the Firewall programmation (for instance the supervisor program and/or data), or even by some physical attacks.
O.MOD_MEMORY	**The TOE shall ensure that sensitive information stored in memories is protected against any corruption or unauthorized modification.** The TOE must provide protection against unauthorized access to embedded software and data stored in memories, either using test commands, or by some embedded software (for instance a non-supervisor user application) that would try to modify the memories protected by the Firewall programmation (for instance the supervisor program and/or data), or even by some physical attacks.
O.CRYPTO	**Cryptographic capability shall be available for users to maintain integrity and confidentiality of sensitive data.** The TOE must provide hardware implementation of some cryptographic algorithms that can be used by the embedded software in conjunction with appropriate counter-measure to achieve cryptographic operations (for instance encryption, decryption, integrity checking, signature, key generation, for algorithms such as DES, TDES, RSA, SHA-1, DSA, Elliptic Curves, ...). These cryptographic operations are used for instance to support establishment and control of a trusted channel between the TOE and the outside environment, or protect confidential data stored in the TOE memories.

4.2 Security Objectives for the Environment

4.2.1 Objectives on Phase 1

O.DEV_DIS	The smartcard IC designer must have procedures to control the sales, distribution, storage and usage of the software and hardware development tools and classified documents, suitable to maintain the integrity and the confidentiality of the assets of the TOE. It must be ensured that: ■ Tools are only delivered to the parties authorized personnel. ■ Confidential information such as data sheets and general information on defined assets are only delivered to the parties authorized personnel on the basis of need-to-know.
O.SOFT_DLV	The smartcard embedded software must be delivered from the smartcard embedded software developer (Phase 1) to the IC designer through a trusted delivery and verification procedure that shall be able to maintain the integrity of the software and its confidentiality, if applicable.
O.SOFT_MECH	To achieve the level of security required by this Security Target Lite, the smartcard embedded software shall use IC security features and security mechanisms (for example, sensors) as specified in the smartcard IC documentation [TD].
O.DEV_TOOLS	The smartcard embedded software shall be designed in a secure manner, by using exclusively software development tools (compilers, assemblers, linkers, simulators etc.) and software-hardware integration testing tools (emulators) that will grant the integrity of program and data.

4.2.2 Objectives on Phase 2 (Development Phase)

O.SOFT_ACS	Embedded software shall be accessible only by authorized personnel within the IC designer on the basis of need-to-know.
O.DESIGN_ACS	IC specifications, detailed design, IC databases, schematics/layout or any further design information shall be accessible only by authorized personnel within the IC designer on the basis of need-to-know (physical, personnel, organizational, technical procedures).
O.DSOFT_ACS	Any IC dedicated software specification, detailed design, source code or any further information shall be accessible only by authorized personnel within the IC designer on the basis of need-to-know.
O.MASK_FAB	Physical, personnel, organizational, technical procedures during photomask fabrication (including deliveries between photomasks manufacturer and IC manufacturer) shall ensure the integrity and confidentiality of the TOE.
O.MECH_ACS	Details of hardware security mechanisms shall be accessible only by authorized personnel within the IC designer on the basis of need-to-know.
O.TI_ACS	Security relevant technology information shall be accessible only by authorized personnel within the IC designer on the basis of need-to-know.

4.2.3 Objectives on Phase 3 (Manufacturing Phase)

O.TOE_PRT	The manufacturing process shall ensure that protection of the TOE from any kind of unauthorized use such as tampering or theft. During the IC manufacturing and test operations, security procedures shall ensure the confidentiality and integrity of: ■ TOE manufacturing data (to prevent any possible copy, modification, retention, theft or unauthorized use). ■ TOE security relevant test programs, test data, databases and specific analysis methods and tools. These procedures shall define a security system applicable during the manufacturing and test operations to maintain confidentiality and integrity of the TOE by control of: ■ Packaging and storage. ■ Traceability. ■ Storage and protection of manufacturing process specific assets (such as manufacturing process documentation, further data, or samples) ■ Access control and audit to tests, analysis tools, laboratories, and databases. ■ Change/modification in the manufacturing equipment, management of rejects.
O.IC_DLV	The delivery procedures from the IC manufacturer shall maintain the integrity and confidentiality of the TOE and its assets.

4.2.4 Objectives on the TOE Delivery Process (Phases 4 to 7)

O.DLV_PROTECT — Procedures shall ensure protection of TOE material (including sawn and unsawn wafers) and information under delivery, including the following objectives:

- Non-disclosure of any security relevant information.
- Identification of the elements under delivery.
- Meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgement).
- Physical protection to prevent external damage.
- Secure storage and handling procedures are applicable for all TOEs (including rejected TOEs).
- Traceability of TOE during delivery including the following parameters:
  - Origin and shipment details.
  - Reception, reception acknowledgement.
  - Location material and information.

O.DLV_AUDIT — Procedures shall ensure that corrective actions are taken in the event of improper operation in the delivery process (including, if applicable any non-conformance to the confidentiality convention) and highlight all non conformance to this process.

O.DLV_RESP — Procedures shall ensure that people (shipping department, carrier, reception department) dealing with the procedure for delivery get the required skill, training and knowledge to meet the procedure requirements, and to act in full accordance with the above expectations.

4.2.5 Objectives on Phase 4 to 6

O.TEST_OPERATE — Appropriate functionality testing of the IC shall be used in phases 4 to 6.

During all manufacturing and test operations, security procedures shall be used through phases 4, 5, 6, to maintain confidentiality and integrity of the TOE and of its manufacturing and test data. This objective applies to both sawn and unsawn wafers.

4.2.6 Objectives on Phase 7

O.USE_DIAG	Secure communication protocols and procedures shall be used between smartcard and terminal.
O.USE_SYS	The integrity and the confidentiality of sensitive data stored or handled by the system (terminals, communications....) shall be maintained.

TOE Security Functional Requirements

94 The TOE security functional requirements define the functional requirements for the TOE using functional requirements components drawn from the Common Criteria part 2 and functional requirements defined in section 7 of this Security Target Lite.

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


Note

Some functional requirements refer to objects, subjects, attributes and management functions. To formalize this:

- Objects are defined in section 3.1 based on defined assets.
- Subjects are the security roles defined in section 5.2.1.
- Attributes are defined in section 5.1.3.
- Management functions are defined in section 5.2.2.

5.1 Functional Requirements Applicable to Phase 3 Only (Testing Phase)

5.1.1 User Authentication Before any Action (FIA_UAU.2)

96 The TOE security functions shall require each user to be successfully authenticated before allowing any other TOE security functions-mediated actions on behalf of that user.

5.1.2 User Identification Before any Action (FIA_UID.2)

97 The TOE security functions shall require each user to identify itself before allowing any other TOE security functions mediated actions on behalf of that user.

5.1.3 User Attribute Definition (FIA_ATD.1)

98 The TOE security functions shall maintain the following list of security attributes belonging to individual users:

- A1 : Read CPU ROM (O1) access right
- A2 : Write CPU ROM (O1) access right
- A3 : Execute CPU ROM (O1) access right
- A4 : Read CPU EEPROM (O2) access right
- A5 : Write CPU EEPROM (O2) access right
- A6 : Execute CPU EEPROM (O2) access right
- A7 : Read CPU RAM (O3) access right
- A8 : Write CPU RAM (O3) access right
- A9 : Execute CPU RAM (O3) access right
- A10 : Read Peripherals and IO Registers (O4) access right
- A11 : Write Peripherals and IO Registers (O4) access right
- A12 : Execute Peripherals and IO Registers (O4) access right
- A13 : Read Illegal Address (O5) access right
- A14 : Write Illegal Address (O5) access right
- A15 : Execute Illegal Address (O5) access right
- A16 : Execute Illegal Opcode (O6) access right
- A100 : Test signatures of CPU ROM (O1)
- A101 : Test signatures of CPU RAM (O3)
- A102 : Encrypted contents of CPU EEPROM (O2)
- A103 : Checksum32/CRC16 signature result

- A200 : Test command syntax

5.1.4 TOE Security Functions Testing (FPT_TST.1)

99 The TOE security functions shall:

- Run a suite of self tests at the request of the authorized user to demonstrate the correct operation of the TOE security functions.
- Provide authorized users with the capability to verify the integrity of TOE security functions data.
- Provide authorized users with the capability to verify the integrity of stored TOE security functions executable code.

5.1.5 Stored Data Integrity Monitoring (FDP_SDI.1)

100 The TOE security functions shall monitor user data stored within the TOE scope of control for integrity errors on all objects, based on the following attributes:

- A100 : Test signatures of CPU ROM (O1)
- A101 : Test signatures of CPU RAM (O3)
- A102 : Encrypted contents of CPU EEPROM (O2)
- A103 : Checksum32/CRC16 signature result

5.2 Functional Requirements Applicable to Phases 3 to 7

5.2.1 Security Roles (FMT_SMR.1)

101 The TOE security functions shall maintain the role of:

- S.TME_ADMIN: Test Mode Entry (TME) administrator
- S.SUPER: Supervisor
- S.NON_SUPER: Non-supervisor

102 The TOE security functions shall be able to associate users with roles.


Note

When the TOE is used in M.TEST_MODE mode, S.TME_ADMIN, S.SUPER roles can be used.

When the TOE is used in M.USER_MODE mode, only S.SUPER, and S.NON_SUPER roles can be used.

5.2.2 Specification of Management Functions (FMT_SMF.1)

103 The TOE security functions shall be capable of performing the following security management functions of security functions:

- F2 : Enable the function **(Not disclosed in ST-Lite)**
- F3 : Disable the function **(Not disclosed in ST-Lite)**
- F4 : Modify the behaviour of the function **(Not disclosed in ST-Lite)**
- F5 : Modify the behaviour of the function **(Not disclosed in ST-Lite)**

104 The TOE security functions shall be capable of performing the following security management functions of security attributes:

- F10 : Modify **(Not disclosed in ST-Lite)**
- F11 : Modify **(Not disclosed in ST-Lite)**
- F12 : Modify **(Not disclosed in ST-Lite)**
- F13 : Modify **(Not disclosed in ST-Lite)**
- F14 : Modify **(Not disclosed in ST-Lite)**
- F15 : Modify **(Not disclosed in ST-Lite)**
- F16 : Modify **(Not disclosed in ST-Lite)**

5.2.3 Management of Security Functions Behaviour (FMT_MOF.1)

105 The TOE security functions shall restrict the ability to F2 **(Not disclosed in ST-Lite)**

106 The TOE security functions shall restrict the ability to F3 **(Not disclosed in ST-Lite)**.

107 The TOE security functions shall restrict the ability to F4 **(Not disclosed in ST-Lite)**

108 The TOE security functions shall restrict the ability to F5 **(Not disclosed in ST-Lite)**

5.2.4 Management of Security Attributes (FMT_MSA.1)

109 The TOE security functions shall enforce the ACSF_Policy (Access Control Security Functions Policy) and IFCSF_Policy (Information Flow Control Security Functions Policy) to restrict the ability to change the value of the following security attributes: **(Not disclosed in ST-Lite)**

5.2.5 Static Attribute Initialization (FMT_MSA.3)

110 The TOE security functions shall:

- Enforce the ACSF_Policy and IFCSF_Policy to provide restrictive default values for security attributes that are used to enforce the security functions policy
- Allow the S.TME_ADMIN to specify alternate initial values to override the default values when an object or information is created

5.2.6 Complete Access Control (FDP_ACC.2)

111 The TOE security functions shall enforce the ACSF_Policy **(Not disclosed in ST-Lite)** on:

- S.TME_ADMIN, S.SUPER, S.NON_SUPER
- O1 (CPU ROM), O2 (CPU EEPROM), O3 (CPU RAM), O4 (Peripherals and IO Registers), O5 (Illegal Address), O6 (Illegal Opcode)
- and all operations among subjects and objects covered by the security functions policy.

112 The TOE security functions 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 security functions policy.

5.2.7 Security Attribute Based Access Control (FDP_ACF.1)

113 The TOE security functions shall enforce the ACSF_Policy to objects based on:

- A1 : Read CPU ROM (O1) access right
- A2 : Write CPU ROM (O1) access right
- A3 : Execute CPU ROM (O1) access right
- A4 : Read CPU EEPROM (O2) access right

- A5 : Write CPU EEPROM (O2) access right
- A6 : Execute CPU EEPROM (O2) access right
- A7 : Read CPU RAM (O3) access right
- A8 : Write CPU RAM (O3) access right
- A9 : Execute CPU RAM (O3) access right
- A10 : Read Peripherals and IO Registers (O4) access right
- A11 : Write Peripherals and IO Registers (O4) access right
- A12 : Execute Peripherals and IO Registers (O4) access right
- A13 : Read Illegal Address (O5) access right
- A14 : Write Illegal Address (O5) access right
- A15 : Execute Illegal Address (O5) access right
- A16 : Execute Illegal Opcode (O6) access right

114 The TOE security functions shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed.

115 **Firewall rules not disclosed in ST-Lite**

5.2.8 Subset Information Flow Control (FDP_IFC.1)

116 The TOE security functions will enforce the IFCSF_Policy on

- S.TME_ADMIN,
- CPU ROM (O1), CPU EEPROM (O2), CPU RAM (O3), Peripherals and IO Registers (O4)
- Test operations, that cause controlled information to flow to and from controlled subjects covered by the security function policy.

5.2.9 Simple Security Attributes (FDP_IFF.1)

117 The TOE security functions shall enforce the IFCSF_Policy based on the following types of subject and information security attributes: A200 (test command syntax).

118 The TOE security functions shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: test command syntax rules.

119 The TOE security functions shall enforce no additional security functions policy capabilities.

120 The TOE security functions shall provide no additional information flow control security functions policy rules.

121 The TOE security functions shall explicitly authorize an information flow based on the following rules:

122 Test command syntax rules, based on A200 (test command syntax), that explicitly **authorize** an information flow between:

- S.TME_ADMIN and CPU ROM (O1)
- S.TME_ADMIN and CPU EEPROM (O2)
- S.TME_ADMIN and CPU RAM (O3)
- S.TME_ADMIN and Peripherals and IO Registers (O4)

123 The TOE security functions shall explicitly deny an information flow based on the following rules:

124 Test command syntax rules, based on A200 (test command syntax), that explicitly **deny** information flows between:

- S.TME_ADMIN and CPU ROM (O1)
- S.TME_ADMIN and CPU EEPROM (O2)
- S.TME_ADMIN and CPU RAM (O3)
- S.TME_ADMIN and Peripherals and IO Registers (O4)

IFCSF-Policy

Table 5-1 IFCSF-Policy

Rules	Test command syntax rules
Attribute	A200 (Test command syntax)
S.TME_ADMIN	Data flow (1)

(1) All information about possible data flow and Test command syntax can be found in [STI], [TMRUSER], [TMRE2], [ROMUG], and [ROMDD].

5.2.10 Potential Violation Analysis (FAU_SAA.1)

125 The TOE Security Functions shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TOE Security Policy.

126 The TOE security functions shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of abnormal environmental conditions (Supply voltage, clock input frequency, temperature, UV light) known to indicate a potential security violation,

b) Accumulation or combination of physical tampering (Micro-probing, critical FIB modification) known to indicate a potential security violation,

c) Accumulation or combination of Firewall violations (user trying to illegally access controlled memories or objects, user trying to execute illegal opcodes) known to indicate a potential security violation.

d) Accumulation of watchdog violations known to indicate a potential security violation.

e) No other rules.

5.2.11 Unobservability (FPR_UNO.1)

127 The TOE security functions shall ensure that any users are unable to observe the operation of TOE internal activity on TOE objects by authorized users or subjects.

5.2.12 Notification of Physical Attack (FPT_PHP.2)

128 The TOE security functions shall:

- Provide unambiguous detection of physical tampering that might compromise the TOE security functions.
- Provide the capability to determine whether physical tampering with the TOE security functions's devices or TOE security functions's elements has occurred.

129 For values of voltage, clock input frequency, temperature and UV light which go outside acceptable bounds, for micro-probing and critical FIB modification, for Firewall rules violations (including illegal opcodes), and for watchdog violations, the TOE security functions shall monitor the devices and elements and notify S.SUPER when physical tampering with the TOE security functions' devices or TOE security functions' elements has occurred.

5.2.13 Resistance to Physical Attack (FPT_PHP.3)

130 The TOE security functions shall resist tampering of voltage, clock input frequency, temperature, UV light, micro-probing, critical FIB modification, Firewall rules violations (including illegal opcodes), and watchdog violations to the TOE and its security functions by responding automatically such that the TOE security policy is not violated.

5.2.14 Cryptographic Operation (FCS_COP.1)

131 The TSF shall perform hardware data encryption and decryption in accordance with the:

- DES cryptographic algorithm using 56-bit cryptographic key sizes that meets the Data Encryption Standard (DES), FIPS PUB 46-3, 25th October, 1999.
- Triple Data Encryption Standard (TDES) cryptographic algorithm using 112-bit cryptographic key sizes that meets the E-D-E two-key triple-encryption implementation of the Data Encryption Standard, FIPS PUB 46-3, 25th October, 1999.

5.3 TOE Security Assurance Requirements

132 The assurance requirement is EAL5 augmented of additional assurance components listed in the following sections.

133 Some of these components are hierarchical ones to the components specified in EAL5.

134 All the components are drawn from Common Criteria Part 3, V2.2.

5.3.1 ALC_DVS.2 Sufficiency of Security Measures

Developer actions elements

135 The developer shall produce development security documentation.

Content and presentation of evidence elements

136 The development security documentation shall:

- Describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
- Provide evidence that these security measures are followed during the development and maintenance of the TOE.

137 The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

Evaluator actions elements

138 The evaluator shall confirm that the:

- Information provided meets all requirements for content and presentation of evidence
- Security measures are being applied

5.3.2 AVA_VLA.4 Highly Resistant

Developer actions elements

139 The developer shall:

- Perform a vulnerability analysis
- Provide vulnerability analysis documentation

Content and presentation of evidence elements

140 The vulnerability analysis documentation shall:

- describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.
- describe the disposition of identified vulnerabilities.
- show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.
- justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.
- show that the search for vulnerabilities is systematic.
- provide a justification that the analysis completely addresses the TOE deliverables.

Evaluator actions elements

141 The evaluator shall:

- Confirm that the information provided meets all requirements for content and presentation of evidence
- Conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.
- Perform independent vulnerability analysis
- Perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.
- Determine that the TOE is resistant to penetration attacks performed by an attacker possessing a high attack potential.

5.3.3 AVA_MSU.3 Analysis and Testing for Insecure States

Developer actions elements

142 The developer shall:

- Provide guidance document
- Document an analysis of the guidance documentation.

Content and presentation of evidence elements

143 The documentation shall:

- Identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
- Be complete, clear, consistent and reasonable.
- List all assumptions about the intended environment.
- List all requirements for external security measures (including external procedures, physical and personnel controls).
- Demonstrate that the guidance documentation is complete.

Evaluator actions elements

144 The evaluator shall:

- Confirm that the information provided meets all requirements for content and presentation of evidence.
- Repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied user guidance documentation.
- Determine that the use of the guidance documentation allows all insecure states to be detected.
- Confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.
- Perform independent testing to determine that an administrator or user, with an understanding of the guidance documentation, would reasonably be able to determine if the TOE is configured and operating in a manner that is insecure.

145 This section defines the TOE security functions, and Figure 6-1 on page 58 specifies how they satisfy the TOE security functional requirements.

6.1 TOE Security Functions

6.1.1 Test Mode Entry (SF1)

146 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.

147 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.

148 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.

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

6.1.2 Protected Test Memory Access (SF2)

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

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

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

6.1.3 Test Mode Disable (SF3)

153 SF3 shall make provision for:

- M3.1 : Wafer sawing which, once done, shall ensure that none of the test features are available, not even to authenticated users in test mode.

6.1.4 TOE Testing (SF4)

154 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.

155 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)

156 SF5 shall provide means for performing data error detection.

157 Means of performing checksum error detection and parity error detection is provided. The M5.1 32-bit Checksum Accelerator or the M5.2 CRC-16 hardware peripheral can be used by the embedded software to compute fast data error detection on the program and/or data memories before starting any operation.

6.1.6 FireWall (SF6)

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

M6.1 Memory protection

159 The FireWall defines user modes to execute embedded software:

- Supervisor
- Non-supervisor mode (also named user mode).

160 The different modes provide restricted access privileges to the memories, and to the MCU perhiperal registers.

161 If a protected address is accessed by the non-supervisor software, a security interrupt is invoked by SF8.

M6.2 Illegal address

162 If an illegal address is accessed (i.e. an unmapped memory space), a security interrupt is invoked by SF8.

M6.3 Illegal opcode

163 If an attempt is made to execute any opcode that is not implemented in the instruction set, a security non maskable interrupt is invoked by SF8.

6.1.7 Event Audit (SF7)

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

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

- M7.1 The external voltage supply goes outside acceptable bounds
- M7.2 The external clock signal goes outside acceptable bounds
- M7.3 The ambient temperature goes outside acceptable bounds
- M7.4 Application program abnormal runaway.
- M7.5 Attempts to physically probe the device
- M7.6 Attempts to gain illegal access to reserved RAM memory locations
- M7.7 Attempts to gain illegal access to reserved EEPROM memory locations
- M7.8 Attempts to gain illegal access to reserved peripheral or IO register locations
- M7.9 Attempts to execute illegal instruction “LPM” to read the program memory from the non-supervisor program location
- M7.10 Attempts to move the RAM stack to an illegal RAM memory location defined by SPHLC and SPLLC registers
- M7.11 Attempts to execute an AVR opcode that is not implemented
- M7.12 Attempts to illegally write access the device’s EEPROM
- M7.13 Attempts to gain illegal access to P0-supervisor or P1-supervisor modes
- M7.14 Exposure to UV light goes outside acceptable bounds

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

6.1.8 Event Action (SF8)

167 SF8 shall provide an Event Action security function to register occurrences of audited events and take appropriate action.

168 Detection of such occurrences will cause an audit information to be set by SF7, 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 interrupts

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

6.1.9 Unobservability (SF9)

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

- Monitoring power consumption or electromagnetic emission in an attempt to extract information relating to any specific resource or service which is being used is mitigated by means of **(Not disclosed in ST-Lite)**
- Certain physical features of the TOE are very hard to determine using optical means.

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

6.1.10 Cryptography (SF10)

172 The TSF shall provide:

- A cryptographic algorithm to be able to transmit and receive objects in a manner protected from data retrieval or modification.
- M10.1 Hardware DES, TDES data encryption/decryption capability.

173 Those 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.

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

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

- DES algorithm
- TDES algorithm

6.1.11 Security Functions Based on Permutations/combinations

176 Security function SF1 is based on mechanisms using permutation and/or combination properties.**(Not disclosed in ST-Lite)**

Table 6-1 Relationship Between Security Requirements and Security Functions

		Security Functions									
		Test Mode Entry	Protected Test Memory Access	Test Mode Disable	TOE Testing	Data Error Detection	FireWall	Event Audit	Event Action	Unobservability	Cryptography
Security Requirement		**SF1**	**SF2**	**SF3**	**SF4**	**SF5**	**SF6**	**SF7**	**SF8**	**SF9**	**SF10**
FIA_UAU.2	**SR1**	X									
FIA_UID.2	**SR2**	X									
FIA_ATD.1	**SR3**	X	X	X	X	X	X				
FPT_TST.1	**SR4**	X	X	X	X	X					
FDP_SDI.1	**SR5**		X		X	X					
FMT_MOF.1	**SR6**	X		X							
FMT_MSA.1	**SR7**	X	X		X		X				
FMT_SMR.1	**SR8**	X		X			X				
FMT_SMF.1	**SR9**	X		X			X				
FMT_MSA.3	**SR10**		X		X		X				
FDP_ACC.2	**SR11**		X				X				
FDP_ACF.1	**SR12**		X				X				
FDP_IFC.1	**SR13**		X		X						
FDP_IFF.1	**SR14**		X		X						
FAU_SAA.1	**SR15**							X			
FPR_UNO.1	**SR16**									X	
FPT_PHP.2	**SR17**							X	X		
FPT_PHP.3	**SR18**							X	X		
FCS_COP.1	**SR19**										X

6.2 TOE Assurance Measures

177 This section defines the TOE assurance measures and Figure 6-2 on page 61 specifies how they satisfy the TOE security assurance requirements.

6.2.1 Security Target Lite (SA1)

178 SA1 shall provide the “AT90SC6404RT Security Target Lite” document plus its references.

6.2.2 Configuration Management (SA2)

179 SA2 shall provide the “AT90SC6404RT CC Configuration Management (ACM)” interface document plus its references.

6.2.3 Delivery and Operation (SA3)

180 SA3 shall provide the “AT90SC6404RT CC Delivery and Operation (ADO)” interface document plus its references.

6.2.4 Development Activity (SA4)

181 SA4 shall provide the “AT90SC6404RT CC Development Activity (ADV)” interface document plus its references.

6.2.5 Guidance (SA5)

182 SA5 shall provide the “AT90SC6404RT CC Guidance (AGD)” interface document plus its references.

6.2.6 Life Cycle Support (SA6)

183 SA6 shall provide the “AT90SC6404RT CC Life Cycle Support (ALC)” interface document plus its references.

6.2.7 Test Activity (SA7)

184 SA7 shall provide the “AT90SC6404RT CC Test Activity (ATE)” interface document plus its references, and undertaking of testing described therein.

6.2.8 Vulnerability Assessment (SA8)

185 SA8 shall provide the “AT90SC6404RT CC Vulnerability Assessment (AVA)” interface document plus its references, and undertaking of vulnerability assessment described therein.

6.2.9 Smart Card Devices (SA9)

186 SA9 shall provide functional AT90SC6404RT smart card devices.

6.2.10 Development Site (SA10)

187 SA10 shall provide access to the development site.

6.2.11 Test Site (SA11)

188 SA11 shall provide access to the test sites.

6.2.12 Manufacturing Site (SA12)

189 SA12 shall provide access to the manufacturing site.

6.2.13 Sub-contractor Sites (SA13)

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

Table 6-2 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 Sites	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.3			x								x	x	x	x
ADO_DEL.2				x							x	x	x	x
ADO_IGS.1				x							x	x	x	x
ADV_FSP.3					x									
ADV_HLD.3					x									
ADV_IMP.2					x									
ADV_INT.1					x									
ADV_LLD.1					x									
ADV_RCR.2					x									
ADV_SPM.3					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_MSU.3									x	x				
AVA_SOF.1									x	x				
AVA_VLA.4									x	x				
AVA_CCA.1									x	x				

Protection Profile Claims

7.1 Protection Profile Reference

191 This Security Target Lite is compliant with CC Smartcard Integrated Circuit Protection Profile PP/9806, Version 2.0, Issue September 1998, and has been registered at the French Certification Body.

7.2 Protection Profile Refinements

192 Refinements to assumptions A.DLV_PROTECT, A.USE_PROD and objectives O.DLV_PROTECT, O.TEST_OPERATE relate to unsawn wafers and corresponding procedures and guidance.

193 For clarification of this Security Target Lite, 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.

7.3 Protection Profile Additions

7.3.1 Cryptographic Capability

194 In addition to conforming to PP/9806, this Security Target Lite specifies an additional Organizational Security Policy P.CRYPTO in Section 3.4, and an additional Security Objective O.CRYPTO in Section 4.1.

195 The CC security functional requirements to meet this Organizational Security Policy is Cryptographic Operation (FCS_COP.1) which are specified in Section 5.

196 The security function to satisfy the FCS_COP.1 requirements is SF10 and is specified in Section 6.

7.3.2 Specification of Security Management Functions

This is an addition to the Security Management Class (FMT).

The security functions that satisfy the FMT_SMF.1 requirements are SF1, SF3, and SF6. These security functions are described in Section 6.

7.3.3 Analysis and Testing for Insecure States

This is an addition to the Assurance Vulnerability Assessment class (AVA).

The assurance measures that satisfy the AVA_MSU.3 requirements are SA8 and SA9. These assurance measures are described in Section 6.

Appendix A

Glossary

A.1 Terms

Control Bytes	Reserved bytes of EEPROM which can be programmed with traceability information.
CRC-16	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 AT90SC6404RT 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 is not applicable in the case of the TOE since it is a hardware evaluation only.
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.

A.2 Abbreviations

ACSF	Access Control Security Functions
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
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
NTS	North Tyneside
NVM	Non Volatile Memory
OTP	One Time Programmable
PP	Protection Profile
RAM	Random-Access Memory
RISC	Reduced Instruction Set Core
RNG	Random Number Generator
ROM	Read-Only Memory
SPA	Simple Power Analysis
TD	Technical Data
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