General Business Use

AT90SC12836RCT

Security Target Lite

Important notice to readers…

Figures

Section 1

AT90SC12836RCT Security Target Lite

1.1 Identification

1 Title: AT90SC12836RCT 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-Lite) is conformant to the Protection Profile PP/9806, 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 AVR ASL4 and the ‘parent’ device of the family, from which other family members will be derived, is the AT90SC19264RC.

4 The AT90SC12836RCT MCU device:

Product Identification Number	AT58819
Revision	E
Atmel Toolbox Version	00.03.01.03

5 is being evaluated against the CC Smartcard Integrated Circuit Protection Profile PP/9806 to Evaluation Assurance Level 4 (EAL4) augmented with AVA_VLA.4, ADV_IMP.2, ALC_DVS.2 and AVA_MSU.3 under the Common Criteria 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 are in the form of an EAL (assurance package) that is based upon assurance components 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.

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 AT90SC12836RCT Technical Data Sheet [TD].

18 The term *Target of Evaluation* (TOE) is standard CC terminology and refers to the product being evaluated, the AT90SC12836RCT MCU device in this case.The stated toolbox commands are also 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].

19 Security objectives are defined herein with labels in the form O.xx_xx. These labels are used elsewhere for reference. Similarly, threats, assumptions and organizational security policy are defined with labels of the form 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 The following list refers to the latest revision of the documents.

- [ESOF] AT90SC Strength of Security Functions Analysis
- [STI] Standard Test Interface
- [TD] AT90SC12836RCT Technical Data (TPR0139)
- [TestROMDD] AT90SC12836RCT Engineering Software Detailed Description
- [TestROMUG] AT90SC12836RCT Engineering Software User Guide
- [TMRE2] AT90SC12836RCT Production Test Software Detailed Description
- [TMR-User] AT90SC12836RCT 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
- [APP_CRYPT] Efficient use of AdvX for Implementing Cryptographic Operations (TPR0142)
- [TBX_SDD] Toolbox 3.x AdvX Software Development (TPR0152)
- [WSR] Wafer Saw Recommendations (TPG0079)

1.8 Revision History

Rev	Date	Description	Originator
A	26 Jul 05	Initial release, Based on AT90SC9616RC ST-Lite (TPG0034)	Atmel, EKB

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 AT90SC12836RCT 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 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.

26 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]. Package mode can only be entered on sawn wafers.

27 The TOE widely uses ATMEL high density non volatile memories: it features 128K bytes of AVR ROM program memory, 36K bytes of EEPROM program/data memory, 5K bytes of static RAM memory, and 32K bytes dedicated to Atmel’s Crypto Library [TBX].

28 The EEPROM includes 128 bytes of One Time Programmable (OTP) memory and a 384-byte of bit-addressable area.

29 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].

30 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].

31 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

32 The TOE also includes a 32bit Checksum Accelerator, a CRC-16/32 peripheral, a Random Number Generator, a fast hardware DES/3DES peripheral, and a 32bit crypto 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. 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. 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]. . Within the scope of the TOE is the full Atmel Toolbox as detailed in [TBX].

Note

Please note that within the scope of the evaluation is the TOE hardware with and without the Atmel Toolbox software. If the smartcard embedded software developer wishes to create their own cryptographic toolbox they must follow the guidance notes [APP_AdvX] and [APP_CRYPT] to ensure that the security requirements are maintained.

33 The TOE includes security logic comprising detectors which monitor voltage, frequency and temperature.

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

35 The TOE includes a powerful Firewall that protects all memories, peripheral and IO register accesses. This Firewall defines the user modes (Supervisor Mode and Non-Supervisor Mode) and many different address spaces.

2.2 Smartcard Product Life-cycle

36 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.

37 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.

38 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.

39 Figure 2-1 describes the Smartcard product life-cycle.

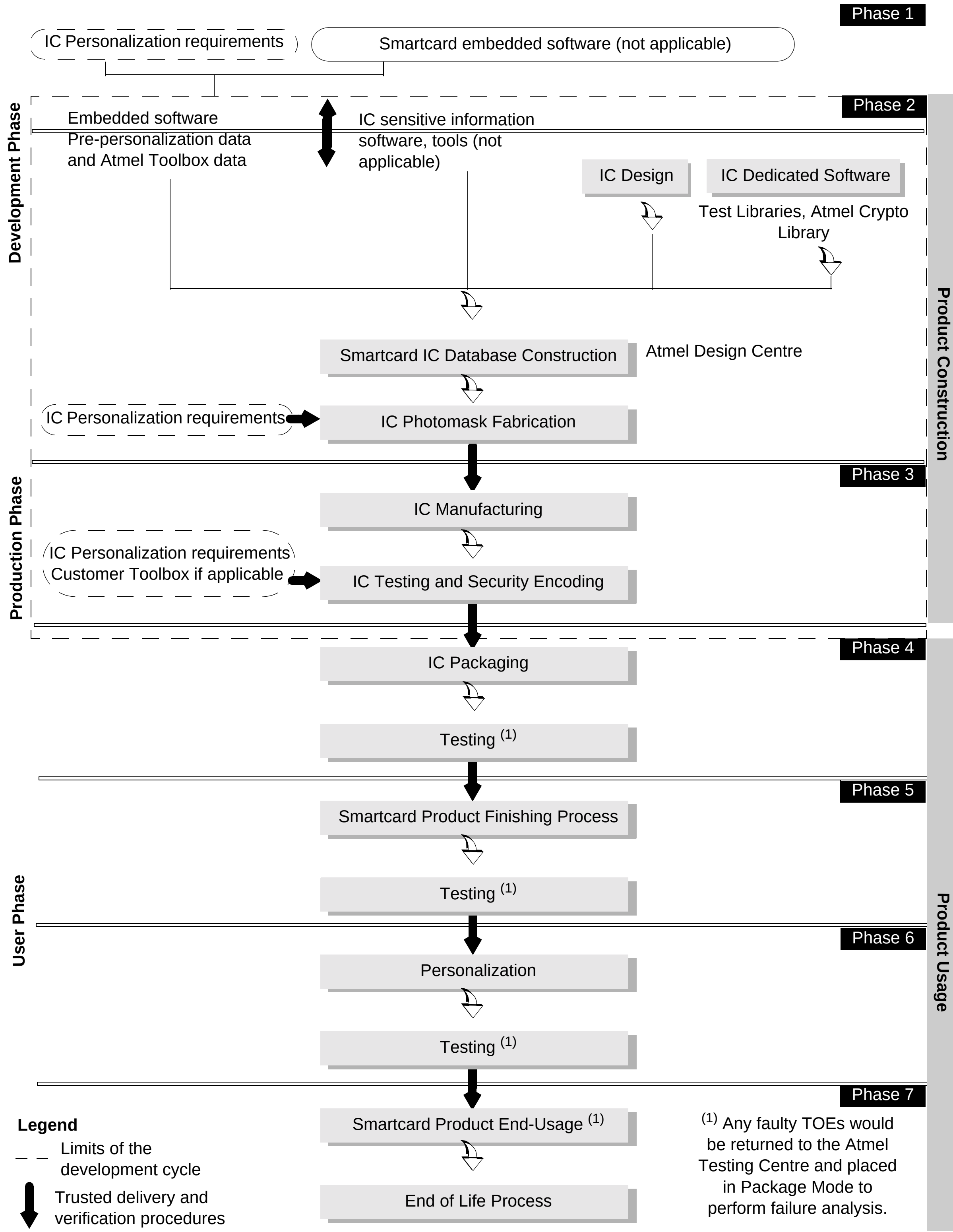

Figure 2-1 Smartcard Product Life Cycle

40 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

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

42 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

43 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

44 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.

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

46 Reticles and photomasks are generated from the verified IC database. The reticles and photomasks are then handcarried to the wafer fab processing facilities.

2.3.2 TOE Production Environment

47 Production starts within the ATMEL Wafer Fabrication Plant; here the silicon wafers undergo diffusion processing in 25-wafer lots. Computer tracking at wafer level throughout the process is achieved by the use of a manufacturing database.

48 The manufacturing database system is an on-line manufacturing tracking system which monitors the progress of the wafers through the fabrication cycle. After fabrication the

wafers are sent to ATMEL Test Fab where they are thinned to a pre-specified thickness and tested. ATMEL Test Fab test the TOE 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.

49 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, the customer is given guidance on wafer saw [WSR].

2.3.3 TOE User Environment

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

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

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

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

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

End-user environment (Phase 7)

55 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.

56 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

57 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

58 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.

59 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

60 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.

61 The MCU may be used in the following modes:

a) 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) 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.

62 During the initial part of the manufacturing process, the MCU is set to test mode. Authorized development staff then test the MCU. After testing, test mode is

permanently disabled by sawing off the test pads, and the MCU is set to user mode.Test Mode is permanently disabled by sawing the wafer.

63 Package Mode is a mode similar to Test Mode for testing returns from Phases 4-7. Package mode runs a limited subset of test commands 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.

64 If a faulty TOE is returned from the field then analysis can be done either in user mode, or package mode by an authorized test engineer.

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

66 The EEPROM includes OTP bytes, which can be used to store security-related information such as cryptographic keys. The OTP bytes cannot be erased in user mode.

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

68 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

69 The TOE IT functionalities consist of 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. data encryption, digital signature verification)

Section 3

TOE Security Environment

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

3.1 Assets

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

- Application data of the TOE comprising the IC pre-personalization requirements, such as the AVR ROM, EEPROM, and OTP contents.
- Smartcard embedded software.
- IC dedicated software, including Crypto Toolbox
- IC specification, design, development tools and technology

72 Therefore, the TOE itself is an asset.

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

3.2 Assumptions

74 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

75 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 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 (e.g. source code and any associated documents) and IC designer proprietary information (tools, software, documentation.) shall exist and be applied in software development.

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

76 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 where 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

77 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.

78 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)

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

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

- Unauthorized disclosure
- Modification or theft of the smartcard embedded software and any additional 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 and any additional application data transmitted during the delivery process from the smartcard embedded software developer to the IC designer.

80 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, design and technology, software and tools if applicable.

T.DIS_DEL	Unauthorized disclosure of the smartcard embedded software and any additional application 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 and any additional application data (such as IC pre-personalization requirements) during the delivery process to the IC designer.
T.T_DEL	Theft of the smartcard embedded software and any additional application data (such as IC pre-personalization requirements) during the delivery process to the IC designer.

3.3.3 Threats on Phases 2 to 7

81 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

82 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. This threat covers the unauthorized disclosure of proprietary elements such as IC specification, IC design, IC technology detailed information, IC hardware security mechanisms specifications.
T.DIS_SOFT	Unauthorized disclosure of smartcard embedded software and data such as access control, authentication system, data protection system, memory partitioning, cryptographic programs.
T.DIS_DSOFT	Unauthorized disclosure of IC dedicated software. This threat covers the unauthorized disclosure of IC dedicated software including security mechanisms specifications and implementation.

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. This threat covers potential disclosure of IC development tools and testing tools (analysis tools, microprobing tools).
T.DIS_PHOTOMASK	Unauthorized disclosure of photomask information, used for photoengraving during the silicon fabrication process.

Theft or unauthorized use of assets

83 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.
T.T_PRODUCT	Theft or unauthorized use of smartcard products.

Unauthorized modification of assets

84 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. This threat covers the unauthorized modification of IC specification, IC design including IC hardware security mechanisms specifications and realization.
T.MOD_PHOTOMASK	Unauthorized modification of TOE photomasks.
T.MOD_DSOFT	Unauthorized modification of IC dedicated software including modification of security mechanisms.
T.MOD_SOFT	Unauthorized modification of smartcard embedded software and data.

85 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

86 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.

87 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, Elliptic Curves, 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. To support these cryptographic functions, the TOE should supply Random Number Generation (RNG) with sufficient unpredictability and entropy. The TOE shall 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.

Section 4

Security Objectives

88 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

89 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, electromagnetic emissions) on the device external interfaces (for example clock, supply, I/O lines, and chip physical surfaces) 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/unauthentified 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 and/or software 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.

The TOE must also provide random number generation and ensure the cryptographic quality of random number generation. For example, random numbers shall not be predictable and shall have a sufficient entropy.

The TOE must 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.

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 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.

Section 5

TOE Security Functional Requirements

90 The TOE security functional requirements define the functional requirements for the TOE using only functional requirements components drawn from the Common Criteria part 2.

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

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

5.1.1 User Authentication Before any Action (FIA_UAU.2)

92 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)

93 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)

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

- Test mode access right
- Read AVR ROM access right
- Write AVR ROM access right
- Execute AVR ROM access right
- Read EEPROM access right
- Write EEPROM access right
- Execute EEPROM access right
- Read Crypto ROM access right
- Write Crypto ROM access right

- Execute Crypto ROM access right
- Read RAM access right
- Write RAM access right
- Execute RAM access right
- Read access right to peripherals and IO registers
- Write access right to peripherals and IO registers
- Execute access right to peripherals and IO registers

5.1.4 TOE Security Functions Testing (FPT_TST.1)

95 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)

96 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:

- Test signatures from AVR ROM
- Test signatures from, and contents of, RAM
- Test signature from Crypto ROM
- Contents of EEPROM

5.2 Functional Requirements Applicable to Phases 3 to 7

5.2.1 Management of Security Functions Behaviour (FMT_MOF.1)

97 The TOE security functions shall restrict the ability to enable the functions available in Test Mode to the Test Mode Entry (TME) administrator.

98 The TOE security functions shall restrict the ability to disable the functions available in Test Mode to the Test Mode Entry (TME) administrator.

5.2.2 Management of Security Attributes (FMT_MSA.1)

99 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 access the following security attributes to TME administrator, PME administrator, and firewall supervisor/ non-supervisor.

Note: the ACSF_Policy is not described in this document. See Figure 5-1 for further information on the IFCSF_Policy

5.2.3 Security Roles (FMT_SMR.1)

100 The TOE security functions shall maintain the role of:

- TME administrator
- Firewall supervisor/non-supervisor
- PME administrator

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

5.2.4 Specification of Management Functions (FMT_SMF.1)

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

- Control entry into and disabling of test mode and entry into user mode and package mode.
- Define the user modes, (Supervisor and Non-supervisor) address space parameters. Which controls the software access between each program user regions, but also between the program user and the data user regions.

5.2.5 Static Attribute Initialization (FMT_MSA.3)

103 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 TME administrator 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)

104 The TOE security functions shall enforce the ACSF_Policy on:

- TME administrator, Supervisor, Non-supervisor, PME administrator.
- AVR ROM, EEPROM, RAM, Crypto ROM, peripheral and IO registers.
- And all operations among subjects and objects covered by the security functions policy.

105 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)

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

- Read AVR ROM access right
- Write AVR ROM access right
- Execute AVR ROM access right
- Read EEPROM access right
- Write EEPROM access right
- Execute EEPROM access right
- Read Crypto ROM access right
- Write Crypto ROM access right
- Execute Crypto ROM access right
- Read RAM Data space access right
- Write RAM Data space access right
- Execute RAM Data space access right
- Read AVR EEPROM Data space access right
- Write AVR EEPROM Data space access right
- Execute AVR EEPROM Data space access right
- Read peripheral and IO registers access right

- Write peripheral and IO registers access right
- Execute peripheral and IO registers access right

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

108 **Firewall rules, that are not disclosed in this ST-Lite document.**

5.2.8 Subset Information Flow Control (FDP_IFC.1)

109 The TOE security functions shall enforce the IFCSF_Policy on TME administrator and PME administrator, test commands and test operations that cause controlled information to flow between the:

- AVR ROM and the Test Mode Entry administrator
- EEPROM and the Test Mode Entry administrator
- EEPROM and the Package Mode Entry administrator
- Crypto ROM and the Test Mode Entry administrator
- RAM and the Test Mode Entry administrator
- Peripheral and IO registers and the Test Mode administrator

5.2.9 Simple Security Attributes (FDP_IFF.1)

110 The TOE security functions shall enforce the IFCSF_Policy based on the following types of subject and information security attributes: **test command syntax**.

111 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.
- Enforce no additional information flow control security functions policy rules.
- Provide no additional security functions policy capabilities.

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

113 Test command syntax rules, based on test command syntax, that explicitly **authorize** information flows between TME administrator and:

- AVR ROM
- EEPROM
- Crypto ROM
- RAM

- Peripheral and IO registers

Note: All information about possible data flow and Test command syntax can be found in [STI], [TMR-USER], [TestROMUG], [TestROMDD] and [TMRE2]

114 Test command syntax rules, based on test command syntax, that explicitly **authorize** information flows between PME administrator and:

- EEPROM

Note: All information about possible data flow and Test command syntax can be found in [STI], [PME]

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

116 Test command syntax rules, based on test command syntax, that explicitly **deny** information flows between TME administrator and:

- AVR ROM
- EEPROM
- Crypto ROM
- RAM
- Peripheral and IO registers

Note: All information about possible data flow and Test command syntax can be found in [STI], [TMR-USER], [TestROMUG], [TestROMDD] and [TMRE2]

117 Test command syntax rules, based on test command syntax, that explicitly **deny** information flows between PME administrator and:

- AVR ROM
- EEPROM
- Crypto ROM
- RAM
- Peripheral and IO registers

Note: All information about possible data flow and Test command syntax can be found in [STI], [PME]

IFCSF_Policy

Table 5-1 IFCSF_Policy

Rules	Test command syntax rules
Attribute	Test command syntax
TME Administrator	Data flow (1)
PME Administrator	Data flow (2)

(1) All information about possible data flow and Test command syntax can be found in [STI], [TMR-USER], [TestROMUG], [TestROMDD] and [TMRE2].

(2) All information about possible data flow and Test command syntax can be found in [STI], [PME].

5.2.10 Potential Violation Analysis (FAU_SAA.1)

118 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.

119 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)

120 The TOE security functions shall ensure that any users are unable to observe the operations that are critical (i.e. cryptographic, read, write and erase), on assets protected in terms of confidentiality by authorized users or subjects.

5.2.12 Notification of Physical Attack (FPT_PHP.2)

121 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.

122 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 the Supervisor 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)

123 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)

124 The TSF shall perform hardware random number generation (RNG) to support security operations performed by cryptographic applications.

125 The TSF shall perform hardware cryptographic checksum generation for integrity and verification of checksum.

126 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.

127 The TSF shall perform software data encryption and decryption in accordance with the:

- Data hash and signature in accordance with the SHA-1 cryptographic algorithm using no cryptographic key that meets the Secure Hash Standard, FIPS PUB 180-1, 17th April, 1995.

128 The TSF shall perform software data encryption and decryption in accordance with the:

- RSA without CRT cryptographic algorithm using cryptographic key sizes that meet PKCS#1 V2.0 01 Oct 1998. Key sizes are between 96 bits and 2624 bits
- RSA with CRT cryptographic algorithm using cryptographic key sizes that meets PKCS#1 V2.0 01 Oct 1998. Key sizes are between 192 and 3520 bits.

5.2.15 Cryptographic Key Generation (FCS_CKM.1)

129 The TSF shall generate cryptographic keys in accordance with cryptographic key generation Miller-Rabin algorithm with confidence criteria (t) between 0 and 255, also specified cryptographic key sizes between 192-bits and 4480-bits (respectively 2 primes of size between 96 bits and 2240 bits) specified by the NIST special publication 800-2, April 1991.

5.3 Functional Requirements Applicable to PMT in Phase 4 to 7 Only

5.3.1 User Authentication Before any Action (FIA_UAU.2)

130 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.

5.3.2 User Identification Before any Action (FIA_UID.2)

131 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.

5.3.3 User Attribute Definition (FIA_ATD.1)

132 The TOE security functions shall maintain the following list of security attributes belonging to PMT users:

- Package mode access right
- Limited write EEPROM access right (The PME Administrator only has access to the physical value of the EEPROM contents not its logical contents (that is the data read/written by the PME Administrator are encrypted data only), only a limited set of values may be written to the EEPROM [PME])
- Limited read EEPROM access right (The PME Administrator only has access to the physical value of the EEPROM contents not its logical contents (that is the data read/written by the PME Administrator are encrypted data only))
- EEPROM internal signal access (charge pump and margin)
- ISO clock access right
- Clock selection right

133 The write to EEPROM access is limited to the following:

- Full erase and program
- Chip erase and program

- Page mode write*

Note: For page mode writes, the data to write is restricted to the following fixed values: **Not disclosed in ST-Lite**

134 The read from EEPROM access is limited to the following

- Page mode read

5.4 TOE Security Assurance Requirements

135 The assurance requirement is EAL4 augmented of additional assurance components listed in the following sections.

136 Some of these components are hierarchical ones to the components specified in EAL4.

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

5.4.1 ADV_IMP.2 Implementation of the TSF

Developer actions elements

138 The developer shall provide the implementation representation for the entire TOE security functions.

Content and presentation of evidence elements

139 The implementation representation shall:

- Unambiguously define the TOE security functions to a level of detail such that the TOE security functions can be generated without further design decisions
- Be internally consistent
- Describe the relationships between all portions of the implementation

Evaluator actions elements

140 The evaluator shall:

- Confirm that the information provided meets all requirements for content and presentation of evidence.
- Determine that the implementation representation is an accurate and complete instantiation of the TOE security functional requirements.

5.4.2 ALC_DVS.2 Sufficiency of Security Measures

Developer actions elements

141 The developer shall produce development security documentation.

Content and presentation of evidence elements

142 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.

143 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

144 The evaluator shall confirm that the:

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

5.4.3 AVA_VLA.4 Highly Resistant

Developer actions elements

145 The developer shall:

- Perform a vulnerability analysis.
- Provide vulnerability analysis documentation.

Content and presentation of evidence elements

146 The 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

147 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.

5.4.4 AVA_MSU.3 Analysis and Testing for Insecure States

Developer action elements

- Shall provide guidance documents
- Document an analysis of the guidance documentation.

Content and presentation of evidence elements

- Guidance documents shall identify all/possible modes of operation of the TOE (including operation failure or operational error), their consequences and implications for maintaining secure operation.
- Guidance documentation shall be complete, clear, consistent and reasonable.
- Guidance documentation shall list all assumptions about the intended environment.
- Guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls)
- The analysis documentation shall demonstrate documentation is complete.

Evaluator action elements

- Shall confirm that the information provided meets all requirements for content and presentation of evidence
- Shall 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 guidance documentation.

- Shall determine that the use of the guidance documentation allows all insecure states to be detected.
- Shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.
- Shall 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.

Section 6

TOE Summary Specification

148 This section defines the TOE security functions, and Figure 6-1 on page 59 specifies how they satisfy the TOE security functional requirements.

6.1 TOE Security Functions

6.1.1 Test Mode Entry (SF1)

149 SF1 shall ensure that only authorized users will be permitted to enter Test Mode. This is provided by Test Mode Entry conditions that are required to enable the TOE to enter Test Mode.

150 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.

151 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.

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

6.1.2 Protected Test Memory Access (SF2)

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

154 Only authorized design and production engineers running tests on the TOE will have access to the TME conditions.

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

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

6.1.3 Test Mode Disable (SF3)

157 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 now available.

6.1.4 TOE Testing (SF4)

158 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.

159 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)

160 SF5 shall provide means for performing data error detection.

161 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 embedded software to compute fast data error detection on the program and/or data memories before starting any operation.

6.1.6 FireWall (SF6)

162 SF6 shall enforce access control based on the FireWall rules as defined in the ACSF_Policy **(not shown in ST-Lite document)**.

Memory protection

163 The FireWall defines modes to execute embedded software:

- Supervisor
- non-supervisor

164 The different modes provide restricted access priveleges to the memories, and to the MCU perhiperal registers.

165 In case of illegal access performed by the embedded software, a security interrupt is invoked.

Illegal address

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

Illegal opcode

167 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)

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

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

1. The external voltage supply goes outside acceptable bounds
2. The external clock signal goes outside acceptable bounds
3. The ambient temperature goes outside acceptable bounds
4. Application program abnormal runaway
5. Attempts to physically probe the device
6. Attempts to gain illegal access to reserved RAM memory locations.
7. Attempts to gain illegal access to reserved EEPROM memory locations
8. Attempts to gain illegal access to reserved peripheral, IO and AdvX register locations

9. Attempts to execute illegal instruction “LPM” to read the program memory from the non-supervisor program location
10. Attempts to move the RAM stack to an illegal RAM memory location defined by SPHLC and SPLLC registers
11. Attempts to execute an AVR opcode that is not implemented.
12. Attempts to illegally write access the device’s EEPROM
13. Attempts to gain illegal access to supervisor mode
14. Exposure to UV light goes outside acceptable bounds

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

6.1.8 Event Action (SF8)

171 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 resets
- Different levels of security interrupts

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

6.1.9 Unobservability (SF9)

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

1. Extracting information, relating to any specific resource or service being used, by monitoring power consumption.
2. Extracting information, relating to any specific resource or service being used, by carrying out timing analyses on cryptographic functions.
3. Extracting information, relating to any specific resource or service being used, by using mechanical, electrical or optical means

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

6.1.10 Cryptography (SF10)

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

176 The TSF shall provide hardware DES, TDES data encryption/decryption capability.

177 The TSF shall provide software, SHA-1 (secure hash, function vTBX_Process(SHA1 and Tbx3Param) of the ToolBox) data signing capability. The TSF shall also provide software RSA without CRT (i.e. modular exponentiation, function vTBX3_Process (ExpMod and Tbx3Param) of the ToolBox) data encryption/ decryption capability, as well as RSA with CRT, function vTBX3_Process (CRT and Tbx3Param) of the ToolBox data encryption/decryption.

Note: The Atmel Toolbox must be considered as a whole.

178 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.

179 The TSF shall provide a hardware Random Number Generator (RNG) to support security operations performed by cryptographic applications. This RNG 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.

180 The TSF shall provide software RSA cryptographic key generation capability using Miller Rabin algorithm with confidence criteria (t parameter) between 0 and 255 (function vTBX3_Process (PrimeGen and Tbx3Param) of the Toolbox).

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

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

- DES algorithm
- TDES algorithm
- SHA-1 algorithm
- RSA without CRT algorithm
- RSA with CRT algorithm
- Miller Rabin algorithm

183 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 AVR 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.

Note Please note that within the scope of the evaluation is the TOE hardware with and without the Atmel Toolbox software. If the smartcard embedded software developer wishes to create their own cryptographic toolbox they must follow the guidance notes [APP_AdvX] and [APP_CRYPT] to ensure that the security requirements are maintained.

6.1.11 Package Mode Entry (SF11)

184 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 these conditions must be met to enter Package Mode.

185 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.

186 It is not possible to enter Test Mode on a sawn wafer, only Package Mode can be entered. So this function is protected by Test Mode Entry and Package Mode Entry.

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

6.1.12 Test Memory Access in Package Mode (SF12)

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

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

190 Only authorized test engineers runing tests on the TOE will have access to the PME conditions.

191 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

192 Not disclosed in ST-Lite document.

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**	**Package Mode Entry**	**Test Memory Access in Package Mode**
Security Requirement		**SF1**	**SF2**	**SF3**	**SF4**	**SF5**	**SF6**	**SF7**	**SF8**	**SF9**	**SF10**	**SF11**	**SF12**
FIA_UAU.2	**O1**	x										x	
FIA_UID.2	**O2**	x										x	
FIA_ATD.1	**O3**	x	x				x					x	x
FPT_TST.1	**O4**	x	x	x	x	x							
FDP_SDI.1	**O5**				x	x							
FMT_MOF.1	**O6**	x		x									
FMT_MSA.1	**O7**	x	x		x		x					x	x
FMT_SMR.1	**O8**	x		x			x					x	
FMT_SMF.1	**O9**	x		x			x					x	
FMT_MSA.3	**10**		x		x		x						
FDP_ACC.2	**O11**	x	x	x			x					x	x
FDP_ACF.1	**O12**	x	x	x			x					x	x
FDP_IFC.1	**O13**	x	x	x	x							x	x
FDP_IFF.1	**O14**	x	x	x	x							x	x

Table 6-1 Relationship Between Security Requirements and Security Functions (Continued)

FAU_SAA.1	**O15**							x					
FPR_UNO.1	**O16**									x			
FPT_PHP.2	**O17**							x	x				
FPT_PHP.3	**O18**							x	x	x			
FCS_COP.1	**O19**										x		
FCS_CKM.1	**O20**										x		

6.2 TOE Assurance Measures

193 This section defines the TOE assurance measures and Figure 6-2 on page 62 specifies how they satisfy the TOE security assurance requirements.

6.2.1 Security Target Lite (SA1)

194 SA1 shall provide the “AT90SC12836RCT Security Target Lite” document plus its references.

6.2.2 Configuration Management (SA2)

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

6.2.3 Delivery and Operation (SA3)

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

6.2.4 Development Activity (SA4)

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

6.2.5 Guidance (SA5)

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

6.2.6 Life Cycle Support (SA6)

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

6.2.7 Test Activity (SA7)

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

6.2.8 Vulnerability Assessment (SA8)

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

6.2.9 Smart Card Devices (SA9)

202 SA9 shall provide functional AT90SC12836RCT smart card devices.

6.2.10 Development Site (SA10)

203 SA10 shall provide access to the development site.

6.2.11 Test Site (SA11)

204 SA11 shall provide access to the test site.

6.2.12 Manufacturing Site (SA12)

205 SA12 shall provide access to the manufacturing site.

6.2.13 Sub-contractor Sites (SA13)

206 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 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				
AVA_SOF.1									x	x				
AVA_VLA.4									x	x				

Section 7

PP Claims

7.1 PP Reference

207 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 PP Refinements

208 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.

7.3 PP Additions

7.3.1 Cryptographic Capability

209 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 objective O.CRYPTO in Section 4.1.

210 The CC security functional requirements to meet this Organizational Security Policy are Cryptographic Operation (FCS_COP.1) and Cryptographic key generation (FCS_CKM.1), which are specified in Section 5.

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

7.3.2 Specification of Management Functions

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

213 The security functions that satisfy the FMT_SMF.1 requirement are SF1, SF3, SF6 and SF11. These security functions are described in Section 6.

7.3.3 Analysis and Testing for Insecure States

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

215 The assurance measures that satisfy the AVA_MSU.3 requirement are SA8 and SA9. These assurance measures are described in n.

7.3.4 Additions to Life Cycle

216 Due to the addition of Package Mode the following functional requirements are now applicable to not only Phase 3, but also Phases 4-7.

- FIA_UAU.2 - User authentication before any action
- FIA_UID.2 - User Identification before any action
- FIA_ATD.1 - User attribute definition

217 This is due to the control of entry into Package Mode, and also the control of what authenticated Package Mode user have access to.

218 The security functions that satisfy the FIA_UAU.2 requirements are SF1 and SF11. The security functions are described in Section 6.

219 The security functions that satisfy the FIA_UID.2 requirements are SF1 and SF11. The security functions are described in Section 6.

220 The security functions that satisfy the FIA_ATD.1 requirement are SF1, SF2, SF6, SF11, and SF12. These security functions are described in Section 6.

Glossary

A.1 Terms

BIST	Built In Self Test. Hardware implementation of an algorithm which tests for stuck at, transition, coupling and address faults in a memory
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 AT90SC12836RCT 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.
MARCH C	Algorithm which tests for stuck at, transition, coupling and address faults in a memory.
MARCH LR	Algorithm which tests for stuck at, transition, coupling and address faults in a memory.
MARCH Y	Algorithm which tests for stuck at, transition, coupling and address faults in a memory.
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.
Workstream	Manufacturing Unix based batch Tracking System.

A.2 Abbreviations

ACSF	Access Control Security Functions
AdvX	32-bit Crypto Accelerator developed and produced by Atmel
AVR	8-bit RISC processor developed and produced by Atmel
BIST	Built-in Self Test
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
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
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

Printed on recycled paper.

TPG0084A–SMIC–26Jul05