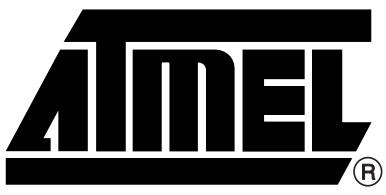
AT05SC3208R

Security Target Lite



Important notice to readers…

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

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

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

Contents

AT05SC3208R Security Target Lite

1.1 Identification

1 Title: AT05SC3208R Security Target Lite

2 A glossary of terms is given in Appendix A.

3 This Security Target Lite has been constructed with Common Criteria (CC) Version 2.1.

1.2 Overview

4 This ST Lite 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 EUROPA and the ‘parent’ device of the family, from which other family members will be derived, is the 3208.

5 The AT05SC3208R (ref AT568D6 Rev E) device is being evaluated against the CC Smartcard Integrated Circuit Protection Profile PP/9806 to Evaluation Assurance Level 4 (EAL4) Augmented. The other EUROPA family members will be evaluated in the future under the Common Criteria maintenance scheme. Atmel Smart Card ICs Ltd. is the developer and the sponsor for the EUROPA evaluations.

6 The devices in the EUROPA family are based on Motorola's M68HC05SC family of single-chip microcontroller devices. The M68HC05SC family, with designed-in security features, is based on the industry-standard M68HC05 low-power HCMOS core and gives access to the powerful instruction set of this widely used device. EUROPA devices are equipped with ROM, RAM 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 CC Conformance Claim

7 This ST Lite is conformant to parts 2 and 3 of the Common Criteria, V2.1, 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 CC requirements for an ST 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 EUROPA devices will be evaluated.

1.5 Document Structure

9 Section 1 Introduces the AT05SC3208R ST 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 PP claims.

16 Appendix A Lists the terms and abbreviations used in this document.

1.6 Scope and Terminology

17 This document is based on the AT05SC3208R Technical Datasheet [TD].

18 The term *Target of Evaluation* (TOE) is standard CC terminology and refers to the product being evaluated, the AT05SC3208R 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, threats and assumptions are defined with labels of the form T.xx_xx and A.xx_xx respectively.

20 Hexadecimal numbers are prefixed by $, e.g. $FF is decimal 255. 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 issue of the following Atmel publications:

- AT05SC3208R Technical Datasheet [TD] (1554)
- AT05SC3208R Test Specification

1.8 Revision History

Rev	Date	Description	Originator
A	24 Nov 03	Initial release. Based on Common Criteria V1.1	Atmel, EKB

TOE Description

22 This section describes the 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 Target of Evaluation (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 AT05SC3208R (AT568D6 Rev E) device from the EUROPA 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 within the scope of this document.

24 The devices in the EUROPA family are based on Motorola's M68HC05SC family of single-chip microcontroller devices. The M68HC05SC family, with designed-in security features, is based on the industry-standard M68HC05 low-power HCMOS core and gives access to the powerful instruction set of this widely used device. Different EUROPA family members offer various options. The EUROPA 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 EEPROM contains both Atmel and customer specific data.

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

28 The TOE is manufactured in a low voltage (3.3V +/- 0.3V) CMOS process. The device will operate at a supply voltage of 3.0V +/- 10% or 5.0V +/- 10%, with the internal supply regulated to the required operating voltage.

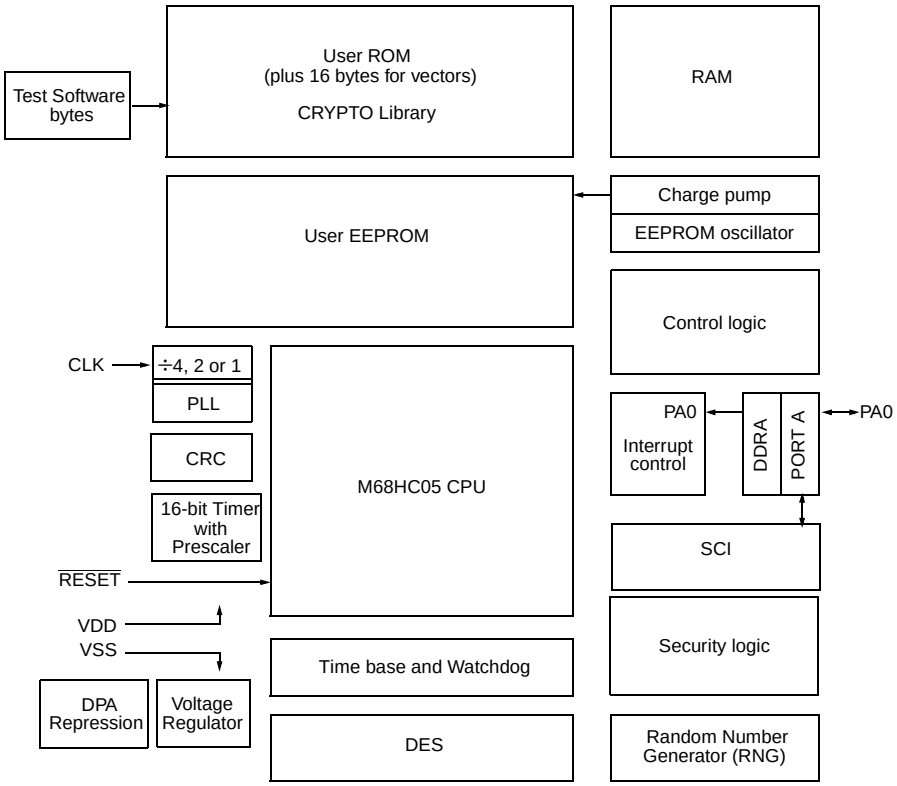


Figure 2-1 AT05SC3208R Block Diagram

2.2 Smartcard Product Life-cycle

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

Table 2-1 Smartcard Product Life-cycle

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

30 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 this document.

31 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 document.

32 Figure 2.2 illustrates the smartcard product life-cycle.

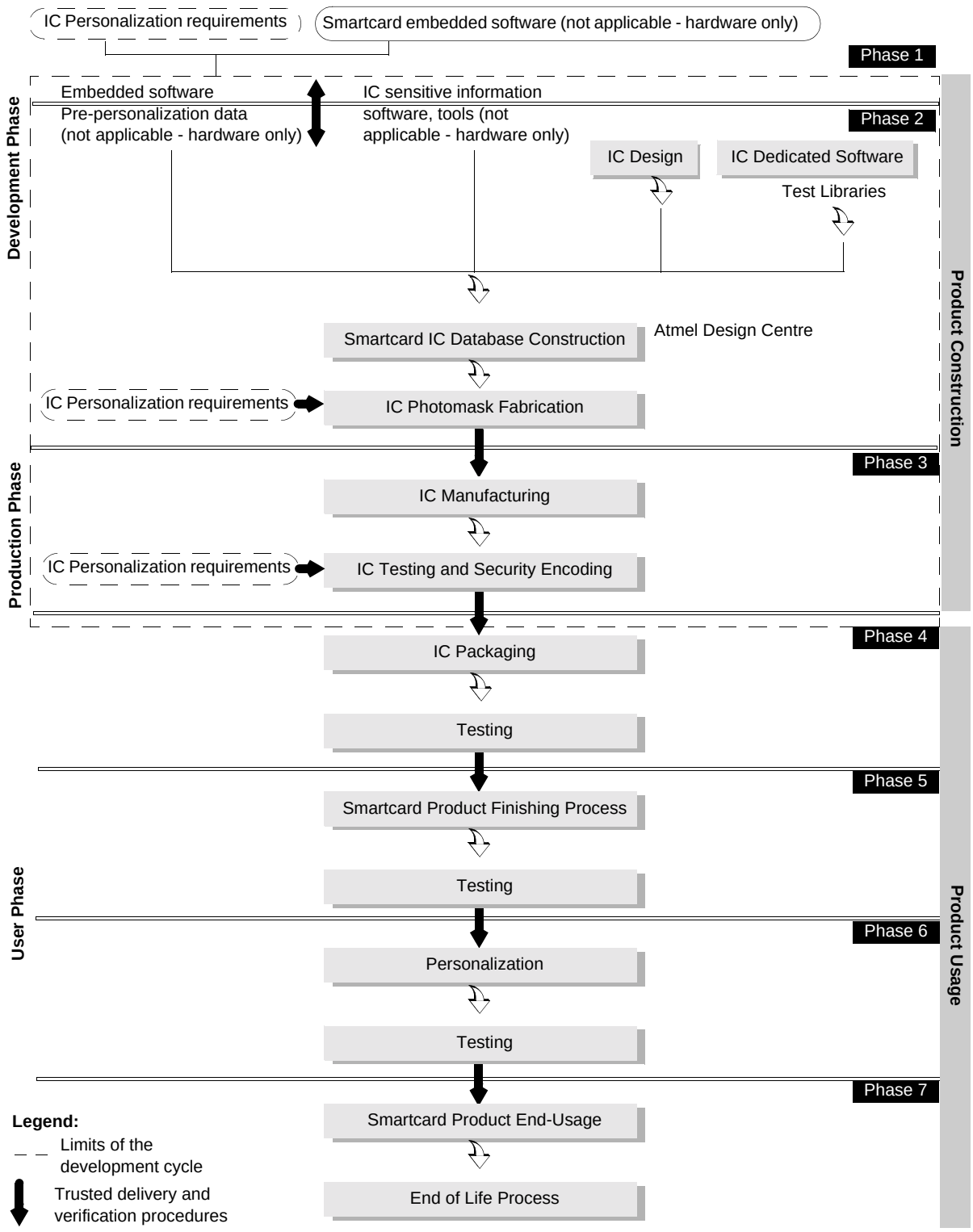


Figure 2-2 Smartcard Product Life Cycle

33 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

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

2.3 TOE Environment

35 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

36 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.

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

38 Reticles and photomasks are generated from the verified IC database. The reticles and photomasks are then shipped to the wafer fab processing facilities by means of a secure carrier.

2.3.2 TOE Production Environment

39 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 the use of a manufacturing database.

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

41 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.

2.3.3 TOE User Environment

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

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

44 Following testing and security encoding in phase 3, the wafers are sawn into individual dies. After the wafers are sawn, the good ICs are assembled into modules in a module assembly plant.

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

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

End-user environment (phase 7)

47 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.

48 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

49 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

50 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.

51 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).

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

Table 2-2 Users of the Product - Phases 4 to 7

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 uses 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.

53 The MCU may be used in the following modes:

a) Test mode, in which the MCU runs under the control of test software 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.

54 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 and the MCU is set to User mode.

55 If a faulty MCU is returned from the field, analysis can be done in User mode only, because Test mode is inhibited prior to devices going to the field.

56 There is no intermediate mode for fault analysis. The only modes of operation are those stated in paragraph 53.

57 Once manufactured, the MCU operates by executing the smartcard embedded software stored in ROM. The contents of the 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.

58 The EEPROM includes control bytes, which can be used to store security-related information. The control bytes cannot be erased in User mode.

59 The I/O port is 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

60 The TOE IT (Information Technology) 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)

TOE Security Environment

61 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

62 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 ROM options and the control byte data.
- Smartcard embedded software.
- IC specification, design, development tools and technology.

63 Therefore, the TOE itself is an asset.

64 Assets must be protected in terms of confidentiality, integrity and availability.

3.2 Assumptions

65 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.

66 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)

67 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.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).

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

68 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.

69 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)

70 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 document.

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.

71 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

72 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

73 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

74 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 (e.g. 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

75 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 threats 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.

76 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

77 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.

78 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.

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.

Security Objectives

79 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

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

O.TAMPER	The TOE must prevent physical tampering with its security critical parts.
O.CLON	The TOE functionality needs to be protected from cloning.
O.OPERATE	The TOE must ensure the continued correct operation of its security functions.
O.FLAW	The TOE must not contain flaws in design, implementation or operation.
O.DIS_MECHANISM	The TOE shall ensure that the hardware security mechanisms are protected against unauthorized disclosure.
O.DIS_MEMORY	The TOE shall ensure that sensitive information stored in memories is protected against unauthorized access.
O.MOD_MEMORY	The TOE shall ensure that sensitive information stored in memories is protected against any corruption or unauthorized modification.
O.CRYPTO	Cryptographic capability shall be available for users to maintain integrity and confidentiality of sensitive data.

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 documentations, 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. It must be ensured that 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 the Security Target, the smartcard embedded software shall use IC security features and security mechanisms as specified in the smartcard IC documentation (e.g. sensors) [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 and any other 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 other 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 to 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 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 copying, 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 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 of 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.

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 confidentiality of sensitive data stored or handled by the system (e.g. terminals, communications) shall be maintained.

TOE Security Functional Requirements

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

82 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)

83 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)

84 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)

85 The TOE security functions shall maintain the following list of security attributes belonging to individual users: read, write and execute access privileges to ROM, RAM, EEPROM, and Test mode functions in Test mode.

5.1.4 TOE Security Functions Testing (FPT_TST.1)

86 The TOE security functions shall:

- Run a suite of self tests at the request of the authorized user, at the conditions in a controlled environment (probe area) 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)

87 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: pass/fail signatures from ROM and RAM, and write/read checks of EEPROM in Test mode to verify the integrity of the device memories.

5.2 Functional Requirements Applicable to Phases 3 to 7

5.2.1 Management of Security Functions Behaviour (FMT_MOF.1)

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

5.2.2 Management of Security Attributes (FMT_MSA.1)

89 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 Test mode to the TME administrator, and restrict the ability to access locked out memory regions, illegal address regions and illegal opcodes to authorized users.

ACFS_ Policy

Table 5-1 ACFS_ Policy in Test Mode

Test Mode	Administrator	User
ROM	Read (Signature)	No Access
RAM	Read/Write	No Access
EEPROM	Read/Write*	No Access
Test Mode Functions	Read/Write	No Access

* If Write access to the EEPROM is required, the administrator would need to execute an appropriate routine in RAM.

Table 5-2 ACFS_ Policy in User Mode

User Mode	Administrator	User
ROM	No Access	Read*
RAM	No Access	Read/Write*
EEPROM	No Access	Read/Write*
Test Mode Functions	No Access	No Access

* Access permitted only if authorized by lock-out

IFCSF_ Policy

Table 5-3 IFCSF_ Policy in Test Mode

Test Mode	Administrator	User
ROM	Signature	No Data Flow
RAM	Read/Write	No Data Flow
EEPROM	Read/Write*	No Data Flow

* If Write information flow to the EEPROM is required, the administrator would need to execute an appropriate routine in RAM.

Table 5-4 IFCSF_ Policy in User Mode

User Mode	Administrator	User
ROM	No Data Flow	Read*
RAM	No Data Flow	Read/Write*
EEPROM	No Data Flow	Read/Write*

* Information flow permitted only if authorized by lock-out

5.2.3 Security Roles (FMT_SMR.1)

90 The TOE security functions shall:

- Maintain the role of TME administrator
- Be able to associate users with roles

5.2.4 Static Attribute Initialization (FMT_MSA.3)

91 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.

5.2.5 Complete Access Control (FDP_ACC.2)

92 The TOE security functions shall:

- Enforce the ACSF_Policy (as described in Table 5-1 and Table 5-2, page 39) on administrator, User, ROM, RAM, EEPROM, Test mode functions, and all operations among subjects and objects covered by the security functions policy.
- 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.

5.2.6 Security Attribute Based Access Control (FDP_ACF.1)

93 The TOE security functions shall:

- Enforce the ACSF_Policy to objects based on Read, Write security attributes.
- Enforce the ACSF_Policy on administrator, User, ROM, RAM, EEPROM, Test mode functions and all operations among subjects and objects covered by the security functions policy.
- Explicitly authorize access of subjects to objects based on the following additional rules: no additional rules.
- Explicitly deny access of subjects to objects based on the lockout, illegal address and illegal opcode rules, based on security attributes, that explicitly deny access of subjects to objects.

5.2.7 Subset Information Flow Control (FDP_IFC.1)

94 The TOE security functions shall enforce the IFCSF_Policy on administrator, User and Read, Write and Execute operations that cause controlled information on flow to and from controlled objects covered by the security functions policy.

5.2.8 Simple Security Attributes (FDP_IFF.1)

95 The TOE security functions shall:

- Enforce the IFCSF_Policy based on the following types of subject and information security attributes: Signature, Read, Write.
- Permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: lockout, illegal address and illegal opcode rules based on security attributes that explicitly deny information flows.
- Provide no additional information flow control security functions policy rules.
- Enforce no additional security functions policy capabilities.
- Explicitly authorize an information flow based on the following rules: lockout, illegal address and illegal opcode rules based on security attributes that explicitly authorize information flows.
- Explicitly deny an information flow based on the following rules: lockout, illegal address and illegal opcode rules based on security attributes that explicitly deny information flows.

5.2.9 Potential Violation Analysis (FAU_SAA.1)

96 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.

97 Enforce the following rules for monitoring audited events:

- Accumulation or combination of abnormal environmental conditions, access control activity or physical tampering would indicate a potential security violation.

5.2.10 Unobservability (FPR_UNO.1)

98 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.

5.2.11 Notification of Physical Attack (FPT_PHP.2)

99 The TOE shall provide unambiguous detection of physical tampering that might compromise the TOE security functions.

100 The TOE security functions shall provide the capability to determine whether physical tampering with the TOE security functions's devices and elements has occurred.

101 For values of voltage, clock input frequency and temperature which go outside acceptable bounds, and for probing, the TOE security functions shall monitor the devices and elements and notify the authorized user when physical tampering with the TOE security functions' devices and elements has occurred.

5.2.12 Resistance to Physical Attack (FPT_PHP.3)

102 The TOE security functions shall resist tampering of voltage, clock input frequency and temperature to the TOE and its security functions by responding automatically such that the TOE security policy is not violated.

5.2.13 Cryptographic Operation (FCS_COP.1)

103 The TSF shall perform hardware data encryption and decryption in accordance with the DES cryptographic algorithm using 56-bit cryptographic key sizes that meet the Data Encryption Standard (DES), FIPS PUB 46-2, 30th December, 1993.

5.3 TOE Security Assurance Requirements

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

105 Some of these components are hierarchical ones to the components specified in EAL4. The others are required for the maintenance process required for the EUROPA family.

5.3.1 ADV_IMP.2 Implementation of the TSF

Developer actions elements:

106 The developer shall provide the implementation representation for the entire TSF.

Content and presentation of evidence elements:

107 The implementation representation shall:

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

Evaluator actions elements:

108 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.

5.3.2 ALC_DVS.2 Sufficiency of Security Measures

Developer actions elements:

109 The developer shall produce development security documentation.

Content and presentation of evidence elements:

110 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.

111 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:

112 The evaluator shall confirm that the:

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

5.3.3 AVA_VLA.4 Highly Resistant

Developer actions elements:

113 The developer shall:

- Perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.
- Document the disposition of identified vulnerabilities.

Content and presentation of evidence elements:

- The evidence shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.
- The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.
- The evidence shall show that the search for vulnerabilities is systematic.
- The analysis documentation shall provide a justification that the analysis completely addresses the TOE deliverables.

Evaluator actions elements:

114 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.
- Conduct 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.

5.3.4 AMA_AMP.1 Assurance Maintenance Plan

Developer action elements:

115 The developer shall provide an AM Plan.

Content and presentation of evidence elements:

116 The AM Plan shall:

- Contain or reference a brief description of the TOE, including the security functionality it provides.
- Identify the certified version of the TOE, and shall reference the evaluation results.
- Reference the TOE component categorisation report for the certified version of the TOE.
- Define the scope of changes to the TOE that are covered by the plan.
- Describe the TOE life-cycle, and shall identify the current plans for any new releases of the TOE, together with a brief description of any planned changes that are likely to have a significant security impact.
- Describe the assurance maintenance cycle, stating and justifying the planned schedule of AM audits and the target date of the next re-evaluation of the TOE.
- Identify the individual(s) who will assume the role of developer security analyst for the TOE.
- Describe how the developer security analyst role will ensure that the procedures documented or referenced in the AM Plan are followed.
- Describe how the developer security analyst role will ensure that all developer actions involved in the analysis of the security impact of changes affecting the TOE are performed correctly.
- Justify why the identified developer security analyst(s) have sufficient familiarity with the security target, functional specification and (where appropriate) high-level design of the TOE, and with the evaluation results and all applicable assurance requirements for the certified version of the TOE.
- Describe or reference the procedures to be applied to maintain the assurance in the TOE, which as a minimum shall include the procedures for configuration management, maintenance of assurance evidence, performance of the analysis of the security impact of changes affecting the TOE, and flaw remediation.

Evaluator action elements:

117 The evaluator shall:

- Confirm that the information provided meets all requirements for content and presentation of evidence.
- Confirm that the proposed schedules for AM audits and re-evaluation of the TOE are acceptable and consistent with the proposed changes to the TOE.

5.3.5 AMA_CAT.1 TOE Component Categorization Report

Developer action elements:

118 The developer shall provide a TOE component categorisation report for the certified version of the TOE.

Content and presentation of evidence elements:

119 The TOE component categorisation report shall:

- Categorise each component of the TOE, identifiable in each TSF representation from the most abstract to the least abstract, according to its relevance to security; as a minimum, TOE components must be categorised as one of TSP-enforcing or non-TSP-enforcing.
- Describe the categorisation scheme used, so that it can be determined how to categorise new components introduced into the TOE, and also when to re-categorize existing TOE components following changes to the TOE or its security target.
- Identify any tools used in the development environment that, if modified, will have an impact on the assurance that the TOE satisfies its security target.

Evaluator action elements:

120 The evaluator shall:

- Confirm that the information provided meets all requirements for content and presentation of evidence.
- Confirm that the categorisation of TOE components and tools, and the categorisation scheme used, are appropriate and consistent with the evaluation results for the certified version.

5.3.6 AMA_EVD.1 Evidence of Assurance Maintenance

Developer action elements:

121 The developer security analyst shall provide AM documentation for the current version of the TOE.

Content and presentation of evidence elements:

122 The AM documentation shall include a configuration list and a list of identified vulnerabilities in the TOE.

123 The configuration list shall describe the configuration items that comprise the current version of the TOE.

124 The AM documentation shall provide evidence that the procedures documented or referenced in the AM Plan are being followed.

125 The list of identified vulnerabilities in the current version of the TOE shall show, for each vulnerability, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

126 The evaluator shall:

- Confirm that the information provided meets all requirements for content and presentation of evidence.
- Confirm that the procedures documented or referenced in the AM Plan are being followed.
- Confirm that the security impact analysis for the current version of the TOE is consistent with the configuration list.
- Confirm that all changes documented in the security impact analysis for the current version of the TOE are within the scope of changes covered by the AM Plan.
- Confirm that functional testing has been performed on the current version of the TOE, to a degree commensurate with the level of assurance being maintained.

5.3.7 AMA_SIA.2 Security Impact Analysis

Developer action elements:

127 The developer security analyst shall, for the current version of the TOE, provide a security impact analysis that covers all changes affecting the TOE as compared with the certified version.

Content and presentation of evidence elements:

128 The security impact analysis shall:

- Identify the certified TOE from which the current version of the TOE was derived.
- Identify all new and modified TOE components that are categorised as TSP-enforcing.
- For each change affecting the security target or TSF representations, briefly describe the change and any effects it has on lower representation levels.
- For each change affecting the security target or TSF representations, identify all IT security functions and all TOE components categorised as TSP-enforcing that are affected by the change.
- For each change which results in a modification of the implementation representation of the TSF or the IT environment, identify the test evidence that shows, to the required level of assurance, that the TSF continues to be correctly implemented following the change.
- For each applicable assurance requirement in the configuration management (ACM), life cycle support (ALC), delivery and operation (ADO) and guidance documents (AGD) assurance classes, identify any evaluation deliverables that have changed, and provide a brief description of each change and its impact on assurance.
- For each applicable assurance requirement in the vulnerability assessment (AVA) assurance class, identify which evaluation deliverables have changed and which have not, and give reasons for the decision taken as to whether or not to update the deliverable.

Evaluator action elements:

129 The evaluator shall:

- Confirm that the information provided meets all requirements for content and presentation of evidence.
- Check that the security impact analysis documents all changes to an appropriate level of detail, together with appropriate justifications that assurance has been maintained in the current version of the TOE.

5.3.8 ALC_FLR.1 Flaw Remediation

Developer action elements:

130 The developer shall document the flaw remediation procedures.

Content and presentation of evidence elements:

131 The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

132 The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

133 The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

134 The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

Evaluator action elements:

135 The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.1 TOE Security Functions

136 This section defines the TOE security functions, and Table 6-1, page 54 specifies how they satisfy the TOE security functional requirements

6.1.1 Test Mode Entry (SF1)

137 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.

138 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.

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

6.1.2 Access Privileges (Read/Write/Execute) (SF2)

140 SF2 shall ensure that authenticated users can have access (Read/Write/Execute) privileges to commands in Test mode.

141 Only, authorized design and production engineers running tests on the TOE will have access to the TME Code.

6.1.3 Test Mode Disable (SF3)

142 SF3 shall make provision for Test mode disable which, once activated, shall ensure that none of the test features are available, not even to authenticated users in Test mode.

6.1.4 TOE Testing (SF4)

143 Testing of Security Functions is dependent on a fault free and fully functional TOE. The RAM, ROM, and standard cell logic (including the MCU) are tested by functional tests under the control of the test interface circuit. EEPROM is tested through the test

interface circuit by external stimulus. CPU to EEPROM data will also be tested using this method.

144 To conform with ISO 7816 standards the TOE embedded software will always return an Anwer-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 and logic).

6.1.5 Data Error Detection (SF5)

145 SF5 shall provide means for performing data error detection. Means of performing CRC error detection and parity error detection shall be provided.

6.1.6 Illegal Access and Lockout (SF6)

146 SF6 shall enforce access and information flow rights based on the lockout, illegal address and illegal opcode rules:

- Lockout - If a locked out address is accessed, a chip reset is invoked.
- Illegal Address - If an illegal address is accessed, a chip reset is invoked.
- Illegal Opcode - If an attempt is made to execute any opcode that is not implemented in the instruction set, a chip reset is invoked.

6.1.7 Event Audit (SF7)

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

1. Accumulation or combination of the following auditable events would indicate a potential security violation:
2. The external voltage supply or clock signal goes outside acceptable bounds (SM.VOLT, SM.FREQ).
3. The ambient temperature goes outside acceptable bounds (SM.TEMP).
4. Application program runaway occurs (SM.WDOG).
5. Attempts to gain illegal access to reserved memory locations (SM.ILLADD).
6. Attempts to probe the device (SM.TAMPER).
7. Attempts to gain illegal access to locked out areas of memory (SM.LOCKOUT).
8. Attempts to execute an opcode that is not implemented (SM.OPCODE).
9. Attempts to illegally enter device Stop mode (SM.STOP).
10. Attempts to illegally access the device EEPROM (SM.EER).
11. Attempts to gain access to Test mode (SM.TMODE).

6.1.8 Event Action (SF8)

148 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 an immediate reset or a suspended reset to occur if the violation warrants such action.

6.1.9 Unobservability (SF9)

149 SF8 shall ensure that users/third parties will have difficulty observing the following operations on the TOE by:

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, in order to examine the topology of the TOE, including address and data bases and regular structures.

6.1.10 Cryptography (SF10)

150 The TSF shall provide a cryptographic algorithm to be able to transmit and receive objects in a manner protected from data modification. The TSF shall provide a hardware DES data encryption capability which may be used by the smartcard embedded software to support security functions such as data encryption and decryption for maintaining data integrity.

151 An assessment of the strength of the DES algorithm does not form part of the evaluation.

152 A Random Number Generator shall be provide to support security operations performed by cryptographic applications.

Table 6-1 Relationship Between Security Requirements and Security Functions

		Security Functions									
		Test Mode Entry	Access Privileges	Test Mode Disable	TOE Testing	Data Error Detection	Illegal access and lockout	Event Audit	Event Action	Unobservability	Cryptography
Security Requirement		**SF1**	**SF2**	**SF3**	**SF4**	**SF5**	**SF6**	**SF7**	**SF8**	**SF9**	**SF10**
FIA_UAU.2	O1	x									
FIA_UID.2	O2	x									
FIA_ATD.1	O3	x	x	x							
FPT_TST.1	O4				x	x					
FDP_SDI.1	O5				x	x					
FMT_MOF.1	O6	x									
FMT_MSA.1	O7	x									
FMT_SMR.1	O8	x		x				x	x		
FMT_MSA.3	O9	x	x	x			x				
FDP_ACC.2	10	x	x	x			x				
FDP_ACF.1	11	x	x	x			x				
FDP_IFC.1	12	x	x	x			x				
FDP_IFF.1	13	x	x	x			x				
FAU_SAA.1	14							x			
FPR_UNO.1	15									x	
FPT_PHP.2	16							x	x		
FPT_PHP.3	17							x	x		
FCS_COP.1	18										x

6.2 Assurance Measures

153 This section defines the TOE assurance measures and Table 6-2, page 57 specifies how they satisfy the TOE security assurance requirements.

6.2.1 Security Target (SA1)

154 SA1 shall provide the “AT05SC3208R Security Target” document plus its references.

6.2.2 Configuration Management (SA2)

155 SA2 shall provide the “AT05SC3208R CC Configuration Management (ACM)” document plus its references.

6.2.3 Delivery and Operation (SA3)

156 SA3 shall provide the “AT05SC3208R CC Delivery and Operation (ADO)” document plus its references.

6.2.4 Development Activity (SA4)

157 SA4 shall provide the “AT05SC3208R CC Development Activity (ADV)” document plus its references.

6.2.5 Guidance (SA5)

158 SA5 shall provide the “AT05SC3208R CC Guidance (AGD)” document plus its references.

6.2.6 Life Cycle Support (SA6)

159 SA6 shall provide the “AT05SC3208R CC Life Cycle Support (ALC)” document plus its references.

6.2.7 Test Activity (SA7)

160 SA7 shall provide the “AT05SC3208R CC Test Activity (ATE)” document plus its references, and undertaking of testing described therein.

6.2.8 Vulnerability Assessment (SA8)

161 SA8 shall provide the “AT05SC3208R CC Vulnerability Assessment (AVA)” document plus its references, and undertaking of vulnerability assessment described therein.

6.2.9 Smartcard Devices (SA9)

162 SA9 shall provide functional AT05SC3208R smartcard devices.

6.2.10 Development Site (SA10)

163 SA10 shall provide access to the development site.

6.2.11 Test Site (SA11)

164 SA11 shall provide access to the test site.

6.2.12 Manufacturing Site (SA12)

165 SA12 shall provide access to the manufacturing site.

6.2.13 Sub-contractor Sites (SA13)

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

6.2.14 Maintenance Process (SA14)

167 SA14 shall provide the “AT05SC3208R CC Maintenance Process (AMA)” document plus its references.

Table 6-2 Relationship Between Assurance Requirements and Measures

ASSURANCE REQUIREMENT	SA1 Security Target	SA2 Configuration Management	SA3 Delivery and Operation	SA4 Development Activity	SA5 Guidance	SA6 Life Cycle Support	SA7 Test Activity	SA8 Vulnerability assessment	SA9 Smartcard Devices	SA10 Development Site	SA11 Test Site	SA12 Manufacturing Site	SA13 Sub-contractor Site	SA14 Maintenance Process
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_FLR.1						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.2								x	x					
AVA_SOF.1								x	x					
AVA_VLA.4								x	x					
AMA_AMP.1														x
AMA_CAT.1														x
AMA_EVD.1														x
AMA_SIA.2														x

PP Claims

7.1 PP Reference

168 This ST 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

169 None.

7.3 PP Additions

7.3.1 Cryptographic Capability

170 In addition to conforming to PP/9806, the Security Target specifies an additional objective O.CRYPTO in Section 4.1.

171 The CC security functional requirement to meet this objective is Cryptographic Operation (FCS_COP.1) and is specified in Section 5.

172 The security function to satisfy the FCS_COP.1 requirement is SF16 and is specified in Section 6.

7.3.2 Maintenance Process

173 In addition to conforming to PP/9806, the Security Target specifies additional security assurance requirements to cover a maintenance process. This maintenance process is necessary because family derivatives of the EUROPA 3208 TOE will be evaluated under the Common Criteria maintenance scheme.

174 The additional security assurance requirements consist of:

- AMA_AMP.1 (see Section 5.3.4)
- AMA_CAT.1 (see Section 5.3.5)
- AMA_EVD.1 (see Section 5.3.6)
- AMA_SIA.2 (see Section 5.3.7)
- ALC_FLR.1 (see Section 5.3.8)

175 The assurance measure to satisfy these requirements is SA14 and is specified in Section 6.2.

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-16	Algorithm used to compute powerful checksum on memory blocks.
FACTORYworks	Manufacturing UNIX based batch Tracking System.
IC Dedicated Software	IC Proprietary software which is required for testing purposes and to implement special functions. For AT05SC3208R 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.
MARCH C+	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.

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.
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

CPU	Central Processor Unit
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable ROM
EKB	East Kilbride
HCMOS	High Speed Complementary Metal Oxide Semiconductor
I/O	Input/Output
IC	Integrated Circuit
MCU	Microcontroller
PLL	Phase Locked Loop
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read-only Access
SOF	Strength of Function
TME	Test Mode Entry
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

Atmel Headquarters

Corporate Headquarters
2325 Orchard Parkway
San Jose, CA 95131
TEL 1(408) 441-0311
FAX 1(408) 487-2600

Europe
Atmel Sarl
Route des Arsenaux 41
Casa Postale 80
CH-1705 Fribourg
Switzerland
TEL (41) 26-426-5555
FAX (41) 26-426-5500

Asia
Atmel Asia, Ltd.
Room 1219
Chinachem Golden Plaza
77 Mody Road Tsimhatsui
East Kowloon
Hong Kong
TEL (852) 2721-9778
FAX (852) 2722-1369

Japan
Atmel Japan K.K.
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
Atmel Corporate
2325 Orchard Parkway
San Jose, CA 95131
TEL 1(408) 436-4270
FAX 1(408) 436-4314

Microcontrollers
Atmel Corporate
2325 Orchard Parkway
San Jose, CA 95131
TEL 1(408) 436-4270
FAX 1(408) 436-4314

Atmel Nantes
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
Atmel Rousset
Zone Industrielle
13106 Rousset Cedex, France
TEL (33) 4-42-53-60-00
FAX (33) 4-42-53-60-01

Atmel Colorado Springs
1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906
TEL 1(719) 576-3300
FAX 1(719) 540-1759

Atmel Smart Card ICs
Scottish Enterprise Technology Park
Maxwell Building
East Kilbride G75 0QR, Scotland
TEL (44) 1355-803-000
FAX (44) 1355-242-743

RF/Automotive
Atmel Heilbronn
Theresienstrasse 2
Postfach 3535
74025 Heilbronn, Germany
TEL (49) 71-31-67-0
FAX (49) 71-31-67-2340

Atmel Colorado Springs
1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906
TEL 1(719) 576-3300
FAX 1(719) 540-1759

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

---

e-mail
literature@atmel.com

Web Site
http://www.atmel.com

TPG0035A (24 Nov03)