Common Criteria
Information Technology
Security Evaluation

Project APACHE II

S3CC9RB

Security Target

Version 1.2

February 21, 2003

SAMSUNG
ELECTRONICS

REVISION HISTORY

UPDATES:

Version	Date	Modification
1.0	24 APR 2003	Creation
1.1	30 MAY 2003	ITSEF & DCSSI Comments
1.2	21 FEB 2004	Chapter 7.2 Assurance Measure Updates

EDITED:

Written by	Title
Kyungsuk YI	Engineer

APPROVAL:

Approved by	Title
Sungman HWANG	Principal Engineer

DISTRIBUTION:

Name	Company/Occupation	Copy
Sungman HWANG	Samsung Electronics	1/3
Stéphane LEBRUN	ITSEF	2/3
Matthieu ROBERT	DCSSI	3/3

CONTENTS

1 ST INTRODUCTION

1.1 ST IDENTIFICATION

Title: Security Target of S3CC9RB 16-Bit RISC Microcontroller for Smart Card
Version: V1.2, issued on February 21, 2004

Version number	Common Criteria
V1.2	version 2.1

1 A glossary of terms used in the ST is given in annex A.

2 This ST has been built with Common Criteria Version 2.1

3 This ST is compliant to Protection Profile of Smart Card Integrated Circuit, PP/9806.

1.2 ST OVERVIEW

4 This Security Target is the work of the Samsung Electronics Co., Ltd. TOE is smart card integrated circuit. The ST is “CC part 2 conformant and CC part 3 conformant”. The TOE is to be evaluated with Common Criteria Version 2.1.

5 The assurance level for this ST is EAL4 augmented by the assurance component ADV_IMP.2 (Implementation representation), ALC_DVS.2 (Sufficiency of security measure) and AVA_VLA.4 (Highly resistant) without their dependencies.

6 The main objectives of this Security Target are:

- To describe the Target of Evaluation (TOE) as a functional product. This ST focuses on the development and use of integrated circuit.
- To describe the security environment of the TOE including the assets to be protected and the threats to be countered by the TOE and by the environment during the development and the operational phases of the card.
- To describe the security objectives of the TOE and its supporting environment in terms of integrity and confidentiality of application data and programs, protection of the TOE and associated documentation during the development phase.
- To specify the security requirements which includes the TOE Security functional requirements and the TOE security assurance requirements.

2 TOE DESCRIPTION

7 This part of the ST 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

8 The Target of Evaluation (TOE) is the single chip microcontroller unit in accordance with the functional specification, independent of the physical interface, the way it is packaged and any other security device supported by the micro module and the plastic card. Generally, a Smart Card product may include other elements (such as specific hardware components, batteries, capacitors, antenna, holograms, magnetic stripes, and security printing...) but these are not in the scope of this Security Target.

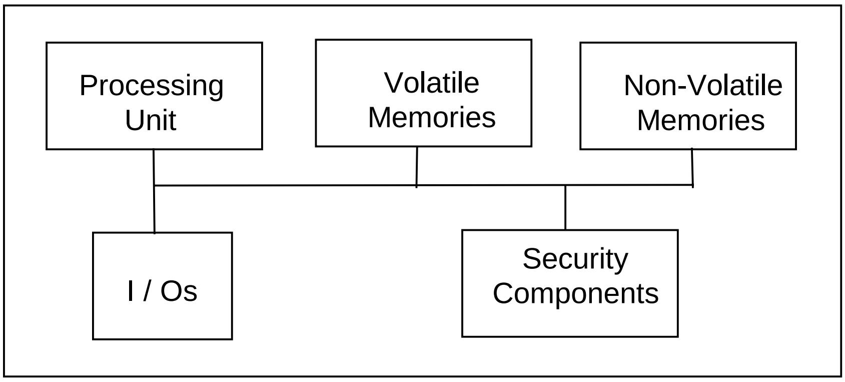

Figure 2-1. Smart card chip block diagram

9 The typical TOE is composed of a processing unit, security components, I/Os and volatile and non-volatile memories. The TOE always comprises a smart card embedded software and an IC dedicated software (Test ROM code). The former is out of scope of the evaluation, while the latter is within the scope of the evaluation.

10 To allow the evaluation of a functional product, the TOE is supplied to the Evaluation Center with a manufacturer proprietary embedded software (called User Test COS and User COS) which allows the operation of the security functions. This software is not in the scope of the evaluation.

The TOE submitted to the evaluation comprises the following components:

TOE component	Reference
S3CC9RB 40dip , S3CC9RB	S3CC9RBX01
S3CC9RB dedicated software	S3CC9RB TEST ROM code, version 1.0
S3CC9RB embedded software (Out of evaluation scope)	S3CC9RB User Test code, version 1.0
S3CC9RB Cryptography library	Cryptography library , version 1.0

Table 2-1. TOE hardware and software components

2.2 SMART CARD PRODUCT LIFE-CYCLE

11 The Smart Card product life-cycle is decomposed into 7 phases, according to the " Smart Card Integrated Circuit Protection Profile ". (PP / 9806 version 2.0, issue September 1998)

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

Table 2-2. Smart card product life-cycle phases

12 The limit of this Security Target correspond to phase 2 and phase3, including the phase 1 delivery and verification procedures and the TOE delivery to the IC packaging manufacturer; phase 1, 4, 5, 6 and 7 are outside the scope of this ST.

13 The figure 2-2. describes the Smartcard product life-cycle.

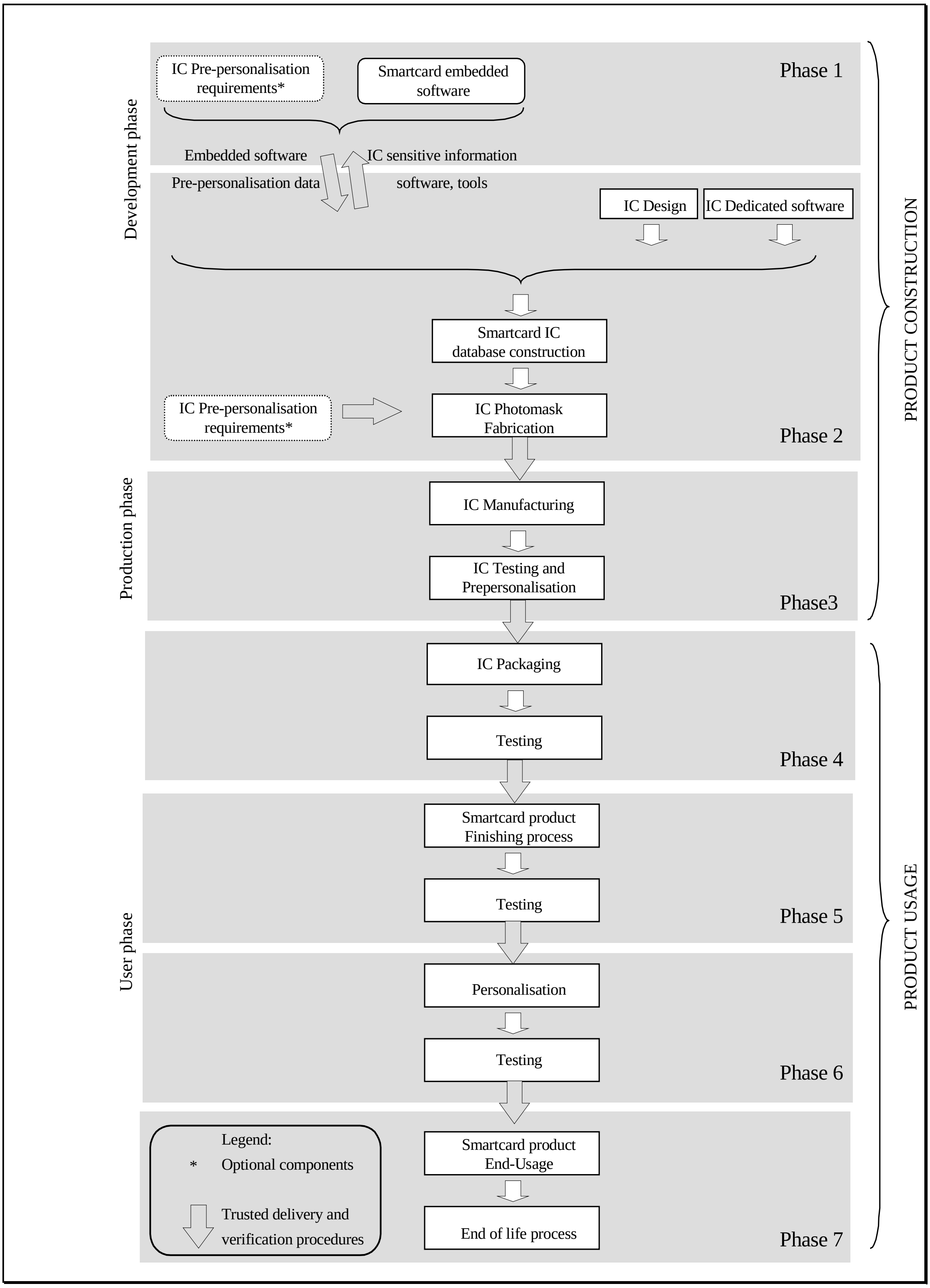

Figure 2-2. Smart card product life-cycle

14 Following table identifies the sites, which are within evaluation perimeter.

Phase	Description	Address for S3CC9RB
Phase 2	IC Development	Chip Card & Microcontroller Development team Samsung Electronics Co., Ltd. San #24, Nongseo-Ri, Giheung-Eup, Yongin-City, Gyeonggi-Do, KOREA 449-711
	IC Photomask Fabrication	Photomask Team, Samsung Electronics Co., Ltd. San #24, Nongseo-Ri, Giheung-Eup, Yongin-City, Gyeonggi-Do, KOREA 449-711
Phase 3	IC Manufacturing	Line 5, Samsung Electronics Co., Ltd. San #24, Nongseo-Ri, Giheung-Eup, Yongin-City, Gyeonggi-Do, KOREA 449-711
	IC wafer Testing	Line 2, Samsung Electronics Co., Ltd. San #24, Nongseo-Ri, Giheung-Eup, Yongin-City, Gyeonggi-Do, KOREA 449-711

Table 2-3. Site identification within the evaluation perimeter

15 Procedures on the delivery process of the TOE must exist and be applied for every delivery within this phase or between phases. This includes any kind of delivery performed from phase 2 to 3, 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.-

16 These procedures shall be compliant with the assumptions [A.DLV].

17 The TOE controls following configurations:

TOE Configuration	Product Life Cycle	Authorized User(Role)
TEST Configuration	Phase 3	Test Administrator
USER Configuration	Phase 4 to 7	User

Table 2-4. TOE configurations

2.3 TOE ENVIRONMENT

18 Considering the TOE, the Development environment is defined as follow:

- Design environment corresponding to phase 2
- Production environment corresponding to phase 3 including the test operations
- User environment, from phase 4 to phase 7

2.3.1 TOE Development Environment

19 To assure security, the environment in which the development takes place shall be made secured with controllable accesses having traceability. Furthermore, it is important that all authorised personnel involved fully understand the importance and the rigid implementation of defined security procedures.

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

21 Design and development of the IC then follows. The engineer uses a secure computer system (preventing unauthorised access) to make his design simulations, circuit performance verifications and generation of the TOE's IC photomask databases. Sensitive documents, databases on tapes, diskettes, and printed circuit layout information are stored in appropriate locked cupboards/safe. Of paramount importance also is the disposal of unwanted data (complete electronic erasures) and documents (e.g. shredding).

22 Reticles and photomasks are generated from the verified IC databases; the formers are used in the silicon Wafer-fab processing. Reticles and photomasks are generated only on-site for security.

2.3.2 TOE Production environment

23 As high volumes of product commonly go through such environments, adequate control procedures are necessary to account for all products at all stages of production.

24 Production starts within the Wafer-fab; here the silicon wafers undergo the diffusion processing typically in 25-wafer lots. Computer tracking at wafer level throughout the process is commonplace. The wafers are then taken into the test area. Testing and security programming (optional) of each TOE occurs. After fabrication, the TOE is tested to assure conformance with the device specification. The wafers will then be delivered for assembly onto the smart card.

2.3.3 TOE user environment

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

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

End-user environment (phase 7)

27 Smart cards are used in a wide range of applications to assure authorised conditional access. Examples of such are Pay-TV, Banking Cards, Portable communication SIM cards, Health cards, and Transportation cards.

28 The end-user environment therefore covers a wide spectrum of very different functions, thus making it difficult to avoid and monitor any abuse of the TOE.

2.4 TOE INTENDED USAGE

29 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 a 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.

30 During the phases 2 and 3, the TOE is being developed. The administrators are as the following:

- Design Team (phase 2): **Design Manager**
- The Photomask Team (phase 2): **Photomask Manager**
- IC Production Team(phase 3): **Production Engineering Manager**
- IC Testing Team(phase 3): **Test Manager**

2.5 GENERAL IT FEATURES OF THE TOE

2.5.1 TOE Features

31 The TOE IT Security functionality's consist of data storage and processing such as:

CPU

- 16-bit CalmRISC Core

Memory

- 320 Kbytes for user application program ROM
- 6 Kbytes static RAM

EEPROM

- 64 Kbytes EEPROM as data memory
- 1 to 128-byte multi-byte write and erase
- 1.5 ms erase / write time cycles

Data Security

- 128 bytes write protected security area
- 128 bytes non erasable EEPROM
- Reset operations are selective if abnormal condition is detected

SuperMAPII Crypto-Coprocessor

- Modulo exponential accelerator
- SHA-1 accelerator
- 21 bytes control registers dedicated to SuperMAPII

DES

- Built in hardware DES

Interrupts

- Two interrupt vectors (FIQ,IRQ)
- Source for FIQ : Invalid memory access
- Source for IRQ : SIO falling edge, 16-bit timer, watchdog timer, buffer available
- Software interrupts

Serial I/O Interface

- UART for handling serial interface in accordance with ISO 7816 communication protocols
- CRC (CRC-CCITT)

16-Bit Random Number Generator

- One 16-bit random number generator for security key generation
- Start and Stop control for power consumption

Memory Protection Unit

- Read / write access control
- Base / limit region registers : 8sets
- Configurable range : 4Mbytes areas with 128bytes resolution

Timer

- 16-bit timer with 8-bit prescaler
- 20-bit watchdog timer

Internal Clock

- Typ. 5Mhz (internal variable clock)
- Typ. 5Mhz (internal fixed clock)

Operating Frequency Range

- 1-5Mhz (external clock from CLK pin)

Operating Temperature

- -25°C to +85°C

Operating Voltage Range

- 2.7V to 5.5V

Packages

- Wafer (180mm thickness)
- 8-pin COB (conforms to ISO standard 7816)

2.5.2 General Cryptography Services

32 The TOE has general cryptography services such as:

16-Bit Random Number Generator

33 The 16-bit Random number from the random number generator is used for security key in the smartcard application. The reset value is undefined.

DES Accelerator

34 The TOE has the hardware DES which consists of key register block, data register block, DES rounding block with s-box and p-box permutation.

SuperMAPII Crypto-coprocessor for public key cryptography

35 The Crypto-coprocessor (SuperMAPII) assists in the acceleration of modulo exponentiations required in the RSA arithmetic. The RSA algorithm involves the modular multiplication of large integers in order to carry out modular exponentiations.

36 The SuperMAPII to be performed is
$C=M^e$ mod N, where all the numbers used are n bits numbers, where n is from 1 to 2048.
And basically, X=A x B mod N operation will be performed repeatedly.

37 There is SHA-1 HASH accelerator for signature generation and verification.

2.5.2 TOE Block Diagram

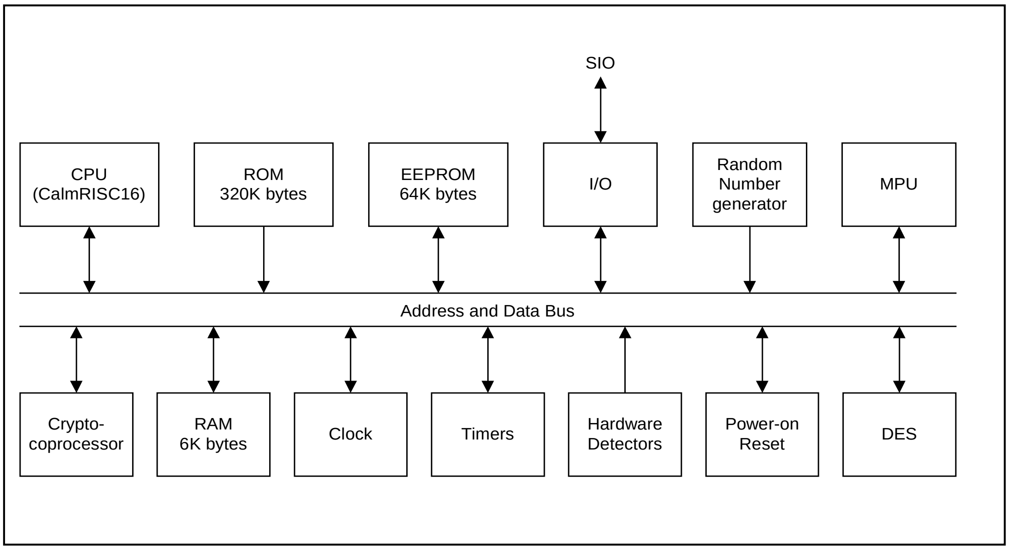

Figure 2-3. S3CC9RB Block diagram

3 TOE SECURITY ENVIRONMENT

38 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 protects, the threats and the organizational security policies.

3.1 ASSETS

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

- The application data of the TOE (such as IC pre-personalization requirements, IC and system specific data),
- The smart card embedded software,
- The IC dedicated software,
- The IC specification, design, development tools and technology.

40 The TOE itself is therefore an asset.

41 Assets have to be protected in terms of confidentiality and integrity.

3.2 ASSUMPTIONS

42 It is assumed that this section concerns the following items:

- Due to the definition of the TOE limits, any assumption for the smart card embedded software development (phase 1 is out side the scope of the TOE),
- Any assumption from phases 4 to 7 for the secure usage of the TOE, including the TOE delivery procedures.

43 Security is always the matter of the whole system: the weakest element of the chain determines the total system security. Assumptions described hereafter has to be considered for a secure system using smart card products:

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

3.2.1 Assumptions on phase 1

A.SOFT_ARCHI The smart card embedded software shall be developed in a secure manner, which 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 smart card 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)

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

A.DLV_PROTECT Procedures shall ensure protection of TOE material/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 smart card and terminal.

A.USE_SYS It is assumed that the integrity and the confidentiality of sensitive data stored/handled by the system (terminals, communications...) is maintained.

A.KEY_DEST It is assumed that the cryptographic key destruction method is implemented by the user embedded software.

3.3 THREATS

45 The TOE as defined in chapter 2 is required to counter the threats described hereafter; a threat age t wishes to abuse the assets either by functional attacks, environmental manipulations, specific hardware manipulation s or by any other types of attacks.

46 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 Unauthorised 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)

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

a) Threats on the smart cards embedded software and its environment of development, such as:

- Unauthorized disclosure, modification or theft of the smart card 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.

b) Threats on the assets transmitted from the IC designer to the smart card embedded software developer during the smart card development

c) Threats on the smart card embedded software and any additional application data transmitted during the delivery process from the smart card embedded software developer to the IC designer.

48 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 smart card embedded software developer such as sensitive information on IC specification, design and technology, software and tools if applicable;

T.DIS_DEL Unauthorized disclosure of the smart card embedded software and any additional application data (such as IC pre-personalisation requirements) during the delivery process to the IC designer;

T.MOD_DEL Unauthorized modification of the smart card embedded software and any additional application data (such as IC pre-personalisation requirements) during the delivery process to the IC designer;

T.T_DEL Theft of the smart card embedded software and any additional application data such as IC pre- personalisation requirements) during the delivery process to the IC designer.

3.3.3 Threats on phases 2 to 7

49 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

50 This type of threat 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 mechanism specifications.

T .DIS_SOFT Unauthorized disclosure of smart card 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, micro-probing tools).

T.DIS_PHOTOMASK Unauthorized disclosure of photomask information, used for photoengraving during the silicon fabrication process.

Theft or unauthorized use of assets

51 Potential attackers may gain access to the TOE and perform operations for which they are not authorized. For example, such attackers may personalize the TOE in an unauthorized manner, or try to gain fraudulent access to the smart card 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 smart card products.

Unauthorized modification of assets

52 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 t 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 mechanism 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 smart card embedded software and data.

53 The Table 3-1 indicates the relationships between the smart card phases and the threats.

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				
Theft or unauthorized 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	Class I	Class I	Class I	Class I
T.MOD_PHOTOMASK		Class II	Class I / II				

Table 3-1. Threats and phases

3.4 ORGANIZATIONAL SECURITY POLICIES

54 One organizational security policy is defined in the scope of this ST:

OSP_CRYPTO The TOE Shall ensure cryptographic calculations such as generation of random numbers, DES, Triple DES and RSA encryption / decryption.

4 SECURITY OBJECTIVES

55 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

56 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.

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 disclosure.

O.MOD_MEMORY The TOE shall ensure that sensitive information stored in memories is protected against any corruption or unauthorized modification.

O.CRYPTO The TOE Shall ensure cryptographic calculations such as generation of random numbers, DES, Triple DES and RSA encryption / decryption.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

4.2.1 Objectives on phase 1

O.DEV_DIS The IC designer must have procedures to control the sales, distribution, storage and usage of the software and hardware development tools and classified documentation, 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 sets and general information on defined assets are only delivered to the parties authorize personnel on the need to know basis.

O.SOFT_DLV The smart card embedded software must be delivered from the smart card 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 a given security target based on this Security Target, the smart card embedded software shall use IC security features and security mechanisms as specified in the smart card IC documentation (e.g. sensors,...).

O.DEV_TOOLS The smart card 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.

Objectives on phase 2 (development phase)

O.SOFT_ACS Smartcard embedded software shall be accessible only by authorized personnel within the IC designer on the need to know basis.

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 the 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 need to know basis.

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 mechanism specifications shall be accessible only by authorized personnel within the IC designer on the need to know basis.

O. TI_ACS Security relevant technology information shall be accessible only by authorized personnel within the IC designer on the need to know basis.

4.2.3 Objectives on phase 3 (manufacturing phase)

O.TOE_PRT The manufacturing process shall ensure the protection of the TOE from any kind of unauthorized use such as tampering or theft.

During the IC manufacturing and test operations, security procedure 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 sets (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 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/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/information.

O.DLV_AUDIT Procedures shall ensure that corrective actions are taken in case 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 have got the required skill, training and knowledge to meet the procedure requirements and to act to be fully in accordance with the above expectations.

4.2.5 Objectives on phases 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 its manufacturing and test data.

4.2.6 Objectives on phase 7

O.USE_DIAG Secure communication protocols and procedures shall be used between smart card and terminal.

O.USE_SYS The integrity and the confidentiality of sensitive data stored/handled by the system (terminals, communications...) shall be maintained.

O.KEY_DEST The cryptographic key destruction method is implemented by the user embedded software.

5 TOE SECURITY FUNCTIONAL REQUIREMENTS

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

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

5.1 FUNCTIONAL REQUIREMENTS ENFORCED BY THE TOE

5.1.1 Functional requirements applicable to phase 3 only (testing phase)

5.1.1.1 User authentication before any action (FIA_UAU.2)

59 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.

5.1.1.2 User Identification before any action (FIA_UID.2)

60 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.

5.1.1.3 User Attribute Definition (FIA_ATD.1)

61 The TOE security functions shall maintain the following list of security attributes belonging to individual users: **TOE configuration security attribute.**

5.1.1.4 TOE Security Functions Testing (FPT_TST.1)

62 The TOE security functions shall run a suite of self tests **at the request of the authorised user, at the conditions *test specific condition** to demonstrate the correct operation of the TOE security functions.

63 The TOE security functions shall provide authorised users with the capability to verify the integrity of TOE security functions data.

64 The TOE security functions shall provide authorised users with the capability to verify the integrity of stored TOE security functions executable code.

65 **Note**: as mentioned in the PP/9806 (version 2.0, issue September 1998), paragraph 18, the IC dedicated software may be either IC embedded software or security-relevant parts of tests programmes outside the IC.

66 **Note**: test specific condition is defined in the Apache II test documentation version 1.0

5.1.1.5 Stored Data Integrity Monitoring (FDP_SDI.1)

67 The TOE security functions shall monitor user data stored within the TOE scope of control for **all integrity errors on** all objects, based on the following attributes: **checksum and ATR**.

5.1.2 Functional requirements applicable to phases 3 to 7

Security Management

Functions	Actions to be considered
FIA_UAU.2	• management of the authentication data by an administrator, • management of the authentication data by the user associated with this data.
FIA_UID.2	• management of the user identities.
FPT_TST.1	• management of the conditions under which TOE security functions self-testing occurs, such as during initial start-up, regular interval, or under specified conditions.
FMT_MOF.1	• managing the group of roles that can interact with the functions in the TOE security functions.
FMT_MSA.1	• managing the group of roles that can interact with the security attributes.
FMT_SMR.1	• managing the group of users that are part of a role.
FMT_MSA.3	• managing the group of roles that can specify initial values. • managing the permissive or restrictive setting of default values For a given access control Security Functions Policy.
FDP_ACF.1	• managing the attributes used to make explicit access or denial Based decisions.
FDP_IFF.1	• managing the attributes used to make explicit access based Decisions.

Table 5-1. Actions to be considered for the management functions in FMT management class

5.1.2.1 Management of security functions behaviour (FMT_MOF.1)

68 The TOE security functions shall restrict the ability to **enable** the functions **SF12 to the TEST administrator.**

5.1.2.2 Management of security attributes (FMT_MSA.1)

69 The TOE security functions shall enforce the **information flow control** to restrict the ability to **change_default** the security attributes **TOE configuration** to the **TEST administrtor.**

Roles	List of security attributes
Test Administrator	• Can change the Test configuation to User configuation
User	• Cannot change the User configuation to Test configuation

Table 5-2. Information flow control attributes

5.1.2.3 Security roles (FMT_SMR.1)

70 The TOE security functions shall maintain the roles of TEST administrator and user.

- **TEST administrator**
- **User**

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

5.1.2.4 Static Attribute Initialisation (FMT_MSA.3)

72 The TOE security functions shall enforce **the information access control** to provide **restrictive** default values for security attributes that are used to enforce the security functions policy.

73 The TOE security functions shall allow **the TEST administrator** to specify alternate initial values to override the default values when an object or information is created.

Roles	List of security attributes
Test Administrator	• Can change the value of EEPROM Security Area
User	• Cannot change the value of EEPROM Security Area • Cannot erase the value of EEPROM Non-Erasable Area

Table 5-3. Static attribute initialisation

(**Note**: not applicable to hardware objects)

5.1.2.5 Complete Access Control (FDP_ACC.2)

74 The TOE security functions shall enforce the **following access control security policies ACP_1 and ACP_2 on the following list of subjects and objects** and all operations among subjects and objects covered by the security functions policy.

75 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.

76 ACP_1: Access Control Policy for IC in TEST configuration

- Whole EEPROM area programmable and erasable
- TEST ROM accessed (read and executable)
- USER ROM accessed (read and executable)
- RAM accessed (read, write and executable)

77 ACP_2: Access Control Policy for IC in USER configuration

- Partial EEPROM area programmable and erasable
- EEPROM Security area (read and executable)
- Non erasable EEPROM area (read, write only (non erasable) and executable)
- No access (read and execution) to TEST_ROM
- RAM accessed (read and write)

Object Table:

Object	Comment
TEST_ROMo	TEST ROM area
USER_ROMo	USER ROM area
SEC_EEo	SECURITY EEPROM area
NONERA_EEo	NON ERASABLE EEPROM area
USER_EEo	USER EEPROM area
USER_RAMo	USER RAM area
USER_REGo	REGISTER area

Table 5-4. Object table

Subject Table:

Subject	Comment
TEST_ROMs	Executable code in TEST ROM area
USER_ROMs	Executable code in USER ROM area
USER_EEs	Executable code in USER EEPROM area
USER_RAMs	Executable code in USER RAM area (test configuration only)

Table 5-5. Subject table

5.1.2.6 Security Attribute Based Access Control (FDP_ACF.1)

78 The TOE security functions shall Enforce the **ACP_1 and ACP_2 access contorl security functions policies** to objects based on **access control security attributes.**

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

- **Access control attribute has only two values :0 (disable) and 1 (enable)**
- **If the attribute enabled, access is authorized. (access for all operation)**
- **If the attribute disabled, access is denied. (access for all operation)**

80 The TOE security functions shall explicitly authorise access of subjects to objects based on the following additional rules :

- **(R1) Access attribute can be enabl ed in TEST_ROMs subject only for ACP_1.**
- **(R2) Access attribute can be enabled in USER_ROMs subject only for ACP_2.**

81 The TOE security functions shall explicitly deny access of subjects to objects based on the rules (R1) and (R2).

82 **In ACP-1**, at the TOE initialization, the executed code always starts at **subject « TEST_ROM »**

Subject / Object	TEST_ROMs	USER_ROMs	USER_EEs	USER_RAMs
TEST_ROMo	R / E	X	R / E	R / E
USER_ROMo	R / E	X	R* / E*	R* / E*
SEC_EEo	R / W / E	X	R* / E*	R* / W* / E*
NONERA_EEo	R / W / E	X	R* / E*	R* / W* / E*
USER_EEo	R / W / E	X	R* / E*	R* / W* / E*
USER_RAMo	R / W / E	X	R* / W* / E*	R* / W* / E*
USER_REGo	R / W	X	R / W	R / W

Table 5-6. ACP_1-TEST Configuration

X: No access R: Read W: Write

E: Branch instructions such as JUMP and CALL can branch to other Objects.

*: Conditional operation by dedicated software in TEST_ROM for each Subject and Object respectively.

Note: In ACP-1, at the TOE initialization, the executed code always starts at subject « TEST_ROM »

83 **In ACP-2**,at the TOE initialisation, the executed code always starts at **subject « USER_ROM »**

Subject / Object	TEST_ROMs	USER_ROMs	USER_EEs	USER_RAMs
TEST_ROMo	X	X	X	X
USER_ROMo	X	R / E	R* / E*	X
SEC_EEo	X	R / E	R* / E*	X
NONERA_EEo	X	R / WO / E	R* / E*	X
USER_EEo	X	R / W / E	R* / E*	X
USER_RAMo	X	R / W	R* / W*	X
USER_REGo	X	R / W	R / W*	X

Table 5-7. ACP_2-USER Configuration

X: No access WO: Write only (not erasable) R: Read W: Write

E: Branch instructions such as JUMP and CALL can branch to other Objects.

*: Conditional operation by embedded software in USER_ROM for each Subject and Object respectively

Note: In ACP-2, at the TOE initialization, the executed code always starts at subject « USER_ROM »

5.1.2.7 Subset Information Flow Control (FDP_IFC.1)

84 The TOE security functions shall enforce the **information flow control security functions policy : IFC-1 on subject TEST_ROMs for all operations.**

Note: IFC_1 : Flow of information stored in objects in **Test Configuration** only.

Note: This security functional requirement is applicable to the IC dedicated software and IC embedded software.

5.1.2.8 Simple Security Attributes (FDP_IFF.1)

85 The TOE security functions shall enforce the **IFC_1 information flow control security functions policy** based on the following types of subject and information security attribute: **TOE configuration**.

86 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 **TOE configuration in TEST configuration.**

87 The TOE security functions shall enforce the **additional information flow control security functions policy rules: none.**

88 The TOE security functions shall provide the following **non-reversibility of TOE configuration**.

89 The TOE security functions shall explicitly authorize an information flow based on the following rules: **none**.

90 The TOE security functions shall explicitly deny an information flow based on the following rules: **none**.

Note: this security functional requirement is applicable to the IC dedicated software and IC embedded software.

5.1.2.9 Potential Violation Analysis (FAU_SAA.1)

91 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.

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

a) Accumulation or combination of **events defined in Table 5-8**. known to indicate a potential security violation;

Event
Invalid Memory Access
Abnormal voltage occurrence
Abnormal frequency occurrence
Abnormal temperature occurrence
Light exposure occurrence
Signal line decapsulation occurrence
Power Glitch Attack occurrence
MET4 Dummy active line attack occurrence

Table 5-8. List of event

b) any other rules**: none**

5.1.2.10 Unobservability (FPR_UNO.1)

93 The TOE security functions shall ensure that **all users** are unable to observe **all operations** on **all objects** by all **subjects**.

Notes:

- In the context of smart card ICs, “unobservability” is defined as the impossibility to obtain the address and value of an information during an operation on this information. Identification(by unautherized user) of the operation itself is not part of the unobservability.
- It is assumed that all user subjects are compliant with the Guidance Documentation

5.1.2.11 Notification of Physical Attack (FPT_PHP.2)

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

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

96 For **the list of TOE security functions devices given in Table 5-9**, the TOE security functions shall monitor the devices and notify **the user** when physical tampering with the TOE security functions’s devices or TOE security functions's elements has occurred.

Note: notification of user defined by the embedded software(USER software).

Elements for Detection	Detection Notification
Voltage Detector	Flag setting
Frequency Detector	Flag setting
Temperature Detector	Flag setting
Light exposure Detector	Flag setting
Decapsulation Detector	Flag setting
Power Glitch Detector	Flag setting
MET4 Dummy Active Line Disconnection Detector	Flag setting

Table 5-9. List of detector elements and attack notification

5.1.2.12 Resistance to Physical Attack (FPT_PHP.3)

97 The TOE security functions shall resist **the physical tampering scenarios given in Table 5-10.** to the **list of detector elements and attack notification (Table 5-9)** by responding automatically such that the TOE security policy is not violated.

Physical Tampering Scenario	Reaction Elements
Abnormal Voltage Attack	RESET status or User software defined
Abnormal Frequency Attack	RESET status or User software defined
Abnormal Temperature Attack	RESET status or User software defined
Light exposure Attack	RESET status or User software defined
Signal line Removal Attack	RESET status or User software defined
Power Glitch Attack	RESET status or User software defined
MET4 Dummy active line attack	RESET status or User software defined

Table 5-10. List of physical attack scenarios, functions and responses

Note: As described in the CC part 2 annexes, technology limitations and relative physical exposure of the TOE must be considered.

5.1.2.13 Cryptographic operation (FCS_COP.1)

98 In order for a cryptographic operation to function correctly, the operation must be performed in accordance with specified algorithm and with a cryptographic key of specified size. The TSF shall perform in accordance with specified cryptographic algorithms.

99 The TSF shall perform **cryptographic operations [see table 5-11.]** in accordance with a specified **cryptographic algorithm [see table 5-11.]** and **cryptographic key sizes [see table 5-11.]** that meet the followings:

Operation	Algorithm	Key size	Standards
Encryption / Decryption	DES	64 bits	FIPS 46-2
Encryption / Decryption	Triple DES	128 effective bits	FIPS 46-2
Encryption / Decryption	RSA	128 to 2048 bits	ANSI X9.31
Encryption / Decryption	DSS	160 / 1024bits	FIPS 186

Table 5-11. List of cryptograhic operations

100 The TSF shall perform cryptographic operations like **HASH** function and **16-bit Random number generator**.

5.1.2.14 Cryptographic key generation (FCS_CKM.1)

101 Cryptographic key generation requires cryptographic keys to be generated in accordance with a specified algorithm and key size which can be based on an assigned standard. The TSF shall generate cryptographic key generation with specified cryptographic algorithms.

102 The TSF shall generate cryptographic key in accordance with a specified **cryptographic key generation algorithm [see Table 5-12]** and **cryptographic key sizes [see Table 5-12]** that meet the followings:

Cryptography	Algorithm	Key size	Standards
RSA Encryption / Decryption	Generation of prime number	512 to 2048 bits	The Rabin-Miller Probabilistic Primality Test
DSS	Generation of prime number	160 / 1024bits	The Rabin-Miller Probabilistic Primality Test

Table 5-12. List of cryptograhic key generations

5.2 FUNCTIONAL REQUIREMENTS ENFORCED BY THE IT ENVIRONMENT

103 IT environment is the user embedded software.

5.2.1 Functional requirements applicable to phase 7

5.2.1.1 Cryptographic key destruction(FCS_CKM.4)

104 The TSF shall destroy cryptographic key in accordance with a specified **cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*]**

6 TOE SECURITY ASSURANCE REQUIREMENTS

105 The Assurance requirement is EAL 4 augmented of additional assurance components as listed in the Protection Profile PP/9806.

Assurance Class	Assurance Family	Abbreviated Name	Component
Configuration Management	CM automation	ACM_AUT	**1**
	CM capabilities	ACM_CAP	**4**
	CM scope	ACM_SCP	**2**
Delivery and Operation	Delivery	ADO_DEL	**2**
	Installation, generation and start up	ADO_IGS	**1**
Development	Functional specification	ADV_FSP	**2**
	High Level Design	ADV_HLD	**2**
	Implementation representation	ADV_IMP	**2**
	Low Level Design	ADV_LLD	**1**
	Representation Correspondence	ADV_RCR	**1**
	Security Policy Model	ADV_SPM	**1**
Guidance Documents	Administrator guidance	AGD_ADM	**1**
	User guidance	AGD_USR	**1**
Life Cycle Support	Development Security	ALC_DVS	**2**
	Flaw Remediation	ALC_FLR	**1**
	Life cycle definition	ALC_LCD	**1**
	Tools and Techniques	ALC_TAT	**1**
Tests	Coverage	ATE_COV	**2**
	Depth	ATE_DPT	**1**
	Functional tests	ATE_FUN	**1**
	Independent testing	ATE_IND	**2**
Vulnerability Assessment	Misuse	AVA_MSU	**2**
	Strength of TOE SF	AVA_SOF	**1**
	Vulnerability analysis	AVA_VLA	**4**

Note: ▨ **Augmentation versus EAL4 level**

Table 6-1. Evaluation assurance level summary

7 TOE SUMMARY SPECIFICATION

7.1 LIST OF SECURITY FUNCTION

SF1: Security violation recording and reaction

106 These security function records in register the events notified by the detectors (refer to list below). The software configures the reaction:

- The TOE is immediately reset when an event is detected.
- Or, a flag is set

List of detectors:

- Abnormal voltage
- Abnormal frequency
- Abnormal temperature
- Light exposure
- Signal line decapsulation
- Power Glitch
- MET4 Dummy active line disconnection

Dependency on other SF:

- SF2 (Abnormal Voltage detection)
- SF3 (Abnormal frequency detection)
- SF4 (Abnormal Temperature detection)
- SF5 (Light detection)
- SF6 (Signal line decapsulation detection)
- SF7 (Abnormal Power Glitch detection)
- SF23 (MET4 Dummy active line disconnection detection)

SF2: Voltage detection

107 This security function detects out of range voltage events. The recording and the reaction (reset of the TOE) are managed by the security function SF1 (Security violation recording and reaction).

Dependency on other SF: none

SF3: Frequency detection

108 This security function detects out of range frequency events. The recording and the reaction (reset of the TOE) are managed by the security function SF1 (Security violation recording and reaction).

Dependency on other SF: none

SF4: Temperature detection

109 This security function detects out of range temperature events. The recording and the reaction (reset of the TOE) are managed by the security function SF1 (Security violation recording and reaction).

Dependency on other SF: none

SF5: Light detection

110 This security function detects out of range light events. The recording and the reaction (reset of the TOE) are managed by the security function SF1 (Security violation recording and reaction).

Dependency on other SF: none

SF6: Signal line decapsulation detection

111 This security function detects signal line decapsulation events. The recording and the reaction (reset of the TOE) are managed by the security function SF1 (Security violation recording and reaction).

Dependency on other SF: none

SF7: Power Glitch detection

112 This security function detects power glitch events. The recording and the reaction (reset of the TOE) are managed by the security function SF1 (Security violation recording and reaction).

Dependency on other SF: none

SF8: Internal variable clock

113 This security function selects an internal variable clock rather than the external clock. This function protects against power monitoring.

Dependency on other SF: none

SF9: Security registers access control

114 The TOE has three security control registers: MASCON, SECCON, and SECMOD (refer to functional specification document and guidance document for more details)

115 This security function manages access to the security control registers through access control security attributes. Write access is allowed only if the code is executed in the ROM.

116 The USER configuration has another function, which is write enable bit for security related registers. If user do not enable this bit in 128cycles after the reset, user can not write security control registers any more.

117 The attributes enforce the following access rights:

	TOE configuration	
Code execution from :	Access to security control registers in TEST configuration	Access to security control registers in USER configuration
TEST_ROM	R/W	No
USER_ROM	R/W	R/W
EEPROM	R	R

Table 7-1. Security registers access control

R: Read access

W: Write access

Dependency on other SF: none

SF10: Invalid address access

118 This function detects invalid address access occurrence. When an event is detected, a FIQ (Fast Interrupt Request) is granted and the FIQ processing starts.

119 The memory access rights are configured in the control register MASCON (refer SF 11) and MPU (Memory Protection Unit).

Dependency on other SF:

- SF11 (access rights for the code executed in EEPROM)

SF11: Access rights for the code executed in EEPROM

120 This security function manages the code execution in EEPROM, through access control security attributes. If an invalid access is detected, then a FIQ occurs (security function SF10).

Access Rights	Attributes
Code Execution in EEPROM	Enable / Disable
Data Access(Read) to ROM	Enable / Disable
Data Access(Read / Write) to RAM	Enabled

Table 7-2. Access rights for the code executed in EEPROM

121 If an invalid access is detected, then a FIQ occurs (security function SF10).

Dependency on other SF: none

SF12: Non reversibility of test configuration and user configuration

122 This function disables the TEST configuration and enables the USER configuration of the TOE. This function ensures the non-reversibility of the configuration. This function is used once in the factory.

Dependency on other SF: none

SF13: Address/Data bus scrambling

123 This function protects address / data bus from probing.

Dependency on other SF: none

SF14: Test configuration communication protocol and data commands

124 This function is the proprietary protocol used to operate the chip in TEST configuration. This function enforces the identification and authentication of the TEST administrator during the test phase of the manufacturing.

Strength of function (SOF): High

Dependency on other SF: none

SF15: Test

125 During the manufacturing, the operation of the TOE and the embedded software checksum are verified. This security function ensures the correct operation of the security functions and the integrity of the embedded software.

Dependency on other SF: none

SF16: High frequency filter

126 This security function is used to cut off extremely high range of frequencies on the external clock pin.

Dependency on other SF: none

SF17: Clock noise filter

127 This noise filter is used to prevent noise and glitches in the external clock line from causing undefined or unpredictable behavior of the chip.

Dependency on other SF: none

SF18: Reset noise filter

128 This noise filter is used to prevent noise and glitches in the external reset line from causing undefined or unpredictable behavior of the chip.

Dependency on other SF: none

SF19: Synthesizable processor core

129 This processor core is synthesizable with glue logic, which makes more difficulty in reverse engineering and signal identification.

Dependency on other SF: none

SF20: Data Encryption Standard engine

130 This function is used for encrypting and decrypting data using a DES.

Dependency on other SF: none

SF21:SuperMAPII Cryptographic coprocessor

131 This function is used for assistance in the acceleration of modulo exponentiations required in the RSA arithmetic.

Dependency on other SF: none

SF22: Random number generator

132 This function is used for generating random numbers for security process in the smart card application.

Dependency on other SF: none

SF23: MET4 Dummy active line disconnection detector

133 This function protects layouts from probing/FIB (Focused Ion Beam) attacks and detects disconnection of MET4 line. The recording and the reaction (reset of the TOE) are managed by the security function SF1 (Security violation recording and reaction).

Dependency on other SF: none

7.2 ASSURANCE MEASURE

Assurance Class	Assurance Family	Assurance Component	Assurance measure(document reference)
ACM: Configuration Management	ACM_AUT	1	Project APACHE-II Configuration Management Documentation (class ACM), Version 1.2, Issued on August 14, 2003 ACM_AUT1 is described in configuration management plan of this document
	ACM_CAP	4	Project APACHE-II Configuration Management Documentation (class ACM), Version 1.2, Issued on August 14, 2003 ACM_CAP4 is described in configuration list, configuration management plan and acceptance plan of this document
	ACM_SCP	2	Project APACHE-II Configuration Management Documentation(class ACM), Version 1.2, Issued on August 14, 2003 ACM_SCP2 is described in configuration list and configuration management plan of this document
ADO: Delivery and Operation	ADO_DEL	2	Project APACHE-II Delivery Procedures Documentation (class ADO), Version 1.0, Issued on June 18, 2004
	ADO_IGS	1	Project APACHE-II Installation, generation and start-up Procedures (class ADO), Version 1.0 Issued on June 18, 2004
ADV: Development	ADV_FSP	2	Project APACHE-II Functional Specification (Class ADV), Version 1.1, Issued on June 18, 2003
	ADV_HLD	2	Project APACHE-II High Level Design (Class ADV), Version 1.1, Issued on July 3, 2003
	ADV_LLD	1	Project APACHE-II Low Level Design (Class ADV), Version 1.2, Issued on February 9, 2004
	ADV_IMP	2	Project APACHE-II Implementation (Class ADV), Version 1.2, Issued on February 7, 2004
	ADV_RCR	1	All representation correspondence analyses are included in the relevant TOE representation documentation (FSP, HLD, LLD, IMP)
	ADV_SPM	1	Project APACHE-II (S3CC9RB) Security Policy Model (Class ADV), Version 1.0, Issued on May 12, 2003
AGD: Guidance Documents	AGD_ADM	1	Project APACHE-II Guidance Documentation (Class AGD), Version 1.4, Issued on February 16, 2004 Guidance Documentation is consists of: - C9PB / RB / P9 User's Manual 2.0 - C9PB / RB / P9 User's Manual Errata 1.0 - Security Application Note 1.5 - Programmer's Guide 1.3 - Test-Administrator Guidance 1.1
	AGD_USR	1	

Table 7-3. Assurance measures table

ALC: Life Cycle Support	ALC_DVS	**2**	Project APACHE-II Development Security Procedures(Class ALC), Version 1.0, Issued on June 18, 2003
	ALC_FLR	**1**	Project APACHE-II Flaw Remediation Procedures(Class ALC), Version 1.0, Issued on June 18, 2003
	ALC_LCD	**1**	Project APACHE-II Life Cycle Definition Documentation(Class ALC), Version 1.0, Issued on June 18, 2003
	ALC_TAT	**1**	Project APACHE-II Development Tool Documentation(Class ALC), Version 1.0, Issued on June 18, 2003
ATE: Tests	ATE_COV	**2**	Test Coverage Analysis(Class ATE), is described in Project APACHE-II Test Documentation(Class ATE) Version 1.1, Issued on August 13, 2003
	ATE_DPT	**1**	Test Depth Analysis(Class ATE) is described in Project APACHE-II Test Documentation(Class ATE) Version 1.1, Issued on August 13, 2003
	ATE_FUN	**1**	Project APACHE Test Documentation(Class ATE), Version 1.1, Issued on August 13, 2003
AVA: Vulnerability Assessment	AVA_MSU	**2**	Project APACHE-II Analysis of the Guidance Documentation (Class AVA) Version 1.0, Issued on June 5, 2003
	AVA_SOF	**1**	Project APACHE-II Strength of TOE SF Analysis (Class AVA) Version 1.0, Issued on June 5, 2003
	AVA_VLA	**4**	Project APACHE Vulnerability Analysis (Class AVA) Version 1.0, Issued on June 10, 2003

Table 7-3. Assurance measures table

8 PP CLAIMS

134 S3CC9RB conforms to requirements of PP / 9806.

135 There are two additional security objectives with respect to the ST:

O.CRYPTO arising from the organisational security policy OSP_CRYPTO. It is a TOE objective realised by the additional functional requirements FCS_COP.1 and FCS_CKM.1

O.KEY_DEST arising from the assumption A.KEY_DEST. It is an IT environment objective realised by the additional functional requirement FCS_CKM.4.

136 No additional assurance requirement is introduced.

9 RATIONALE

9.1 INTRODUCTION

137 This chapter presents the evidence used in the ST redaction. This evidence supports the claims that the ST is complete and coherent.

9.2 SECURITY OBJECTIVES RATIONALE

138 This section demonstrates that the stated security objectives address all of the security environment aspects identified.

9.2.1 Threats and security objectives

139 The following tables show which security objectives counter which threats phase by phase.

Phase 1

140 During Phase 1, the smart card embedded software is being developed and the IC pre-personalization requirements are specified. Phase 1 is outside the scope of this ST and only threats on the assets exchanged between the IC designer and the smart card embedded software developer are relevant to this ST.

141 Such threats are identified in sections 3.3.1 ad 3.3.2 of the ST: ·

- T.CLON,
- T.DIS_INFO,
- T.DIS_DEL,
- T.MOD_DEL,
- T.T_DEL.

142 Since the TOE is undo-construction during this phase, only security objectives for the environment are described during this phase.

143 Table 9-1 indicates that each to be countered threat during phase 1 is mapped to at least one security objective. No organizational security policy has to be considered.

Threats/Objecti	O.DEV_DIS	O.SOFT_DLV	O.DEV_TOOLS	O.SOFT_MECH
T.CLON	X	X	X	X
T.DIS_INFO	X			
T.DIS_DEL		X		
T.MOD_DEL		X		
T.T_DEL		X		

Table 9-1. Mapping of security objectives to threats at phase 1

144 O.DEV_DIS addresses all the threats on the assets transmitted from the IC designer to the smart card embedded software developer during the smart card development, which is the major concern of T.DIS_INFO. This objective also partially addresses the T.CLON threat since it requires well-defined and controlled procedures to the delivery of any IC proprietary assets.

145 O.SOFT_DLV addresses all the threats applicable to the delivery of the smart card embedded software to the IC designer since it requires the application of a trusted delivery and verification procedure (T.T_DEL) maintaining the integrity (T.MOD_DEL) and the confidentiality of the software if applicable (T.DIS_DEL, T.T_DEL).

146 The threats identified at phase 1 are countered by the security objectives in the way described above; nevertheless, T.CLON is partially countered by the four objectives which prevent the functional cloning of the TOE but can not avoid it completely.

Phase 2

147 Since the TOE is under construction during this phase (the IC is being developed), Only security objectives for the environment are described during this phase. There is also no assumption for this phase.

148 Table 9-2 shows the mapping of security objectives to threats during phase 2. T.T_PRODUCT and T.DIS_TEST are not applicable to this phase as referred by the Tab1e 3-1 of the ST. No organizational security policy has to be considered.

Threats/Objectives	O.SOFT _ACS	O.DESIGN _ACS	O.DSOFT _ACS	O.MASK _FAB	O.MECH _ACS	O.TI _ACS
T.CLON	X	X	X	X	X	X
T.DIS_DESIGN		X			X	X
T.DIS_SOFT	X					
T.DIS_DSOFT			X			
T.DIS_TOOLS		X				
T.DIS_PHOTOMASK				X		
T.T_SAMPLE		X				
T.T_PHOTOMASK				X		
T.MOD_DESIGN		X			X	X
T.MOD_DSOFT			X			
T.MOD_SOFT	X					
T.MOD_PHOTOMASK				X		

Table 9-2. Mapping of security objectives to threats at phase 2

149 O.SOFT_ACS addresses the threats T.DIS_SOFT and T.MOD_SOFT by restricting access to the smart card embedded software when delivered to the IC designer only to authorized personnel.

150 O.DESIGN_ACS addresses the threats T.DIS_DESIGN, T.DIS_TOOLS, T.MOD_DESIGN, T.T_SAMPLE by restricting access to the IC design assets only to authorized personnel.

151 O.MECH_ACS addresses the threat T.DIS_DESIGN ad T.MOD_DESIGN by limiting access to the hardware security mechanism specifications only to authorized personnel.

152 O.TI_ACS addresses the threats T.DIS_DESIGN, T.MOD_DESIGN by restricting access to the security relevant information on IC techno1ogy during the IC design to authorized personnel.

153 O.DSOFT_ACS addresses the threats T.DIS_DSOFT, T.MOD_DSOFT by restricting access to the IC dedicated software information only to authorized personnel.

154 O.MASK_FAB addresses T.DIS_PHOTOMASK, T.T_PHOTOMASK, T.MOD_PHOTOMASK by providing procedures to ensure the confidentiality and the integrity of the TOE during photomask fabrication and delivery between the IC manufactured and the photomasks manufacturer.

155 The T.CLON threat is partially countered by a11 of the objectives described above since they limit the possibility to access any sensitive relevant information of the TOE during phase 2.

Phases 3 to 7

Security objectives for the environment at phase 3

156 At phase 3, the TOE is constructed and tested then operational. Security objectives for the environment have been developed for phase 3 and address the TOE environment during this phase.

157 This section explains the mapping of security objectives for the environment to threats during the manufacturing process, as detailed in Tab1e 9-3. The mapping of TOE security objectives to threats during phase 3 is described in Table 9-4.

Threats/Objectives	O.TOE_PRT	O.IC_DLV
T.CLON	X	X
T.DIS_DESIGN	X	
T.DIS_SOFT	X	
T.DIS_DSOFT	X	
T.DIS_TEST	X	
T.DIS_TOOLS	X	
T.DIS_PHOTOMASK	X	
T.T_SAMPLE	X	X
T.T_PHOTOMASK	X	
T.T_PRODUCT	X	X
T.MOD_DESIGN	X	
T.MOD_DSOFT	X	
T.MOD_SOFT	X	
T.MOD_PHOTOMASK	X	

Table 9-3. Mapping of security objectives for the environment to threats at phase 3

158 O.TOE_PRT addresses all the threats by ensuring the protection of the TOE during the manufacturing process, pre-personalization and testing, since it provides a security system applicable to the IC manufacturing and testing phase to ensure the confidentiality and integrity of the TOE.

159 O.IC_DLV addresses the threats T.T_SAMPLE, T.T_PRODUCT by providing a well-defined and controlled delivery procedure of the TOE.

160 The T.CLON threat is partial countered by all of the objectives described above since they limit the possibility access any sensitive relevant information on the TOE during the manufacturing and testing phase (phase 3).

TOE security objectives from phase 3 to 7

161 The Table 9-4. maps the TOE security objectives to the threats identified at phase 3 to 7.

Threats/ Objectives	O. TAMPER	O. CLON	O. OPERATE	O. FLAW	O.DIS_MECHANISM	O.DIS_ MEMORY	O.MOD_ MEMORY
T.CLON		X					
T.DIS_DESIGN	X				X		
T.DIS_SOFT	X					X	
T.DIS_DSOFT	X					X	
T.DIS_TEST	X					X	
T.T_SAMPLE			X				
T.T_PRODUCT			X				
T.MOD_DESIGN	X		X	X			
T.MOD_DSOFT	X		X	X			X
T.MOD_SOFT	X		X	X			X

Table 9-4. Mapping TOE security objectives to threats at phase 3 to 7

162 O.TAMPER addresses the threats T.DIS_DESIGN, T.DIS_SOFT, T.DIS_DSOFT, TDIS_TEST, T.MOD_DESIGN, T.MOD_DSOFT, T.MOD_SOFT by ensuring the integrity protection of the security critical parts of the TOE and protecting them any disclosure.

163 O.CLON addresses the threat T.CLON.

164 O.OPERATE addresses the threats T.T_SAMPLE, T.T_PRODUCT, T.MOD_DESIGN, T.MOD_DSOFT, T.MOD_SOFT by providing the TOE protection against unauthorized use (modification of the TOE or theft as an example)

165 O.FLAW addresses the threats T.MOD_DESIGN, T.MOD_DSOFT, T.MOD_SOFT by preventing any unauthorized modification of the TOE during its design, production or operation.

166 O.DIS_MECHANISM addresses the threats T.DIS_DESIGN by preventing any unauthorized disclosure of the hardware security mechanisms.

167 ODIS_MEMORY addresses the meats T.DIS_SOFT, T.DIS_DSOFT, T.DIS_TEST by protecting all information contained in memories from unauthorized access.

168 O.MOD_MEMORY addresses the threats T.MOD_DSOFT, T.MOD_SOFT by protecting all information contained in memories from any unauthorized modification.

169 It has to be noted that the threats T.DIS_TOOLS, T.T_PHOTOMASK, T.DIS_PHOTOMASK, T.MOD_PHOTOMASK are countered by security objectives for the environment during the manufacturing and testing phase (phase 3).

9.2.2 Assumptions and security objectives

170 The following tables show which security objectives counter which threats phase by phase.

Phase 1

171 Table 9-5 indicates the relationships between assumptions and security objective for the environment. It shows that each assumption is covered by at least one security objective for the environment.

Assumptions/ Objectives	O.DEV_DIS	O.SOFT_DLV	O.DEV_TOOLS	O.SOFT_MECH
A.SOFT_ARCHI			X	X
A.DEV_ORG		X	X	

Table 9-5. Mapping TOE security objectives to assumptions at phase 1

TOE delivery process (phase 4 to 7)

172 Table 9-6 indicates the relationships between assumptions and security objective for the environment. It shows that each assumption is covered by at least one security objective for the environment.

Assumptions/ Objectives	O.DLV_PROTECT	O.DLV_AUDIT	O.DLV_RESP
A.DLV_PROTECT	X		
A.DLV_AUDIT		X	
A.DLV_RESP			X

Table 9-6. Mapping of security objectives to assumptions at phase 4 to 7

Phase 4 to 6

173 Table 9-7 indicates the relationships between assumptions and security objectives for the environment. It shows that each assumption is covered by at least one security objective for the environment.

Assumptions/ Objectives	O.TEST_OPERATE
A.USE_TEST	X
A.USE_PROD	X

Table 9-7. Mapping of security objectives to assumptions at phase 4 to 6

Phase 7

174 Table 9-8 indicates the relationships between assumptions and security objectives for the environment at phase 7. It shows that each assumption is covered by at least one security objective for the environment.

Assumptions/ Objectives	O.USE_SYS	O.USE_DIAG	O.KEY_DEST
A.USE_SYS	X		
A.USE_DIAG		X	
A.KEY_DEST			X

Table 9-8. Mapping of security objectives to assumptions at phase 7

9.2.3 Cryptographic OSP and security objectives (phase 4 to 7)

175 Table 9-9 indicates the relationships between Cryptographic OSP and security objectives for the TOE. It shows that each OSP is covered by at least one security objective for the TOE.

Cryptographic OSP /Objectives	O.CRYPTO
OSP_CRYPTO	X

Table 9-9. Mapping of security objectives to OSP at phase 7

9.3 SECURITY REQUIREMENTS RATIONALE

176 The security requirement rationale shall demonstrate that the set of security requirements (TOE and environment) is suitable to meet the security objectives.

9.3.1 Security functional requirements rationale

177 This section demonstrates that the combination of the security requirements is suitable to satisfy the identified TOE security objectives.

178 Each of the TOE security objectives is addressed by either functional or assurance requirements

179 The following table demonstrates which requirements contribute to the satisfaction of the satisfaction of the TOE and IT-environment security objective.

Requirements	O.TAMPER	O. CLON	O.OPERATE	O. FLAW	O.DIS_MECHANISM	O.DIS_MEMORY	O.MOD_MEMORY	O. CRYPTO	O.KEY_DEST
EAL4 requirements				X					
FIA_UAU.2(phase 3)	X	Partial	X		X	X	X		
FIA_UID.2(phase 3)	X	Partial	X		X	X	X		
FIA_ATD.1(phase 3)	X	Partial	X		X	X	X		
FPT_TST.1(phase 3)			X				X		
FDP_SDI.1(phase 3)							X		
FMT_MOF.1			X						
FMT_MSA.1			X						
FMT_SMR.1			X						
FMT_MSA.3			X						
FDP_ACC.2		Partial	X		X	X	X		
FDP_ACF.1		Partial	X		X	X	X		
FDP_IFC.1		Partial	X		X	X	X		
FDP_IFF.1		Partial	X		X	X	X		
FAU_SAA.1		Partial	X						
FPR_UNO.1	X	Partial	X		X	X			
FPT_PHP.2	X	Partial	X		X	X	X		
FPT_PHP.3	X	Partial	X		X	X	X		
FCS_COP.1								X	
FCS_CKM.1								X	
FCS_CKM.4									X

Table 9-10. Mapping of security requirements and TOE security objectives

180 This section describes why the security requirements are suitable to meet each of the TOE security objectives.

181 The EAL4 assurance requirements contribute to the satisfaction of the O.FLAW security objective. They are suitable because they provide the assurance that the TOE is designed, implemented and operates so that the IT functional requirements are correctly provided.

182 At phase 3 (testing phase), the identification and authentication functions (FIA_UAU.2, FIA_UID.2, FIA_ATD.1) are necessary to ensure that the testing operations of the TOE are done under control and that only authorized employees/processes will be able to run the testing operations of the TOE. This set of functional requirements is required by all the TOE security objectives during this phase. FIA_UID.2, FIA_ATD.1, FIA_UAU.2 provide the capability to identify and authenticate the user prior to performing any functions for the user.

183 The objective O.CLON is partially countered by the functional requirements listed in the Table 9-9 since they provide the capability to limit the operations on the TOE to a set of authorized operations by authorized users, but in fact, this objective would require a specific function to avoid the functional cloning of the TOE which is in fact not the case.

184 At phase 3, FPT_TST.1 ensures the correct operation of security functions by providing security functionalities testing during phase 3, required by the objective O.OPERATE and O.MOD_MEMORY (integrity of TOE security functions data that are stored in memories). This is important for the TOE especially for the security controls when changing from phase 3 to the others.

185 At phase 3, FDP_SDI.1 provides protection against integrity errors that may affect all user information stored in memories, required by the O.MOD_MEMORY objective.

186 At all phases, FAU_SAA.1 provides the capability of indicating a potential violation of the TOE Security Policy. The rules defined by the TOE Security Policy could be different at phase 3 compared to phases 4 to 7. This security function works in support of the O.OPERATE.

187 At all phases, FDP_ACC.2 will provide the protection of all information contained in memories and of the hardware security mechanisms, required by the objectives O.DIS_MEMORY, O.MOD_MEMORY, O.DIS_MECHANISM and O.OPERATE. The rules defined by the Access control security functions policy could be different at phase 3 compared to phases 4 to 7. FDP_ACF.1 enforces also these objectives. For the IC dedicated software, FDP_IFC.1 and FDP_IFF.1 are a1so applicable to provide the capability to ensure a subset information flow control, required by the objectives listed above.

188 At all phases the functions FMT_MOF.1, FMT_MSA.1, FMT_SMR.1, FMT_MSA.3 provide the administration of security functions and security attributes during all the phases, required by the O.OPERATE objective. This is a major concern for the TOE especially for the changes from one phase to another under the TOE control.

189 At all phases the unobservability functional requirement FPR_UNO. 1 provides the protection against unauthorized disclosure and use of sensitive information, required by the objectives O.TAMPER, O.OPERATE, O.DIS_MEMORY, O.DIS_MECHANISM since unobservability ensure that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used. There is no potential conflict with identification and authentication requirement (FIA_UAU.2, FIA_UID.2 and FIA_ATD.1) because there is only one authenticated user at a time and internal operations on behalf of that user shall not be observable for unauthorized users.

190 At all phases, FPT_PHP.2 provide the capability to notify physical attacks to some extents, required, due to the TOE definition, by all the objectives.

191 At all phases, FPT_PHP.3 provides the capability to resist to physical attacks, required, due to the T0E definition, by all the objectives.

192 At phase 4 to phase 7, FCS_COP.1 provides cryptographic operations in accordance with specified cryptographic algorithm and cryptographic key sizes.

193 At phase 4 to phase 7, FCS_CKM.1 provides cryptographic key generation in accordance with specified cryptographic algorithm and cryptographic key sizes.

194 At phase 7, FCS_CKM.4 provides cryptographic key destruction in accordance with specified cryptographic destruction method.

9.3.2 Security functional requirements dependencies

195 This section demonstrates that all dependencies between security functional requirements components included in this ST are satisfied.

196 The following table lists all functiona1 components, with a numeric number. The dependencies of each component are listed alongside that component with a reference to the line number of the component, which satisfies them. Component reference line numbers followed by (H) indicate that the dependency is satisfied by a hierarchical component to that referenced.

Number	NAME	Dependent	Line number
1	FIA_UAU.2	FIA_UID.1	H(2)
2	FIA_UID.2	No dependencies	-
3	FIA_ATD.1	No dependencies	-
4	**FPT_TST.1**	**FPT_AMT.1**	**See Reference [B]**
5	FDP_SDI.1	No dependencies	-
5	FAU_SAA.1	**FAU_GEN.1**	**See Reference [A]**
6	FMT_MOF.1	FMT_SMR.1	8
7	FMT_MSA.1	FMT_SMR.1,FDP_ACC.1 or FDP_IFC.1	8,H(10),12
8	FMT_SMR.1	FIA_UID.1	H(2)
9	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	7,8
10	FDP_ACC.2	FDP_ACF.1	11
11	FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	H(10),9
12	FDP_IFC.1	FDP_IFF.1	13
13	FDP_IFF.1	FDP_IFC.1, FMT_MSA_3	12,9
14	FPR_UNO.1	No dependencies	-
15	FPT_PHP.2	FMT_MOF.1	6
16	FPT_PHP.3	No dependencies	-
17	FCS_COP.1	FDP_ITC.1 or FCS_CKM.1, FCS_CKM.4 FMT_MSA.2	-
18	FCS_CKM.1	FDP_ITC.1 or FCS_COP.1, FCS_CKM.4 FMT_MSA.2	-
19	FCS_CKM.4	FDP_ITC.1 or FCS_COP.1, FCS_CKM.1 FMT_MSA.2	-

Table 9-11. Functional dependencies analysis

197 Tab1e 9-11. shows that the functiona1 components dependencies are satisfied by any functional components of the ST except for the components stated in bold characters, which are discussed hereafter.

Reference [Al:

198 The dependency of FAU_SAA.1 with FAU_GEN.1 is not applicable to the TOE; the FAU_GEN component forces many security relevant events to be recorded (due to dependencies with other functional security components) and this is not achievable to a smart card IC considering state of the art implementation. It is then assumed that the function FAU_SAA.1 may still be used and the specific audited events will have to be defined in the ST independently with FAU_GEN.1.

Reference [B]:

199 The dependency of FPT_TST.1 with FPT_AMT.1 is not clearly relevant for a smart card IC; FPT_TST.1 is self-consistent for the TOE (hardware and firmware) and does not require the FPT_AMT.1 function (Abstract Machine Testing) which seems to be more appropriate for operating systems TOEs.

9.3.3 Strength of functional level rationale

200 Due to the definition of the TOE, it is very important that the claimed SOF should be high since the product critical security mechanisms have to be only defeated by attackers possessing a high level of expertise, opportunity and resources, successful attack being judged to be beyond normal practicality.

9.3.4 Security assurance requirements rationale

201 The assurance requirements of the Security Target are summarised in the following table 9-12.

Requirements	Name	Type
EAL4	Methodically Designed, Tested and Reviewed	Assurance level
ADV_IMP.2	Implementation of the TSF	Higher hierarchical component
ADV_DVS.2	Sufficiency of security measures	Higher hierarchical component
AVA_VLA.4	Highly resistant	Higher hierarchical component

Table 9-12. ST Assurance requirements

Evaluation assurance level rationale

202 An assurance level of EAL4 is required for this type of TOE since it is intended to defend against sophisticated attacks. This evaluation assurance level was selected since it is designed to permit a developer to gain maximum assurance from positive security engineering based on good commercial practices. EAL4 represents the highest practical level of assurance expected for a commercial grade product. In order to provide a meaningful level of assurance that the TOE provides an adequate level of defense against such attacks, the evaluator should have access to the low-level design and source code.

203 The assurance level EAL4 is achievable, since it requires no specialist techniques on the part of the developer.

Assurance augmentations rationale

204 Additional assurance requirements are also required due to the definition of the TOE.

ADV_IMP.2 Implementation of the TSF

205 The implementation representation is used to express the notion of the least abstract representation of the TSF, specifically the one that is used to create the TSF itself without further design refinement. IC dedicated software source code and IC hardware drawings are examples of TSF implementation representation.

206 This assurance component is a higher hierarchical component to EAL 4 (only ADV_IMP.1). It is important for a smart card IC that the evaluator evaluates the implementation representation of the entire TSF and determines if the functional requirements in the Security Target are addressed by the representation of the TSF.

207 ADV_IMP.2 has dependencies with ADV_LLD.1 "Descriptive Low Level design ", ADV_RCR.1 "Informal correspondence demonstration", ALC_TAT.1 "Well defined development tools". These assurance components are included in EAL4, then these dependencies are satisfied.

ALC_DVS.2 Sufficiency of security measures

208 Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE.

209 This assurance component is a higher hierarchical component to EAL4 (only ALC_DVS.1). Due to the nature of the TOE, there is a need for any justification of the sufficiency of these procedures to protect the confidentiality and integrity of the TOE.

210 ALC_DVS.2 has no dependencies.

AVA_VLA.4 Highly resistant

211 Due to the definition of the TOE, it must be shown to be highly resistant to penetration attacks.

212 This assurance requirement is achieved by the AVA_VLA.4 component. Independent vulnerability analysis is based on highly detailed technical information. The attacker is assumed to be thoroughly familiar with the specific implementation of the TOE. The attacker is presumed to have a high level of technical sophistication.

213 AVA_VLA.4 has dependencies with ADV_FSP.1 "Informal functional specification", ADV_HLD.2 "Security enforcing high-level design", ADV_LLD.1 "Descriptive low-1evel design", ADV_IMP.1 "Subset of the implementation of the TSF", AGD_ADM.1 "Administrator Guidance", AGD-USR.1 "User Guidance". All these dependencies are satisfied by EAL4.

9.3.5 Security requirements are mutually supportive and internally consistent

214 The purpose of this part of the ST Rationale is to show that the security requirements are mutually supportive and internally consistent.

215 EAL4 is an established set of mutual-supportive and internally consistent assurance requirements.

216 The dependencies analysis for the additional assurance components in the previous section has shown that the assurance requirements are mutually supportive and internally consistent (all the dependencies have been satisfied).

217 The dependencies analysis for the functional requirements described above demonstrates mutual support and internal consistency between the functional requirements.

218 Inconsistency between functional and assurance requirements can only arise if there are functional-assurance dependencies that are not met, a possibility which has been shown not to arise.

9.4 THE TOE SUMMARY SPECIFICATION RATIONALE

(Table for relationship between security function and functional requirement)

219 The following table shows that the set of Security Functions covers all Functional Requirements:

SR SF	FIA_UAU.2	FIA_UID.2	FIA_ATD.1	FPT_TST .1	FDP_SDI.1	FMT_MOF 1	FMT_MSA.1	FMT_SMR.1	FMT_MSA.3	FDP_ACC.2	FDP_ACF .1	FDP_I FC.1	FDP_I FF. 1	FAU_SAA.1	FPR_UNO.1	FPT_PHP.2	FPT_PHP.3	FCS_COP.1	FCS_CKM.1
SF1														✓					
SF2																✓	✓		
SF3																✓	✓		
SF4																✓	✓		
SF5																✓	✓		
SF6																✓	✓		
SF7																✓	✓		
SF8															✓				
SF9												✓	✓						
SF10														✓					
SF11										✓	✓								
SF12			✓			✓	✓	✓	✓			✓	✓						
SF13															✓				
SF14	✓	✓																	
SF15				✓	✓														
SF16																	✓		
SF17																	✓		
SF18																	✓		
SF19															✓				
SF20																		✓	
SF21																		✓	✓
SF22																		✓	
SF23															✓	✓	✓		

Table 9-13. Relationship between security function and functional requirement

220 The combination of security function SF1 to SF23 works together to satisfy the security requirements of the ST. The use of any security function does not disable any other security function. The following table summarizes the dependencies between security functions:

Dependency on: SF	sf1	sf2	sf3	sf4	sf5	sf6	sf7	sf8	sf9	sf10	sf11	sf12	sf13	sf14	sf15	sf16	sf17	sf18	sf19	Sf20	Sf21	Sf22	Sf23
SF1		✓	✓	✓	✓	✓	✓																✓
SF2																							
SF3																							
SF4																							
SF5																							
SF6																							
SF7																							
SF8																							
SF9																							
SF10											✓												
SF11																							
SF12																							
SF13																							
SF14																							
SF15																							
SF16																							
SF17																							
SF18																							
SF19																							
SF20																							
SF21																							
SF22																							
SF23																							

Table 9-14. Security function dependencies

User authentication before any action (FIA_UAU.2)

221 The security function:

- SF14 : Test configuration communication protocol and test commands

Enforces the TEST administrator authentication before any action in TEST configuration.

222 This Security Function contributes to the TOE security objective (Highly resist).

User identification before any action (FIA_UID.2)

223 The security function:

- SF14 : Test configuration communication protocol and test commands

Enforces the TEST administrator authentication before any action in TEST configuration.

224 This Security Function contributes to the TOE security objective (Highly resist).

User attribute definition (FIA_ATD.1)

225 The security function:

- SF12: Non reversibility of test configuration and user configuration

Maintains the TOE configuration security attributes.

TOE security function testing (FPT_TST.1)

226 The security function:

- SF15: Test

Demonstrates the correct operation of the TOE security functions.

Stored data integrity monitoring (FDP_SDI.1)

227 The security function:

- SF15: Test

Monitors and verifies the integrity of the user data stored in the TOE.

Management of security function behavior (FMT_MOF.1)

228 The security function:

- SF12: Non reversibility of test configuration and user configuration

Restricts the ability to enable the function TOE configuration to the TEST administrator.

Management of security attributes (FMT_MSA.1)

229 The security function:

- SF12: Non reversibility of test configuration and user configuration

Enforces the information flow control to restrict the ability to change the security attributes, to the TEST administrator.

Management of security attributes (FMT_SMR.1)

230 The security function:

- SF12: Non reversibility of test configuration and user configuration

Maintains the roles of TEST administrator and USER.

Static attribute initialization (FMT_MSA.3)

231 The security function:

- SF12: Non reversibility of test configuration and user configuration

Enforce the information flow control security functions policy.

Complete access control (FDP_ACC.2)

232 The security function:

- SF11: Access rights for the code executed in EEPROM

Enforce the memory access control.

Security attribute based access control (FDP_ACF.1)

233 The security function:

- SF11: Access rights for the code executed in EEPROM

Enforce the memory access control.

Subset information flow control (FDP_IFC.1)

234 The security function:

- SF9: Security registers access control
- SF12: Non reversibility of test configuration and user configuration

Enforce the information flow control, based on the TOE configuration.

Simple security attributes (FDP_IFF.1)

235 The security function:

- SF9: Security registers access control
- SF12: Non reversibility of test configuration and user configuration

Enforce the information flow control, based on the TOE configuration.

Potential violation analysis (FAU_SAA.1)

236 The security function:

- SF1: Security violation recording and reaction
- SF10: Invalid address access

Cover the potential violation events listed in Table 5-8.

Unobservability (FPR_UNO.1)

237 The security function:

- SF8: Internal variable clock.
- SF13: Address/Data bus scrambling
- SF19: synthesizable processor core
- SF23: MET4 Dummy active line

Protect against the observability of the operation of the TOE.

Notification of Physical attack (FPT_PHP.2)

238 The security function:

- SF2: Voltage detection
- SF3: Frequency detection
- SF4: Temperature detection
- SF5: Light detection
- SF6: Signal line decapsulation detection
- SF7: Power glitch detection
- SF23: MET4 Dummy active line attack detection

Cover the potential violation events listed in Table 5-9.

Resistance to Physical attack (FPT_PHP.3)

239 The security function:

- SF2: Voltage detection
- SF3: Frequency detection
- SF4: Temperature detection
- SF5: Light detection
- SF6: Passivation decapsulation detection
- SF7: Power Glitch detection
- SF13: Address/Data bus scrambling
- SF16: High frequency filter
- SF17: Clock noise filter
- SF18: Reset noise filter
- SF23: MET4 Dummy active layer

Cover the potential violation events listed in Table 5-10.

Cryptographic operation (FCS_COP.1)

240 The security function:

- SF20: Data Encryption Standard engine
- SF21: SuperMAPII cryptographic coprocessor
- SF22: Random number generator

Enhanced the cryptographic operation.

Cryptographic key generation (FCS_CKM.1)

241 The security function:

- SF21: SuperMAPII cryptographic coprocessor

Enhanced the cryptographic key generation.

242 The assurance measures of “**Table 7-3. Assurance measures table**” are compliant with the Evaluation Assurance Level 4 (Common Criteria, version 2.l, issue August 1999, part3, paragraph 196) augmented by ADV_IMP.2 (Implementation representation), ALC_DVS.2 (Sufficiency of security measure) and AVA_VLA.4 (Highly resistant).

243 The augmentation is chosen to include in the scope of the evaluation, independent penetration tests.

244 The dependencies of the assurance components ACM_CAP, ADO_IGS, ADV_FSP, ADV_RCR, AGD_ADM, AGD_USR, ATE_IND are compliant with the CC, part 3.

245 Security Function SF14 is the unique function which, through its use of a permutational or probabilistic mechanism, could be subject to a direct attack. It claims a SOF level: SOF_High. The level is chosen as "High" because the TOE, for its uncontrolled user environment which eases attack opportunities, must not be defeated by attackers even with high attack resources."

9.5 THE PP CLAIMS RATIONALE

246 The present ST conforms to requirements of PP / 9806.

ANNEX A

GLOSSARY

Application Software (AS)

Is the part of ES in charge of the Application of the Smart Card IC.

Basic Software (BS)

Is the part of ES in charge of the generic functions of the Smart Card IC such as Operating System, general routines and Interpreters.

DAC

Discretionary Access Control

Dedicated Software (DS)

Is defined as the part of ES provided to test the component and/or to manage specific functions of the component.

Embedded Software (ES)

Is defined as the software embedded in the Smart Card Integrated Circuit. The ES may be in any part of the non-volatile memories of the Smart Card IC.

Embedded software developer

Institution (or its agent) responsible for the Smart Card embedded software development and the specification of pre-personalization requirements.

Initialization

Is the process to write specific information in the NVM during IC manufacturing and testing (phase 3) as well as to execute security protection procedures by the IC manufacturer. The information could contain protection codes or cryptographic keys.

Initialization Data

Specific information written during manufacturing or testing of the TOE

Integrated Circuit (IC)

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

IC designer

Institution (or its agent) responsible for the IC development.

IC manufacturer

Institution (or its agent) responsible for the IC manufacturing, testing, and pre-personalization.

IC packaging manufacturer

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

Personaliser

Institution (or its agent) responsible for the Smart Card personalization and final testing.

Personalization data

Specific information in the NVM during personalization phase

RBAC

Role-Based Access Control

Security Information

Secret data, initialization data or control parameters for protection system)

Smart Card

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

Smart Card Issuer

Institution (or its agent) responsible for the Smart Card product delivery to the Smart Card end-user.

Smart Card product manufacturer

Institution (or its agent) responsible for the Smart Card product finishing process and testing.

Smart Card Application Software (AS)

is the part of ES dedicated to the applications

ABBREVIATIONS

CC

Common Criteria

EAL

Evaluation Assurance Level

IT

Information Technology

PP

Protection Profile

SF

Security Function

SOF

Strength of Function

ST

Security Target

TOE

Target of Evaluation

TSC

TSF Scope of Control

TSF

TOE Security Functions

TSFI

TSF Interface

TSP

TOE Security Policy