Common Criteria
Information Technology
Security Evaluation

S3CC9PB

Security Target Lite

Version 0.1

November 29, 2002

SAMSUNG
ELECTRONICS

CONTENTS

1 ST INTRODUCTION

1.1 ST IDENTIFICATION

Title: S3CC9PB Security Target (ST-Lite)

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.

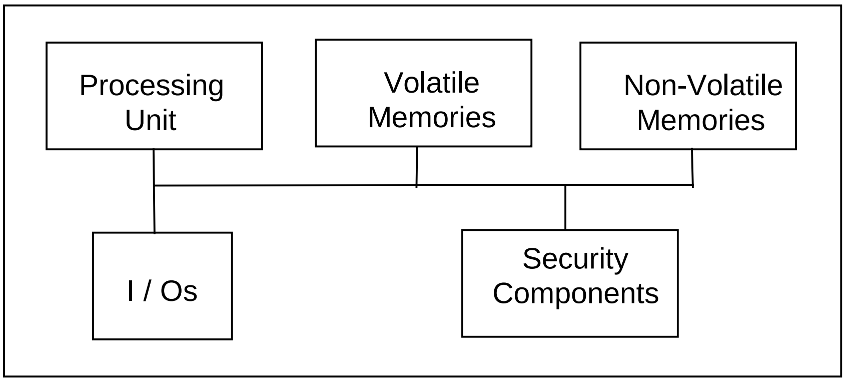

Figure 2-1. Smart card chip block diagram

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.

The TOE submitted to the evaluation comprises the following components:

TOE component	Reference
S3CC9PB	S3CC9PBX01
S3CC9PB dedicated software	S3CC9PB TEST ROM code, version 1.0
S3CC9PB Cryptography library	Cryptography library , version 1.0

Table 2-1. TOE hardware and software components

2.2 SMART CARD PRODUCT LIFE-CYCLE

10 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

11 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.

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

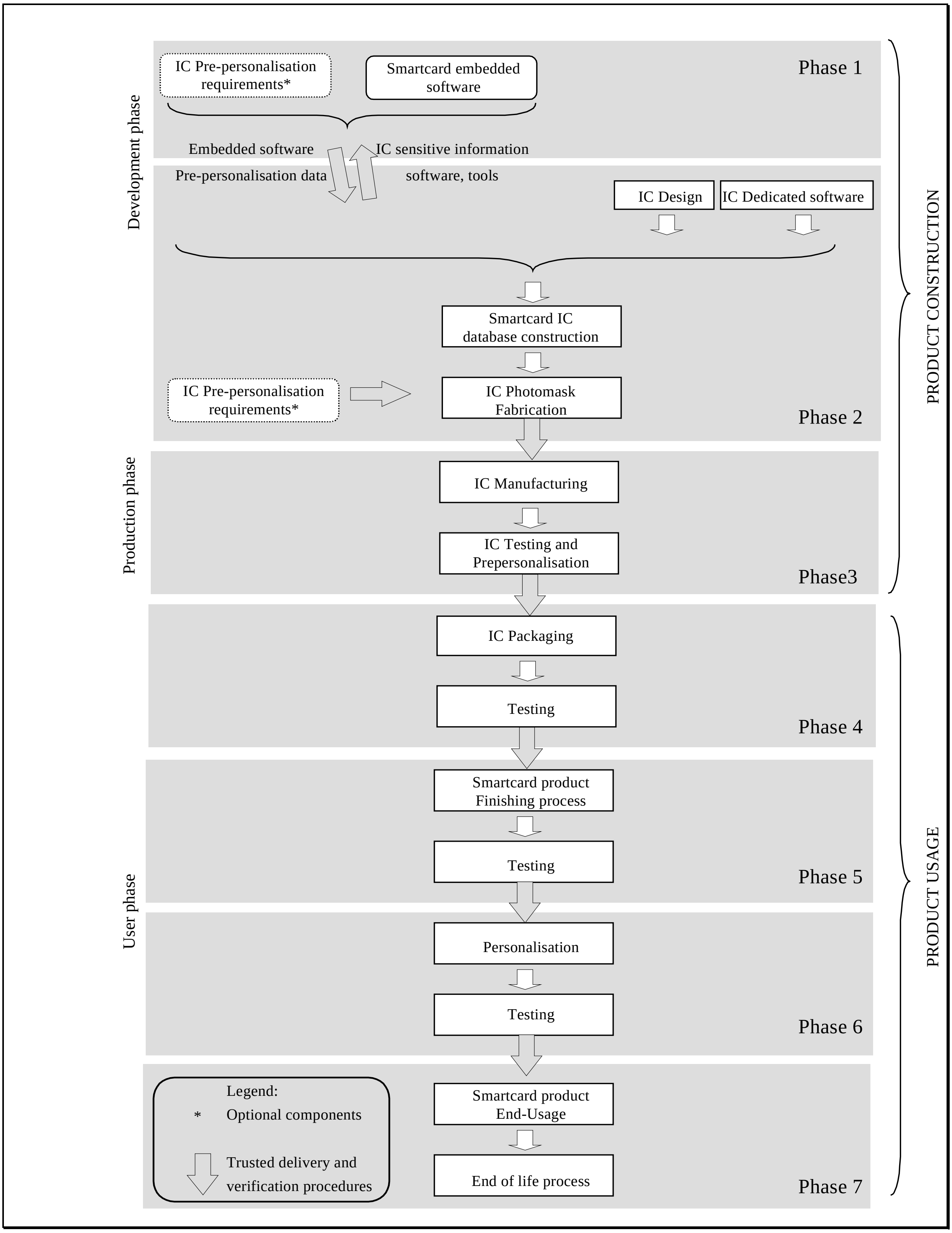

Figure 2-2. Smart card product life-cycle

13 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.

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

15 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 2-3. TOE configurations

2.3 TOE ENVIRONMENT

16 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

17 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.

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

19 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).

20 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

21 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.

22 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

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

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

<u>End-user environment (phase 7)</u>

25 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.

26 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

27 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.

28 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

29 The TOE IT Security functionalities consist of data storage and processing such as:

- arithmetical functions (e.g. incrementing counters in electronic purse, calculating currency conversion in electronic purse…),
- data communication,
- cryptographic operations (e.g. date encryption, digital signature)

2.5.2 TOE Block Diagram

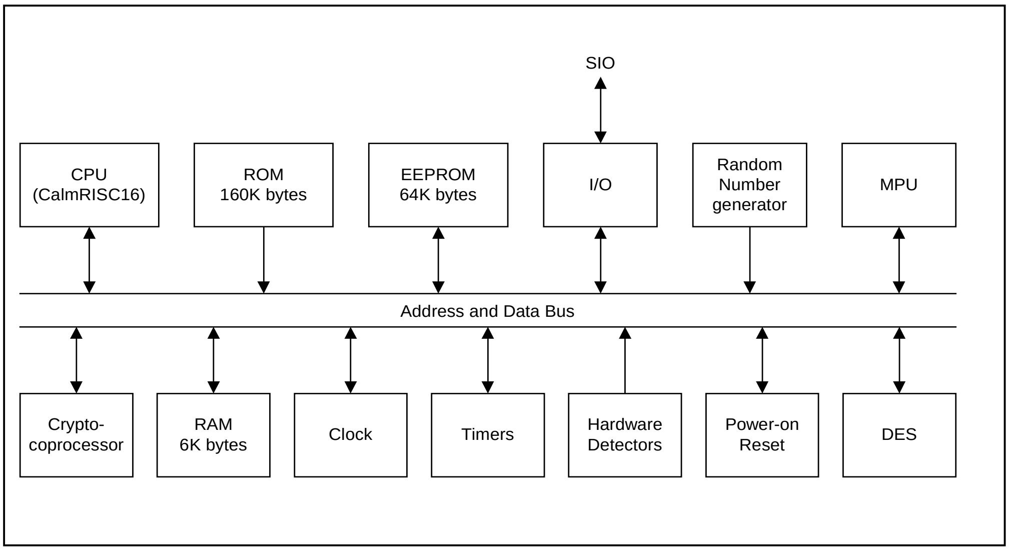

Figure 2-3. S3CC9PB Block diagram

3 TOE SECURITY ENVIRONMENT

30 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

31 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.
- The TOE itself is therefore an asset.

32 The TOE itself is therefore an asset.

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

3.2 ASSUMPTIONS

34 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.

35 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)

36 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

37 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.

38 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)

39 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.

40 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

41 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

42 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

43 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

44 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.

45 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_PHOTOMAS		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_PHOTOMA		Class II	Class I/II				

Table 3-1. Threats and phases

3.4 ORGANIZATIONAL SECURITY POLICIES

46 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

47 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

48 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.

4.2.2 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

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

50 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)

51 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)

52 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)

53 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)

54 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.

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

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

5.1.1.5 Stored Data Integrity Monitoring (FDP_SDI.1)

57 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)

58 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)

59 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 administrator.

5.1.2.3 Security roles (FMT_SMR.1)

60 The TOE security functions shall maintain the rols of TEST administrator and user.

5.1.2.4 Static Attribute Initialisation (FMT_MSA.3)

61 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.

62 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.

5.1.2.5 Complete Access Control (FDP_ACC.2)

63 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.

64 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.

65 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)

66 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)

5.1.2.6 Security Attribute Based Access Control (FDP_ACF.1)

67 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.

68 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)

69 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.

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

5.1.2.7 Subset Information Flow Control (FDP_IFC.1)

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

5.1.2.8 Simple Security Attributes (FDP_IFF.1)

72 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**.

73 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.**

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

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

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

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

5.1.2.9 Potential Violation Analysis (FAU_SAA.1)

78 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.

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

a) Accumulation or combination of **abnormal evironments or physical tampering** would indicate a potential security violation.

5.1.2.10 Unobservability (FPR_UNO.1)

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

5.1.2.11 Notification of Physical Attack (FPT_PHP.2)

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

82 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.

83 For **memory access, voltage, frequency, temperature, light** and **probing**, the TOE security functions shall monitor the devices and notify the user when physical tampering with the TOE security functions’ devices or TOE security functions' elements has occurred.

5.1.2.12 Resistance to Physical Attack (FPT_PHP.3)

84 The TOE security functions shall resist **the physical tampering** to the **TOE and its security functions** by responding automatically such that the TOE security policy is not violated.

5.1.2.13 Cryptographic operation (FCS_COP.1)

85 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.

5.1.2.14 Cryptographic key management (FCS_CKM.1)

86 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.

5.2 FUNCTIONAL REQUIREMENTS ENFORCED BY THE IT ENVIRONMENT

87 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)

88 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

89 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

90 These security functions records in register the events notified by the SF2: Voltage detection, SF3: Frequency detection, SF4: Temperature detection, SF5: Light detection, SF6: Signal line decapsulation detection, SF7: Power Glitch detection and SF23: MET4 Dummy active line disconnection detector.

SF8: Internal variable clock

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

SF9: Security registers access control

92 This security function manages access to the security control registers through access control security attributes.

SF10: Invalid address access

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

SF11: Access rights for the code executed in EEPROM

94 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).

SF12: Non reversibility of test configuration and user configuration

95 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.

SF13: Address/Data bus scrambling

96 This function protects address/data bus from probing.

SF14: Test configuration communication protocol and data commands

97 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.

SF15: Test

98 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.

SF16: High frequency filter

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

SF17: Clock noise filter

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

SF18: Reset noise filter

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

SF19: Synthesizable processor core

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

SF20: Data Encryption Standard engine

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

SF21: Cryptographic coprocessor

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

SF22: Random number generator

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

7.2 ASSURANCE MEASURE

Assurance Class	Assurance Family	Assurance Component	Assurance measure(document reference)
ACM: Configuration Management	ACM_AUT	1	S3CC9PB Configuration Management Documentation(class ACM) ACM_AUT1 is described in configuration management plan of this document
	ACM_CAP	4	S3CC9PB Configuration Management Documentation(class ACM) ACM_CAP4 is described in configuration list, configuration management plan and acceptance plan of this document
	ACM_SCP	2	S3CC9PB Configuration Management Documentation(class ACM) ACM_SCP2 is described in configuration list and configuration management plan of this document
ADO: Delivery and Operation	ADO_DEL	2	S3CC9PB Delivery Procedures Documentation (class ADO)
	ADO_IGS	1	S3CC9PB Installation, generation and start-up Procedures (class ADO)
ADV: Development	ADV_FSP	2	S3CC9PB Functional Specification (Class ADV)
	ADV_HLD	2	S3CC9PB High Level Design (Class ADV)
	ADV_LLD	1	S3CC9PB Low Level Design (Class ADV)
	ADV_IMP	2	S3CC9PB Implementation (Class ADV)
	ADV_RCR	1	All representation correspondence analyses are included in the relevant TOE representation documentation (FSP, HLD, LLD, IMP)
	ADV_SPM	1	S3CC9PB Security Policy Model (Class ADV)
AGD: Guidance Documents	AGD_ADM	1	S3CC9PB Guidance Documentation(Class AGD)
	AGD_USR	1	
ALC: Life Cycle Support	ALC_DVS	2	S3CC9PB Development Security Procedures(Class ALC)
	ALC_FLR	1	S3CC9PB Flaw Remediation Procedures(Class ALC)
	ALC_LCD	1	S3CC9PB Life Cycle Definition Documentation(Class ALC
	ALC_TAT	1	S3CC9PB Development Tool Documentation(Class ALC)
ATE: Tests	ATE_COV	2	S3CC9PB Test Coverage Analysis(Class ATE)
	ATE_DPT	1	Test Depth Analysis(Class ATE) is described in Test Documentation(Class ATE)
	ATE_FUN	1	S3CC9PB Test Documentation(Class ATE),
AVA: Vulnerability Assessment	AVA_MSU	2	S3CC9PB Analysis of the Guidance Documentation(Class AVA)
	AVA_SOF	1	S3CC9PB Strength of TOE SF Analysis (Class AVA)
	AVA_VLA	4	S3CC9PB Vulnerability Analysis (Class AVA)

Table 7-3. Assurance measures table

8 PP CLAIMS

106 S3CC9PB conforms to requirements of PP/9806.

107 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.

108 No additional assurance requirement is introduced.

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