Common Criteria
Information Technology
Security Evaluation

S3CJ9QD

Security Target Lite

Version 1.0
October 1, 2005

SAMSUNG ELECTRONICS

CONTENTS

1 ST INTRODUCTION

1.1 ST IDENTIFICATION

Title: Security Target Lite of Project Blackfoot (S3CJ9QD)

Version: V1.0, issued on October 1, 2005

Version number	Common Criteria
V1.0	version 2.2

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

2 This ST has been built with Common Criteria Version 2.2

3 This ST is based on Protection Profile of Smart Card Integrated Circuit, PP/9806(version 2.0, September 1998).

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 2.2.

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.3 (Moderate resistant) with the dependencies of the chosen hierarchically higher assurance components are satisfied).

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 that 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 addresses 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.

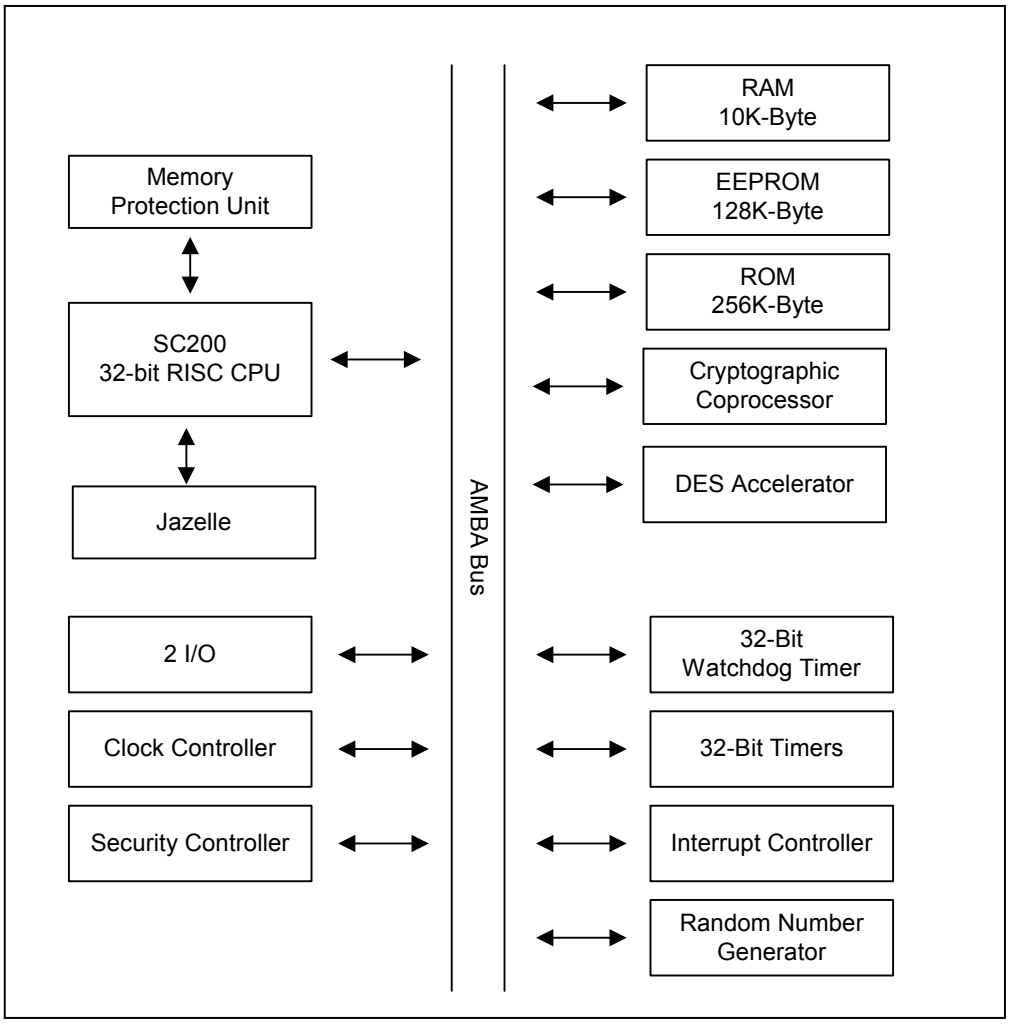

Figure 2-1. S3CJ9QD Block diagram

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 and crypto. library). 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			
S3CJ9QD 40dip	S3CJ9QDX01 rev.6			
S3CJ9QD dedicated software	**Elements**	**Storage Area**	**Version**	**Comments**
	Test ROM Code	ROM	2.0	Within the Evaluation perimeter
	Standard Crypto. Library	ROM	3.0N	Out of evaluation perimeter
	Secure Crypto. Library	EEPROM	3.2S	Within the Evaluation perimeter
S3CJ9QD embedded software	S3CJ9QD User Test code, version 1.0			Out of evaluation perimeter

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 corresponds 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.

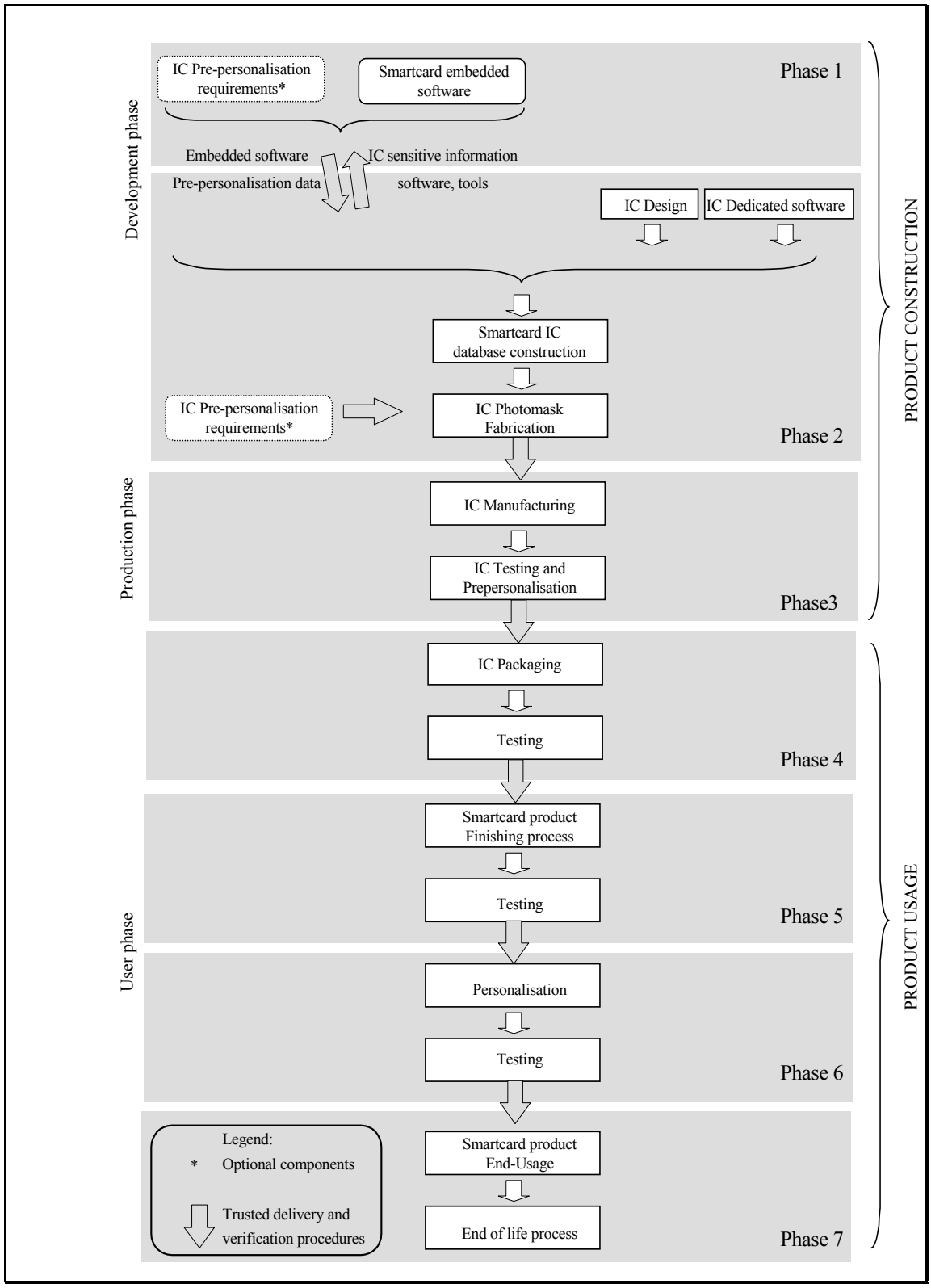

Figure 2-2. Smart card product life-cycle

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 Design 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.

End-user environment (phase 7)

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 LOGICAL PHASES

27 During its construction usage, the TOE may be under several life logical phases. These phases are sorted under a logical controlled sequence. The change from one phase to the next shall be under the TOE control.

2.5 TOE INTENDED USAGE

28 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.

29 During the phases 2 and 3, the TOE is being developed. The administrators are 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**

2.6 GENERAL IT FEATURES OF THE TOE

2.6.1 TOE Features

30 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)

3 TOE SECURITY ENVIRONMENT

31 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

32 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.

33 The TOE itself is therefore an asset.

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

3.2 ASSUMPTIONS

35 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.

36 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)

37 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 user embedded software implements the cryptographic key destruction method.

3.3 THREATS

38 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.

39 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)

40 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.

41 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

42 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

43 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

44 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

45 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.

46 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	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	Class I	Class I	Class I	Class I
T.DIS_DSOFT		Class II	Class	Class I	Class I	Class I	Class I
T.DIS_DESIGN		Class II	Class	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				
Theft or unauthorized of assets							
T.T_DEL	Class II						
T.T_SAMPLE		Class II	Class	Class I	Class I		
T.T_PHOTOMASK		Class II	Class II				
T.T_PRODUCT			Class	Class I	Class I	Class I	Class I
Unauthorized modification threats							
T.MOD_DEL	Class II						
T.MOD_SOFT		Class II	Class	Class I	Class I	Class I	Class I
T.MOD_DSOFT		Class II	Class	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				

Table 3-1. Threats and phases

3.4 ORGANIZATIONAL SECURITY POLICIES

47 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, CRC, DES and RSA encryption/decryption.

4 SECURITY OBJECTIVES

48 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

49 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, on-the-fly CRC, 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

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

51 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)

52 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)

53 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)

54 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)

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

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

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

58 **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 programs outside the IC.

59 **Note**: test specific condition is defined in the test documentation version 1.0

5.1.1.5 Stored Data Integrity Monitoring (FDP_SDI.1)

60 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 behavior (FMT_MOF.1)

61 The TOE security functions shall restrict the ability **to enable** the functions SF3 to the **TEST administrator.**

5.1.2.2 Management of security attributes (FMT_MSA.1)

62 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)

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

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

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

5.1.2.4 Static Attribute Initialisation (FMT_MSA.3)

65 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.

66 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)

67 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.

68 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.

69 ACP_1: Access Control Policy for IC in TEST configuration

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

70 ACP_2: Access Control Policy for IC in USER configuration

- Partial EEPROM area (exclude security and non erasable area) read, write 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
- USER ROM and Cryptographic ROM accessed (read and executable)
- RAM accessed (read, write and executable)

Object Table:

Object	Comment
TEST_ROMo	TEST ROM area
USER_ROMo	USER ROM area
Crypto_ROMo	Cryptographic 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 5-2. Object table

Subject Table:

Subject	Comment
TEST_ROMs	Executable code in TEST ROM area
USER_ROMs	Executable code in USER ROM area
Crypto_ROMs	Executable code in Cryptographic ROM area
SEC_EEs	Executable code in SECURITY EEPROM area
NONERA_EEs	Executable code in NON ERASABLE EEPROM area
USER_EEs	Executable code in USER EEPROM area
USER_RAMs	Executable code in USER RAM area (test configuration only)

Table 5-3. Subject table

5.1.2.6 Security Attribute Based Access Control (FDP_ACF.1)

71 The TOE security functions shall enforce the **ACP_1 and ACP_2 access control security functions policies** to objects based on **access control security attributes**.

72 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)**

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

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

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)

74 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)

75 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**.

76 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.**

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

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

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

80 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.

Event
CPU exceptions*
Abnormal voltage occurrence
Abnormal frequency occurrence
Abnormal temperature occurrence
Light exposure occurrence
Inner insulation removal occurrence
Power Glitch Attack occurrence
Active shield removal attack occurrence

Table 5-4. List of event

5.1.2.9 Potential Violation Analysis (FAU_SAA.1)

81 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.

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

a) Accumulation or combination of **events defined in Table 5-4**. known to indicate a potential security violation;

b) any other rules**: none**

* CPU exceptions include invalid memory access, invalid instruction and data

5.1.2.10 Unobservability (FPR_UNO.1)

83 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 information during an operation on this information. Identification (by unauthorized 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)

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

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

Elements for Detection	Detection Notification
Voltage Detector	Flag setting
Frequency Detector	Flag setting
Temperature Detector	Flag setting
Light exposure Detector	Flag setting
Inner insulation removal Detector	Flag setting
Power Glitch Detector	Flag setting
Active shield removal Disconnection Detector	Flag setting

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

5.1.2.12 Resistance to Physical Attack (FPT_PHP.3)

86 The TOE security functions shall resist **the physical tampering scenarios given in Table 5-6.** to the **list of detector elements and attack notification (Table 5-5)** by responding automatically such that the TOE security policy is not violated.

Physical Tampering Scenario	Reaction Elements
Abnormal Voltage Attack	RESET state
Abnormal Frequency Attack	RESET state
Abnormal Temperature Attack	RESET state
Light exposure Attack	RESET state
Inner insulation removal Attack	RESET state
Power Glitch Attack	RESET state
Active shield removal attack	RESET state
Noise introduction attack (on Clock and Reset interfaces)	Noise removal

Table 5-6. 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)

87 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.

Operation	Algorithm	Key size	Standards
Encryption/Decryption	DES	64 bits	FIPS 46-2
Encryption/Decryption	RSA	128 to 2048 bits	ANSI X9.31
Random number generation	Factorization of Trinomials	16 bits length number	FIPS 140-2*
On-the-fly CRC	CRC-16	-	CCITT V.41

Table 5-7. List of cryptographic operations

* RNG tests as described in FIPS 140-2(1999). These tests were removed from FIPS140-2(2002).

5.1.2.14 Cryptographic key management (FCS_CKM.1)

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.

Cryptography	Algorithm	Key size	Standards
RSA Encryption/Decryption	Generation of prime number	128 to 2048 bits	The Rabin-Miller Probabilistic Primality Test

Table 5-8. List of cryptographic key generations

5.2 FUNCTIONAL REQUIREMENTS ENFORCED BY THE IT ENVIRONMENT

88 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)

89 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

90 The Assurance requirement is EAL 4 augmented of additional assurance components as listed in the following sections.

91 These components are hierarchical ones to the components specified in EAL 4.

6.1 ADV_IMP.2 IMPLEMENTATION OF THE TSF

Developer actions elements:

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

Content and presentation of evidence elements:

93 The implementation representation shall unambiguously define the TOE security functions to a level of detail such that the TOE security functions can be generated without further design decisions.

94 The implementation representation shall be internal-consistent.

95 The implementation representation shall describe the relationships between all portions of the implementation.

Evaluator action elements:

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

97 The evaluator shall determine mat the implementation representation is an accurate and complete instantiation of the TOE security functional requirements.

6.2 ALC_DVS.2 SUFFICIENCY OF SECURITY MEASURES

Developer actions elements:

98 The developer shall produce development security documentation.

Content and presentation of evidence elements:

99 The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

100 The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

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

Evaluator action elements:

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

103 The evaluator shall confirm that the security measures are being applied.

6.3 AVA_VLA.3 MODERATE RESISTANT

Developer actions elements:

104 The developer shall perform vulnerability analysis.

105 The developer shall provide vulnerability analysis document.

Content and presentation of evidence elements:

106 The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search way in which a user can violate the TSP.

107 The vulnerability analysis documentation shall describe the deposition of identified vulnerabilities.

108 The vulnerability analysis documentation shall show, for all of identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

109 The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

110 The vulnerability analysis documentation shall show that the search for vulnerabilities is systematic.

Evaluator action elements:

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

112 The evaluator ***shall conduct*** penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

113 The evaluator ***shall perform*** an independent vulnerability analysis.

114 The evaluator ***shall perform*** independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

115 The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a moderate attack potential.

7 TOE SUMMARY SPECIFICATION

7.1 LIST OF SECURITY FUNCTION

SF1: Environmental Security violation recording and reaction

116 These security function records in register the events notified by the detectors (refer to list below).

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

List of detectors:

- Abnormal voltage
- Abnormal frequency
- Abnormal temperature
- Light
- Inner insulation removal
- Power Glitch
- Active shield removal

SF2: Access Control

1) Security registers access control

117 This security function manages access to the security control registers.. This is write-enable bit for security related registers. If user does not enable this bit in 128 cycles after the reset, user cannot write security control registers any more.

2) Invalid address access

118 This function detects invalid address access occurrence. When an event is detected, an ABORT is evoked. The memory access rights are configured in MPU (Memory Protection Unit).

SF3: Non reversibility of test configuration and user configuration

119 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.

SF4: Hardware countermeasures for unobserability

120 This function enforces hardware counter measures to enhance unobservability :

- Scrambling of address and data buses
- Encryption of data stored in ROM, RAM, EEPROM memories (static ROM data encryption, dynamic RAM/EEPROM encryption)
- Synthesizable processor core (glue logic)

SF5: Test configuration communication protocol and data commands

121 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.

SF6: Test

122 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.

SF7: Preventing Environmental Stress

123 1) High Frequency Filter

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

124 2) Clock Noise Filter

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

125 3) Reset Noise Filter:

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

SF8: : Software countermeasures for unobserability

126 This function enforces software counter measures to enhance unobservability :

- polarity swap, conditional instruction execution, uniform branch, dummy branch insertion, dummy multiplier activity
- internal variable clock

SF9: Cryptography

127 1) Data Encryption Standard Engine

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

128 2) Random Number Generator

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

129 3) TORNADO™ Cryptography Engine

- This function assists in the acceleration of modulo exponentiations required in the RSA encryption/decryption algorithm.

130 4) TORNADO™ Cryptography Library

- TORNADO™ Crypto Library is optimized for Samsung chips with TORNADO cryptographic co-processor. TORNADO is a hardware which operates Montgomery multiplication. There are two kinds of CPU's which Samsung crypto chips use. They are 32-bit ARM and 16-bit Calm. Furthermore, there exist many chips with TORNADO. Therefore, Samsung RSA Crypto Library is developed to be applied all these chips. That is, Samsung RSA Crypto Library is developed not to be dependent on a specific chip.

131 5) On-the-fly CRC

- This function is used for on-the-fly CRC block for error detection during data access.

7.2 ASSURANCE MEASURES

Assurance Class	Assurance Family	Assurance Component	Assurance measure(document reference)
ACM: Configuration Management	ACM_AUT	**1**	Blackfoot Configuration Management
	ACM_CAP	**4**	
	ACM_SCP	**2**	
ADO: Delivery and Operation	ADO_DEL	**2**	Blackfoot Delivery Procedures
	ADO_IGS	**1**	Blackfoot Installation, generation and start-up Procedures
ADV: Development	ADV_FSP	**2**	Blackfoot Functional Specification
	ADV_HLD	**2**	Blackfoot High Level Design
	ADV_LLD	**1**	Blackfoot Low Level Design
	ADV_IMP	**2**	Blackfoot Implementation
	ADV_RCR	**1**	All representation correspondence analyses are included in the relevant TOE representation documentation (FSP, HLD, LLD, IMP)
	ADV_SPM	**1**	Blackfoot Security Policy Model
AGD: Guidance Documents	AGD_ADM	**1**	Blackfoot Guidance Documentation
	AGD_USR	**1**	
ALC: Life Cycle Support	ALC_DVS	**2**	Blackfoot Development Security Procedures
	ALC_FLR	**1**	Blackfoot Flaw Remediation Procedures
	ALC_LCD	**1**	Blackfoot Life Cycle Definition
	ALC_TAT	**1**	Blackfoot Development Tool
ATE: Tests	ATE_COV	**2**	Blackfoot ATE Documentation
	ATE_DPT	**1**	
	ATE_FUN	**1**	
AVA: Vulnerability Assessment	AVA_MSU	**2**	Blackfoot Analysis of the Guidance Documentation
	AVA_SOF	**1**	Blackfoot Strength of TOE SF Analysis
	AVA_VLA	**3**	Blackfoot Vulnerability Analysis

Table 7-1. Assurance measures table

8 PP CLAIMS

132 S3CJ9QD based on requirements of PP/9806 (version 2.0, September 1998).

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

O.CRYPTO	arising from the organizational security policy OSP_CRYPTO. It is a TOE objective realized 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 realized by the additional functional requirement FCS_CKM.4.

134 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