Common Criteria
for Information Technology
Security Evaluation

V-WAY64 V3.0
(μPD79216000)
Security Target Lite

Approved By		Checked By		Prepared By	
J.F. CHOUTEAU		J.F. LEON		J.F. LEON	

Revisions

Revision date	Version	Author	Comments
2004-July-12	1.00	J.F. LEON	Final review and Release.

Table of contents

List of tables

List of figures

Chapter 1 ST Lite introduction

1.1 ST Lite identification

1 ST Lite title : V-WAY64 V3.0 (µPD79216000) Security Target Lite

2 ST Lite version number : V1.00-Ref:33-55N1-10001

TOE identity

3 The TOE, identified V-WAY64 V3.0, is composed of:
- µPD79216000 (V-WAY64) microcontroller from NEC, Version 3.0 (labelled V01005V30054)
- and the libraries delivered in linkable-form:
  - LLL (Low-Level Library) Version 3.0: LibcryptLLL.a
  - RSA (PKCS 1.5) Version 2.0: RSAlib.a

4 This ST Lite has been built with the CC version 2.1.

5 Annex A gives a glossary of terms used in this ST Lite, as well as of the referenced documents.

1.2 ST Lite overview

6 This ST Lite is produced in the frame of the security evaluation and certification of µPD79216000 V3.0, known hereafter in the ST Lite as V-WAY64 V3.0. This security evaluation and certification is conducted under the French IT Security Evaluation and Certification Scheme, with the work of DCSSI, as the Certification Body, and of CEACI as the Evaluation Laboratory (also called ITSEF).

7 The intent of this ST Lite is to specify the functional and assurance requirements that are applicable to the V-WAY64 V3.0 microcontroller used as a smartcard integrated circuit for smartcard applications.

8 A smartcard is usually seen as a credit card sized card having a non-volatile memory and a processing unit embedded within it.

9 The complex development and manufacturing processes of a smartcard before it is issued to the users can be separated into three distinct stages:
- The development stage: Microcontroller design, smartcard embedded software development, application software development, integration and photomask fabrication.
- The production stage: Microcontroller manufacturing, testing, preparation and shipping to the module and card assembly line.
- The smartcard production stage: Microcontroller packaging into a module (with testing), first, then into the plastic card body, and finally the smartcard product finishing process with printing and testing. After these operations, the smartcard is prepared and shipped to the personalisation line.

10 In addition, two other important stages are considered into the smartcard life cycle:
- The smartcard personalisation and testing stage where the end-user data are loaded into the smartcard's memory.
- The smartcard usage by its issuers and end-user.

11 The increase in the number and complexity of applications in the smartcard market is reflected in the increase of the level of data security required. The security needs for a smartcard can be summarised as being able to counter those who want to defraud, gain unauthorised access to data and control a system using a smartcard.

12 Therefore it is mandatory to:
- Maintain the integrity and the confidentiality of the content of the smartcard non-volatile memory (program and data memories).
- Maintain the integrity and the confidentiality of the security enforcing and security relevant architectural components (security mechanisms and associated functions) embedded into the integrated circuit.

13 Protected information is in general secret data as Personal Identification Numbers, Balance Value (Stored Value Cards), and Personal Data Files. Another set of protected information is the access rights; these include any cryptographic algorithms and keys needed for accessing and using the services provided by the system through use of the smartcard.

14 The intended environment is very large; and generally once issued the smartcard can be stored and used anywhere in the world, at any time, and no control can be applied to the smartcard and the end-user. An exception to this is the controls that are applicable when the smartcard is in its end usage in the system working according to its specifications.

15 Presently the major smartcard applications, where the V-WAY64 V3.0 microcontroller from NEC may be used, are:
- Banking and finance market for credit/debit cards, electronic purse (stored value cards) and electronic commerce.
- Network based transaction processing such as mobile phones (GSM SIM cards), pay-TV (subscriber and pay-per-view cards), communication highways (Internet access and transaction processing).
- Transport and ticketing market (access control cards).
- Governmental cards (ID-cards, health cards, driver license etc.).
- New emerging sectors such as the multimedia commerce and Intellectual Proprietary Rights protection.

16 The main objectives of this ST Lite are to:
- Describe the Target of Evaluation (TOE) as a product and position it in the life cycle of the smartcard. The ST Lite includes the development and the production phase of the microcontroller with its dedicated software, without the smartcard embedded software development phase.
- 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 operational environment during the development, production phases.
- Describe the security objectives for the TOE and for its environment in terms of integrity and confidentiality of application data and programs, protection of the TOE and associated documentation during the development and production phases.
- Specify the security requirements that include the TOE security functional requirements and the TOE security assurance requirements.
- Describe the TSF.

1.3 CC conformance claim

17 This ST Lite has been built with Common Criteria for Information Technology Security Evaluation, Version 2.1 (cf. Ref. [1], [2], [3]), as the following:
- Part 2 conformant,
- Part 3 conformant with EAL4 augmented level,
- PP/9806 (cf. Ref. [6]) conformant.

18 The EAL4 level from CC Part 3 is augmented with the assurance components ADV_IMP.2, ALC_DVS.2 and AVA_VLA.4.

Chapter 2 TOE description

19 This part of the ST Lite describes the TOE as an aid to the understanding of its security requirements and address the product type, the intended usage and the general IT features of the TOE.

2.1 Product type

20 The TOE is composed of the single chip microcontroller unit named V-WAY64 V3.0, independent of the physical interface and the way it is packaged, and the libraries LLL V3.0 and RSA V2.0.

21 The V-WAY64 V3.0 is a security cryptocontroller, to be used in a smartcard product.

22 The TOE runs according to two main modes:

- Test mode: it is a special mode which must only run at the end of the production phase to test that the TOE works properly. Then, the device is definitely locked in user mode.
- User mode: this is the normal operating mode.

23 The TOE has got the following dedicated features:

Processing unit

- A NEC V850ES CPU core, which is a small-size 32-bit RISC engine based on the Harvard architecture, with 32 “general purpose” registers of 32 bits and a processing mode using a 5-stage pipeline with short-path and automatic wait insertion. Dedicated to embedded applications, the core has 83 specific instructions with: bit, byte, half-word and word manipulation. The instruction set is well suited for greater code compactness and low power consumption.

Memories

- 192 Kbytes of ROM, named USER_ROM, split in:
  - a “system” domain named SOS,
  - an “application” domain named AOS.
- 8 Kbytes of a ROM area (named TEST_ROM) dedicated to the IC test firmware. The TEST_ROM area is only accessible in test mode, but not in user mode.
- 64 Kbytes of EEPROM split in:
  - a “code and data” domain named EEPROM CODE,
  - a “data only” domain named EEPROM DATA,
  - a 64-byte OTP page, named OTP, divided in read-only 32-byte “NEC OTP” area including a unique identification number, and 32-byte “User OTP” area.
- 64 bytes of OTP, named OTP2, dedicated to the TSF data. OTP2 is only accessible in test mode, but not in user mode.
- SFR area, split in:
  - USER_SFR, which contains the user-accessible registers,
  - TEST_SFR, which contains registers only visible for testing.
- 4 Kbytes of RAM.

24 Note: The high voltage required for writing or erasing operations in EEPROM, and writing operations in OTP and OTP2 is produced internally.

Crypto-processor

- The V-WAY64 V3.0 microcontroller is equipped with a NEC SuperMAP co-processor for fast public key encryption. The NEC SuperMAP enables high-speed arithmetic and modular operations, such as multiplication and exponentiation on large numbers up to 2048 bits long. The SuperMAP access for software developers must be made through a set of arithmetic and modular routines delivered in a linkable-form library, known as Low-Level Library (LLL).
- A secure 1024-bit RSA library, which is making use of some of the LLL, and the LLL itself are part of the TOE.

DES accelerator

- The DES accelerator is a dedicated hardware intended to perform fast DES encryption and decryption. The DES accelerator provides support to triple-DES ECB and CBC operations.

Clock generator

- Internal clock, up to 36 MHz.

random number generator

- 1 16-bit random number generator.

Timers

- 2 16-bit timers, with either internal or external clock source.

Interrupt controller

- 7 maskable internal interrupts.
- 2 exception traps.
- 32 software exceptions.
- 8 levels of interrupt priority

I/O port

- 1 I/O port with smart serial interface conforming to ISO 7816-3 and EMV standards (cf. Ref. [4], [5]), for smartcard communication protocol.

Security circuits

- The V-WAY64 V3.0 is equipped with a full set of security circuits that:
  - shield the device from unspecified voltage and frequency range, exposure to UV light and physical attacks, illegal operations on memory areas
  - make more difficult from outside, the analysis of internal activity of the device.

Standby functions

- HALT, IDLE, STOP.

Power On/Off circuit

- Reset generator,
- Internal voltage regulator.

Test circuits

- The TOE includes test circuits. After completion of the testing operations, the device is definitively locked in user mode.
- To perform the tests, an IC dedicated software is included in the TOE. In accordance with the definition in the PP/9806 (cf. Ref. [6]), this IC dedicated software is composed with both an IC test firmware, masked within the TEST_ROM, and tests programs outside the IC.

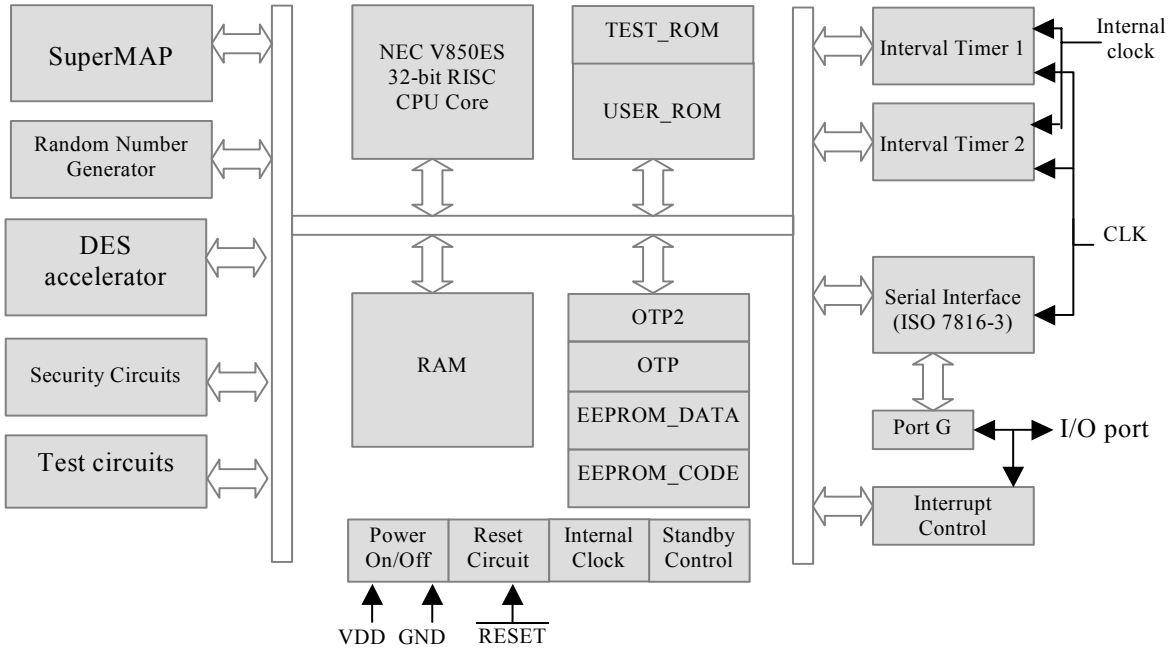

Figure 2.1 - Microcontroller block diagram

2.2 Smartcard product life cycle

25 The smartcard product life cycle is decomposed into 7 phases where the following authorities are involved:

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

26 The limits of this ST Lite correspond to the phases 2 and 3, including the phase 1 delivery and verification procedures and the TOE delivery to the IC packaging manufacturer. Procedures corresponding to phases 1, 4, 5, 6 and 7 are outside the scope of this ST Lite.

27 The figure that following describes the smartcard product life cycle.

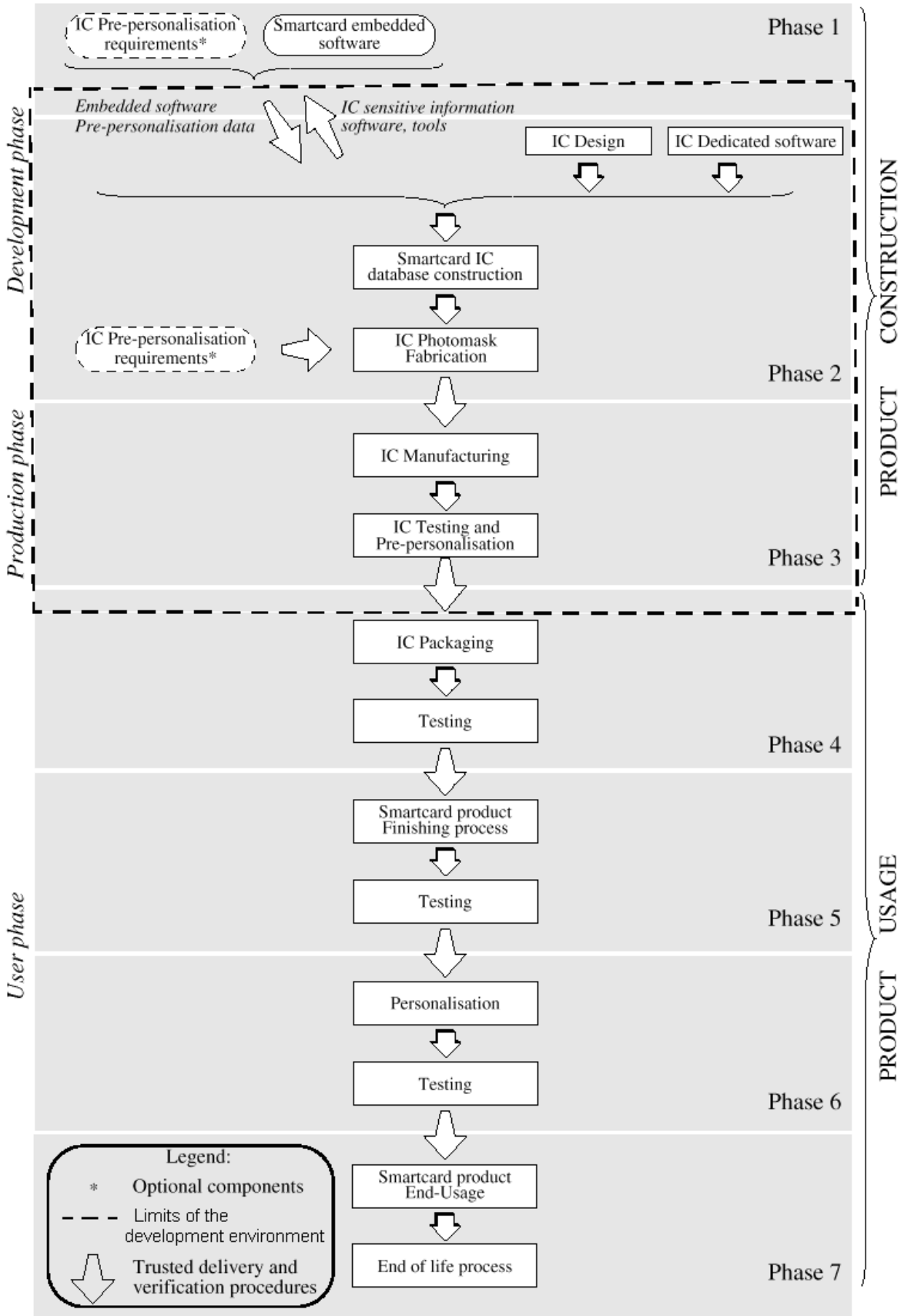

Figure 2.2 - Smartcard product life cycle

2.3 TOE environment

28 Considering the TOE, three types of environments were identified:
- Development environment corresponding to phase 2,
- Production environment corresponding to phase 3,
- User environment, from phase 4 to phase 7.

2.3.1 Development environment of the TOE

29 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.

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

31 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).

32 Reticles and photomasks are generated from the verified IC databases; the formers are used in the silicon Wafer-fab processing. When reticles and photomasks are generated off-site, they are transported and worked on in a secure environment with accountability and traceability of all (good and bad) products. During the transfer of sensitive data electronically, procedures shall be established to ensure that the data arrive only at the destination and are not accessible at intermediate stages (e.g. stored on a buffer server where system administrators make backup copies).

2.3.2 Production environment of the TOE

33 As high volumes of product commonly go through such environment, adequate control procedures are necessary to account for all pieces at all stages of production.

34 Production starts within the Wafer-fab; here the silicon wafers undergo the diffusion processing. 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 securely delivered for assembly onto the smartcard.

35 Whether carried out under the control of the IC manufacturer or the packaging manufacturer, wafers shall be scribed and broken such as to separate the functional from the non-functional ICs. The latter is discarded in a controlled accountable manner. The good ICs are then packaged. When testing, programming and deliveries are done offsite, ICs shall be transported and worked on in a secure environment with accountability and traceability of all (good and bad) products. Further testing occurs, followed by smartcard personalisation, retesting then delivery to the smartcard issuer.

2.3.3 User environment of the TOE

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

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

38 Phase 7 is the end-user environment that covers a wide spectrum of very different functions, thus making it difficult to avoid and monitor any abuse of the TOE.

39 The TOE user environment is not covered by the present ST Lite.

2.4 TOE logical phases

40 During its construction usage, the TOE may be under several life logical phases.

41 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

42 The TOE can be incorporated in several applications such as those described inside the paragraph 15.

43 During the phases 1, 2 and 3, the TOE is being developed and produced. The **administrators** are the following:

- The smartcard embedded software developer,
- The IC designer,
- The IC manufacturer.

2.6 General IT features of the TOE

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

- Arithmetical functions (e.g. incrementing counters in electronic purses, calculating currency conversion in electronic purses...);
- Data communication;
- Cryptographic operations (e.g. data encryption/decryption, digital signature verification), when applicable.

Chapter 3 TOE security environment

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

3.1 Assets

46 Assets are security relevant elements of the TOE that include:
- The application data of the TOE (such as IC pre-personalisation requirements, IC and system specific data),
- The smartcard embedded software,
- The IC dedicated software,
- The IC specification, design, development tools and technology.

47 The TOE itself is therefore an asset.

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

3.2 Assumptions

49 It is assumed that this section concerns the following items:
- Due to the definition of the TOE limits, any assumption for the smartcard embedded software development (phase 1 is outside the scope of the TOE).
- Any assumption from phases 4 to 7 for the secure usage of the TOE, including the TOE delivery procedures.

50 Security is always the matter of the whole system: the weakest element of the chain determines the total system security. Assumptions described hereafter have to be considered for a secure system using smartcard products:
- Assumptions on phase 1,
- Assumptions on the TOE delivery process (phases 4 to 7),
- Assumptions on phases 4-5-6,
- Assumptions on phase 7.

3.2.1 Assumptions on phase 1

A.SOFT_ARCHI The smartcard embedded software shall be developed in a secure manner, that is focusing on the integrity of program and of data.

A.DEV_ORG Procedures dealing with physical, personnel, organisational, technical measures for the confidentiality and integrity of smartcard embedded software (e.g. source code and any associated documents) and IC designer proprietary information (tools, software, documentation...) shall exist and be applied in software development.

3.2.2 Assumptions on the TOE delivery process (phases 4 to 7)

51 Procedures shall guarantee the control of the TOE delivery and storage process and the conformance to 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, has 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 unauthorised use).

3.2.4 Assumptions on phase 7

A.USE_DIAG It is assumed that secure communication protocols and procedures are used between smartcard and terminal.

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

3.3 Threats

52 The TOE as defined in Chapter 2 is required to counter the threats described hereafter; a threat agent wishes to abuse the assets either by functional attacks, environmental manipulations, specific hardware manipulations or by any other types of attacks.

53 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 unauthorised disclosure, modification or theft of assets at different phases. Specially, some functionalities of the TOE may be cloned by observing its behaviour or getting information by reverse engineering.

3.3.2 Threats on phase 1 (delivery and verification procedures)

54 Considering the limits of the TOE, two types of threats have to be considered during phase 1:

- Threats on the assets transmitted from the IC designer to the embedded software developer during the smartcard development.
- Threats on the smartcard embedded software and any additional application data transmitted during the delivery process from the embedded software developer to the IC designer.

55 These threats are described hereafter:

T.DIS_INFO — Unauthorised disclosure of the assets delivered by the IC designer to the smartcard embedded software developer such as sensitive information on IC specification, design and technology, software and tools if applicable.

T.DIS_DEL — Unauthorised disclosure of the smartcard embedded software and any additional application data (such as IC pre-personalisation requirements) during the delivery process to the IC designer.

T.MOD_DEL — Unauthorised modification of the smartcard 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 smartcard 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

56 During these phases, the assumed threats could be described in three types:

- Unauthorised disclosure of assets,
- Theft or unauthorised use of assets,
- Unauthorised modification of assets.

Unauthorised disclosure of assets

57 This type of threats covers unauthorised 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	Unauthorised disclosure of IC design. This threat covers the unauthorised disclosure of proprietary elements such as IC specification, IC design, IC technology detailed information, IC hardware security mechanism specifications.
T.DIS_SOFT	Unauthorised disclosure of smartcard embedded software and data such as access control, authentication system, data protection system, memory partitioning, cryptographic programs.
T.DIS_DSOFT	Unauthorised disclosure of IC dedicated software. This threat covers the unauthorised disclosure of IC dedicated software including security mechanisms specifications and implementation.
T.DIS_TEST	Unauthorised disclosure of test information such as full results of IC testing including interpretations.
T.DIS_TOOLS	Unauthorised disclosure of development tools. This threat covers potential disclosure of IC development tools and testing tools (analysis tools, microprobing tools).
T.DIS_PHMASK	Unauthorised disclosure of photomask information, used for photoengraving during the silicon fabrication process.

Theft or unauthorised use of assets

58 Potential attackers may gain access to the TOE and perform operations for which they are not authorised. For example, such attackers may personalise the TOE in an unauthorised manner, or try to gain fraudulous access to the smartcard system.

T.T_SAMPLE	Theft or unauthorised use of TOE silicon samples (e.g. bond out chips, ...).
T.T_PHMASK	Theft or unauthorised use of TOE photomasks.
T.T_PRODUCT	Theft or unauthorised use of smartcard products.

Unauthorised modification of assets

59 The TOE may be subjected to different types of logical or physical attacks that may compromise security. Due to the intended usage of the TOE (the TOE environment may be hostile), the TOE security parts may be bypassed or compromised reducing the integrity of the TOE security mechanisms and disabling their ability to manage the TOE security. This type of threats includes the implementation of malicious trojan horses.

T.MOD_DESIGN Unauthorised modification of IC design.

This threat covers the unauthorised modification of IC specification, IC design including IC hardware security mechanism specifications and realisation...

T.MOD_PHMASK Unauthorised modification of TOE photomasks.

T.MOD_DSOFT Unauthorised modification of IC dedicated software including modification of security mechanisms.

T.MOD_SOFT Unauthorised modification of smartcard embedded software and data.

60 The table below indicates the relationships between the smartcard 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
Unauthorised 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_PHMASK		Class II	Class II				
T.DIS_TEST			Class I/II	Class I	Class I	Class I	
Theft or unauthorised use of assets							
T.T_DEL	Class II						
T.T_SAMPLE		Class II	Class I/II	Class I	Class I		
T.T_PHMASK		Class II	Class II				
T.T_PRODUCT			Class I/II	Class I	Class I	Class I	Class I
Unauthorised modification threats							
T.MOD_DEL	Class II						
T.MOD_SOFT		Class II	Class I/II	Class I	Class I	Class I	Class I
T.MOD_DSOFT		Class II	Class I/II	Class I	Class I	Class I	Class I
T.MOD_DESIGN		Class II	Class I/II	Class I	Class I	Class I	Class I
T.MOD_PHMASK		Class II	Class II				

Table 3.1 - Class Statement of Threats versus Phases

3.4 Organisational security policies

P.CRYPTO The TOE shall offer cryptographic capabilities to embedded software in order to maintain integrity and confidentiality of sensitive data, particularly during transfer outside the TSC.

Chapter 4 Security objectives

61 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

62 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. Typically, the TOE must include a protection against micro-probing. It must also include a protection against security information leakage which could be deduced from the observation of the TOE (such as its power consumption).
O.CLON	The TOE functionality needs to be protected from cloning. For instance, the TOE must prevent the possibility of getting security relevant information by reverse engineering or by observing its behaviour.
O.OPERATE	The TOE must ensure the continued correct operation of its security functions. Particularly, the TOE security functions must be continuously operational so that theft or unauthorised use of silicon samples or smartcard products, or unauthorised modification of its security functions, do not allow to jeopardise the integrity of the TOE.
O.FLAW	The TOE must not contain flaws in design, implementation or operation.
O.DIS_MECHAN	The TOE shall ensure that the hardware security mechanisms are protected against unauthorised disclosure (such as reverse engineering).
O.DIS_MEMORY	The TOE shall ensure that sensitive information stored in memories is protected against unauthorised disclosure. For instance, the TOE must provide a protection against unauthorised access to memory, whether by a logical interface or by a physical attack, in the aim of dumping its contents.
O.MOD_MEMORY	The TOE shall ensure that sensitive information stored in memories is protected against any corruption or unauthorised modification, by any means (whether by a logical interface or by a physical attack).
O.CRYPTO	The TOE shall provide RSA and DES cryptographic algorithms to perform data encryption/decryption in order to allow smartcard applications to transfer sensitive data out of the TSC in a secure way.

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 authorised personnel. It must be ensured that confidential information such as data sheets and general information on defined assets are only delivered to the parties authorised personnel on the need to know basis.
O.SOFT_DLV	The smartcard embedded software must be delivered from the smartcard embedded software developer (Phase 1) to the IC designer through a trusted delivery and verification procedure that shall be able to maintain the integrity of the software and its confidentiality, if applicable.
O.SOFT_MECH	To achieve the level of security required by this ST lite, the smartcard embedded software shall use IC security features and security mechanisms as specified in the smartcard IC documentation (e.g. sensors, …).
O.DEV_TOOLS	The smartcard embedded software shall be designed in a secure manner, by using exclusively software development tools (compilers, assemblers, linkers, simulators etc…) and software-hardware integration testing tools (emulators) that will grant the integrity of program and data.

4.2.2 Objectives on phase 2 (development phase)

O.SOFT_ACS	Smartcard embedded software shall be accessible only by authorised 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 authorised personnel within the IC designer on the basis of the need to know (physical, personnel, organisational, technical procedures).
O.DSOFT_ACS	Any IC dedicated software specification, detailed design, source code or any further information shall be accessible only by authorised personnel within the IC design on the need to know basis.
O.MASK_FAB	Physical, personnel, organisational, technical procedures during photomask fabrication (including deliveries between photomask 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 authorised personnel within the IC designer on the need to know basis.
O.TI_ACS	Security relevant technology information shall be accessible only by authorised 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 unauthorised use such as tampering or theft.

During the IC manufacturing and test operations, security procedures shall ensure the confidentiality and integrity of:
- TOE manufacturing data (to prevent any possible copy, modification, retention, theft or unauthorised 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 of the TOE by control of:
- packaging and storage,
- traceability,
- storage and protection of manufacturing process specific assets (such as manufacturing process documentation, further data, or samples),
- access control and audit to tests, analysis tools, laboratories, and databases,
- change/modification in the manufacturing equipment, management of rejects.

O.IC_DLV — The delivery procedures from the IC manufacturer shall maintain the integrity and confidentiality of the TOE and its assets.

4.2.4 Objectives on the TOE delivery process (phase 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 of its manufacturing and test data.

4.2.6 Objectives on phase 7

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

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

Chapter 5 IT security requirements

63 This part of the ST Lite defines the detailed IT security requirements that shall be satisfied by the TOE or its environment.

5.1 TOE security functional requirements

64 The TOE security functional requirements define the functional requirements for the TOE using only functional requirement components drawn from the CC Part 2.

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

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

5.1.1.1 User authentication before any action (FIA_UAU.2)

66 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.1.2 User identification before any action (FIA_UID.2)

67 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.1.3 User attribute definition (FIA_ATD.1)

68 The TSF shall maintain the following list of security attributes belonging to individual users: **mode_of_use**.

69 **Note: mode_of_use has 3 possible values:**

- ***user mode* : the TOE is in user mode,**
- ***test mode entry* : transition state for test mode because the user is successfully identified but not authenticated yet,**
- ***test mode*: the TOE is in test mode.**

5.1.1.4 TOE security functions testing (FPT_TST.1)

70 The TSF shall run a suite of self-tests **at the conditions that an authorised user requests it and mode_of_use is *test mode***, to demonstrate the correct operation of the TSF.

71 The TSF shall provide authorised users with the capability to verify the integrity of TSF data.

72 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

5.1.1.5 Stored data integrity monitoring (FDP_SDI.1)

73 The TSF shall monitor user data stored within the TSC for **integrity errors** on all objects, based on the following attributes: **USER_ROM BIST signature and EEPROM/OTP/OTP2 memory contents**.

5.1.2 Functional requirements applicable to phases 3 to 7

5.1.2.1 Management of security functions behaviour (FMT_MOF.1)

5.1.2.1.1 iteration 1: Unobservability

74 The TSF shall restrict the ability to **modify the behaviour of** the function **of unobservability** to **user and administrator**.

5.1.2.1.2 iteration 2: Testing

75 The TSF shall restrict the ability to **disable** the function **of testing** to **administrator**.

76 **Refinement: once performed, the functions of testing are definitively disabled.**

5.1.2.2 Management of security attributes (FMT_MSA.1)

iteration 1: Memory access control

77 The TSF shall enforce the **memory access control SFP** to restrict the ability to **modify** the security attributes **memory_configuration and memory_access_control** to **user**.

iteration 2: Testing information flow control

78 The TSF shall enforce the **testing information flow control SFP** to restrict the ability to **modify** the security attributes **test_type** to **administrator**.

5.1.2.3 Security roles (FMT_SMR.1)

79 The TSF shall maintain the roles**:**

- **Administrator: user whose associated security attribute mode_of_use is set to *test mode*, so that he has the ability to perform testing operations onto the TOE.**
- **User: user whose associated security attribute mode_of_use is set to *user mode*. It can be either an identified user with no test mode privileges or the embedded software.**

80 The TSF shall be able to associate users with roles.

5.1.2.4 Static attribute initialisation (FMT_MSA.3)

iteration 1: Memory access control

81 The TSF shall enforce the **memory access control SFP** to provide **restrictive** default values for security attributes that are used to enforce the security functions policy.

82 The TSF shall allow the **user** to specify alternate initial values to override the default values when an object or information is created.

iteration 2: Testing information flow control

83 The TSF shall enforce the **testing information flow control SFP** to provide **restrictive** default values for security attributes that are used to enforce the security functions policy.

84 The TSF shall allow the **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)

85 The TSF shall enforce the **memory access control SFP** on **embedded software and IC dedicated software, and all the objects USER_ROM SOS, USER_ROM AOS, EEPROM CODE, EEPROM DATA, OTP, RAM, USER_SFR, TEST_ROM, OTP2, TEST_SFR**, and all operations among subjects and objects covered by the security functions policy.

86 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control policy.

5.1.2.6 Security Attribute Based Access Control (FDP_ACF.1)

87 The TSF shall enforce the **memory access control SFP** to objects based on **mode_of_use, memory_configuration and memory_access_control**.

88 **Note:**

1) **memory_configuration splits USER_ROM into USER_ROM AOS and USER_ROM SOS, and EEPROM into EEPROM CODE and EEPROM DATA.**
2) **memory_access_control controls data load accesses from EEPROM CODE to EEPROM DATA, from EEPROM CODE to EEPROM CODE, and from EEPROM CODE to USER_ROM AOS.**

89 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **Branch accesses from and to memory areas delimited by the memory_configuration security attribute apply access control rules defined by the following matrix:**

				Code executed in memory area:		
				USER_ROM AOS/SOS	EEPROM CODE	USER_SFR / RAM / other memories
Branch to memory area:	USER_ROM	AOS		Authorised	Authorised	Prohibited
		SOS		Authorised	Prohibited	Prohibited
	EEPROM	CODE	If EEPROM available	Authorised	Authorised	Prohibited
			Otherwise	Prohibited	Prohibited	Prohibited
		DATA		Prohibited	Prohibited	Prohibited
		OTP		Prohibited	Prohibited	Prohibited
	USER_SFR			Prohibited	Prohibited	Prohibited
	RAM			Prohibited	Prohibited	Prohibited
	Other memories			Prohibited	Prohibited	Prohibited

Table 5.1 - Branch access control matrix

- **Data accesses from and to memory areas delimited by the memory_configuration security attribute apply access control rules defined by the following matrix:**

				Code executed in memory area:		
				USER_ROM AOS/SOS	EEPROM CODE	USER_SFR / RAM / other memories
Data access to memory area:	USER_ROM	AOS		Authorised	Conditioned	Prohibited
		SOS		Authorised	Prohibited	Prohibited
	EEPROM	CODE	Store	Authorised	Prohibited	Prohibited
			Load	Authorised	Conditioned	Prohibited
		DATA	Store	Authorised	Prohibited	Prohibited
			Load	Authorised	Conditioned	Prohibited
		OTP	Store	Authorised	Prohibited	Prohibited
			Load	Authorised	Conditioned	Prohibited
	USER_SFR		Store	Authorised	Prohibited	Prohibited
			Load	Authorised	Authorised	Prohibited
	RAM			Authorised	Authorised	Prohibited
	Other memories			Prohibited	Prohibited	Prohibited

Table 5.2 - Data access control matrix

- **The key "Conditioned" means that the access is authorised according to the values contained in the memory_access_control attribute**

90 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

- **The TSF shall explicitly authorise access of IC dedicated software to appropriate memory areas if mode_of_use is *test mode*.**
- **The TSF shall explicitly authorise access of IC dedicated software to some TEST_SFR if mode_of_use is *test mode entry*.**

91 The TSF shall explicitly deny access of subjects to objects based on the **rules:**

- **the TSF shall explicitly deny access of all software to TEST_ROM and OTP2 if mode_of_use is not *test mode*.**
- **the TSF shall explicitly prohibit write access of all software to NEC OTP area if mode_of_use is not *test mode*.**

5.1.2.7 Subset Information Flow Control (FDP_IFC.1)

92 The TSF shall enforce the **testing information flow control SFP** on **the following list of subjects, information and operations**:

Subjects	IC dedicated software
Information	Information in TEST_ROM, OTP2 and TEST_SFR
Operations	Read, Write

Table 5.3 – List of subjects, information and operations for testing information flow control SFP

5.1.2.8 Simple Security Attributes (FDP_IFF.1)

93 The TSF shall enforce the **testing information flow control SFP** based on the following types of subject and information security attributes **command, test_type, mode_of_use**.

Notes:

1) "command" represents a well-defined instruction-data exchange.
2) "test_type" specifies several test capabilities of the test software:
   a) TEST ROM mode: this mode mainly allows the user to authenticate himself and select one of the test modes below,
   b) Code execution from the TOE external test software in TEST ROM mode,
   c) Memory Tester mode: this mode is intended to perform EEPROM behavioural tests and to initialise OTP2 area,
   d) ROMless mode: code executed from the TOE external test software with the right to access to all the data,
   e) User ROM BIST mode: code executed from the TOE external test software to check the User ROM BIST signature,
   f) Test ROM BIST mode: code executed from the TOE external test software to check the Test ROM BIST signature,
   g) Peripheral test mode: code executed from the TOE external test software to check the peripheral components (within the TOE) without CPU.

94 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

Operation	Test type	Information in TEST_ROM
Read	TEST ROM mode	no command
	Memory Tester mode	no command
	ROMless mode	no command
	User ROM BIST mode	no command
	Test ROM BIST mode	TEST_ROM check command
	Peripheral test mode	no command
Write	All test types	Note: write operation is impossible in TEST_ROM

Table 5.4 - TEST_ROM information flow control

Operation	Test type	Information in OTP2
Read	TEST ROM mode	no command
	Memory Tester mode	OTP2 information read commands
	ROMless mode	no command
	User ROM BIST mode	no command
	Test ROM BIST mode	no command
	Peripheral test mode	no command
Write	TEST ROM mode	no command
	Memory Tester mode	OTP2 information write commands
	ROMless mode	no command
	User ROM BIST mode	no command
	Test ROM BIST mode	no command
	Peripheral test mode	no command

Table 5.5 - OTP2 information flow control

Operation	Test type	Information in TEST_SFR
Read	TEST ROM mode	TEST_SFR information read commands
	Memory Tester mode	TEST_SFR information read commands
	ROMless mode	TEST_SFR information read commands
	User ROM BIST mode	no command
	Test ROM BIST mode	no command
	Peripheral test mode	no command
Write	TEST ROM mode	TEST_SFR information write commands
	Memory Tester mode	TEST_SFR information write commands
	ROMless mode	TEST_SFR information write commands
	User ROM BIST mode	no command
	Test ROM BIST mode	no command
	Peripheral test mode	no command

Table 5.6 - TEST_SFR information flow control

95 The TSF shall enforce **none**.

96 The TSF shall provide **none**.

97 The TSF shall explicitly authorise an information flow based on the following rules: **none**.

98 The TSF shall explicitly deny an information flow based on the following rules: **Read/Write operations to information stored in TEST_ROM, OTP2 and TEST_SFR is forbidden when mode_of_use is not *test mode*.**

5.1.2.9 Potential Violation Analysis (FAU_SAA.1)

99 The TSF 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.

100 The TSF shall enforce the following rules for monitoring audited events:
1) Accumulation or combination of **auditable events listed below** known to indicate a potential security violation;

Events indicating a potential security violation	Nature of the violation
UV light exposure	Because EEPROM/OTP/OTP2 cells are sensitive to UV light, their exposure may corrupt the data stored in them
Out of specification power supply	Out of specification power supply may cause an abnormal operation or even a damage of the TOE
Out of specification external frequency	Out of specification external frequency may decrease the efficiency of the RNG
Abnormal behaviour of EEPROM/OTP/OTP2 erasing or writing voltage	Abnormal behaviour may not guarantee the correct data erasing or writing
Forbidden memory access	Illegal memory access may lead to jeopardise the secrecy of data stored in EEPROM or modify the behaviour of the TOE by branching to unauthorised areas in USER_ROM
Physical attack to strategic areas of the TOE	Physical attacks may jeopardise the contents of strategic areas of the TOE
Bad user authentication	unauthorised access to the TOE may jeopardise the integrity and the confidentiality of the memory contents and security mechanisms

Table 5.7 - Auditable events indicating a potential security violation

2) none

5.1.2.10 Unobservability (FPR_UNO.1)

101 The TSF shall ensure that **unauthorised users** are unable to observe the operation **of critical TOE internal activity** on **any objects** by **the embedded software**.

5.1.2.11 Notification of Physical Attack (FPT_PHP.2)

102 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

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

104 For **the detection devices of UV light exposure, out of specification power supply, out of specification external frequency, bad EEPROM/OTP/OTP2 writing or erasing voltage, and physical modification,** the TSF shall monitor the devices and elements and notify **the embedded software** when physical tampering with the TOE security function’s devices or TOE security function's elements has occurred.

5.1.2.12 Resistance to Physical Attack (FPT_PHP.3)

105 The TSF shall resist **the following physical tampering scenarios** to the **following list of TSF devices/elements** by responding automatically such that the TOE security policy is not violated.

Physical tampering scenarios	List of TSF devices/elements
Out of specification power supply that may cause an abnormal operation or even a damage of the TOE	All TSF devices/elements
Out of specification external frequency	RNG
Physical modifications	All TSF devices/elements

Table 5.8 - Resistance to physical attack

5.1.2.13 Cryptographic operation (FCS_COP.1)

5.1.2.13.1 iteration 1: RSA

106 The TSF shall perform **encryption/decryption** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **of 1024 bits** that meet the following: **RSAES-PKCS1-v1_5 encryption scheme (cf. Ref. [7])**.

5.1.2.13.2 iteration 2: DES

107 The TSF shall perform **encryption/decryption** in accordance with a specified cryptographic algorithm **DES** and cryptographic key sizes **of 56 bits** that meet the following: **FIPS PUB 46-2 (cf. Ref. [8])**.

Note:

108 Given that the strength of cryptographic algorithms is outside the scope of the CC, the minimum SOF claim (at § 65) does not apply to this requirement.

5.2 TOE security assurance requirements

109 The assurance requirements are EAL4 augmented of additional CC Part 3 assurance components listed in the following sections.

110 These components are hierarchical ones to the components specified in EAL4.

5.2.1 ADV_IMP.2 Implementation of the TSF

Developer action elements:

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

Content and presentation of evidence elements:

112 The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

113 The implementation representation shall be internally consistent.

114 The implementation representation shall describe the relationship between all portions of the implementation..

Evaluator action elements:

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

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

5.2.2 ALC_DVS.2 Sufficiency of security measures

Developer action elements:

117 The developer shall produce development security documentation.

Content and presentation of evidence elements:

118 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.

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

120 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:

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

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

5.2.3 AVA_VLA.4 Highly resistant

Developer action elements:

123 The developer shall perform a vulnerability analysis.

124 The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence elements:

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

126 The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.

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

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

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

130 The vulnerability analysis documentation shall provide a justification that the analysis completely addresses the TOE deliverables.

Evaluator action elements:

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

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

133 The evaluator shall perform an independent vulnerability analysis.

134 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.

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

5.3 Security requirements for the IT environment

136 The TOE has no asserted dependencies on the IT environment.

Chapter 6 TOE summary specification

6.1 TOE security functions

137 This section defines the TOE security functions.

138 At the end of the section, a mapping shows how these security functions satisfy the TOE security functional requirements.

6.1.1 Test mode entry (SF1)

139 SF1 controls the access to test mode. This control is implemented by an identification/authentication procedure.

140 If user_mode_locking is *true* then test mode is forbidden; mode_of_use is automatically set to *user mode*.

141 Note: by default, user_mode_locking is set to *false*.

142 SF1 first checks an identification code:

1) If identification succeeds, then mode_of_use is set to *test mode entry* and SF1 checks the authentication code:
   a) If authentication succeeds, then mode_of_use is set to *test mode*.
   b) If authentication fails, SF1 detects a potential violation and triggers a CPU lock.
2) If the identification code does not allow to enter in test mode, then mode_of_use is set to *user mode.*

143 Both identification and authentication are realised by probabilistic mechanisms. The strength of function claimed for SF1 is SOF-high.

6.1.2 Testing (SF2)

144 If the security attribute mode_of_use is *test mode*, then SF2 checks the value of test_type selected by the authenticated user and performs the appropriate test.

145 SF2 performs the following tests according to the value of test_type:

- Control the correct operation of the mechanisms supporting the TOE security functions.
- Check the integrity of the TEST_ROM by computation and comparison of a digital signature from its contents.
- Check the integrity of the USER_ROM by computation and comparison of a digital signature from its contents.
- Check the integrity of the data included in EEPROM/OTP/OTP2, if any, by reading of its contents and comparison with the previously stored data.

146 Otherwise, if the security attribute mode_of_use is not *test mode*, then SF2 does not run any test and forbids data flow to/from TEST_ROM, OTP2, TEST_SFR.

147 Note: by default, test_type is set to *TEST ROM mode*.

148 In a software point of view, SF2 is implemented by the IC dedicated software which is for one part in the TEST_ROM and the other part outside the chip.

149 Consequently, SF2 implements a control to secure the TSF data flow between the chip and the external test software.

6.1.3 User mode locking (SF3)

150 When the testing is achieved, the authorised user definitively switches the TOE into user mode by performing SF3.

151 If the security attribute mode_of_use of the authenticated user is set to *test mode*, then SF3 definitively locks the TOE in user mode by setting user_mode_locking to *true*.

152 Once SF3 has been performed, it is no more possible to switch again in test mode because this disables SF1.

6.1.4 Memory access control (SF4)

153 SF4 enforces the rules defined in FDP_ACF.1 and detect if the TOE is operating forbidden memory access.

154 Upon detection of illegal access, SF4 raises a specific security control flag to notify the potential violation to embedded software and triggers a CPU lock.

155 SF4 allows users to:

- Select the sizes of USER_ROM AOS and SOS in the one hand, and EEPROM CODE and DATA in the other hand, by modifying the memory_configuration attribute.
- Control the memory_access_control attribute to authorise or not the data load accesses from EEPROM CODE to EEPROM DATA, from EEPROM CODE to EEPROM CODE, and from EEPROM CODE to USER_ROM AOS.

156 By default these attributes have restrictive values:

- The sizes of USER_ROM SOS and EEPROM DATA are set to the maximum.
- Accesses from EEPROM CODE to EEPROM DATA and from EEPROM CODE to EEPROM CODE are authorised. But access from EEPROM CODE to USER_ROM AOS is forbidden.

6.1.5 Unobservability (SF5)

157 SF5 treats unobservability of TOE internal activity through two aspects:
- TOE power consumption,
- Data transfer to and from TOE RAM and EEPROM memories.

158 In this purpose, SF5 implements two mechanisms:

Protection against DPA

159 This protection consists in randomly stretching (in a wide range) the code execution time of CPU operations and/or SuperMAP and DES operations. Due to these stretching operations the average power consumption is decreased. To compensate it, SF5 then generates a random dummy current.

160 SF5 allows the embedded software to:
- enable or disable the protection for CPU and peripherals on the one hand, or for SuperMAP and DES on the other hand, both independently.
- choose the average percentage of hidden pulses for each of them.

161 The randomness and the average percentage are obtained by a 16-bit Random Number Generator (RNG) with these characteristics: FIPS140-2 and MAURER compliant (cf. Ref. [9], [10]).

162 For testing purpose, the administrator via the IC dedicated software can also modify the configuration.

RAM/EEPROM bus ciphering

163 SF5 ciphers the data from RAM and EEPROM memories in order to make them unobservable during read or write accesses by CPU via the data buses.

164 To increase the performance of the ciphering, the buses connections must be physically scrambled (data bus, address bus).

165 This security function is realised with permutational mechanisms. The strength of function claimed for SF5 is SOF-high.

6.1.6 Abnormal environmental condition monitoring (SF6)

166 SF6 ensures that the environmental conditions are respected. With this aim in view, it shall monitor the following events: UV light exposure, out of specification of power supply, and out of specification of external frequency.

UV light exposure

167 SF6 detects UV light exposure in order to avoid any EEPROM data corruption, as EEPROM cells are sensible to UV light.

168 For that, SF6 has got a UV light detector composed of special EEPROM cellS. This feature allows to detect a UV light exposure even if the TOE was not powered. In this case, the UV light detection will be taken into account after the next power-on.

169 Upon detection of UV light exposure, SF6 raises a specific security control flag to notify the potential violation to embedded software and triggers an interrupt request.

Out of specification of power supply

170 The external power supply gets through a voltage regulator which delivers an internal power supply.

171 SF6 detects if the external power supply goes out of a specified range to prevent any risk of abnormal operation or even damage of the TOE.

172 Upon detection of an out of specification of power supply, SF6 raises a specific security control flag to notify the potential violation to embedded software and triggers a CPU lock.

Out of specification of external frequency

173 As seen above, the security function unoservability (SF5) makes use of a RNG (defined at paragraph 161). To reach the efficiency required by its specification, the RNG uses the external clock as one of its inputs.

174 In order to preserve the efficiency of the RNG, SF6 continuously monitors the external frequency and detects if it goes out of a specified range.

175 Upon detection of an out of specification of external frequency, SF6 raises a specific security control flag to notify the potential violation to embedded software and triggers a CPU lock.

6.1.7 EEPROM/OTP/OTP2 high voltage monitoring (SF7)

176 SF7 is only active when writing/erasing in EEPROM or writing in OTP/OTP2. During this period of time, SF7 monitors the EEPROM/OTP/OTP2 writing or erasing voltage, detecting if an abnormal voltage level occurs, in order to guaranty that the operation is correctly performed.

177 Upon detection of abnormal voltage level, SF7 raises a specific security control flag to notify the potential violation to embedded software and triggers an interrupt request.

6.1.8 Physical attack protection (SF8)

178 To protect the TOE security functions, a physical active shield, constituted by a complicated wiring, is placed above strategic areas. Thus, a physical attack will most probably cut off the wiring, that will be detected by SF8.

179 If the cut-off appears when the TOE is not powered, then the detection will be taken into account after the next power-on.

180 Upon detection of a cut-off of the wiring, SF8 triggers a CPU lock.

181 While the wiring is cut off, the detection stays active. The effect is that the TOE continuously operates a CPU lock.

6.1.9 RSA cryptography (SF9)

182 SF9 provides a secure RSA data encryption/decryption capability, with 1024-bit cryptographic keys, compliant with RSAES-PKCS1-v1_5 encryption scheme.

183 SF9 lean on hardware modular and arithmetic capabilities provided by the SuperMAP coprocessor. Access to SuperMAP is made through a library of modular and arithmetic routines, known as Low-Level Library (LLL).

184 In order to prevent disclosure of the RSA private key during computation, SF9 provides the following countermeasures:

- Randomising computation timing,
- Randomising power consumption both by software and hardware means,
- Detecting tampering by fault injection.

6.1.10 DES cryptography (SF10)

185 SF10 consists of a DES accelerator dedicated hardware that provides a secure DES data encryption/decryption capability, with 56-bit cryptographic keys, compliant with FIPS PUB 46-2.

6.1.11 Mapping between security functions and security functional requirements

186 The table below shows which functions satisfy which requirements and that all requirements are met. Note that each security function contribute to the satisfaction of at least one TOE security functional requirement.

Security functions / Security Requirements	SF1	SF2	SF3	SF4	SF5	SF6	SF7	SF8	SF9	SF10
FIA_UAU.2	X									
FIA_UID.2	X									
FIA_ATD.1	X									
FPT_TST.1		X								
FDP_SDI.1		X								
FMT_MOF.1			X		X					
FMT_MSA.1		X		X						
FMT_SMR.1	X									
FMT_MSA.3		X		X						
FDP_ACC.2				X						
FDP_ACF.1				X						
FDP_IFC.1		X								
FDP_IFF.1		X								
FAU_SAA.1	X			X		X	X	X		
FPR_UNO.1					X			X	X	
FPT_PHP.2						X	X	X		
FPT_PHP.3						X		X		
FCS_COP.1									X	X

Table 6.1 - Relationship between security requirements and security functions

6.2 Assurance measures

187 This section specifies the assurance measures of the TOE. Table 6.2 that follows, shows how these measures satisfy the stated assurance requirements.

6.2.1 Security target (AM1)

188 AM1 consists in providing the “V-WAY64 V3.0 (µPD79216000) Security Target” document (cf. Ref. [11]).

6.2.2 CM documentation (AM2)

189 AM2 consists in providing a CM documentation that includes a reference for the TOE, a configuration list, a CM plan and an acceptance plan.

6.2.3 Delivery manual (AM3)

190 AM3 consists in providing a manual that describes the procedures for :

- reception of embedded software from the embedded software developer,
- delivery of TOE sensitive information to the embedded software developer,
- delivery of the TOE to the user.

6.2.4 Guidance (AM4)

191 AM10 consists in providing the guidance documents, including user guidance, administrator guidance, and secure installation, generation and start-up procedures, as appropriate.

6.2.5 Functional specification (AM5)

192 AM5 consists in providing a functional specification document.

6.2.6 High-level design (AM6)

193 AM6 consists in providing a high-level design document.

6.2.7 Implementation (AM7)

194 AM7 consists in providing a documentation that describes the development tools used in the one hand, and the implementation representation in the other hand.

6.2.8 Low-level design (AM8)

195 AM8 consists in providing a low-level design document.

6.2.9 Correspondence analysis (AM9)

196 AM8 consists in providing a correspondence analysis between the TOE summary specification, the functional specification, the high-level design, the low-level design and the implementation representation.

6.2.10 TOE security policy model (AM10)

197 AM9 consists in providing a TOE security policy model.

6.2.11 Development security (AM11)

198 AM11 consists in providing a development security documentation.

6.2.12 Life cycle definition (AM12)

199 AM12 consists in providing a life cycle definition documentation.

6.2.13 Test documentation (AM13)

200 AM13 consists in providing a test documentation that includes the test coverage analysis, the depth of testing analysis, and documents for functional testing and its results.

6.2.14 TOE for testing (AM14)

201 AM14 consists in providing version 3.0 of V-WAY64 TOE suitable for testing.

6.2.15 Documentation analysis (AM15)

202 AM15 consists in providing an analysis document on the completeness and the correctness of the guidance.

6.2.16 Strength of TOE security functions (AM16)

203 AM16 consists in providing an analysis document for the mechanisms that have a strength of TOE security function claim.

6.2.17 Vulnerability analysis (AM17)

204 AM17 consists in providing a vulnerability analysis document.

6.2.18 Trace of assurance measures to assurance requirements

Assurance requirements \ Assurance measures	AM1	AM2	AM3	AM4	AM5	AM6	AM7	AM8	AM9	AM10	AM11	AM12	AM13	AM14	AM15	AM16	AM17
ASE	X																
ACM_AUT.1		X															
ACM_CAP.4		X															
ACM_SCP.2		X															
ADO_DEL.2			X														
ADO_IGS.1				X													
ADV_FSP.2					X												
ADV_HLD.2						X											
ADV_IMP.2							X										
ADV_LLD.1								X									
ADV_RCR.1									X								
ADV_SPM.1										X							
AGD_ADM.1				X													
AGD_USR.1				X													
ALC_DVS.2											X						
ALC_LCD.1												X					
ALC_TAT.1							X										
ATE_COV.2													X				
ATE_DPT.1													X				
ATE_FUN.1													X				
ATE_IND.2														X			
AVA_MSU.2															X		
AVA_SOF.1																X	
AVA_VLA.4														X			X

Table 6.2 - Relationship between assurance requirements and assurance measures

Chapter 7 PP claims

7.1 PP reference

205 This ST Lite is compliant with CC Smartcard Integrated Circuit Protection Profile PP/9806, Version 2.0, Issue September 1998, registered at the French Certification Body.

7.2 PP tailoring

206 None.

7.3 PP additions

207 In addition to conforming to PP/9806, this ST Lite specifies an additional Organisational Security Policy P.CRYPTO in section 3.4.

208 To cover this Organisational Security Policy, the following objective is added: O.CRYPTO, specified in section 4.1.

209 To meet this objective, one functional requirement is added: FCS_COP.1 (including two iterations), which is specified in section 5.1.2.13.

Annex A Glossary

A.1 Abbreviations and acronyms

BIST
Built-in self test.

CC
Common Criteria (for Information Technology Security Evaluation, Version 2.1).

CM
Configuration Management.

EAL
Evaluation Assurance Level.

EEPROM
Electronically Erasable Programmable Read Only Memory.

IC
Integrated Circuit.

IT
Information Technology.

LLL
Low Level Library providing cryptographic capabilities.

OSP
Organisational Security Policies.

OTP
One Time Programmable memory.

PP
Protection Profile.

RAM
Random Access Memory.

ROM
Read Only Memory.

SF
Security Function.

SFP
Security Function Policy.

SFR
Special Function Register.

ST
Security Target.

SuperMAP
High-speed Modular Arithmetical Processor.

TEST_SFR
Dedicated registers available in test mode.

TOE
Target Of Evaluation.

TSC
TSF Scope of Control.

TSF
TOE Security Functions.

TSFI
TSF Interface.

TSP
TOE Security Policy.

USER_SFR
Registers available in user mode dedicated to CPU or I/O peripherals.

A.2 Vocabulary

Embedded software
Software embedded in a smartcard IC. Embedded software may be in any part of the non-volatile memory of the IC.

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

IC dedicated software
IC proprietary software which is required for testing purpose; it may either be IC embedded software (also known as IC firmware) or tests programs outside the IC.

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-personalisation.

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

IC pre-personalisation data
Any data that is stored in the non-volatile memory for shipment between phases.

I/O peripherals
Material components of the TOE that manage its inputs/outputs.

Personaliser
Institution (or its agent) responsible for the smartcard personalisation and final testing.

Smartcard
A card according to ISO 7816 requirements which has a non volatile memory and a processing unit embedded within it.

Smartcard embedded software
Composed of embedded software in charge of generic functions of the smartcard IC such as operating system, general routines and interpreters (smartcard basic software) and embedded software dedicated to the applications (smartcard application software).

Smartcard embedded software developer
Institution (or its agent) responsible for the smartcard embedded software development and the specification of IC pre-personalisation requirements.

System integrator
Institution (or its agent) responsible for the smartcard product system integration (terminal software developer, system developer, …).

A.3 References

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 2.1, August 1999.

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 2.1, August 1999.

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 2.1, August 1999.

[4] ISO/IEC 7816-3:1997 Identification Cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols

[5] EMV2000, Integrated Circuit Card, Specification for Payment Systems, Book 1: Application Independent ICC to Terminal Interface Requirements, Version 4.0, December 2000.

[6] Common Criteria for Information Technology Security Evaluation, Protection Profile, Smartcard Integrated Circuit, Version 2.0, September 1998, registered by French Certification Board under number PP/9806.

[7] PKCS #1 v2.0: RSA Cryptography Standard, RSA Laboratories October 1, 1998.

[8] Federal Information Processing Standards Publication (FIPS PUB) 46-2, Data Encryption Standard (DES). U.S. Department of Commerce, National Institute of Standards and Technology (NIST), December 30, 1993.

[9] Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules. U.S. Department of Commerce, National Institute of Standards and Technology (NIST), May 25, 2001.

[10] Journal of Cryptology, vol.5, no 2, 1992 pp. 89-105, "Universal Test For Random Bit Generators", by Ueli M. Maurer.

[11] V-WAY64 V3.0 (µPD79216000) Security Target, V1.34-Ref:33-55N1-10000.