ST19WK08
SECURITY TARGET

COMMON CRITERIA FOR IT SECURITY EVALUATION

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 Identification

1 Document identification: ST19WK08 SECURITY TARGET.

2 Version number: V1_0, issued July 2004.

3 Registration: registered at ST Microelectronics under number SMD_ST19WK08_ST_04_001_V01.00.

4 TOE identification: given in Chapter 2.

1.2 Purpose

5 This document presents **the ST19WK08 Security Target (ST)** of Smartcard Integrated Circuit (IC), with its Dedicated Software (DSW), designed on the **ST19W platform of STMicroelectronics**.

6 This document is a sanitized version of the Security Target used for the evaluation. Its purpose is the conformance to the Common Criteria Recognition Agreement (CC RA). It is classified as public information.

7 The precise references of the Target of Evaluation (TOE) and the secure IC general features are given in Chapter 2.

8 A glossary of terms and abbreviations used in this document is given in Annex A and Annex B.

1.3 Context

9 The Target of Evaluation (TOE) referred in Chapter 2, is evaluated under the French IT Security Evaluation and Certification Scheme and is developed by the Smartcard product division of STMicroelectronics (STM).

10 The assurance level of the performed Common Criteria (CC) IT Security Evaluation is EAL 4 augmented. The minimum strength level for the TOE Security Functions (SFs) is SOF-high for all the security functions implemented by the TOE.

11 The intent of this ST is to specify the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) applicable to the ST19WK08 secure IC, and to summarise its chosen SFs and assurance measures.

12 This ST claims to be an ***extended*** instantiation of the "Smartcard Integrated Circuit" Protection Profile (PP) registered and certified under the reference PP/9806 in the French IT Security Evaluation and Certification Scheme.

13 Extensions to the SFRs of the "Smartcard Integrated Circuit" Protection Profile (PP) are **exclusively** drawn from the Common Criteria part 2 standard SFRs.

14 This ST makes various refinements to the above mentioned PP. They are all properly identified in the text as they appear ***as indicated here***. The original text of the PP is repeated in this document for reading convenience. It is easily identified as it appears as indicated here. The deleted text of these paragraphs appears ***[***~~as indicated here~~***]***.

1.4 Common Criteria conformance claims

15 The ST19WK08 Security Target is:

- PP/9806 **conformant**,
- EAL 4 augmented by ***ADV_FSP.3***, ADV_IMP.2, ALC_DVS.2, ***ALC_FLR.1***, AVA_VLA.4 and ***AVA_CCA.1***,
- The minimum strength of functions level for the SFRs is **SOF-high**,
- ISO/IEC 15408-2:1999 **conformant**,
- ISO/IEC 15408-3:1999 **conformant**.

16 The following CC "final interpretations" concerning the ASE security assurance requirement component were taken into account (source http://www.commoncriteria.org):

Interpretation Number	Effective Date	Interpretation Title	Reference: CC	Reference: CEM
008	31/07/01	Augmented and Conformant overlap	CCv2.1 Part 1 Section 5.4	CEM Part 2 v1.0 **ASE_INT**
032	15/10/00	Strength of Function Analysis in ASE_TSS	CCv2.0, CC v2.1; Part 1, Annex C; Part 3, **ASE_TSS**	
043	16/02/01	What does "clearly stated" mean?	CC v2.1 Part 3 APE_OBJ.1, **ASE_OBJ.1**	
049	16/02/01	Not Completely met	CC v2.1 Part 1 Annex B/C.2.5, Part 3 APE/ **ASE_OBJ.1.3C**	
084	16/02/01	Aspects of objectives in TOE and environment		CEM Part 2, v1.0, APE_REQ.1-20, **ASE_REQ.1-20**

2 ST19WK08 TOE DESCRIPTION

2.1 ST19WK08 TECHNICAL PARAMETERS

17 This section describes the ST19WK08 product as assembly of the highly reliable CMOS ST19W platform.

18 The general features of the circuit are:

- 8-bit processing unit
- volatile (SRAM) and non volatile memories (ROM and EEPROM)
- security blocks : Memory Access Control Logic (MACL), clock generator, security administrator, power manager
- supporting functions : I/O ports (contact only), 8-bit timers, Unpredictable Number Generator

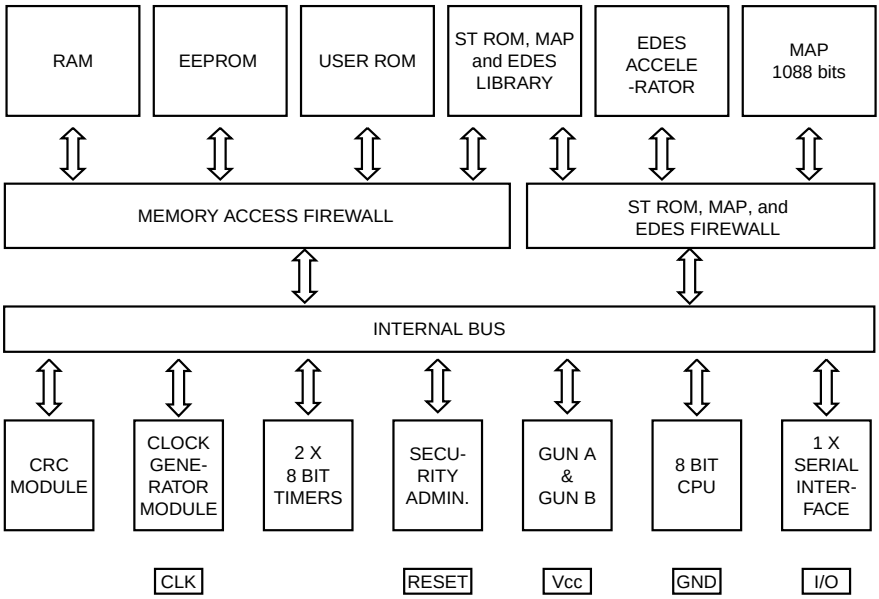
19 The TOE also includes in the ROM a Dedicated Software which comprises test capabilities (test operating system, called "autotest") and libraries (system ROM library, cryptographic library for DES (EDES implentation) and RSA algorithms).

20 The TOE is a silicon chip with its Dedicated Software.

21 The TOE submitted to evaluation does not comprise any specific application : there is no applicative Embedded Software, but the ROM of the tested samples contains an operating system called "Card Manager" that allows the evaluators to use a set of commands with the I/O, and to load in EEPROM (or in RAM) test softwares.

22 Figure 1 provides a block diagram overview of the ST19WK08.

Figure 1 ST19WK08 block diagram



2.2 *SECURE IC BASED PRODUCT* LIFE-CYCLE

23 The ***secure IC based product*** life-cycle is decomposed into 7 phases.

24 The authorities involved in each phase are described in Table 1.

25 The **limit of the evaluation** defines the scope of responsibility of STM in terms of security. This limit is defined by the parameter **C_DELIVERY_PHASE**. This parameter takes the value ***3*** for deliveries in the form of wafers, either unsawn or sawn (dice).

26 The limit of ***the evaluation*** corresponds to phases 2 ***through C_DELIVERY_PHASE***, including the delivery and verification procedures of phase 1, and the TOE delivery to the phase ***C_DELIVERY_PHASE authority***; procedures corresponding to ***all other phases*** are outside the scope of this ***evaluation***.

27 Figure 2 describes the secure IC based product life cycle.

Table 1 ***Secure IC based product*** authorities ***by life-cycle phase***

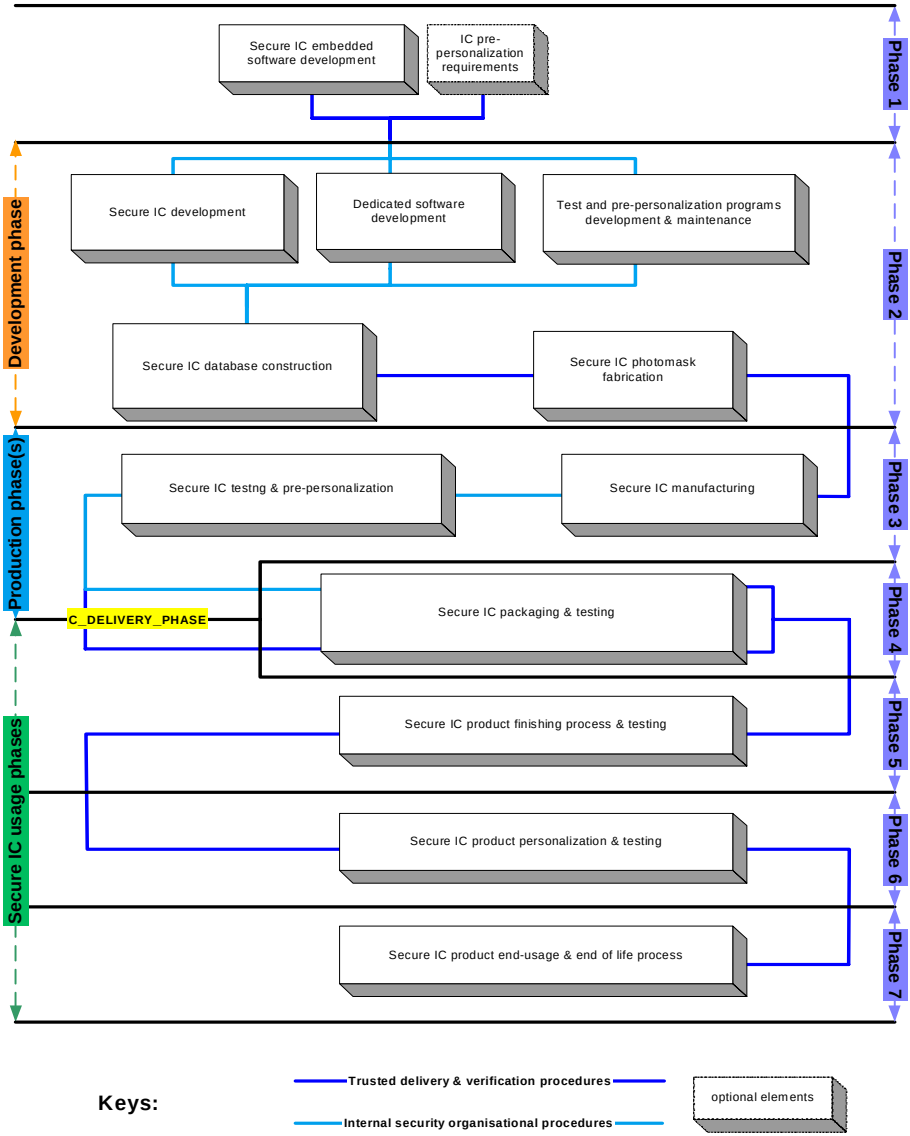
Phase	Name, authority and description	
1	***Secure IC*** embedded software development: the **secure IC embedded software developer** is in charge of the ***secure IC*** embedded software development and the specification of IC pre-personalization requirements.	
2	IC development: **STM** designs the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

28 These different phases may be performed at different sites; procedures on the delivery process of the TOE shall exist and be applied for every delivery within a phase or between phases. This includes any kind of delivery performed from phase 1 to phase 7, including:

- intermediate delivery of the TOE or the TOE under construction within a phase,
- delivery of the TOE or the TOE under construction from one phase to the next.

29 These procedures shall be compliant with the secure usage assumptions [A.DLV_*] developed in Section 3.2.2 of the PP/9806.

Figure 2 ***Secure IC based product life-cycle***



2.3 TOE ENVIRONMENT

30 Considering the TOE, three types of environment are defined:

- Development environment corresponding to phase 2,
- Production environment corresponding ***to phases 3 up to*** **C_DELIVERY_PHASE**,
- User environment, ***corresponding to phases*** **C_DELIVERY_PHASE** ***+ 1 up to 7***.

2.3.1 TOE Development Environment

31 The development environment is described in the PP/9806, section 2.3.1.

32 This description has been refined in the ST19W Generic Security Target to include industrial parameters whose definition is reproduced hereafter for readers convenience.

33 The development centres actually involved in the development of the TOE are the following: **ST ROUSSET AND ST ANG MO KIO**, for the design activities, **ST ROUSSET**, for the engineering activities and for the software development activities.

2.3.2 TOE Production environment

34 The production environment is described in the PP/9806, section 2.3.2.

35 This description has been refined in the ST19W Generic Security Target to include industrial parameters whose definition is reproduced hereafter for readers convenience.

36 The authorized front-end plant actually involved in the manufacturing of the TOE is **ST ROUSSET**.

37 The authorized sub-contractor actually involved in the TOE mask manufacturing is **DNP**.

38 The authorized EWS plant actually involved in the testing of the TOE is **ST ROUSSET**.

2.3.3 TOE User environment

39 The TOE User environment is described in the PP/9806, section 2.3.3.

2.4 TOE LOGICAL PHASES

40 During its construction and usage, the TOE is under several life logical phases. These phases are ordered under a logical controlled sequence. The change from one phase to the next ***is under control of the TOE***.

41 The logical phases available on the ST19WK08 are:

- TEST configuration, then
- ISSUER configuration, then
- USER configuration.

42 Once into a given configuration, the TOE cannot be stepped back to any previous configuration.

43 During phases 4 to 6, the TOE may be in ISSUER or USER configuration according to the SICESW developer request.

44 Table 2 shows what the different TOE configuration can be facing the authorities who perform the phase activities for phases 4 to 7.

Table 2 TOE configurations

Phase & condition	TOE Configuration	Authority
Phase 4 & **C_DELIVERY_PHASE** = ***4***	ISSUER	STM
Phase 4 & **C_DELIVERY_PHASE** = ***3***	ISSUER or USER	Packaging manufacturer (not STM)
Phase 5	ISSUER or USER	Secure IC product manufacturer (not STM)
Phase 6	ISSUER or USER	Personalizer (not STM)
Phase 7	USER	End-usage

2.5 TOE INTENDED USAGE

45 The TOE can be incorporated in several applications such as:

- banking and finance market for credit/debit cards, electronic purse (stored value cards) and electronic commerce,
- network based transaction processing such as mobile phones (GSM SIM cards), pay-TV (subscriber and pay-per-view cards), communication highways (Internet access and transaction processing),
- transport and ticketing market (access control cards),
- governmental cards (ID-cards, healthcards, driver licenses etc....),
- new emerging sectors such as multimedia commerce and Intellectual Property Rights protection.

46 The TOE intended usage is further described in the PP/9806, section 2.5.

2.6 General IT features of the TOE

47 The TOE IT functionality 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, digital signature verification...).

3 TOE SECURITY ENVIRONMENT

48 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

49 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 ***secure IC*** embedded software,
- the IC dedicated software,
- the IC specification, design, development tools and technology.

50 The TOE itself is therefore an asset.

51 Assets have to be protected in terms of confidentiality***, authenticity*** and integrity.

52 In the following, unauthorized disclosure of an asset means that an attacker can determine a meaningful part of the asset that leads to a violation of the security policy enforced by the TOE (TSP).

53 In the following, unauthorized modification of an asset means that an attacker can perform an alteration of the asset, meaningful with respect to the security policy enforced by the TOE (TSP), that leads to a violation of the latter.

3.2 Assumptions

54 The assumptions are described in the PP/9806, section 3.2.

3.3 Threats

55 The threats are described in the PP/9806, section 3.3.

3.4 Organisational Security Policies

56 ***As some applications to be embedded in the ST19WK08 may require the use of hardware supported cryptography to develop high performance cryptographic operations, the following Organisational Security Policies (OSP) have been defined.***

OSP.SKCS ***The Symmetric Key Cryptographic Support provided by the TOE, and its associated documentation, shall enable the SICESW developer to design accurate, efficient and secure cryptographic operations.***

OSP.AKCS ***The Asymmetric Key Cryptographic Support provided by the TOE, and its associated documentation, shall enable the SICESW developer to design accurate, efficient and secure cryptographic operations.***

57 ***No other Organisational Security Policy (OSP) has been defined in this ST since their specifications depend heavily on the applications in which the TOE will be integrated. The security targets for the applications embedded in these TOE should further define them.***

4 SECURITY OBJECTIVES

58 The security objectives of the TOE cover principally the following aspects:

- integrity***, authenticity*** and confidentiality of assets,
- protection of the TOE and associated documentation during development and production phases.

4.1 Security objectives for the TOE

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

O.TAMPER	The TOE must prevent physical tampering with its security critical parts***, i.e. its TSF***.
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 ***or processed within its TSC*** is protected against unauthorized disclosure ***by any operational mean (explicit communications, information leakage, bus probing, failure analysis,...).***
O.MOD_MEMORY	The TOE shall ensure that sensitive information stored in memories ***or processed within its TSC*** is protected against any controlled corruption or unauthorized modification ***by any operational mean (explicit communications, operational environment perturbation, physical manipulation, energy and particle exposures, electrical stimulation,...)***.

60 Notice that no new security objectives are introduced to cope with the cryptographic support policies, i.e. OSP.SKCS and OSP.AKCS. The PP/9806 security objectives for the TOE, O.DIS_MEMORY and O.MOD_MEMORY, are instead refined to address information processing within the TSF Scope of Control. O.DIS_MEMORY requires information confidentiality that addresses both introduced organisational security policies. O.FLAW and O.MOD_MEMORY require the accurate and faithful information processing demanded by those OSPs.

4.2 Security objectives for the environment

4.2.1 Objectives on phase 1

O.DEV_DIS ***STM has*** 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.

STM ensures that tools are only delivered to the parties authorized personnel.

STM ensures that confidential information such as data sheets and general information on defined assets are only delivered to the parties authorized personnel on the need to know basis.

O.SOFT_DLV The ***secure IC*** embedded software must be delivered from the ***secure IC*** embedded software developer (Phase 1) to ***STM*** through a trusted delivery and verification procedure that ***is*** able to maintain the integrity ***and authenticity*** of the software and its confidentiality, if applicable.

O.SOFT_MECH To achieve the level of security required by ***an application*** security target ***composed of this security target***, the ***secure IC*** embedded software shall use IC security features and security mechanisms as specified in the ***secure IC*** documentation (e.g. ***Security Application Manual, Data Sheet, Programming Manual, User Manuals,***...).

O.DEV_TOOLS The ***secure IC*** 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.

61 The objectives on the remaining phases are described in the PP/9806, sections 4.2.2 to 4.2.6.

5 TOE SECURITY FUNCTIONAL REQUIREMENTS

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

63 All extensions to the SFRs of the "Smartcard Integrated Circuit" Protection Profile (PP) are **exclusively** drawn from the Common Criteria part 2 standard SFRs.

64 All iterations on SFRs have been performed according to section 2.1.4 of Common Criteria part 2. They are easily identified in the following text as they are properly labelled. Iteration labels appear as a suffix of the component standard identifier between square brackets, i.e. "FCC_FFF.e[LABEL]", where "FCC" stands for the functional class, "FFF" stands for the family within that class and "e" stands for the selected component. Dependent components have either the same label as that of the component they depend on, or a label that shares a common prefix with the latter.

65 All assignments, selections, or refinements on SFRs have been performed according to section 2.1.4 of Common Criteria part 2. They are easily identified in the following text as they appear ***as indicated here***.

66 The rules defined by the TOE Security Policy during phase 3 (access control and information flow control Security Functions Policies) ***are*** different from those prevailing during phases 4 to 7.

67 Since the TOE can be in the ISSUER configuration in Phases 4 to 6, as specified in paragraph 44, the functional requirements applicable only to phase 3 in the PP/9806, are refined into the functional requirements applicable to ***the logical phases TEST and ISSUER configurations (TST&ISR, for short)***.

68 The minimum strength of function level for the TOE security functions is SOF-high.

69 In order to ease the definition and the understanding of these security functional requirements, a simplified presentation of the TOE Security Policy (TSP) is given in the following section. For confidentiality reasons, security attributes and their related policies, TSF data, user data and acceptance/deny rules enforced by the TSF are not described in this document.

5.1 SUBJECTS, OBJECTS, OPERATIONS AND DATA

70 This section introduces in turn subjects, objects and operations relevant to the definition of the TSP.

5.1.1 Subjects

71 For any given TOE of the ST19W platform, the TSP identifies the following subjects:

S.TRUST STM **trusted process** always activated by a power on of the TOE. This process exhibits three different behaviours according to the TOE configuration. Please note that this process denotes all the active resources of the TOE controlled by the TSF, not only the executing DSW.

S.PLAIN **Untrusted process** activated by S.TRUST. This process denotes all the active resources of the TOE **not** controlled by the TSF, notably the SICESW in USER configuration.

S.LIB	STM **trusted functional process** activated during a call to execute a service available in the STM library when the TOE is in USER configuration. This process denotes only the executing DSW.
S.ANY	Any human user that can get access to the TOE either locally (i.e. that interacts with the TOE via TOE devices) or remotely (i.e. that interacts with the TOE via another IT product) when the TOE is in any configuration.

5.1.2 Objects and operations

72 For any given TOE of the ST19W platform, the TSP identifies the following objects with their associated operations. For confidentiality reasons, those objects are not completely described here.

OB.**F**_IC	Secure IC carrying the TOE in any of its forms.
OB.ROM	Any part of the Read Only Memory. These objects contain executable programs and/or data of STM and of the user (ST_ROM & USR_ROM). The latter may also reside in OB.NVM.
OB.RAM	Any part of the Volatile Memory. These objects are used for processing user and TSF data.
OB.REG	Any Register of the TOE. These objects are used to control TOE resources and to exchange data with the secure IC internal subjects.
OB.NVM	Non Volatile Memory that contains user data, TSF data and/or user programs.
OB.CMD_TST	Any command available to the user when the TOE is in TEST configuration.
OB.CMD_ISR	Any command available to the user when the TOE is in ISSUER configuration.
OB.CALL_USR	Any STM library service available to the user when the TOE is in USER configuration..

5.2 FUNCTIONAL REQUIREMENTS APPLICABLE TO *TST&ISR*

5.2.1 User attribute definition (FIA_ATD.1)

73 The TSF shall maintain the following list of security attributes belonging to individual users:

- ***the TOE configuration ,***
- ***the user authentication status ,***

5.2.2 User identification before any action (FIA_UID.2)

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

5.2.3 User authentication before any action (FIA_UAU.2)

75 The TOE Security Functions (TSF) shall require each user to be successfully authenticated before allowing any other TSF mediated actions on behalf of that user.

5.2.4 TOE Security Functions Testing (FPT_TST.1)

76 The TSF shall run a suite of self tests ***at the request of the authorised user and at TOE operating conditions*** to demonstrate the correct operation of the TSF.

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

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

5.2.5 Stored data integrity monitoring (FDP_SDI.1)

79 The TSF shall monitor user data stored within the TSC for ***user ROM or NVM pre-personalization integrity errors*** on all objects, based on the following attributes: ***memory content signature***.

5.3 FUNCTIONAL REQUIREMENTS APPLICABLE TO PHASES 3 TO 7

5.3.1 Security roles (FMT_SMR.1)

80 The TSF shall maintain the ***following*** roles:

- ***TEST administrator: this role allows to perform the test of the TOE in a secure environment.***
- ***ISSUER administrator: this role allows to perform reduced test operations and personalization of the TOE if needed during phases 4 to 6.***
- ***USER: this role has capabilities defined by the SICESW functionality and the STM library services in the DSW. The functionality available to the USER role is dependent on the SICESW, the pre-personalization and the customer mask options.***

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

5.3.2 Subset Information Flow Control (FDP_IFC.1)

82 The TOE Security Functions shall enforce the ***SFP.IFC.SFP_MNGT*** on the ***all subjects defined in*** Section 5.1.1***, the content of all objects defined in*** Section 5.1.2***, and the commands available in*** OB.CMD_TST***,*** OB.CMD_ISR ***and*** OB.CALL_USR ***objects***.

83 The TOE Security Functions shall enforce the ***SFP.IFC.USR_CFG*** on the ***all subjects defined in*** Section 5.1.1***, the content of all objects defined in*** Section 5.1.2 ***and all operations that cause controlled information to flow from and to these subjects***.

5.3.3 Simple Security Attributes (FDP_IFF.1)

84 The TOE Security Functions shall enforce the ***SFP.IFC.SFP_MNGT*** and the ***SFP.IFC.USR_CFG*** based on the following types of subject and information security attribute:

- ***subject and object locations and TOE configuration.***

85 The TOE Security Functions shall permit an information flow between a controlled subject and a controlled information via a controlled operation if the following rules hold:

- ***In TEST configuration, enforce the rules of SFP.IFC.TST_CFG.***
- ***In ISSUER configuration, enforce the rules of SFP.IFC.ISR_CFG.***
- ***In USER configuration, enforce the rules of SFP.IFC.USR_CFG.***
- ***For confidentiality reasons, other rules are not described here***

86 The TSF shall provide the additional information flow control SFP rules: ***SFP.IFC.SKC and SFP.IFC.COP***.

87 The TSF shall enforce the following additional SFP capabilities: ***None***.

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

89 The TSF shall explicitly deny an information flow based on the following rules: ***None***.

5.3.4 Management of security attributes (FMT_MSA.1)

90 The TSF shall enforce the ***SFP.ACC.SFP_MNGT*** to restrict the ability to ***change from TEST to ISSUER*** the ***TOE configuration*** security attribute to ***the TEST administrator.***

91 The TSF shall enforce the ***SFP.ACC.SFP_MNGT*** to restrict the ability to ***change from ISSUER to USER*** the ***TOE configuration*** security attribute to ***the ISSUER administrator.***

5.3.5 Static attribute initialisation (FMT_MSA.3)

92 The TSF shall enforce the ***SFP.ACC.SFP_MNGT*** to provide ***restrictive*** default values for security attributes that are used to enforce the security function policy.

93 The TSF shall enforce the ***SFP.ACC.PACL*** to provide ***permissive*** default values for security attributes that are used to enforce the security function policy.

94 The TSF shall enforce the ***SFP.ACC.LOCK*** to provide ***permissive*** default values for security attributes that are used to enforce the security function policy.

95 The TOE Security Functions shall allow the ***TEST administrator and the ISSUER administrator*** to specify alternate initial values to override the default values when an object or information is created.

5.3.6 Complete Access Control (FDP_ACC.2)

96 The TOE Security Functions shall enforce the ***SFP.ACC.SFP_MNGT*** on ***all subjects defined in*** Section 5.1.1 ***and objects defined in*** Section 5.1.2 and all operations among subjects and objects covered by the SFP.

97 The TOE Security Functions shall enforce the ***SFP.ACC.USR_CFG*** on ***all controlled subjects and objects*** and all operations among subjects and objects covered by the SFP.

98 The TOE Security Functions shall enforce the ***SFP.ACC.MACL*** on ***all controlled subjects and*** OB.ROM, OB.RAM ***and*** OB.REG ***objects*** and all operations among subjects and objects covered by the SFP.

99 The TOE Security Functions shall enforce the ***SFP.ACC.PACL*** on ***all controlled subjects and*** OB.NVM ***objects*** and all operations among subjects and objects covered by the SFP.

100 The TOE Security Functions shall enforce the ***SFP.ACC.LOCK*** on ***all controlled subjects and*** OB.NVM ***objects*** and all operations among subjects and objects covered by the SFP.

101 The TOE Security Functions shall enforce the ***SFP.ACC.SACL*** on ***all controlled subjects and ST_ROM objects*** and all operations among subjects and objects covered by the SFP.

102 The TOE Security Functions shall enforce the ***SFP.ACC.RACL*** on ***all controlled subjects and*** OB.REG ***objects*** and all operations among subjects and objects covered by the SFP.

103 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.

5.3.7 Security Attribute based Access Control (FDP_ACF.1)

104 The TOE Security Functions shall enforce ***SFP.ACC.SFP_MNGT*** to objects based on ***TOE configuration .***

105 The TOE Security Functions shall enforce ***SFP.ACC.USR_CFG*** to objects based on ***subject and object locations .***

106 The TOE Security Functions shall enforce ***SFP.ACC.MACL*** to objects based on ***subject and object locations .***

107 The TOE Security Functions shall enforce ***SFP.ACC.PACL*** to objects based on ***subject and object locations and page access classes .***

108 The TOE Security Functions shall enforce ***SFP.ACC.LOCK*** to objects based on ***page access classes and page access erasing .***

109 The TOE Security Functions shall enforce ***SFP.ACC.SACL*** to objects based on ***subject and object locations and the entry point of the STM library service .***

110 The TOE Security Functions shall enforce ***SFP.ACC.RACL*** to objects based on ***subject and object locations and the register protection status .***

111 The TOE Security Functions shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- ***In TEST configuration, enforce the rules of SFP.ACC.TST_CFG.***
- ***In ISSUER configuration, enforce the rules of SFP.ACC.ISR_CFG.***
- ***In USER configuration, enforce the rules of SFP.ACC.USR_CFG.***
- ***For confidentiality reasons, other rules are not described here.***

112 The TOE Security Functions shall explicitly authorise access of subjects to objects based on the following additional rules: ***None.***

113 The TOE Security Functions shall explicitly deny access of subjects to objects based on additional rules.

5.3.8 Basic internal transfer protection (FDP_ITT.1)

114 The TSF shall enforce the ***SFP.IFC.USR_CFG and SFP.IFC.ISR_CFG*** to prevent the ***disclosure*** of user data when it is transmitted between physically-separated parts of the TOE.

5.3.9 Subset residual information protection (FDP_RIP.1)

115 The TSF shall ensure that any previous information content of a resource is made unavailable upon ***the allocation of the resource to***, ***deallocation of the resource from*** the following objects: OB.RAM ***objects and*** OB.REG ***objects but the illegal condition register and the CRC control register when in warm reset***.

5.3.10 Stored data integrity monitoring and action (FDP_SDI.2)

116 The TSF shall monitor user data stored within the TSC for:

- ***single bit fails upon a read operation,***

- ***other actions are not described here***,

in OB.NVM***,*** on all objects, based on the following attributes: ***redundancy data***.

5.3.11 TSF Generation of secrets (FIA_SOS.2)

117 The TSF shall provide a mechanism to generate secrets that meet ***the*** NIST FIPS PUB-140-2:1999 ***standard for a Security Level 3 cryptographic module (statistical test upon demand)***.

118 The TSF shall be able to enforce the use of TSF generated secrets for ***SF_ALEA_A and SF_OBS_A***.

5.3.12 Potential Violation Analysis (FAU_SAA.1)

119 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.

120 The TOE Security Functions shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of auditable events ***in ISSUER and USER configurations, resulting from:***
- ***operating changes by the environment,***
- ***access control violation attempts,***
- ***bad NVM or CPU usages,***

known to indicate a potential security violation;

b) ***Make these indications available to the user after a warm reset.***

5.3.13 Unobservability (FPR_UNO.1)

121 ***In this security target, ability to observe an operation means revealing the value of a data during an operation on this data.***

122 The TOE Security Functions shall ensure that ***all end-users*** are:

- unable to observe the operation ***read*** on OB.ROM***,*** OB.RAM***,*** OB.REG ***and*** OB.NVM by S.TRUST ***and*** S.LIB.
- unable to observe the operation ***write*** on OB.RAM by S.TRUST ***and*** S.LIB.
- unable to observe the operation ***program or erase*** on OB.NVM by S.TRUST ***and*** S.LIB.

5.3.14 Notification of physical attack (FPT_PHP.2)

123 The TOE Security Functions shall provide unambiguous detection of physical tampering that might compromise the TOE Security Functions

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

125 For the ***clock and voltage supply operating changes by the environment in ISSUER and USER configurations,*** the TOE security functions shall monitor the devices and elements and notify the ***ISSUER administrator or the USER*** when physical tampering with the TOE security functions devices has occurred.

5.3.15 Resistance to physical attack (FPT_PHP.3)

126 The TOE Security Functions shall resist ***operating changes by the environment, and physical integrity tampering,*** to the ***clock and voltage supply*** by responding automatically such that the TOE security policy is not violated.

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

5.4 FUNCTIONAL REQUIREMENTS APPLICABLE TO USER CONFIGURATION

5.4.1 CRYPTOGRAPHIC OPERATION (FCS_COP.1)

128 The TSF shall perform:

- ***Encryption and decryption in Electronic Code Book (ECB) mode*** in accordance with a specified cryptographic algorithm:
  - ***the Data Encryption Standard (DES),*** and cryptographic key sizes ***of 56 effective bits*** ,
  - ***the Triple Data Encryption Standard (3DES),*** and cryptographic key sizes ***of 112 effective bits***

  that meet the following standards: ISO 8372:1987**,** ISO 8731-1:1987 ***and*** ISO/IEC 10116:1997**.**
- ***Encryption and decryption in Cipher Block Chaining (CBC) mode and compute a Message Authentication Code (MAC)*** in accordance with a specified cryptographic algorithm:
  - ***the Data Encryption Standard (DES),*** and cryptographic key sizes ***of 56 effective bits***,
  - ***the Triple Data Encryption Standard (3DES),*** and cryptographic key sizes ***of 112 effective bits,***

  that meet the following standards: ISO 8372:1987**,** ISO 8731-1:1987**,** ISO/IEC 9797:1994 ***and*** ISO/IEC 10116:1997**.**
- ***RSA recovery (encryption)*** in accordance with a specified cryptographic algorithm***, Rivest, Shamir & Adlemanís algorithm,*** and cryptographic key sizes ***multiples of 64 bits up to 1088 bits*** or cryptographic key sizes ***multiples of 64 bits larger than 1088 bits and up to 2176 bits*** that meet the following ***standards***: ISO/IEC 9796-2:1997 ***and*** MIT/LCS/TR-212.
- ***RSA signature (decryption) without the Chinese Remainder Theorem*** in accordance with a specified cryptographic algorithm***, Rivest, Shamir & Adlemanís algorithm,*** and cryptographic key sizes ***multiples of 64 bits up to 1088 bits*** or cryptographic key sizes ***multiples of 64 bits larger than 1088 bits and up to 2176 bits*** that meet the following ***standards***: ISO/IEC 9796-2:1997 ***and*** MIT/LCS/TR-212.
- ***Secure hash function*** in accordance with a specified cryptographic algorithm***, revised Secure Hash Algorithm (SHA-1),*** and ***result size of 160 bits on chained blocks of 512 bits*** that meet the following ***standards***: NIST FIPS PUB 180-1:1995 ***and*** ISO/IEC 10118-3:1998.

5.4.2 SUBSET INFORMATION FLOW CONTROL (FDP_IFC.1)

129 The TOE Security Functions shall enforce the ***SFP.IFC.SKC*** on ***the DSW cryptographic libraries (***S.LIB***), user keys and cryptographic sensitive data (***UD.KEY***,*** UD.CSD***) for the SKC operations specified in the iterations FCS_COP.1[SKC_*] of the FCS_COP.1 component***.

130 The TOE Security Functions shall enforce the ***SFP.IFC.COP*** on ***the DSW cryptographic libraries (***S.LIB***), user keys and cryptographic sensitive data (***UD.KEY***,*** UD.CSD***) for the cryptographic operations specified in all iterations of components of the cryptographic support class (FCS*[COP*]) selected***.

5.4.3 SIMPLE SECURITY ATTRIBUTES (FDP_IFF.1)

131 The TOE Security Functions shall enforce the ***SFP.IFC.SKC*** and the ***SFP.IFC.COP*** based on the following types of subject and information security attribute:

- ***the entry point of the STM library service .***

132 The TOE Security Functions shall permit an information flow between a controlled subject and a controlled information via a controlled operation.

133 The TSF shall provide the additional information flow control SFP rules:

- ***source and destination recipients must be authorised objects when loading and unloading SFP.IFC.SKC controlled information via SFP.IFC.SKC controlled operations.***
- ***source and destination recipients must be authorised objects when loading and unloading SFP.IFC.COP controlled information via SFP.IFC.COP controlled operations.***

134 The TSF shall enforce the following additional SFP capabilities: ***None***.

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

136 The TSF shall explicitly deny an information flow based on the following rules: ***None***.

5.4.4 PARTIAL ELIMINATION OF ILLICIT INFORMATION FLOWS (FDP_IFF.4)

137 The TSF shall:

- enforce the ***SFP.IFC.SKC*** to limit the capacity of ***electrical power consumption variations*** to ***a HODPA SOF high resistance level***.
- enforce the ***SFP.IFC.COP*** to limit the capacity of ***electrical power consumption and electromagnetic emanations variations*** to ***an SPA and EMA SOF high resistance level***.

138 The TSF shall:

- prevent ***electrical power consumption variations revealing SFP.IFC.COP controlled information thereby being DPA and HODPA proof***.
- prevent ***electrical power consumption and electromagnetic emanation variations revealing SFP.IFC.SKC controlled information thereby being SPA, DPA and EMA proof***.

5.4.5 CRYPTOGRAPHIC KEY GENERATION (FCS_CKM.1)

139 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm:

- ***Random number generation,*** and specified cryptographic key sizes ***of 1088 bits*** that meet the following ***standards***: NIST FIPS PUB-140-2:1999 ***for a security level 3 cryptographic module (statistical test on demand)***.
- ***Primes and RSA primes generation algorithm,*** and specified cryptographic key sizes ***multiples of 64 bits up to 1088 bits*** that meet the following ***standards***: NIST FIPS PUB-140-2:1999**,** ISO/IEC 9796-2:1997**,** NIST FIPS PUB 186**,** JoCSS ***and*** JoNT.
- ***RSA public and private keys computation algorithm,*** and specified cryptographic key sizes ***multiples of 64 bits greater than 128 bits and up to 2176 bits*** that meet the following ***standards***: NIST FIPS PUB-140-2:1999**,** ISO/IEC 9796-2:1997 ***and*** MIT/LCS/TR-212.

6 TOE SECURITY ASSURANCE REQUIREMENTS

140 The assurance requirements ***are*** EAL 4 augmented of additional assurance components listed in the following sections.

141 ***The components introduced by the*** PP/9806 are hierarchical to the components specified in EAL 4.

142 The components introduced by this Security Target are either hierarchical to those of the PP/9806 (ADV_FSP.3), or required to satisfy a dependency on either an additional SFR (AVA_CCA.1) or the maintenance of assurance class (ALC_FLR.1).

6.1 ASE: Security Target evaluation class

143 Although it is not explicitly required by the PP/9806, this class of security assurance requirements, not detailed here (see ISO/IEC 15408-3:1999), aims at establishing that this Security Target is complete, consistent, technically sound and hence suitable for use as the basis of the corresponding TOE evaluations.

6.2 ADV_FSP.3 Semiformal functional specification

Dependencies:

144 ADV_RCR.1.

Developer actions elements:

145 The developer shall provide a functional specification.

Content and presentation of evidence elements:

146 The functional specification shall describe the TSF and its external interfaces using a **semiformal** style, **supported by informal, explanatory text where appropriate**.

147 The functional specification shall be internally consistent.

148 The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

149 The functional specification shall completely represent the TSF.

150 The functional specification shall include rationale that the TSF is completely represented.

Evaluator action elements:

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

152 The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

6.3 ADV_IMP.2 Implementation of the TSF

Developer actions elements:

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

Content and presentation of evidence elements:

154 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.

155 The implementation representation shall be internally consistent.

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

Evaluator action elements:

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

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

6.4 ALC_DVS.2 Sufficiency of security measures

Developer actions elements:

159 The developer shall produce development security documentation.

Content and presentation of evidence elements:

160 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.

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

162 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:

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

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

6.5 ALC_FLR.1 Basic flaw remediation

Dependencies:

165 No dependencies.

Developer actions elements:

166 The developer shall document the flaw remediation procedures.

Content and presentation of evidence elements:

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

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

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

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

Evaluator action elements:

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

6.6 AVA_VLA.4 Highly resistant

Developer actions elements:

172 The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TOE security policy.

173 The developer shall document the disposition of identified vulnerabilities.

Content and presentation of evidence elements:

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

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

176 The evidence shall show that the search for vulnerabilities is systematic.

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

Evaluator action elements:

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

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

180 The evaluator shall perform an independent vulnerability analysis.

181 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.

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

6.7 AVA_CCA.1: Covert channel analysis

Dependencies:

183 ADV_FSP.2, ADV_IMP.2, AGD_ADM.1, AGD_USR.1.

Developer actions elements:

184 The developer shall conduct a search for covert channels for each information flow control policy.

185 The developer shall provide covert channel analysis documentation.

Content and presentation of evidence elements:

186 The analysis documentation shall identify covert channels and estimate their capacity.

187 The analysis documentation shall describe the procedures used for determining the existence of covert channels, and the information needed to carry out the covert channel analysis.

188 The analysis documentation shall describe all assumptions made during the covert channel analysis.

189 The analysis documentation shall describe the method used for estimating channel capacity, based on worst case scenarios.

190 The analysis documentation shall describe the worst case exploitation scenario for each identified covert channel.

Evaluator action elements:

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

192 The evaluator shall confirm that the results of the covert channel analysis show that the TOE meets its functional requirements.

193 The evaluator shall selectively validate the covert channel analysis through testing.

7 TOE SUMMARY SPECIFICATION

7.1 STATEMENT OF TOE SECURITY FUNCTIONS

194 The following security functions are an abstraction of the TOE Functional Specification.

7.1.1 SF_INIT_A: Hardware initialisation & TOE attribute initialisation

195 In TEST, ISSUER and USER configurations, this functionality ensures the following:

- the TOE starts running in a secure state,
- the TOE is securely initialised,
- the reset operation is correctly managed.

7.1.2 SF_CONFIG_A : TOE configuration switching and control

196 In TEST , ISSUER and USER configurations, this functionality ensures the switching and the control of TOE configuration.

197 This functionality ensures that the TOE is either in TEST, ISSUER or USER configuration.

198 The only authorised TOE configuration modifications are:

- TEST to ISSUER configuration by TEST administrator,
- ISSUER to USER configuration by ISSUER administrator.

199 This functionality is responsible for the TOE configuration detection and notification to the other resources of the TOE.

7.1.3 SF_INT_A: TOE logical integrity

200 This functionality is responsible for the following operations, performed according to actual TOE configuration:

- NVM, USR_ROM and ST_ROM integrity content verifications in TEST and ISSUER configurations,
- valid CPU usage and stack overflow verification in TEST, ISSUER and USER configurations.
- for correcting single bit fails upon a read operation,
- other actions not described here.

201 This functionality is responsible for reporting to SF_ADMINIS_A detected errors on CPU usage, stack overflow and EEPROM.

7.1.4 SF_TEST_A: Test of the TOE

202 This functionality is responsible for restricting access of the TOE TEST functionality to the TEST administrator in TEST configuration.

203 This functionality is responsible for restricting access of the TOE ISSUER functionality to the ISSUER administrator in ISSUER configuration.

204 In USER configuration, this functionality ensures that neither TOE TEST nor TOE ISSUER functionality can be accessed.

205 In TEST configuration, this functionality ensures the test of TOE functionality with respect to the IC specification.

7.1.5 SF_AUTH_A: Administrators authentication

206 In TEST configuration, this SF ensures that the only allowed TOE user is a TEST administrator.

207 In ISSUER configuration, this SF ensures that the only allowed TOE user is a ISSUER administrator.

208 A **SOF-high** strength of function is claimed for this SF.

7.1.6 SF_FWL_A: Storage and Function Access Firewall

209 TOE memories are partitioned. This partitioning is partially defined by the TOE user and partially by STM:

- ST_ROM mapping is STM defined,
- USR_ROM mapping is user defined,
- RAM and NVM mappings are partly STM defined and partly user defined.

210 In TEST, ISSUER and USER configurations, this security functionality monitors:

- access from memory locations to other locations for ROM, RAM and NVM,
- NVM use,
- register access,

and is responsible for the notification of violation attempts to SF_ADMINIS_A.

211 An access can be:

- a read, to registers, ROM, RAM or NVM,
- a write, to registers or RAM,
- a program, to NVM,
- an erase, to NVM.

212 Executability, Read, Write, Program and Erase right classes are defined by the user and STM for ROM, RAM and NVM.

7.1.7 SF_PHT_A: Physical tampering security function

213 In TEST, ISSUER and USER configurations, this functionality ensures the following:

- the TOE detects clock and voltage supply operating changes by the environment,

- the TOE detects attempts to violate its physical integrity,
- the TOE is always clocked with shape and timing within specified operating conditions.

7.1.8 SF_ADMINIS_A : Security violation administrator

214 In TEST, ISSUER and USER configurations, this functionality ensures the management of security violations attempts.

215 The security violations attempts which are managed are:

- access to unavailable or reserved memory locations,
- unauthorised access to user memories,
- unauthorised access to STM memories,
- bad CPU usage,
- bad NVM use,
- EEPROM single bit fails ,
- clock and voltage supply operating changes,
- TOE physical integrity abuse.

7.1.9 SF_OBS_A: Unobservability

216 In ISSUER and USER configurations, this security function addresses the Unobservability (FPR_UNO.1) and the Basic internal transfer protection (FDP_ITT.1) security functional requirements expressed in this document.

7.1.10 SF_SKCS_A: Symmetric Key Cryptography Support

217 In USER configuration, this security function implements the following standard symmetric key cryptography algorithms:

- Data Encryption Standard (DES) with 64 bits long keys (56 effective bits).

218 This functionality supports the following standard modes of operation, both for encryption and for decryption:

- DES by itself,
- Triple DES, chaining two DES encryption and one DES decryption.

219 Each of these modes of operation can be chained in the standard Cipher Block Chaining mode (CBC). In the encryption operation mode, this function can compute either a 64 bits long Message Authentication Code (MAC) or the encrypted data.

7.1.11 SF_AKCS_A: Asymmetric Key Cryptography Support

220 In USER configuration, this security function implements the following standard asymmetric key cryptography algorithms:

- RSA verification (encryption) with an RSA modulo up to 1088 bits,

- RSA verification (encryption) with an RSA modulo up to 2176 bits,
- RSA signature (decryption) without the Chinese Remainder Theorem (CRT), with an RSA modulo up to 1088 bits,
- RSA signature (decryption) with the Chinese Remainder Theorem (CRT), with an RSA modulo up to 2176 bits,
- RSA secret and public keys computation with an RSA modulo up to 2176 bits,
- Prime number and RSA prime number generation up to 1088 bits, with Rabin-Miller primality tests.

221 In USER configuration, this security function implements the following standard hash function:

- SHA-1 hash function chaining blocks of 512 bits to get a 160 bits result.

7.1.12 SF_ALEAS_A: Unpredictable Number Generation Support

222 In all configurations, this security function provides two unpredictable and unrelated 8 bits numbers.

223 In ISSUER and USER configurations, this security function supports the prevention of information leakage.

224 This security function ensures the generation of unpredictable numbers of 1088 bits, in USER configuration.

225 This security function can be qualified with the test metrics required by the NIST FIPS PUB-140-2:1999 standard for a Security Level 3 cryptographic module (statistical test upon demand).

7.2 STATEMENT OF ASSURANCE MEASURES

226 The ST19W Documentation Report shows the assurance measures, through a list of documents delivered, which are claimed to satisfy the stated assurance requirements.

8 PP CLAIMS

8.1 PP References

227 The ST19WK08 Generic Security Target **is compliant with** the requirements of the Smartcard Integrated Circuit Protection Profile PP/9806, Revision 2.0.

8.2 PP Refinements

228 The main refinements operated on the PP are:

- "Smartcard product" is refined into "Secure IC based product" to emphasize the packaging independence of the TOE,
- The product life-cycle is refined to include industrial parameters such as the delivery phase and the sites where the life-cycle processes are performed,
- Two security objectives for the TOE are refined to address the introduced organisational security policies, namely O.DIS_MEMORY and O.MOD_MEMORY,
- The SFR applicable to phase 3 are refined to be applicable to the logical phases TEST and ISSUER configurations,
- The "subset information flow control" SFR (FDP_IFC.1) and the corresponding "simple security attributes" SFR (FDP_IFF.1) are refined to be applicable to the whole TOE.

229 In Chapters 2, 3, 4 and 6, and in Annex A, PP refinements are indicated with typesetting text ***as indicated here***, original text being typeset as indicated here. Deleted parts are ***[***~~as indicated here~~***]***.

8.3 PP Additions

230 Two organisation security policies are added to provide hardware supported cryptography to users, namely OSP.SKCS and OSP.AKCS.

231 There are no additional objectives to those described in the PP/9806.

232 A simplified presentation of the TOE Security Policy (TSP) is added.

233 The following SFRs are added to the PP:

- **FDP_ITT.1 Basic internal transfer protection**, dependent on [FDP_ACC.1 or FDP_IFC.1],
- **FDP_RIP.1 Subset residual information protection**, no dependencies,
- **FDP_SDI.2 Stored data integrity monitoring and action**, no dependencies,
- **FIA_SOS.2 TSF Generation of secrets**, no dependencies,
- **FCS_COP.1 Cryptographic operation**, dependent on [FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2,
- **FCS_CKM.1 Cryptographic key generation**, dependent on [FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2,

- **FDP_IFF.4 Partial elimination of illicit information flows**, dependent on AVA_CCA.1, FDP_IFC.1.

234 The following SARs are added to the PP:

- **ADV_FSP.3 Semiformal functional specification**, dependent on ADV_RCR.1,
- **ALC_FLR.1 Basic flow remediation**, no dependencies,
- **AVA_CCA.1 Covert channels analysis**, dependent on ADV_FSP.2, ADV_IMP.2, AGD_ADM.1, AGD_USR.1,

9 RATIONALE

235 The rationale has been established for the whole ST19W platform and has been presented and evaluated in the ST19W Generic Security Target.

236 For confidentiality reasons, the rationale is not reproduced here.

10 REFERENCES

237 Protection Profile reference

Component description	Reference	Revision
Smartcard Integrated Circuit	PP/9806	2.0

238 Standards references

Identifier	Description
NIST FIPS PUB-140-2:1999	Security Requirements for Cryptographic Modules
NIST FIPS PUB 180-1:1995	Secure Hash Standard
NIST FIPS PUB 186	Recommended simplified Rabin-Miller primality tests for DSS
ISO 8372:1987	Information processing - Modes of operation for a 64-bit block cipher algorithm
ISO 8731-1:1987	Banking - Approved algorithms for message authentication -Part 1: DEA
ISO/IEC 9796-2:1997	Information technology - Security techniques - Digital signature scheme giving message recovery - Part 2: Mechanism using a hash function
ISO/IEC 9797:1994	Information technology - Security techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm
ISO/IEC 10116:1997	Information technology - Modes of operation of an n-bit block cipher algorithm
ISO/IEC 10118-3:1998	Information technology - Security techniques - Hash functions - Part 3: Dedicated hash functions
ISO/IEC 15408-1:1999	Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model
ISO/IEC 15408-2:1999	Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements
ISO/IEC 15408-3:1999	Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements
CC RA	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.
MIT/LCS/TR-212	On digital signatures and public key cryptosystems, Rivest, Shamir & Adleman Technical report MIT/LCS/TR-212, MIT Laboratory for computer sciences, January 1979
JoCSS	Riemann's hypothesis and tests for primality, Miller Journal of computer and system sciences, vol 13 n 3 p300-317
JoNT	Probabilistic algorithm for testing primality, Miller Journal of number theory, vol 12 n 1 p 128-138

Annex A : Glossary

Authentication data

Information used to verify the claimed identity of a user.

Authorised user

A user who may, in accordance with the TSP, perform an operation.

Cryptographic sensitive data (CSD)

User data appearing in plain text or otherwise unprotected form and whose disclosure or modification can compromise the security of a cryptographic module or the security of the information protected by the module.

Differential Power Analysis (DPA)

An analysis in variations of the electrical power consumption of a device, using advanced statistical methods and/or error correction techniques, for the purpose of extracting information correlated to secrets processed in the device. When several consumption traces are recombined during analysis to remove randomisation counter-measures, the analysis is known as Higher Order DPA (HODPA).

Embedded software

Software embedded in a ***secure IC*** may be ***located*** in any part of the nonvolatile memory ***(ROM and NVM)*** of the IC.

Secure IC based product

Packaged secure IC integrated in its end-usage carrier such as a Smartcard, a card reader, a set-top box, a PC board or any other suitable device.

Integrated Circuit (IC)

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

IC Dedicated Software

STM proprietary Dedicated SoftWare (DSW), embedded in ST_ROM, whose design is parameterised by the STM product assembly definition. This software contributes to the enforcement of the TSP. It also includes testing functionality and system libraries that are part of the API of the TOE; it is embedded in the IC (it is also known as IC firmware).

IC *developer*

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.

IC pre-personalization data

Any data that is stored in the nonvolatile memory for shipment between phases.

Memory access

Read and Modification (Write, Erase, program) access.

Object

An entity within the TSC that contains or receives information and upon which subjects perform operations.

Packaged IC

IC embedded in a physical package such as micromodules, DIPs, SOICs or TQFPs.

Personalizer

Institution (or its agent) responsible for the ***secure IC based product*** personalization and final testing.

Secret

Information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP.

Secure IC* Embedded SoftWare *(SICESW)

Embedded software in charge of generic functions of the ***secure IC*** such as Operating System, general routines and interpreters (***secure IC*** basic software) and embedded software dedicated to the applications (***secure IC*** application software).

***Secure IC* embedded software developer**

Institution (or its agent) responsible for the ***secure IC*** embedded software development and the specification of IC pre-personalization requirements***, if any***.

Security attribute

Information associated with subjects, users and/or objects that is used for the enforcement of the TSP.

Security derivation

The process by which a TOE summary specification is derived from the identification of the threatened assets in the TOE environment, establishing in turn: a security environment, a set of security objectives, a set of security requirements and finally a set of security functions and assurance measures (see CC, part 1, section 4.3 for a detailed explanation, notably figure 4.5).

Sensitive information

Any information identified as a security relevant element of the TOE such as:

- the application data of the TOE (such as IC pre-personalization requirements, IC and system specific data),
- the secure IC embedded software,
- the IC dedicated software,

- the IC specification, design, development tools and technology.

Simple Power Analysis (SPA)

A direct analysis, primarily visual, of patterns of instruction execution (or execution of individual instructions), obtained through monitoring the variations in electrical power consumption of a device, for the purpose of revealing the features and implementations of (cryptographic) algorithms and subsequently the values of the secrets they process in the device.

Smartcard

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

Software library

Set of software functions provided by STM in the DSW that implement driving and functional services offered to the embedded software of the secure IC based product.

Subject

An entity within the TSC that causes operations to be performed.

System integrator

Institution (or its agent) responsible for the ***secure IC based*** product system integration (terminal software developer, system developer ...).

TSF data

Data created by and for the TOE, that might affect the operation of the TOE.

User

Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

User data

Data created by and for the user, that doesnít affect the operation of the TOE.

Warm reset

Reset operation on the TOE without lowering power under the Power on Reset (POR) level.

Annex B: Abbreviations

ANSI

American National Standards Institute.

API

Application Program Interface.

CSD

Cryptographic Sensitive Data.

CC

Common Criteria ***Version 2.1 (ISO-15408).***

CFG

Configuration.

COP

Coprocessing.

CPU

Central Processing Unit.

DES

Data Encryption Standard.

DPA

Differential Power Analysis.

DSW

IC Proprietary Dedicated Software.

EAL

Evaluation Assurance Level.

EEPROM

Electrically Erasable Programmable Read Only Memory.

EMA

Electromagnetic Analysis.

FIPS

Federal Information Processing Standard.

HODPA

Higher Order Differential Power Analysis.

IOCI

Input Output and Control Interface.

ISO

International Standards Organisation.

IT

Information Technology.

LOCK

Lock of Page Attribute.

MACL

Memory Access Control Logic.

MAP

Modular Arithmetical Processor.

NIST

National Institute of Standards and Technology.

NVM

Non Volatile Memory.

OP

Operation Performed.

OSP

Organisational Security Policy.

PACL

Page Access Control Logic.

PC

Program Counter register.

PP

Protection Profile.

PUB

Publication Series.

RACL

Register Access Control Logic.

RAM

Random Access Memory.

ROM

Read Only Memory.

SAR

Security Assurance Requirement.

SF

Security function.

SFP

Security Function Policy.

SFP_MNGT

Management of policies.

SFR

Security Functional Requirement.

SICESW

Secure IC Embedded SoftWare.

SKC

Symmetric Key Cryptography.

SOF

Strength of function.

SP

Stack Pointer register.

SPA

Simple Power Analysis.

ST

Security Target.

ST_ROM

STM reserved ROM.

STM

STMicroelectronics.

TOE

Target of Evaluation.

TSC

TSF Scope of Control.

TSF

TOE Security Functions.

TSFI

TSF Interface.

TST&ISR

The logical phases TEST and ISSUER configurations.

TSP

TOE Security Policy.

TSS

TOE Summary Specification.

USR_ROM

User reserved ROM.

CONFIDENTIALITY OBLIGATIONS:
THIS DOCUMENT CONTAINS NO SENSITIVE INFORMATION.
ITS DISTRIBUTION IS NOT SUBJECT TO THE SIGNATURE OF AN NON-DISCLOSURE AGREEMENT (NDA).
IT IS CLASSIFIED **"PUBLIC"**

FURTHER COPIES CAN BE PROVIDED, PLEASE CONTACT
YOUR LOCAL ST SALES OFFICE OR THE FOLLOWING ADDRESS:

STMicroelectronics SA
SMART CARDS PRODUCTS MARKETING DPT
BP2 / ZI de Peynier Rousset / F-13106 ROUSSET Cedex / FRANCE
Fax: +33 4 42 68 87 29