

**ST19NA18
SECURITY TARGET - PUBLIC VERSION**

COMMON CRITERIA FOR IT SECURITY EVALUATION



TABLE OF CONTENTS

- 1 INTRODUCTION 5**
 - 1.1 IDENTIFICATION 5
 - 1.2 PURPOSE 5
 - 1.3 CONTEXT 5
 - 1.4 COMMON CRITERIA CONFORMANCE CLAIMS 6

- 2 ST19NA18 TOE DESCRIPTION 7**
 - 2.1 ST19NA18 PRODUCT DESCRIPTION 7
 - 2.2 SECURE IC BASED PRODUCT LIFE-CYCLE 9
 - 2.3 TOE ENVIRONMENT 12
 - 2.3.1 TOE Development Environment 12
 - 2.3.2 TOE production environment 12
 - 2.3.3 TOE user environment 12
 - 2.4 TOE LOGICAL PHASES 12
 - 2.5 TOE INTENDED USAGE 13
 - 2.6 GENERAL IT FEATURES OF THE TOE 13

- 3 TOE SECURITY ENVIRONMENT 14**
 - 3.1 ASSETS 14
 - 3.2 ASSUMPTIONS 14
 - 3.2.1 Assumptions on phase 1 17
 - 3.3 THREATS 17
 - 3.3.1 Threats on phases 2 to 7 18
 - 3.4 ORGANISATIONAL SECURITY POLICIES 18

- 4 SECURITY OBJECTIVES 20**
 - 4.1 SECURITY OBJECTIVES FOR THE TOE: 22
 - 4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT 22
 - 4.2.1 Objectives on phase 1 23
 - 4.3 SECURITY OBJECTIVES RATIONALE 24

- 5 SECURITY REQUIREMENTS 25**
 - 5.1 SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE 25
 - 5.1.1 SUBJECTS, OBJECTS, OPERATIONS AND DATA 28
 - 5.1.2 FUNCTIONAL REQUIREMENTS APPLICABLE TO TST&ISR 29
 - 5.1.3 FUNCTIONAL REQUIREMENTS APPLICABLE TO PHASES 3 TO 7 30

- 5.1.4 FUNCTIONAL REQUIREMENTS APPLICABLE TO USER CONFIGURATION 37
- 5.2 TOE SECURITY ASSURANCE REQUIREMENTS 39
- 5.3 REFINEMENT OF THE SECURITY ASSURANCE REQUIREMENTS 40
- 5.4 SECURITY REQUIREMENTS FOR THE ENVIRONMENT 41
 - 5.4.1 Security requirements for the operational IT environment 41
 - 5.4.2 Security requirements for the Non-IT environment 41
- 5.5 SECURITY REQUIREMENTS RATIONALE 43
- 6 TOE SUMMARY SPECIFICATION 44**
 - 6.1 STATEMENT OF TOE SECURITY FUNCTIONS 44
 - 6.1.1 SF_INIT_A: Hardware initialisation & TOE attribute initialisation 44
 - 6.1.2 SF_CONFIG_A: TOE configuration switching and control 44
 - 6.1.3 SF_INT_A: TOE logical integrity 44
 - 6.1.4 SF_TEST_A: Test of the TOE 45
 - 6.1.5 SF_AUTH_A: Administrators authentication 45
 - 6.1.6 SF_FWL_A: Storage and Function Access Firewall 45
 - 6.1.7 SF_PHT_A: Physical tampering security function 46
 - 6.1.8 SF_ADMINIS_A: Security violation administrator 46
 - 6.1.9 SF_OBS_A: Unobservability 46
 - 6.1.10 SF_SKCS_A: Symmetric Key Cryptography Support 47
 - 6.1.11 SF_AKCS_A: Asymmetric Key Cryptography Support 47
 - 6.1.12 SF_ALEAS_A: Unpredictable Number Generation Support 47
 - 6.2 STATEMENT OF ASSURANCE MEASURES 48
- 7 PP CLAIMS 49**
 - 7.1 PP REFERENCES 49
 - 7.2 PP REFINEMENTS 49
 - 7.3 PP ADDITIONS 49
 - 7.4 PP CLAIMS RATIONALE 50
- 8 RATIONALE 51**
- 9 REFERENCES 52**
- Annex A 54**

LIST OF FIGURES

Figure 1	ST19NA18 block diagram.....	9
Figure 2	Secure IC based product life-cycle.....	11

LIST OF TABLES

Table 1	Secure IC based product authorities by life-cycle phase	10
Table 2	TOE configurations	13
Table 3	Summary of security environment	15
Table 4	Summary of security objectives	20
Table 5	Summary of functional security requirements for the TOE	26
Table 6	FMT_MOF.1 iterations (management of security functions behaviour)	31
Table 7	FMT_MSA.3 and FMT_MSA.1 iterations (initialisation and management)	31
Table 8	Subjects, objects and applicable access control rules	33
Table 9	FPR_UNO.1 iterations (unobservability)	35
Table 10	FCS_COP.1 iterations (cryptographic operations)	37
Table 11	FCS_CKM.1 iterations (cryptographic key generation)	39
Table 12	TOE security assurance requirements	40
Table 13	Impact of EAL5 selection on BSI-PP-002-2001 refinements	41
Table 14	Summary of security requirements for the operational IT environment	42
Table 15	Summary of security requirements for the non-IT environment	42



ST19NA18

SECURITY TARGET - PUBLIC VERSION

COMMON CRITERIA FOR IT SECURITY EVALUATION

1 INTRODUCTION

1.1 IDENTIFICATION

- 1 Document identification: ST19NA18 SECURITY TARGET - PUBLIC VERSION.
- 2 Version number: V01.01, issued March 2007.
- 3 Registration: registered at ST Microelectronics under number SMD_ST19NA18_ST_07_001_V01.01.
- 4 TOE identification: given in [Chapter 2](#).

1.2 PURPOSE

- 5 This document presents **the ST19NA18 Security Target - Public version (ST)** of Smartcard Integrated Circuit (IC), with its Dedicated Software (DSW), designed on the **ST19N platform of STMicroelectronics**.
- 6 This document is a sanitized version of the Security Target used for the evaluation. It is classified as public information.
- 7 The ST19NA18 is an advanced Secure IC with Modular Arithmetic processor (MAP), IART, high speed CPU clock and 18KBytes high density EEPROM, perfectly fitting for applications needing high security and performance, including Pay TV and banking.
- 8 The precise references of the Target of Evaluation (TOE) and the secure IC general features are given in [Chapter 2](#).
- 9 A glossary of terms and abbreviations used in this document is given in [Annex A](#).

1.3 CONTEXT

- 10 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 IC's division of STMicroelectronics (ST).
- 11 The assurance level of the performed Common Criteria (CC) IT Security Evaluation is EAL 5 augmented. The minimum strength level for the TOE Security Functions (SFs) is SOF-high for all the security functions implemented by the TOE.
- 12 The intent of this ST is to specify the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) applicable to the ST19NA18 secure IC, and to summarise its chosen SFs and assurance measures.

- 13 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. The original text of this PP is typeset as [indicated here](#) when it is reproduced in this document.
- 14 This ST claims to be an instantiation of the "[Smartcard IC Platform](#)" Protection Profile (PP) registered and certified under the reference [BSI-PP-002-2001](#) in the German IT Security Evaluation and Certification Scheme **with the following augmentations**:
- Addition #1: "Support of Cipher Schemes" from [AUG](#)
 - Addition #4: "Area based Memory Access Control" from [AUG](#)
- The original text of this PP is typeset as [indicated here](#), its augmentations from [AUG](#) as [indicated here](#), when they are reproduced in this document.
- 15 Certifying authorities have recognized both Protection Profiles to lead to comparable chip security evaluations, as stated in "[BSI_9806_0002_2001](#)" and in "[DCSSI_CCN.624](#)", although with slightly different conclusions with respect to composition, see "[DCSSI_CCN.648](#)".
- 16 Extensions introduced in this ST to the SFRs of both Protection Profile (PP) are **exclusively** drawn from the Common Criteria part 2 standard SFRs.
- 17 This ST makes various refinements to the above mentioned PPs. They are all properly identified in the text typeset as **indicated here**. The original text of the PPs is repeated as scarcely as possible in this document for reading convenience. All PPs identifiers have been however prefixed by their respective PP origin label: **9806** for [PP/9806](#), **BSI** for [BSI-PP-002-2001](#), **AUG1** for Addition #1 of [AUG](#) and **AUG4** for Addition #4 of [AUG](#). This conservative approach leads undoubtedly to some redundancy but enables full traceability.

1.4 COMMON CRITERIA CONFORMANCE CLAIMS

- 18 The ST19NA18 Security Target is:
- [PP/9806](#) conformant, extended with two [CCMB-2005-08-002](#) SFRs,
 - [BSI-PP-002-2001](#) conformant, augmented with [AUG](#) additions #1 and #4,
 - **EAL 5** augmented by ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4,
 - The minimum strength of functions level for the SFRs is **SOF-high**,
 - [CCMB-2005-08-002](#) extended (as per [BSI-PP-002-2001](#) requirements)
 - [CCMB-2005-08-003](#) conformant.

2 ST19NA18 TOE DESCRIPTION

2.1 ST19NA18 PRODUCT DESCRIPTION

19 This section describes the ST19NA18, a serial access microcontroller specially designed for cost-effective secure portable applications, member of the ST19N platform.

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

21 The ST19NA18 is manufactured using an advanced highly reliable ST CMOS EEPROM submicron technology.

The ST19N platform is based on the ST19W platform which comprise many already EAL5+ certified products. The ST19NA18 offers even enhanced security functionalities and mechanisms.

It is based on the STMicroelectronics 8-bit CPU already implemented on the ST19W product family and includes on-chip memories: User ROM, User RAM and EEPROM with state-of-the-art security features. ROM, RAM and EEPROM memories can be configured into partitions with customized access rules.

The CPU includes the Arithmetic Logic Unit (ALU), the control logic and registers available to the User.

Access from any memory area to another is protected by 3 hardware firewalls, protecting memories, MAP and EDES. Access rules are user-defined and can be selected by mask options.

A specific logic block, named 'Security Administrator', is added to the microcontroller to achieve an extremely high level of security against software and hardware attacks.

This device also includes two True Random Number Generators compliant with both FIPS 140-2 and AIS31.

An Enhanced DES accelerator is accessible via cryptographic software libraries located in ST ROM for symmetrical algorithms (DES, Triple DES computations and CBC mode). This module provides a mathematically proven protection against side channel attacks (SPA, DPA, EMA, DEMA, DFA).

To support efficiently Public Key cryptography, a Modular Arithmetic Processor (MAP) based on a 1088-bit processor architecture processes very efficiently modular arithmetic up to 2176 bits using Montgomery method, including modular exponentiation with or without CRT. A software library provides additional primitives, including prime numbers generation up to 1088 bits, enabling the card to generate its own RSA and DSA keys.

A software library supporting the Advanced Encryption Standard (AES) with 128-bit key, allows AES-128 block encryption and decryption. This module provides a mathematically proven protection against side channel attacks.

Two serial interfaces compatible with the ISO 7816-3 standard are available. The ISO Asynchronous Receiver Transmitter (IART) provides high speed serial data capability.

A CRC calculation accelerator block is also available and is directly accessible by the User.

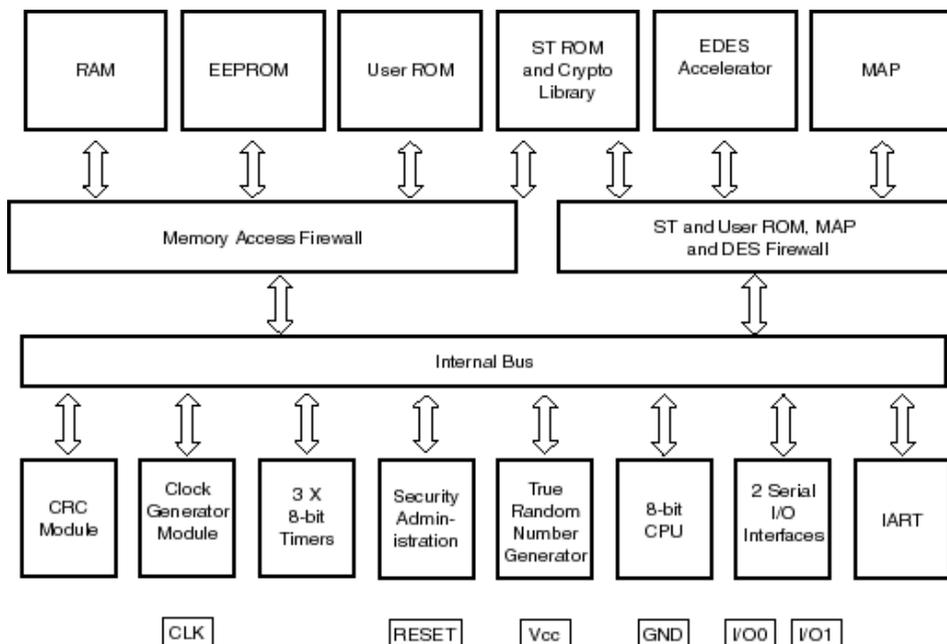
High performance can be reached by using high speed internal clock frequency (up to 28 MHz).

To summarize, the ST19NA18 provides very powerful features for high level security:

- Die integrity,
- Glitch detector,
- Signal filtering,
- Memories scrambling,
- Power-on reset management,
- EEPROM flash programming,
- RAM destruction after POR and Reset,
- True Random Number Generator,
- Environment sensors,
- Firewall against unauthorized access to memories,
- Security administrator to manage security detector alerts including fault injection control,
- EEPROM memory integrity check,
- Code Signature mechanism,
- User ROM access protected area,
- Extra Security Control register.

- 22 The TOE 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 implementation), AES and RSA algorithms).
- 23 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.
- 24 [Figure 1](#) provides a block diagram overview of the ST19NA18.

Figure 1 ST19NA18 block diagram



558

2.2 SECURE IC BASED PRODUCT LIFE-CYCLE

25 The secure IC based product life-cycle is decomposed into 7 phases. Each of these phases has the very same boundaries as those defined in both claimed protection profiles.

26 The authorities involved in each phase are described in [Table 1](#).

27 The **limit of the evaluation** defines the scope of responsibility of ST in terms of security. This limit, corresponding to the term "TOE Delivery" of [BSI-PP-002-2001](#), is phase 3.

28 The limit of **the evaluation** corresponds to phases 2 and 3, including the delivery and verification procedures of phase 1, 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 **evaluation**.

29 [Figure 2](#) describes the secure IC based product life cycle.

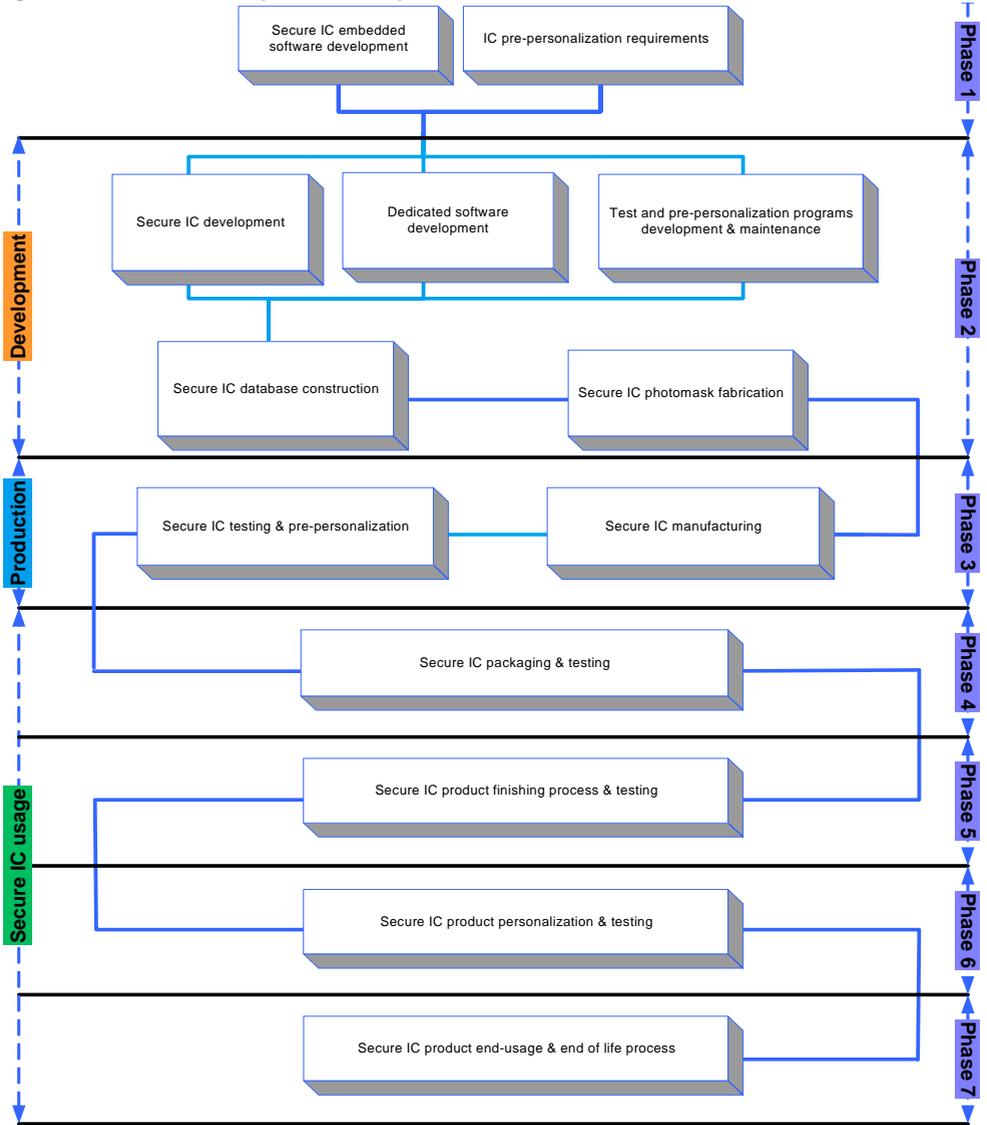
Table 1 Secure IC based product authorities by life-cycle phase

Phase	Name, authority and description
1	<p>Secure IC embedded software development:</p> <p>the secure IC embedded software developer is in charge of the secure IC embedded software development and the specification of IC pre-personalization requirements.</p>

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

Phase	Name, authority and description
2	<p style="text-align: center;">IC development:</p> <p>ST 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.</p>
3	<p style="text-align: center;">IC manufacturing and testing:</p> <p>ST is responsible for producing the IC through three main steps: IC manufacturing, IC testing, and IC pre-personalization.</p>
4	<p style="text-align: center;">IC packaging and testing:</p> <p>the IC packaging manufacturer is responsible for the IC packaging and testing.</p>
5	<p style="text-align: center;">Secure IC product finishing process:</p> <p>the secure IC product manufacturer is responsible for the secure IC product finishing process and testing.</p>
6	<p style="text-align: center;">Secure IC personalization:</p> <p>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.</p>
7	<p style="text-align: center;">Secure IC end-usage:</p> <p>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.</p>

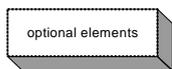
Figure 2 Secure IC based product life-cycle



Keys:

Trusted delivery & verification procedures

Internal security organisational procedures



2.3 TOE ENVIRONMENT

- 30 Considering the TOE, three types of environment are defined:
- Development environment corresponding to phase 2,
 - Production environment corresponding to phase 3,
 - User environment, from phase 4 to phase 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 [ST19NA18 Security Target](#) to include industrial parameters whose definition is reproduced hereafter for readers convenience.
- 33 The development centres 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 [ST19NA18 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 Japan**.
- 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 ST19NA18 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	ISSUER or USER	Packaging manufacturer (not ST)
Phase 5	ISSUER or USER	Secure IC product manufacturer (not ST)
Phase 6	ISSUER or USER	Personalizer (not ST)
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.

49 A summary of all these security aspects and their respective conditions is provided in [Table 3](#). Note that the origin of each aspect is clearly identified in the prefix of its label.

50 Most of these security aspects can therefore be easily found in the respective protection profiles. Only those originating in [AUG](#) are detailed in the following sections.

3.1 ASSETS

51 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 User Data, especially those that can be manipulated and/or disclosed while being stored or processed by the TOE,
- the **secure IC** embedded software,
- the IC dedicated software,
- the IC specification, design, development tools and technology,
- **TOE's correct operation (including its random number generator and added functionality, if any).**

52 The TOE itself is therefore an asset.

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

54 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).

55 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

56 The assumptions are described in the [PP/9806](#), section 3.2 and in the [BSI-PP-002-2001](#), section 3.2. Only those originating in [AUG](#) are detailed in the following sections.

Table 3 Summary of security environment

	Label	Title	Condition
Assumptions	9806.A.SOFT_ARCHI	Software Architecture	Phase 1
	BSI.A.Plat-Appl	Usage of Hardware Platform	
	BSI.A.Resp-APPL	Treatment of User Data	
	AUG1.A.Key-Function	Usage of key-dependent functions	
	9806.A.DEV_ORG	Development Organization	Phases 4 to 7
	BSI.A.Process-Card	Protection during Packaging, Finishing, Personalisation	
	9806.A.DLV_PROTECT	Delivery Protection	
	9806.A.DLV_AUDIT	Delivery Audit	
	9806.A.DLV_RESP	Delivery Responsibility	
	9806.A.USE_TEST	Use of Testing	Phases 4 to 6
9806.A.USE_PROD (BSI.A.Process-Card)	Use of Security Procedures		
9806.A.USE_DIAG	Use of Secure Dialogue	Phase 7	
9806.A.USE_SYS	Use of Secure System		
TOE threats	9806.T.CLON	Functional cloning of the TOE	See Table 4 of the ST19NA18 Security Target
	9806.T.DIS_SOFT	Unauthorized disclosure of secure IC embedded software and data	
	9806.T.DIS_DSOFT	Unauthorized disclosure of IC dedicated software	
	BSI.T.Leak-Inherent	Inherent Information Leakage	
	BSI.T.Leak-Forced	Forced Information Leakage	
	BSI.T.Phys-Probing	Physical Probing	
	BSI.T.RND	Deficiency of Random Numbers	
	9806.T.DIS_DESIGN	Unauthorized disclosure of IC design	
	BSI.T.Abuse-Func	Abuse of Functionality	
	AUG4.T.Mem-Access	Memory Access Violation	
	9806.T.MOD_SOFT	Unauthorized modification of secure IC embedded software and data	
	9806.T.MOD_DSOFT	Unauthorized modification of IC dedicated software	
	9806.T.MOD_DESIGN	Unauthorized modification of IC design	
	BSI.T.Malfunction	Malfunction due to Environmental Stress	
BSI.T.Phys-Manipulation	Physical Manipulation		

Table 3 Summary of security environment

	Label	Title	Condition
Environment threats	9806.T.DIS_INFO	Disclosure of assets delivered by ST	See Table 4 of the ST19NA18 Security Target
	9806.T.DIS_DEL	Disclosure of assets during delivery to ST	
	9806.T.DIS_TEST	Unauthorized disclosure of test information	
	9806.T.DIS_TOOLS	Unauthorized disclosure of development tools	
	9806.T.DIS_PHOTOMASK	Unauthorized disclosure of photomask information	
	9806.T.T_DEL	Theft of assets during delivery to ST	
	9806.T.T_SAMPLE	Theft or unauthorized use of TOE silicon samples	
	9806.T.T_PHOTOMASK	Theft or unauthorized use of TOE photomasks	
	9806.T.T_PRODUCT	Theft or unauthorized use of secure IC based products	
	9806.T.MOD_DEL	Modification of assets during delivery to ST	
9806.T.MOD_PHOTOMASK	Theft or unauthorized use of TOEs photomasks		
OSPs	BSI.P.Process-TOE	Protection during TOE Development and Production	
	AUG1.P.Add Functions	Additional Specific Security Functionality (Cipher Scheme Support)	

3.2.1 Assumptions on phase 1

AUG1.A.Key-Function Usage of key-dependent functions:

Key-dependent functions, if any, shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to leakage attacks (as described under [BSI.T.Leak-Inherent](#) and [BSI.T.Leak-Forced](#)).

Note that here the routines that may compromise keys when being executed are part of the Smartcard Embedded Software. In contrast to this the threats [BSI.T.Leak-Inherent](#) and [BSI.T.Leak-Forced](#) address (i) the cryptographic routines which are part of the TOE and (ii) the processing of User Data including cryptographic keys.

3.3 THREATS

57 The threats are described in the [PP/9806](#), section 3.3 and in [BSI-PP-002-2001](#), section 3.3. Only those originating in [AUG](#) are detailed in the following sections.

3.3.1 Threats on phases 2 to 7

3.3.1.1 Theft or unauthorized use of assets.

AUG4.T.Mem-Access

Memory Access Violation:

Parts of the Smartcard Embedded Software may cause security violations by accidentally or deliberately accessing restricted data (which may include code). Any restrictions are defined by the security policy of the specific application context and must be implemented by the Smartcard Embedded Software.

Clarification: This threat does not address the proper definition and management of the security rules implemented by the Smartcard Embedded Software, this being a software design and correctness issue. This threat addresses the reliability of the abstract machine targeted by the software implementation. To avert the threat, the set of access rules provided by this TOE should be undefeated if operated according to the provided guidance. The threat is not realized if the Embedded Software is designed or implemented to grant access to restricted information. It is realized if an implemented access denial is granted under unexpected conditions or if the execution machinery does not effectively control a controlled access.

Here the attacker is expected to (i)take advantage of flaws in the design and/or the implementation of the TOE memory access rules (refer to BSI.T.Abuse-Func but for functions available after TOE delivery), (ii)introduce flaws by forcing operational conditions (refer to BSI.T.Malfunction) and/or by physical manipulation (refer to BSI.T.Phys-Manipulation). This attacker is expected to have a high level potential of attack

3.4 ORGANISATIONAL SECURITY POLICIES

- 58 The TOE provides specific security functionality that can be used by the Smartcard Embedded Software. In the following specific security functionality is listed which is not derived from threats identified for the TOE's environment because it can only be decided in the context of the smartcard application, against which threats the Smartcard Embedded Software will use the specific security functionality.
- 59 **ST** applies the policy Additional Specific Security Functionality (AUG1.P.Add Functions) as specified below.
- 60 **ST** applies the policy Protection during TOE Development and Production (BSI.P.Process-TOE) as specified below.
- 61 **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 this TOE should further define them.**

AUG1.P.Add Functions Additional Specific Security Functionality:

The TOE shall provide the following specific security functionality to the Smartcard Embedded Software:

- Data Encryption Standard (DES),
- Triple Data Encryption Standard (3DES),
- Advanced Encryption Standard (AES),
- **Secure Hashing (SHA-1)**,
- **Rivest-Shamir-Adleman (RSA)**,
- **Prime Number Generation (Miller-Rabin test)**

Note that DES is no longer recommended as an encryption function in the context of smart card applications. Hence, Smartcard Embedded Software may need to use triple DES to achieve a suitable strength, see [AUG1.A.Key-Function](#).

4 SECURITY OBJECTIVES

- 62 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,
 - provide random numbers,
 - provide cryptographic support and access control functionality.
- 63 A summary of all security objectives is provided in Table 4. Note that the origin of each objective is clearly identified in the prefix of its label.
- 64 Most of these security aspects can therefore be easily found in the respective protection profiles. Only those originating in AUG are detailed in the following sections..

Table 4 Summary of security objectives

	Label	Title
TOE	9806.O.TAMPER	Prevent physical tampering of security critical parts
	BSI.O.Phys-Probing	Protection against Physical Probing
	BSI.O.Phys-Manipulation	Protection against Physical Manipulation
	9806.O.CLON	Prevent functional cloning
	BSI.O.Identification	TOE Identification
	9806.O.OPERATE	Ensure SF continued correct operation
	BSI.O.Malfunction	Protection against Malfunctions
	BSI.O.RND	Random Numbers
	AUG1.O.Add-Functions	Additional Specific Security Functionality
	9806.O.FLAW	Flawless design, implementation and operation
	9806.O.DIS_MECHANISM	Protection of hardware security mechanisms against unauthorized disclosure
	BSI.O.Abuse-Func	Protection against Abuse of Functionality
	9806.O.DIS_MEMORY	Protection of sensitive information stored in memories against unauthorized disclosure
	BSI.O.Leak-Inherent	Protection against Inherent Information Leakage
	BSI.O.Leak-Forced	Protection against Forced Information Leakage
	9806.O.MOD_MEMORY	Protection of sensitive information stored in memories against any controlled corruption or unauthorized modification
	AUG4.O.Mem Access	Area based Memory Access Control

Table 4 Summary of security objectives

	Label	Title
Environments	9806.O.DEV_DIS	Controlled distribution of TOE information for development
	9806.O.SOFT_DLV	Trusted delivery of secure IC embedded software
	9806.O.SOFT_MECH	Usage of secure IC as recommended in guidance
	BSI.OE.Plat-AppI	Usage of Hardware Platform with AUG1.Clarification & AUG4.Clarification
	BSI.OE.Resp-AppI	Treatment of User Data with AUG1.Clarification & AUG4.Clarification
	9806.O.DEV_TOOLS	Usage of secure development tools
	BSI.OE.Process-TOE	Protection during TOE Development and Production
	9806.O.SOFT_ACS	Controlled access to secure IC embedded software
	9806.O.DESIGN_ACS	Controlled access to the design of the secure IC
	9806.O.DSOFT_ACS	Controlled access to the dedicated software
	9806.O.MECH_ACS	Controlled access to security mechanisms specifications
	9806.O.TI_ACS	Controlled access to security relevant technology
	9806.O.MASK_FAB	Protection of mask deliveries and fabrication
	9806.O.TOE_PRT	TOE protection during production
	9806.O.IC_DLV	Protection of secure IC during deliveries
	9806.O.DLV_PROTECT	Protection of TOE material/information under delivery
	9806.O.DLV_AUDIT	Tracked delivery process
	9806.O.DLV_RESP	Qualified personnel for delivery
	BSI.OE.Process-Card	Protection during Packaging, Finishing and Personalisation
	9806.O.TEST_OPERATE	Test securely operated
9806.O.USE_DIAG	Secure communications in user environment	
9806.O.USE_SYS	Secure system in user environment	

4.1 SECURITY OBJECTIVES FOR THE TOE:

AUG1.O.Add-Functions

Additional Specific Security Functionality:

The TOE must provide the following specific security functionality to the Smartcard Embedded Software:

- Data Encryption Standard (DES),
- Triple Data Encryption Standard (3DES),
- Advanced Encryption Standard (AES),
- **Secure Hashing (SHA-1)**,
- Rivest-Shamir-Adleman (RSA),
- **Prime Number Generation (Miller-Rabin test)**.

AUG4.O.Mem Access

Area based Memory Access Control:

The TOE must provide the Smartcard Embedded Software with the capability to define restricted access memory areas. The TOE must then enforce the partitioning of such memory areas so that access of software to memory areas is controlled as required, for example, in a multi-application environment.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

4.2.1 Objectives on phase 1

BSI.OE.Plat-Appl

Usage of Hardware Platform:

To ensure that the TOE is used in a secure manner the Smartcard Embedded Software shall be designed so that the requirements from the following documents are met:

- (i) hardware data sheet for the TOE,
- (ii) TOE application notes dedicated software user manuals,
- (iii) TOE security user guidance, and
- (iii) findings of the TOE evaluation reports relevant for the Smartcard Embedded Software.

AUG1.Clariication: When the TOE supports cipher schemes as additional specific security functionality and if required, the Smartcard Embedded Software shall use these cryptographic services of the TOE and their interface as specified. When key-dependent functions implemented in the Smartcard Embedded Software are just being executed, the Smartcard Embedded Software must provide protection against disclosure of confidential data (User Data) stored and/or processed in the TOE by using the methods described under "Inherent Information Leakage" ([BSI.T.Leak-Inherent](#)) and "Forced Information Leakage" ([BSI.T.Leak-Forced](#)).

AUG4.Clariication: For the separation of different applications, the Smartcard Embedded Software may implement a memory management scheme based upon security mechanisms of the TOE as required by the security policy defined for the specific application context.

BSI.OE.Resp-AppI

Treatment of User Data:

Security relevant User Data (especially cryptographic keys) are treated by the Smartcard Embedded Software as required by the security needs of the specific application context.

For example the Smartcard Embedded Software will not disclose security relevant user data to unauthorised users or processes when communicating with a terminal.

AUG1.Clarification: By definition cipher or plain text data and cryptographic keys are User Data. The Smartcard Embedded Software shall treat these data appropriately, use only proper secret keys (chosen from a large key space) as input for the cryptographic function of the TOE and use keys and functions appropriately in order to ensure the strength of cryptographic operation.

This means that keys are treated as confidential as soon as they are generated. The keys must be unique with a very high probability, as well as cryptographically strong. For example, it must be ensured that it is beyond practicality to derive the private key from a public key if asymmetric algorithms are used. If keys are imported into the TOE and/or derived from other keys, quality and confidentiality must be maintained. This implies that appropriate key management has to be realised in the environment.

AUG4.Clarification: The treatment of User Data is still required when a multi-application operating system is implemented as part of the Smartcard Embedded Software on the TOE. In this case the multi-application operating system should not disclose security relevant user data of one application to another application when it is processed or stored on the TOE.

4.3 SECURITY OBJECTIVES RATIONALE

- 65 The security objectives rationale has been presented and evaluated in the [ST19NA18 Security Target](#).
- 66 For confidentiality reasons, this rationale is not reproduced here.

5 SECURITY REQUIREMENTS

67 This chapter on security requirements contains a section on security functional requirements (SFRs) for the TOE (Section 5.1), a section on security assurance requirements (SARs) for the TOE (Section 5.2), a section on the refinements of these SARs (Section 5.3) and a section on security requirements for the environment (Section 5.4) as required by the "BSI-PP-002-2001" Protection Profile. This chapter includes a section with the security requirements rationale (Section 5.5).

5.1 SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE

68 Security Functional Requirements (SFRs) from the "PP/9806" Protection Profile (PP) are **exclusively** drawn from CCMB-2005-08-002.

69 The following SFRs from the "BSI-PP-002-2001" Protection Profile are **extensions** to CCMB-2005-08-002:

- **FCS_RND** Generation of random numbers,
- **FMT_LIM** Limited capabilities and availability,
- **FAU_SAS** Audit data storage.

The reader can find their certified definitions in the text of the "BSI-PP-002-2001" Protection Profile.

70 All extensions to the SFRs of the "PP/9806" and of the "BSI-PP-002-2001" Protection Profiles (PPs) are **exclusively** drawn from CCMB-2005-08-002.

71 All iterations, assignments, selections, or refinements on SFRs have been performed according to section 4.4.1.3.2 of CCMB-2005-08-001. They are easily identified in the following text as they appear **as indicated here**. Note that in order to improve readability, iterations are often expressed within tables.

72 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.

73 Since the TOE can be in the ISSUER configuration in Phases 4 to 6, as specified in Table 2, 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)**.

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

75 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.

76 The selected security functional requirements for the TOE and their respective origin and type are summarized in the following pages in Table 5.

Table 5 Summary of functional security requirements for the TOE

	Label	Title	Addressing	Origin	Type
TST&ISR	FIA_ATD.1	User attribute definition	All objectives in TST&ISR	PP/9806 Operated	CCMB-2005-08-002
	FIA_UID.2	User identification before any action		PP/9806	
	FIA_UAU.2	User authentication before any action		PP/9806	
	FPT_TST.1	TOE Security Functions testing	Correct operation	PP/9806 Operated	
	FDP_SDI.1	Stored data integrity monitoring	TOE Integrity	PP/9806 Operated	
	FAU_SAS.1	Audit storage	Lack of TOE identification	BSI-PP-002-2001	

Table 5 Summary of functional security requirements for the TOE

	Label	Title	Addressing	Origin	Type	
Phases 3 to 7	FMT_SMR.1	Security roles	Correct operation	PP/9806 Operated	CCMB-2005-08-002	
	FMT_MOF.1	Management of security functions behaviour				
	FMT_MSA.3	Static attribute initialisation				
	FMT_MSA.1	Management of security attribute				
	FMT_SMF.1	Specification of management functions				New dependency Operated
	FMT_LIM.1	Limited capabilities	Abuse of functionality	BSI-PP-002-2001	Extended	
	FMT_LIM.2	Limited availability				
	FDP_ACC.2	Complete Access control	Memory access violation	PP/9806 Operated	CCMB-2005-08-002	
	FDP_ACF.1	Security attribute based access control				
	FRU_FLT.2	Limited fault tolerance	Malfunction	BSI-PP-002-2001		
	FPT_FLS.1	Failure with preservation of secure state				
	FAU_SAA.1	Potential violation analysis				PP/9806 Operated
	FPT_SEP.1	TSF domain separation				BSI-PP-002-2001
	FDP_SDI.2	Stored data integrity monitoring and action	TOE Integrity	Security Target Operated		
	FPT_PHP.2	Notification of physical attack	Physical manipulation & probing	PP/9806 Operated		
	FPT_PHP.3	Resistance to physical attack		PP/9806 Operated BSI-PP-002-2001		
	FPR_UNO.1	Unobservability	Leakage	PP/9806 Operated		
	FDP_ITT.1	Basic internal transfer protection		BSI-PP-002-2001		
	FPT_ITT.1	Basic TSF data internal protection				
	FDP_IFC.1	Subset information flow control		PP/9806 Operated BSI-PP-002-2001		
FDP_IFF.1	Simple security attributes	PP/9806 Operated				
FDP_RIP.1	Subset residual information protection	Security Target Operated				
FCS_RND.1	Quality metrics for random numbers	Weak cryptographic quality of random numbers		BSI-PP-002-2001 Operated	Extended	

Table 5 Summary of functional security requirements for the TOE

	Label	Title	Addressing	Origin	Type
USER	FCS_COP.1	Cryptographic operation	Cipher scheme support	AUG #1 Operated	CCMB-2005-08-002
	FCS_CKM.1	Cryptographic key generation		Security Target Operated	

5.1.1 SUBJECTS, OBJECTS, OPERATIONS AND DATA

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

5.1.1.1 Subjects

78 For the ST19NA18, the TSP identifies the following subjects:

- S.TRUST ST **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 ST **trusted functional process** activated during a call to execute a service available in the ST 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.

5.1.1.2 Objects and operations

79 For the ST19NA18, 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 ST 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 ST library service available to the User when the TOE is in USER configuration.
OB.PROT_ROM	Any part of the protected User ROM. These objects can be operated as any OB.ROM object.

5.1.2 FUNCTIONAL REQUIREMENTS APPLICABLE TO TST&ISR**5.1.2.1 User attribute definition (FIA_ATD.1)**

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

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

5.1.2.2 User identification before any action (FIA_UID.2)

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

5.1.2.3 User authentication before any action (FIA_UAU.2)

82 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.

5.1.2.4 TOE Security Functions testing (FPT_TST.1)

83 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**.

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

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

5.1.2.5 Stored data integrity monitoring (FDP_SDI.1)

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

5.1.2.6 Audit storage (FAU_SAS.1)

87 The TSF shall provide **test personnel before TOE Delivery** with the capability to store the **Initialisation Data and/or Pre-personalisation Data and/or supplements of the Smartcard Embedded Software** in the audit records.

Clarification:

- **test personnel before TOE Delivery, means TEST administrator if TOE delivery is in ISSUER configuration,**
- **test personnel before TOE Delivery, means TEST administrator and/or ISSUER administrator if TOE delivery is in USER configuration.**

5.1.3 FUNCTIONAL REQUIREMENTS APPLICABLE TO PHASES 3 TO 7

5.1.3.1 Security roles (FMT_SMR.1)

88 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 ST 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.**

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

5.1.3.2 Management of security functions behaviour (FMT_MOF.1)

90 The TOE Security Functions shall restrict the ability to **perform as indicated in Table 6** on the functions **listed in Table 6** to **the authorised identified roles in Table 6**.

Table 6 FMT_MOF.1 iterations (management of security functions behaviour)

[selection: determine the behaviour of, disable, enable, modify the behaviour of]	[assignment: list of functions]	[assignment: the authorised identified roles]
<i>Modify the behaviour of</i>	<ul style="list-style-type: none"> - SF_INIT_A - SF_CONFIG_A - SF_INT_A - SF_AUTH_A - SF_TEST_A - SF_ADMINIS_A - SF_OBS_A 	<i>TEST administrator</i>
<i>Modify the behaviour of</i>	<ul style="list-style-type: none"> - SF_CONFIG_A - SF_INT_A - SF_AUTH_A - SF_TEST_A - SF_ADMINIS_A - SF_ALEA_A 	<i>ISSUER administrator</i>

5.1.3.3 Static attribute initialisation (FMT_MSA.3)

91 The TSF shall enforce the **Location Based Access Control Policy and the Construction Flow Control Policy** to provide default values for security attributes that are used to enforce the security function policy **as indicated in Table 7**.

92 The TOE Security Functions shall allow the **authorised identified roles in Table 7** to specify alternate initial values to override the default values when an object or information is created.

5.1.3.4 Management of security attributes (FMT_MSA.1)

93 The TSF shall enforce the **Location Based Access Control Policy and the Construction Flow Control Policy** to restrict the ability to **perform operations in Table 7** to security attributes **in Table 7** to **the authorised identified roles in Table 7**.

Table 7 FMT_MSA.3 and FMT_MSA.1 iterations (initialisation and management)

[assignment: list of security attributes]	[selection: choose any of restrictive, permissive, [assignment: other property]]	FMT_MSA.3 [assignment: the authorised identified roles]	FMT_MSA.1 [selection: change_default, query, modify, delete, [assignment: other operations]]
			[assignment: the authorised identified roles]
For confidentiality reasons, this table content is detailed in the ST19NA18 Security Target			

5.1.3.5 Specification of management functions (FMT_SMF.1)

94 The TOE Security Functions shall be capable of performing the following security management function:

- **Modifying the TOE configuration**
- **Authenticating the TEST administrator and the ISSUER administrator**
- **Modifying the security functions behaviour as indicated in Table 6**

5.1.3.6 Limited capabilities (FMT_LIM.1)

95 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: Limited capability and availability Policy.

5.1.3.7 Limited availability (FMT_LIM.2)

96 The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: Limited capability and availability Policy.

97 **SFP_1: Limited capability and availability Policy**

Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.

98 **Refinement:**

Test Features are those provided by the commands in the DSW :

- **OB.CMD_TST, if TOE delivery is in ISSUER configuration;**
- **OB.CMD_TST and OB.CMD_ISR, if TOE delivery is in USER configuration.**

5.1.3.8 Complete access control (FDP_ACC.2)

99 The TOE Security Functions shall enforce the **Location Based Access Control Policy** on **all subjects and objects in Table 8** and all operations among subjects and objects covered by the SFP.

100 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.

101 For confidentiality reasons, rules are not shown in Table 8. They can be found in the [ST19NA18 Security Target](#).

Table 8 Subjects, objects and applicable access control rules

Subjects	S.TRUST	S.PLAIN	S.LIB	S.ANY
OB.F_IC	Not applicable			
OB.ROM	Memory Access Control Logics (MACL) rules			Not applicable
OB.CALL_USR	System Access Control Logics (SACL) rules			
OB.PROT_ROM	Call Gate Access Control Logics (CGACL) rules			
OB.CMD_TST	Test Access Control Logics (TACL) rules			
OB.CMD_ISR	Issuer Access Control Logics (IACL) rules			
OB.REG	Register Access Control Logics (RACL) rules			
OB.RAM	Memory Access Control Logics (MACL) rules			
OB.NVM	Memory Access Control Logics (MACL) rules			

5.1.3.9 Security attribute based access control (FDP_ACF.1)

102 The TOE Security Functions shall enforce **Location Based Access Control Policy** to objects based on **security attributes** defined in the [ST19NA18 Security Target](#).

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

- **Grant S.TRUST initialisation access to OB.RAM and OB.REG.**
- **Grant S.TRUST flash access to OB.NVM.**
- **Those in Table 12** of the [ST19NA18 Security Target](#).
- **Those in Table 13** of the [ST19NA18 Security Target](#), **when TOE is not in test configuration.**

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

105 The TOE Security Functions shall explicitly deny access of subjects to objects based on the following additional rules:

- **Those "explicitly denied" of Table 12 and Table 13** of the [ST19NA18 Security Target](#).

For confidentiality reasons, Table 12 and Table 13 are not shown in this document. They can be found in the [ST19NA18 Security Target](#).

5.1.3.10 Limited fault tolerance (FRU_FLT.2)

106 The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: **exposure to operating conditions which are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1).**

5.1.3.11 Failure with preservation of secure state (FPT_FLS.1)

107 The TSF shall preserve a secure state when the following types of failures occur:

exposure to operating conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur.

108 Refinement:

The term "failure" above means "circumstances". The TOE prevents failures for the "circumstances" defined above.

Regarding application note 16 of [BSI-PP-002-2001](#), the TOE provides information on the operating conditions monitored during Smartcard Embedded Software execution and after a warm reset. No audit requirement is however selected in this security target.

5.1.3.12 Potential violation analysis (FAU_SAA.1)

109 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.

110 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,*
 - *fault detected,*
 - *code signature bad usage,*
- known to indicate a potential security violation;

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

5.1.3.13 TSF domain separation (FPT_SEP.1)

111 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

112 The TSF shall enforce separation between the security domains of subjects in the TSC.

113 Refinement:

Those parts of the TOE that support the security functional requirements "Limited fault tolerance (FRU_FLT.2)" and "Failure with preservation of secure state (FPT_FLS.1)" shall be protected from interference of the Smartcard Embedded Software.

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

- 114 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.**
- 115 Upon detection of a data integrity error, the TSF shall perform actions that cannot be described here, for confidentiality reasons.

5.1.3.15 Notification of physical attack (FPT_PHP.2)

- 116 The TOE Security Functions shall provide unambiguous detection of physical tampering that might compromise the TOE Security Functions.
- 117 The TOE Security Functions shall provide the capability to determine whether physical tampering with the TOE security function's devices or elements has occurred.
- 118 For **operating changes or fault injections performed on the clock, the voltage supply or other chip functions, 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.

5.1.3.16 Resistance to physical attack (FPT_PHP.3)

- 119 The TOE Security Functions shall resist **physical manipulation and physical probing**, to the **TSF** by responding automatically such that the TOE security policy is not violated.
- 120 Note: as described in the CC part 2 annexes, technology limitations and relative physical exposure of the TOE must be considered.

121 **Refinement**

The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, "automatic response" means here (i)assuming that there might be an attack at any time and (ii)countermeasures are provided at any time.

5.1.3.17 Unobservability (FPR_UNO.1)

- 122 ***In this security target, ability to observe an operation means revealing the value of a data during an operation on this data.***
- 123 The TOE Security Functions shall ensure that **all end-users** are unable to observe the operations **listed in Table 9** on **objects listed in Table 9** by **S.TRUST and S.LIB**.

Table 9 FPR_UNO.1 iterations (unobservability)

[assignment: list of operations]	[assignment: list of objects]
READ	OB.ROM, OB.RAM, OB.REG and OB.NVM
WRITE	OB.RAM
PROGRAM, ERASE	OB.NVM

5.1.3.18 Basic internal transfer protection (FDP_ITT.1)

124 The TSF shall enforce the **Data Processing Policy** to prevent the **disclosure** of user data when it is transmitted between physically-separated parts of the TOE.

5.1.3.19 Basic internal TSF data transfer protection (FPT_ITT.1)

125 The TSF shall protect TSF data from **disclosure** when it is transmitted between separate parts of the TOE.

126 Refinement:

The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as separated parts of the TOE.

This requirement is equivalent to FDP_ITT.1 above but refers to TSF data instead of User Data. Therefore, it should be understood as to refer to the same **Data Processing Policy**.

127 SFP_2: Data Processing Policy

User Data and TSF data shall not be accessible from the TOE except when the Smartcard Embedded Software decides to communicate the User Data via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the Smartcard Embedded Software.

5.1.3.20 Subset information flow control (FDP_IFC.1)

128 The TOE Security Functions shall enforce the **Construction Flow Control Policy** on **all subjects defined in Section 5.1.1.1, the content of all objects defined in Section 5.1.1.2, and the commands available in OB.CMD_TST, OB.CMD_ISR and OB.CALL_USR objects.**

5.1.3.21 Simple security attributes (FDP_IFF.1)

129 The TOE Security Functions shall enforce the **Construction Flow Control Policy** based on the following types of subject and information security attribute:

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

130 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:

- **Those in Table 15** of the [ST19NA18 Security Target](#).

131 The TSF shall provide the additional information flow control SFP rules: **None**.

132 The TSF shall enforce the following additional SFP capabilities: **Data Processing Policy**.

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

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

5.1.3.22 Subset residual information protection (FDP_RIP.1)

135 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.**

5.1.3.23 Quality metric for random numbers (FCS_RND.1)

136 The TSF shall provide a mechanism to generate random numbers that meet [NIST FIPS PUB-140-2:1999 standard for a Security Level 3 cryptographic module \(statistical test upon demand\)](#) and *P2 class "High" of BSI-AIS31*.

5.1.4 FUNCTIONAL REQUIREMENTS APPLICABLE TO USER CONFIGURATION

5.1.4.1 Cryptographic operation (FCS_COP.1)

137 The TSF shall perform *the operations in Table 10* in accordance with a specified cryptographic algorithm *in Table 10* and cryptographic key sizes *of Table 10* that meet the *standards in Table 10*.

Table 10 FCS_COP.1 iterations (cryptographic operations)

[assignment: list of cryptographic operations]	[assignment: cryptographic algorithm]	[assignment: cryptographic key sizes]	[assignment: list of standards]
- encryption - decryption in Electronic Code Book (ECB) mode	Data Encryption Standard (DES)	56 effective bits	ISO 8372:1987 ISO 8731-1:1987 ISO/IEC 10116:1997
	Triple Data Encryption Standard (3DES)	112 effective bits	
- encryption - decryption in Cipher Block Chaining (CBC) mode - compute a Message Authentication Code (MAC)	Data Encryption Standard (DES)	56 effective bits	ISO 8372:1987 ISO 8731-1:1987 ISO/IEC 9797:1994 ISO/IEC 10116:1997
	Triple Data Encryption Standard (3DES)	112 effective bits	
- cipher - inverse cipher - key expansion operations	Advanced Encryption Standard	128 bits	NIST FIPS PUB 197 with block size of 128 bits and 10 rounds (AES-128 option)

Table 10 FCS_COP.1 iterations (cryptographic operations)

[assignment: list of cryptographic operations]	[assignment: cryptographic algorithm]	[assignment: cryptographic key sizes]	[assignment: list of standards]
- <i>RSA recovery (encryption)</i>	<i>Rivest, Shamir & Adleman's</i>	<i>multiples of 64 bits up to 1088 bits</i>	<i>ISO/IEC 9796-2:1997 MIT/LCS/TR-212</i>
- <i>RSA signature (decryption) without the Chinese Remainder Theorem</i>		<i>multiples of 64 bits larger than 1088 bits and up to 2176 bits</i>	
- <i>RSA signature (decryption) with the Chinese Remainder Theorem</i>		<i>multiples of 64 bits up to 1088 bits</i>	
- <i>secure hash function</i>	<i>revised Secure Hash Algorithm (SHA-1)</i>	<i>this algorithm has no key, so the assignment is pointless¹⁾</i>	

1) *result size of 160 bits on chained blocks of 512 bits*

5.1.4.2 Cryptographic key generation (FCS_CKM.1)

138 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm, *in Table 11*, and specified cryptographic key sizes *of Table 11* that meet the following **standards in Table 11**.

Table 11 FCS_CKM.1 iterations (cryptographic key generation)

Iteration label	[assignment: cryptographic key generation algorithm]	[assignment: cryptographic key sizes]	[assignment: list of standards]
[COP_RSA_RANDOM] ¹⁾	random number generation	1088 bits	Not applicable
[COP_RSA_PRIMES]	primes and RSA primes generation algorithm	multiples of 64 bits up to 1088 bits	NIST FIPS PUB-140-2:1999 ISO/IEC 9796-2:1997 NIST FIPS PUB 186 JoCSS JoNT
[COP_RSA_KEYS]	RSA public and private keys computation algorithm	multiples of 64 bits greater than 128 bits and up to 2176 bits	NIST FIPS PUB-140-2:1999 ISO/IEC 9796-2:1997 MIT/LCS/TR-212

1) Note that this requirement is complementary to FCS_RND.1. The former asks for random numbers ready to use in a cipher scheme, as it is clearly recommended in paragraph n° 693 of CCMB-2005-08-002, whereas the latter insists on the quality of the random source.

5.2 TOE SECURITY ASSURANCE REQUIREMENTS

139 The assurance requirements are EAL 5 augmented of additional assurance components listed in the following sections.

140 **The components introduced by the PP/9806 and BSI-PP-002-2001** are hierarchical to the components specified in EAL 5.

141 The augmentations relative to EAL 5 are the following:

- ALC_DVS.2 Sufficiency of security measures
this increases the confidence in the vital area of developer security measures to the highest CC level,
- AVA_MSU.3 Analysis and testing for insecure states
this adds evaluator testing of the potential for misuse of the TOE within the evaluation scope,
- AVA_VLA.4 Highly resistant
this increases the attack potential assumed for the vulnerability analysis and penetration testing to its highest CC level.

142 Regarding application note 18 of BSI-PP-002-2001, the continuously increasing maturity level of evaluations of Smartcard ICs justifies the selection of a higher-level assurance package.

143 The set of security assurance requirements (SARs) is presented in [Table 12](#), indicating the origin of the requirement.

Table 12 TOE security assurance requirements

Label	Title	Origin
ACM_AUT.1	Partial CM automation	EAL5/BSI-PP-002-2001/PP/9806
ACM_CAP.4	Generation support and acceptance procedures	EAL5/BSI-PP-002-2001/PP/9806
ACM_SCP.3	Development tools CM coverage	EAL5
ADO_DEL.2	Detection of modification	EAL5/BSI-PP-002-2001/PP/9806
ADO_IGS.1	Installation, generation and start-up procedures	EAL5/BSI-PP-002-2001/PP/9806
ADV_SPM.3	Formal security policy model	EAL5
ADV_FSP.3	Semiformal functional specification	EAL5
ADV_HLD.3	Semiformal high-level design	EAL5
ADV_INT.1	Modularity	EAL5
ADV_LLD.1	Descriptive low-level design	EAL5/BSI-PP-002-2001/PP/9806
ADV_IMP.2	Implementation of the TSF	EAL5/BSI-PP-002-2001/PP/9806
ADV_RCR.2	Semiformal correspondence demonstration	EAL5
AGD_USR.1	User guidance	EAL5/BSI-PP-002-2001/PP/9806
AGD_ADM.1	Administrator guidance	EAL5/BSI-PP-002-2001/PP/9806
ALC_DVS.2	Sufficiency of security measures	BSI-PP-002-2001/PP/9806
ALC_LCD.2	Standardised life-cycle model	EAL5
ALC_TAT.2	Compliance with implementation standards	EAL5
ATE_COV.2	Analysis of coverage	EAL5/BSI-PP-002-2001/PP/9806
ATE_DPT.2	Testing: low-level design	EAL5
ATE_FUN.1	Functional testing	EAL5/BSI-PP-002-2001/PP/9806
ATE_IND.2	Independent testing - sample	EAL5/BSI-PP-002-2001/PP/9806
AVA_VLA.4	Highly resistant	BSI-PP-002-2001/PP/9806
AVA_CCA.1	Covert channel analysis	EAL5
AVA_MSU.3	Analysis and testing for insecure states	BSI-PP-002-2001
AVA_SOF.1	Strength of TOE security function evaluation	EAL5/BSI-PP-002-2001/PP/9806

5.3 REFINEMENT OF THE SECURITY ASSURANCE REQUIREMENTS

144 As [BSI-PP-002-2001](#) defines refinement for selected SARs, these refinements are also claimed in this security target. [PP/9806](#) defines no refinement on SARs.

145 The main customizing is that the Dedicated Software is an operational part of the TOE after delivery, although the Test Dedicated Software is no more available.

146 Regarding application note 19 of [BSI-PP-002-2001](#), the refinements for all the assurance families have been reviewed for the hierarchically higher-level assurance components selected in this security target.

147 The text of the impacted refinements of [BSI-PP-002-2001](#) is to be found in the [ST19NA18 Security Target](#).

148 For reader's ease, an impact summary is provided in [Table 13](#).

Table 13 Impact of EAL5 selection on [BSI-PP-002-2001](#) refinements

Assurance Family	BSI-PP-002-2001 Level	ST Level	Impact on refinement
ADO_DEL	2	2	None
ALC_DVS	2	2	None
ACM_SCP	2	3	None, refinement is still valid
ACM_CAP	4	4	None
ADV_FSP	2	3	<i>Presentation style changes</i>
ATE_COV	2	2	<i>Dedicated Software is included</i>
ADO_IGS	1	1	<i>Difference on ISSUER or USER delivery</i>
AGD_USR	1	1	<i>Terminal is not a direct user</i>
AGD_ADM	1	1	<i>Difference on ISSUER or USER delivery</i>

5.4 SECURITY REQUIREMENTS FOR THE ENVIRONMENT

149 Although security requirements specified below are respectively applicable:

- to the smart card embedded software for those in [Section 5.4.1](#),
- to the embedded software developer and the card manufacturer for those in [Section 5.4.2](#),

150 it is neither necessary nor appropriate for this security target to define functional and assurance security requirements for the TOE environment¹⁾. These are however included here to be conformant to the claimed protection profiles.

5.4.1 Security requirements for the operational IT environment

151 [BSI-PP-002-2001](#) selects no security requirement for the IT operational environment. However, the extra functionality provided by the ST19NA18, introduced in this security target as recommended in [AUG](#), results in the security requirements summarized in [Table 14](#).

5.4.2 Security requirements for the Non-IT environment

152 The security requirements for the Non-IT environment selected in this security target, after [BSI-PP-002-2001](#) and [AUG](#) are summarized in [Table 15](#). Do remark that they are not evaluated. Only those after [AUG](#) are detailed hereafter.

1 The TOE being a product-type TOE, dependencies on the environment should remain at the assumption and security objective levels because they are not in the scope of the evaluation (as a matter of fact, they will not be evaluated). Satisfaction of these requirements is a design issue for the smart card embedded software developer and a design/organizational issue for the card manufacturer. They should state and provide evidence on how they comply with these "safe conditions of use" of the product in order to claim, as element of evidence, the certification report of a TOE in a composite evaluation. Evaluators of the composite TOE should then evaluate and test this provided evidence.

Table 14 Summary of security requirements for the operational IT environment

Label	Title	Traces to...	Origin	Remark
FDP_ITC.1 or FCS_CKM.1	Import of user data without security attributes Cryptographic key generation	BSI.OE.Resp-AppI (FCS_COP.1)	CCMB-2005-08-002	ST19NA18's FCS_CKM.1, Section 5.1.4.2 and FCS_COP.1, Section 5.1.4.1 can be used.
FCS_CKM.4	Cryptographic key destruction			
FMT_MSA.2	Secure security attributes			
FCS_CKM.2 or FCS_COP.1	Cryptographic key distribution Cryptographic operation	BSI.OE.Plat-AppI BSI.OE.Resp-AppI (FCS_CKM.1)		
FCS_CKM.4	Cryptographic key destruction			
FMT_MSA.2	Secure security attributes			

Table 15 Summary of security requirements for the non-IT environment

Label	Title	Traces to...
BSI.RE.Phase-1	Design & implementation of the smart card embedded software	AUG1.A.Key-Function BSI.A.Plat-AppI BSI.A.Resp-APPL AUG1.P.Add Functions AUG4.T.Mem-Access BSI.T.Leak-Inherent BSI.T.Phys-Probing BSI.T.Phys-Manipulation BSI.T.Leak-Forced BSI.T.Abuse-Func BSI.T.RND (BSI.A.Process-Card)
BSI.RE.Process-Card	Protection during packaging, finishing and personalisation	BSI.A.Process-Card
AUG1.RE.Cipher	Cipher schemes	BSI.OE.Plat-AppI BSI.OE.Resp-AppI (FCS_COP.1, Section 5.1.4.1) (FCS_CKM.1, Section 5.1.4.2)

153

AUG1.RE.Cipher**Cipher Schemas**

The developers of Smartcard Embedded Software must not implement routines in a way which may compromise keys when the routines are executed as part of the Smartcard Embedded Software. Performing functions which access cryptographic keys could allow an attacker to misuse these functions to gather information about the key which is used in the computation of the function.

Keys must be kept confidential as soon as they are generated. The keys must be unique with a very high probability, as well as cryptographically strong. For example, it must be ensured that it is not possible to derive the private key from a public key if asymmetric algorithms are used. If keys are imported into the TOE and/or derived from other keys, quality and confidentiality must be maintained. This implies that an appropriate key management has to be realised in the environment.

5.5 SECURITY REQUIREMENTS RATIONALE

154 The security requirements rationale has been presented and evaluated in the [ST19NA18 Security Target](#).

155 For confidentiality reasons, this rationale is not reproduced here.

6 TOE SUMMARY SPECIFICATION

6.1 STATEMENT OF TOE SECURITY FUNCTIONS

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

6.1.1 SF_INIT_A: Hardware initialisation & TOE attribute initialisation

157 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.

6.1.2 SF_CONFIG_A: TOE configuration switching and control

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

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

160 The only authorised TOE configuration modifications are:

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

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

6.1.3 SF_INT_A: TOE logical integrity

162 In TEST and ISSUER configurations, this functionality is responsible for the following operations:

- NVM, USR_ROM and ST_ROM integrity contents verifications.

163 In TEST, ISSUER and USER configurations, this functionality is responsible for:

- correcting single bit fails upon a read operation on each byte,
- verifying valid CPU usage and stack overflow,
- checking integrity loss when accessing NVM, USR_ROM and ST_ROM,
- monitoring fault injection attempts,
- providing a code signature and comparison engine,
- other actions are not described here.

164 This functionality is responsible for reporting to SF_ADMINIS_A all detected errors resulting from the above operations.

6.1.4 SF_TEST_A: Test of the TOE

- 165 This functionality is responsible for restricting access of the TOE TEST functionality to the TEST administrator in TEST configuration.
- 166 This functionality is responsible for restricting access of the TOE ISSUER functionality to the ISSUER administrator in ISSUER configuration.
- 167 In USER configuration, this functionality ensures that neither TOE TEST nor TOE ISSUER functionality can be accessed.
- 168 In TEST configuration, this functionality ensures the test of TOE functionality with respect to the IC specification.
- 169 In ISSUER and USER configurations, it ensures that critical test functionality is disabled.
- 170 In TEST configuration, this functionality provides commands to store data and/or pre-personalisation data and/or supplements of the Smartcard Embedded Software (personnalisation). In ISSUER configuration, these commands are still available but in a more restricted operation mode.

6.1.5 SF_AUTH_A: Administrators authentication

- 171 In TEST configuration, this SF ensures that the only allowed TOE user is an authenticated TEST administrator.
- 172 In ISSUER configuration, this SF ensures the authentication of the ISSUER administrator.
- 173 A **SOF-high** strength of function is claimed for this SF.

6.1.6 SF_FWL_A: Storage and Function Access Firewall

- 174 TOE memories are partitioned. This partitioning is partially defined by the TOE user and partially by ST:
- ST_ROM mapping is ST defined,
 - USR_ROM mapping is user defined,
 - RAM and NVM mappings are partly ST defined and partly user defined.
- 175 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.
- 176 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.

- 177 Executability, Read, Write, Program and Erase right classes are defined by the User and ST in a Memory Access Control Logic for ROM, RAM and NVM.
- 178 ST_ROM and registers access rights are defined by ST in a ST_ROM and Register Firewall.
- 179 User ROM and registers access rights are defined by the User in a User ROM and Register Firewall.
- 180 These access rights and access right classes are implemented in the TOE hardware and cannot be further modified.

6.1.7 SF_PHT_A: Physical tampering security function

- 181 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, and glitch attacks,
 - the TOE is always clocked with shape and timing within specified operating conditions.

6.1.8 SF_ADMINIS_A: Security violation administrator

- 182 In TEST, ISSUER and USER configurations, this functionality ensures the management of security violations attempts.
- 183 The security violations attempts which are managed are:
- access to unavailable or reserved memory locations,
 - unauthorised access to User memories,
 - unauthorised access to ST memories,
 - bad CPU usage,
 - bad NVM use,
 - EEPROM single bit fails,
 - clock and voltage supply operating changes,
 - TOE physical integrity abuse,
 - fault injection,
 - code signature alarm.

6.1.9 SF_OBS_A: Unobservability

- 184 In ISSUER and USER configurations, this security function addresses the [Unobservability \(FPR_UNO.1\)](#), the [Basic internal transfer protection \(FDP_ITT.1\)](#) and the [Basic internal TSF data transfer protection \(FPT_ITT.1\)](#) security functional requirements expressed in this document. It relies on SFP_2: Data Processing Policy.

6.1.10 SF_SKCS_A: Symmetric Key Cryptography Support

185 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).

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.

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.

186 In USER configuration, this functionality implements the following standard symmetric key cryptography algorithms:

- Advanced Encryption Standard (AES) with 128 bits long keys, 128 bits long blocks, 10 rounds, providing cipher, inverse cipher and key expansion operations.

6.1.11 SF_AKCS_A: Asymmetric Key Cryptography Support

187 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.

188 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.

6.1.12 SF_ALEAS_A: Unpredictable Number Generation Support

189 In all configurations, this security function provides 8 bits true random numbers.

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

191 In USER configuration, this security function provides 1088 bits true random numbers.

192 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),
- the test metrics required by the [BSI-AIS31](#) standard for a P2 class "High" device.

6.2 STATEMENT OF ASSURANCE MEASURES

193 The [ST19NA18 Documentation Report](#) shows the assurance measures, through a list of documents delivered, which are claimed to satisfy the stated assurance requirements.

7 PP CLAIMS

7.1 PP REFERENCES

- 194 The ST19NA18 Security Target **is compliant with** the requirements of the [Smartcard Integrated Circuit Protection Profile PP/9806, Revision 2.0](#).
- 195 The ST19NA18 Security Target **is compliant with** the requirements of the [Smartcard IC Platform Protection Profile BSI-PP-002-2001, Revision 1.0](#).

7.2 PP REFINEMENTS

- 196 The main refinements operated on the [PP/9806](#) are:
- "Smartcard product" is refined into "Secure IC based product" to emphasize the packaging independence of the TOE,
 - The SFR applicable to phase 3 are refined to be applicable to the logical phases TEST and ISSUER configurations.
- 197 [PP/9806](#) refinements are indicated with type setting text **as indicated here**, original text being typeset **as indicated here**. Deleted parts are [~~as indicated here~~]. Text originating in [AUG](#) is typeset **as indicated here**.
- 198 The main refinements operated on the [BSI-PP-002-2001](#) are:
- The definition of "Test Features" in the [Limited capabilities \(FMT_LIM.1\)](#) policy,
 - Addition #1: "Support of Cipher Schemes" from [AUG](#),
 - Addition #4: "Area based Memory Access Control" from [AUG](#),
 - Refinement of assurance requirements.
- 199 [BSI-PP-002-2001](#) refinements are indicated with type setting text **as indicated here**, original text being typeset **as indicated here**. Deleted parts are [~~as indicated here~~]. Text originating in [AUG](#) is typeset **as indicated here**.

7.3 PP ADDITIONS

- 200 The security environment additions relative to each PP are summarized in [Table 3](#). Remind that most of them are redundant to each other but enable full traceability and rationale reuse.
- 201 The additional security objectives relative to each PP are summarized in [Table 4](#). Remind that most of them are redundant to each other but enable full traceability and rationale reuse.
- 202 A simplified presentation of the TOE Security Policy (TSP) is added.
- 203 The additional SFRs for the TOE relative to each PP are summarized in [Table 5](#). Remind that some of them are redundant to each other but enable full traceability and rationale reuse.

204 The additional SFRs for the environment relative to both PPs are summarized in [Table 14](#)
and [Table 15](#).

205 The additional SARs relative to each PP are summarized in [Table 12](#).

7.4 PP CLAIMS RATIONALE

206 The differences between this Security Target security objectives and requirements and those of [PP/9806](#) and those of [BSI-PP-002-2001](#), to both of which conformance is claimed, have been identified and justified in [Chapter 4](#) and in [Chapter 5](#). They have been recalled in the previous section.

207 The security objectives rationale referred to in [Section 4.3](#) clearly identifies modifications and additions made to the rationale presented in the [PP/9806](#) and in [BSI-PP-002-2001](#).

208 Similarly, the security requirements rationale referred to in [Section 5.5](#) has been consistently updated with respect to both protection profiles.

209 All PP requirements have been shown to be satisfied in the extended set of requirements whose completeness, consistency and soundness has been argued in the rationale sections of the [ST19NA18 Security Target](#).

8 RATIONALE

210 The rationale has been presented and evaluated in the [ST19NA18 Security Target](#).

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

9 REFERENCES

212 Protection Profile references

Component description	Reference	Revision
Smartcard Integrated Circuit	PP/9806	2.0
Smartcard IC Platform	BSI-PP-002-2001	1.0

213 ST19NA18 Security Target reference

Component description	Reference
ST19NA18 Security Target	SMD_ST19NA18_ST_06_001

214 Target of Evaluation referenced documents

215 For security reasons, all these documents are classified and their applicable revisions are referenced in th ST19NA18 Documentation Report.

Component description	Reference
ST19NA18 Documentation Report	SMD_ST19NA18_DR_06_001

216 Standards references

Identifier	Description
BSI-AIS31	A proposal for Functionality classes and evaluation methodology for true (physical) random number generators, W. Killmann & W. Schindler BSI, Version 3.1, 25-09-2001
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
NIST FIPS PUB 197	Advanced Encryption Standard (AES), November 2001
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
CCMB-2005-08-001	Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, August 2005, version 2.3
CCMB-2005-08-002	Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, August 2005, version 2.3

Identifier	Description
CCMB-2005-08-003	Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, August 2005, version 2.3
BSI_9806_0002_2001	Assessment on the substitution of an evaluation based on PP/9806 by an evaluation based on BSI-PP-0002-2001, BSI, version 1.1, May 2002
DCSSI_CCN.624	Fiche relative au profil de protection BSI-PP-0002-2001, C. Blad, version 1.1, 27 mai 2002
DCSSI_CCN.648	Fiche relative à l'utilisation du profile de protection BSI-PP-0002-2001 pour une évaluation PP/9911, DCSSI, 19 septembre 2002
AUG	Smartcard Integrated Circuit Platform Augmentations, Atmel, Hitachi Europe, Infineon Technologies, Philips Semiconductors, Version 1.0, March 2002.
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

ST proprietary Dedicated SoftWare (DSW), embedded in ST_ROM, whose design is parameterised by the ST 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 ST 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 doesn't affect the operation of the TOE.

Warm reset

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

Abbreviations

ACC

Accumulator register.

AES

Advanced Encryption Standard.

AIS

Application notes and Interpretation of the Scheme (BSI)

ALU

Arithmetical and Logical Unit.

ANSI

American National Standards Institute

API

Application Program Interface.

BSI

Bundesamt für Sicherheit in der Informationstechnik

CBC

Cipher Block Chaining.

CC

[Common Criteria](#) **Version 2.3 (CCMB)**.

CCR

Condition Code Register.

CSD

Cryptographic Sensitive Data.

CSR

Code Segment Register.

CPU

Central Processing Unit.

DCSSI

Direction Centrale de la Sécurité des Systèmes Informatique

DEMA

Differential Electromagnetic Analysis.

DES

Data Encryption Standard.

DFA

Differential Fault Analysis.

DIP

Dual-In-Line Package.

DPA

Differential Power Analysis.

DSR

Data Segment Register.

DSW

IC Proprietary Dedicated Software.

EAL

[Evaluation Assurance Level.](#)

ECB

Electronic Code Book.

ECC

Error Correcting Code.

EEPROM

Electrically Erasable Programmable Read Only Memory.

EMA

Electromagnetic Analysis.

FIPS

Federal Information Processing Standard.

GPIO

General Purpose Input Output.

HODPA

Higher Order Differential Power Analysis.

I2C

Inter Integrated Circuit bus.

IART

ISO-7816 Asynchronous Receiver Transmitter.

IOCI

Input Output and Control Interface.

ISO

International Standards Organisation.

IT

Information Technology.

Kbps

Kilo bits per second.

LPC

Low Pin Count.

MAP

Modular Arithmetical Processor.

NIST

National Institute of Standards and Technology.

NVM

Non Volatile Memory.

OP

Operation Performed.

OSP

Organisational Security Policy.

PC

Program Counter register.

PP

Protection Profile.

PUB

Publication Series.

RAM

Random Access Memory.

RF

Radio Frequency.

ROM

Read Only Memory.

SAR

Security Assurance Requirement.

SF

Security function.

SFP

Security Function Policy.

SFR

Security Functional Requirement.

SICESW

Secure IC Embedded SoftWare.

SOF

Strength of function.

SOIC

Small Outline IC.

SP

Stack Pointer register.

SPA

Simple Power Analysis.

ST

Security Target or STMicroelectronics, depending on the context.

ST_ROM

ST reserved ROM.

TOE

Target of Evaluation.

TQFP

Thin Quad Flat Package.

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.

RF-UART

Radio Frequency Universal Asynchronous Receiver Transmitter.

USR_ROM

User reserved ROM.

USB

Universal Serial Bus.

XIR

X Index Register.

YIR

Y Index Register.

CONFIDENTIALITY OBLIGATIONS:

THIS DOCUMENT CONTAINS NO CONFIDENTIAL INFORMATION.
ITS DISTRIBUTION IS NOT SUBJECT TO THE SIGNATURE OF A 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

Information furnished is believed to be accurate and reliable. However, STMicroelectronics assumes no responsibility for the consequences of use of such information nor for any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of STMicroelectronics. Specifications mentioned in this publication are subject to change without notice. This publication supersedes and replaces all information previously supplied. STMicroelectronics products are not authorized for use as critical components in life support devices or systems without the express written approval of STMicroelectronics.

© 2007 STMicroelectronics - Printed in France - All Rights Reserved
BULL CP8 Patents

STMicroelectronics GROUP OF COMPANIES

Australia - Brazil - Canada - China - France - Germany - Italy - Japan - Korea - Malaysia - Malta -
Morocco - The Netherlands - Singapore - Spain - Sweden - Switzerland - Taiwan - Thailand - United Kingdom - U.S.A.