PUBLIC SECURITY TARGET

for

“SMARTCARD IC DEVELOPMENT FLOW – JAPAN”

SmartCard IC Development Section – Kumamoto - Japan

NEC SmartCard Application Center

Version 1.0 - Issue October 2002

Public Security Target for “SmartCard IC Development Flow – Japan”:			
Version Number	**Comments/Modifications**	**Prepared by/Signature**	**Date**
V 1.0	Original.	Le Bihan J.	28 October 02

Table of contents

Chapter 1
ST Introduction……………………………………………………………5
1.1 ST Identification…………………………………………………………...5
1.2 ST Overview……………………………………………………………6
1.3 Common Criteria Conformance Claim……………………………….…8

Chapter 2
TOE Description……………………………………………………………8
2.1 System Type and Scope of TOE………………………………………...8
2.2 Phases of the TOE & Phases outside of the TOE..………………………..10
2.3 Boundaries of the TOE…………………………………………………10
2.4 Environment of the TOE………………………………………………..10
2.5 General IT Features of the TOE…………………………………………...12

Chapter 3
TOE Security Environment………………………………………………….13
3.1 TOE Intended Usage…………………………………………………….13
3.2 Assets……………………………………………………………………15
3.3 Assumption..……………………………………………………………..15
3.4 Assumptions for conformance to PP/9806…………………………………16
3.5 Threats……………………………………………………………………...16
3.6 Threats for conformance to PP/9806……………………………………….17
3.7 Organizational Security Policies…………………………………………20
3.8 Organizational Security Policies for conformance to PP/9806…………….21

Chapter 4
Security Objectives……………………………………………………………22
4.1 IT Security Objectives for the TOE.…………..………………………....22
4.2 Non-IT Security Objectives for the TOE.………………………………..22
4.3 Security Objectives for the TOE Environment……………………………..22
4.4 Objectives for conformance to PP/9806……………………………………23

Chapter 5
TOE Security Functional Requirements…………………………………….25
5.1 TOE IT Security Requirements……….………………………………………25
5.2 TOE NON-IT Security Requirements……………….……………….……….43
5.3 TOE Environment Security Requirements……………….……………...45

Chapter 6
TOE Summary Specification…………………………………………………47
6.1 Statement of TOE Security Functions……………………………………...47
6.2 Statement of TOE Assurance Measures……………………………………50
6.3 Statement of Non-IT Security Measures for the TOE…………..………..55
6.4 Statement of Security Measures for the Environment………..…………..57

Chapter 7
PP Claims……………………………………………………………………….60

Annex A
Definitions & Acronyms……………………………………………………..…61

Chapter 1

1. Security Target Introduction

1.1 Security Target Identification

Title: Public Security Target for “SmartCard IC Development Flow – Japan”.

N.B: For easiness in the reading of this document, wording in the text hereafter, will be using the definition of Security Target, and its associated acronym “ST”, as the generic name for this public security target.

The version number of this ST is Version 1.0, issue October 2002.

This ST has been built with the Common Criteria Version 2.1.

Author of this ST is the Project & IT Security Manager of NEC SmartCard Application Center (SCAC).

A definition list of acronyms used in this ST is given in annex A.

This ST is referring to the “SmartCard IC Development Flow – Japan” and its associated “Information Technology” (IT) used within the “SmartCard IC Development Section”. This section is located in Kumamoto – Japan.

This studied environment of development is encompassing:

- For the TOE: The development flow, known as being the “SmartCard IC Development Flow – Japan”, including its associated “Information Technology” (TOE IT).
- And for the environment of the TOE: The Environment of the “SmartCard IC Development Flow – Japan”, including its Information Technology (IT of the TOE Environment), in which the TOE itself is operated.

Therefore, the TOE is known as being the “SmartCard IC Development Flow – Japan”. This TOE is uniquely identified by this name and by an associated version number. This “SmartCard IC Development Flow – Japan” name is made unique within NEC, and is really dedicated to the operations used for the design activities in Japan related to the “smartcard micocontrollers”.

The version number of the TOE is insured by a configuration management method giving the detailed list of all the parts (reference/identification and version number) that are security relevant within this development flow. This list is reported into a document entitled “Reference and Version Number to the “SmartCard IC Development Flow - Japan” – ACM_CAP.1”. Any change to the content of this list will result into the increase of the version number of the list itself and into the increase of the version number of the TOE.
The present version number for both the TOE is 1.0.

This is this version of the TOE that is being evaluated in the frame of the Common Criteria certification of the “SmartCard IC Development Flow - Japan”.

1.2 ST Overview

1.2.1 General

This ST was conducted under the French IT Security Evaluation and Certification Scheme.

This ST was developed in the frame of the Common Criteria Evaluation, in order to get a Common Criteria Certification, of the “SmartCard IC Development Flow - Japan”, including its associated “Information Technology”.

Evaluation and Certification were both run to demonstrate and offer guarantee in the level of security implemented in the “SmartCard IC Development Section” to the NEC’ s customers and/or potential customers, and particularly in the “SmartCard IC Development Flow - Japan”, that is the flow used for the development of the smartcard microcontroller components.

In addition, a forecasted continuous improvement methodology will maintain the security level of this development flow at the state of the art level of the industry. After this present evaluation is completed, the continuous improvement methodology will be supported by the implementation of a “Certification Maintenance Program”. This “Certification Maintenance Program” will be supported by an update of the ST and will include the security components from the “AMA” class (Maintenance of Assurance).

1.2.2 Need for Security

The security needs for a smartcard can be summarized as being able to counter those who want to defraud, gain unauthorized access to data and control a system using a smartcard, usually by breaking the integrity and the confidentiality of the content of the non-volatile memory (program and data memories) and of the security relevant architectural components (security mechanisms and associated functions) embedded into the integrated circuit.

Therefore, it becomes also mandatory that all the relevant data-base, files, security and proprietary information related to these content of the non-volatile memory (program and data memories), security relevant architectural components, security mechanisms and associated functions are also protected against unauthorized access and use.

Because product data, features and security components are proprietary information, because their integrity and confidentiality are being built during the development phase of the semiconductor product (design phase of the component), and then consolidated during its

production phase, it was requested to security evaluate and certify this “SmartCard IC Development Flow - Japan” as per the Common Criteria.
It is reminded that this phase of development is involving the “SmartCard IC Development Flow - Japan” itself, including the “Information Technology” (IT) associated to this development flow, and the “Environment” in which this TOE is operated, also including the “Information Technology” (IT) associated to this environment. It is also made relevant that they are able to maintain their own integrity and confidentiality in order to ensure the protection of the security relevant elements of the microcontroller components.

1.2.3 Certification Process

The intent of this ST is to specify the functional and assurance requirements applicable to the “SmartCard IC Development Flow - Japan” used by the “SmartCard IC Development Section” for the design (development) operations of the microcontroller components dedicated to the smartcard applications.

These ST and its evaluation are product independent.

The main objectives of this ST is:

- To describe the Target of Evaluation (TOE).
- To describe the security environment of the TOE.
- To describe the assets to be protected and the threats to be countered by the TOE and by the TOE environment during the development phase of the smartcard microcontroller components.
- To describe the security objectives for the TOE and for its environment.
- To specify the security requirements which includes the TOE security functional requirements and the TOE security assurance requirements.
- To specify the TOE security functions and the TOE assurance measures.

During the completion of both continuous improvement plan and “Maintenance Program” of certification, any other product could be then added to the list of these commercial names, without any in depth change to the security and to this ST, as soon as the added product is resulting from the same “SmartCard IC Development Flow - Japan”.

1.3 Common Criteria Conformance Claim

The conformance claimed for this Security Target is:

- Part 2 conformant.
- Part 3 conformant, with EAL1 augmented level.

The EAL1 level from CC Part 3 is augmented with the assurance component:

- AVA_VLA.2 “Independent Vulnerability Analysis”.

Chapter 2

2. TOE Description

Editorial Note:

This part of the ST describes the Target Of Evaluation (TOE) as an aid to the understanding of its security requirements and address the type, the environment, the logical phases, the intended usage and the general IT features of the TOE.

2.1 System Type and Scope of the TOE

2.1.1 System Type Statement

For the reasons explained hereafter, the TOE is considered to be as of a "System Type".

2.1.2 Security Strategy Statement

From this Evaluation/Certification process, it is expected the implementation of the security requirements, rules and practices to be applied to:

- The **"SmartCard IC Development Flow - Japan"**, including its **"Information Technology"**,
- The **"Environment**" of this development flow, including its **"Information Technology"**,

That is to say that the security emphasis will be stressed to the TOE, that is the **"SmartCard IC Development Flow - Japan"** and its **"Information Technology"**, included. However for consistency into the stated security strategy, and in order to achieve the protection of all the assets that have been identified by NEC, it is also asked that the TOE environment and its information technology can realize those of the necessary security measures that are required to it.

This TOE and its Environment could be part of a smartcard product security Evaluation/Certification process, performed in accordance with PP/9806 Version 2.0 and its claimed Evaluation Assurance Level (EAL4 augmented). Therefore, the present ST is also taking into account the security requirements from this PP/9806 Version 2.0, that the environment of development (development flow) needs to be compliant with. This is explained inside the following content of this ST, by the chapters: "Conformance to PP/9806 Version 2.0 Phase 2 (IC Development Phase)".

2.1.3 TOE Definition Statement

The TOE (i.e.: the **“SmartCard IC Development Flow - Japan”,** including its **“Information Technology”**) is used for the design activity. That is to say that the TOE is used to produce the electronic files (data-base) of the operating functions and blocks, of the security functions and features, of the mask data, that are made necessary to the production of the photomasks and finally to the manufacturing of the semiconductor product that is answering to a specification issued from the market need.

The mask data, when issued from the TOE, is supplied to the mask maker to manufacture the photomasks (also named the reticles). Photomasks that will be later used into the production sites to produce the silicon wafers.

The TOE is also producing all the necessary documentation, under a “physical format” (hard document and hard copy), associated to these electronic files. Part of this documentation is necessary to the users and to the administrators of these microcontroller components to understand their behavior, their capability and characteristics when they are used in smartcard applications, and to use them in the best possible secure manner.

The TOE, for its identification, is labeled with the name of “SmartCard IC Development Flow - Japan”. This name is unique and, within NEC, is strictly dedicated to the design operations of the microcontrollers that are used for the smartcard applications.

After the operations in the “SmartCard IC Development Flow - Japan” are completed, this is the production flow, for mass production, that is taking place.

“SmartCard IC Development Flow - Japan” – The TOE

The TOE is made of computerized sequential operations. The change from one operation to the next one is under the control of the TOE.

This flow is calling for “trusted deliveries and verification procedures” to exchange information/data and material:

- Electronic Files.
- Hard Document (ex: hard document of electronic files,…) and Hard Copy (ex: test and evaluation programs).

The exchange may be performed within the TOE itself (from one phase of the TOE to the next phase of the TOE) and to outside of the TOE. When the exchange is using the Information System, “trusted deliveries and verification procedures” are used throughout this information system. When the exchange is using “physical mail posting” a “trusted deliveries and verification procedures” is also used.

2.2 Phases of the TOE and Phases outside of the TOE

The phases of the TOE are shown hereafter. These are the sequential operations noted from phase 1 to 3 and phase numbered 6.

The steps numbered 4, 5 and 7 are taking place outside of the TOE.

The “trusted deliveries and verification procedures” have to be used for any shipment made from the phases of the TOE towards any of these steps numbered 4, 5, and 7.

Phases of the TOE	Steps outside of the TOE
1- SYSTEM DESIGN.	
2- CIRCUIT DESIGN.	
3- LAY-OUT DESIGN.	
	4- MASK SHOP.
	5- WAFER DIFFUSION.
6- EVALUATION.	
	7- MASS PRODUCTION.

2.3 Boundaries of the TOE

The TOE, as being the “SmartCard IC Development Flow - Japan”, is including:

- The “SmartCard IC Development Flow - Japan” itself, with the sequence of phases numbered from 1 to 3 and with the phase numbered 6, as shown in the above table.
- The physical pieces of equipment, within the “SmartCard IC Development Flow - Japan”, that are used to accordingly perform the operations at the phases numbered 1, 2, 3 and 6. These are mainly the computer workstations, the server machines and the testing equipment. All of them are housing the Information Technology of the “SmartCard IC Development Flow - Japan”.
- The Information Technology of the “SmartCard IC Development Flow - Japan” (TOE IT).

2.4 Environment of the TOE

Considering the TOE, the below elements are viewed as being part of the environment of the TOE (“Environment of the TOE”):

- The physical areas where the TOE is located.
- The Information Technology of the “Environment of the TOE”.
- The personnel from the “SmartCard IC Development Section”.

- The “trusted deliveries and verification procedures” to exchange any information/data and material (Electronic Files, Hard Document and Hard Copy). The exchange may be performed either between phases of the TOE or to outside of the TOE.

2.4.1 Physical Areas

The Physical Areas:

- Where the phases numbered 1, 2, 3 and 6 of the “SmartCard IC Development Flow - Japan” are taking place.
- The “Tester Room” where the phase numbered 6 of the “SmartCard IC Development Flow - Japan” is taking place.

2.4.2 Information Technology of the Environment of the TOE

For a better understanding of the Information Technology of the “Environment of the TOE”, some explanations are made hereafter:

- The Information System implemented for the operation of the “SmartCard IC Development Section” is called the “SmartCard IC Development Information System”.
- This “SmartCard IC Development Information System” is composed of two subsystems”: The “SmartCard IC Development Flow - Japan” (the TOE) and the “Environment of the TOE”.
- Both the TOE and the “Environment of the TOE” have their own associated Information Technology. The Information Technology of the “Environment of the TOE” is the information technology of the “SmartCard IC Development Information System” that is not part of the TOE.

The Information Technology of the “Environment of the TOE” has got the role to ensure the correct overall operation and the protection of the “SmartCard IC Development Information System” itself, and also of the “SmartCard IC Development Flow - Japan”.

The Information Technology of the “Environment of the TOE” has been given the objectives to protect against external intrusion and attacks the TOE and its Information Technology and the information/data (Electronic Files) that is either delivered inside the TOE or delivered to outside of the TOE.

2.4.3 Personnel

The personnel are the members employed and/or contracted by the “SmartCard IC Development Section”. It is required to the personnel to have the right skills and knowledge, in order to be able to correctly and securely perform the operations of the department. That means the personnel shall act in accordance with the objectives given to the “SmartCard IC Development Section”, and in accordance with the policies and procedures defining the rules to be executed in order to accordingly run the job.

2.4.4 Trusted Delivery and Verification Procedure

These “trusted delivery and verification procedure” are used to exchange information/data and material (Electronic Files, Hard Document and Hard Copy) either within the TOE itself (from one phase of the TOE to the next phase of the TOE) or to outside of the TOE.

When the exchange is using the information system, the “trusted deliveries and verification procedures” methodology is implemented throughout this information system.

When the exchange is using “physical mail posting” means, the “trusted deliveries and verification procedures” are based upon security policies and procedures implemented in order to guarantee that all the necessary security measures are implemented in order to protect the information/data and material being delivered.

2.5 General IT Features of the TOE

2.5.1 Description of the TOE IT

The TOE is including its own Information Technology (TOE IT). For the correct and secure operation of the TOE, this TOE IT is using several Operating Systems and several pieces of application software.

The Operating Systems are listed hereafter:

- “Windows” Operating System.
- “Unix” Operating System, used to run several Server Machines and to run the pieces of application software.

2.5.2 What the “TOE IT” is not

Those of the Information Technology, that are not listed into the previous paragraph, are understood as being part of the Information Technology of the Environment of the TOE (IT of the TOE Environment).

Chapter 3

3. TOE Security Environment

Editorial Note about CC:

The “TOE Security Environment” section describes the security aspects of the environment in which the TOE is intended to be used, and the manner in which it is expected to be employed (cf: CC part 1).

This section also addresses the description of the assets to be protected, the assumptions, the threats and the organizational security policies.

3.1 TOE Intended Usage

In order to strengthen such usage, the TOE is made accessible strictly under a “Need To Know” basis to authorized personnel.

With the use of “Security Functional Requirements”, within the Information Technology that is associated to the TOE, a full control and management of the authorized access is insured by the TOE itself. Furthermore, this control and management, of the authorized access, is also insured by all the environmental and physical security aspects implemented within the Environment of the TOE (TOE Environment).

3.1.1 System Design

Describes all the operating functions that the device will offer. For this purpose design data will be prepared for the total chip and for each individual block-units.

3.1.2 Circuit Design

Translates the above design data into “transistor blocks” to insure the operating functions required to the device.

3.1.3 Lay-out Design

Makes the physical implementation of all the design entries, at the surface of the die (“block-units”, “transistor blocks”, electrical connections).

When completed, validation of the compliance of the designed device, to its specification as per the market requirements, is performed.

3.1.4 Evaluation Phase

Evaluates, for the first samples, the compliance of the operating functions and of the electrical parameters against device specification.

This last operation is also used to achieve the full characterization of the product.

3.2 Assets

Assets have to be protected in terms of confidentiality, integrity and availability, by the TOE and/or by the TOE Environment.

Assets are:

- Security relevant elements from the TOE.
- And security relevant elements used by the TOE.

3.2.1 Assets from the TOE – “Computerized” Assets

- Electronic Files.
- Assembler Script Electronic Files.
- Circuit Data Electronic Files.
- Mask Data Electronic Files.
- EEPROM Electronic Files.
- Dedicated Software Electronic Files:
  . Evaluation Program Electronic Files for evaluation of the security circuits.
  . Test Program Electronic Files (used for “mass production”).
  . IC Embedded Software Electronic Files.
- Evaluation Results Electronic Files.
- Customer ROM Code Data Electronic Files (Smartcard Embedded Software).

From the concept of the “Security Strategy Statement” as earlier defined in this ST (see 2.1.2), it is possible to claim that the security of the assets from the TOE will be mainly ensured by the TOE itself and by the “TOE Environment”.

3.2.2 Assets used or issued by the TOE – "Non-Computerized" Assets

- Hard Document of all these Electronic Files.
- Product Samples.
- Hard Copy of Dedicated Software:
  . Evaluation Program.
  . Test Program (used for mass production).
  . IC Embedded Software.
- Hard Document of Evaluation Results.
- Emulator.
- Simulator.

Again, from the concept of the "Security Strategy Statement" as earlier defined in this ST (see 2.1.2), it is possible to claim that the security of the assets used or issued by the TOE will be ensured by the TOE itself and by the "TOE Environment".

3.2.3 The TOE itself is an asset.

From the same concept of "Security Strategy Statement", as earlier defined in this ST, it is possible to claim that the security of the TOE will be ensured by the TOE itself and by the "TOE Environment".

3.3 Assumption

Editorial Note about CC:

Hereafter is listed the assumption relative to information about the intended usage of the TOE and information about the environment of use of the TOE (cf: CC Part 1).

This assumption has to be met by the Environment of the TOE in order for the TOE to be considered secure (cf: CC Part 1).

A.SKL_PERSONNEL: It is assumed that personnel involved in the smartcard development operations have got the required skills and have been educated to the security rules to be used and that this personnel is following these rules.

3.4 Conformance to PP/9806 Version 2.0 - Phase 2 (IC Development Phase) - Assumptions:

No additional assumption is required to the above listed for a conformance to PP/9806 Version 2.0, on phase 2.

3.5 Threats

Editorial Note about CC:

This section describes the threats to the assets against which specific protection within the TOE or its environment is required (cf: CC Part 1).

Editorial Note:

TOE as defined in chapter 2 or its environment is required to counter the threats.

A threat agent wishes to abuse the assets either by functional attacks, environmental manipulations, specific hardware manipulations or by any other type of attacks. In all cases the objective of the threat is to defeat the confidentiality or the integrity or the availability of the asset which is attacked.

Basically, the assumed threats could be described in three types:

- **Unauthorized disclosure of assets,**
- **Unauthorized modification of assets,**
- **Theft or unauthorized use of assets.**

Unauthorized disclosure of assets:

T.DIS_ELECFILES: Unauthorized disclosure of Electronic Files. This is concerning all the Electronic Files as listed in the assets section of this Security Target.

T.DIS_HARDDOC: Unauthorized disclosure of hard document, as listed in the assets section of this Security Target.

T.DIS_HARDCOPY: Unauthorized disclosure of hard copy, as listed in the assets section of this Security Target (hard copy is under physical format: Such as floppy disk,…).

Unauthorized modification of assets:

T.MOD_ELECFILES: Unauthorized modification of Electronic Files. This is concerning all the Electronic Files as listed in the assets section of this Security Target. Modification may include deletion of the Electronic Files.

T.MOD_HARDCOPY: Unauthorized modification of hard copy, as listed in the assets section of this Security Target (hard copy is under physical format: Such as floppy disk,…).

Theft or unauthorized use of assets:

T.T_ELECFILES: Theft or unauthorized use of Electronic Files. This is concerning all the Electronic Files as listed in the assets section of this Security Target.

T.T_HARDDOC: Theft or unauthorized use of hard document, as listed in the assets section of this Security Target.

T.T_HARDCOPY: Theft or unauthorized use of “hard-copy”, as listed in the assets section of this Security Target (when under physical format: Such as floppy disk,…).

T.T_PRODUCT: Theft or unauthorized use of smartcard products or samples.

T.T_EMUL: Theft or unauthorized use of smartcard emulator.

T.T_SIMUL: Theft or unauthorized use of smartcard simulator.

T.COPY_ELECFILES: Unauthorized electronic copy of the Electronic Files. This is concerning all the Electronic Files as listed in the assets section of this Security Target.

T.PRINT_ELECFILES: Unauthorized “print-out” of Electronic Files. This is concerning all the Electronic Files as listed in the assets section of this Security Target.

3.6 Conformance to PP/9806 Version 2.0 - Phase 2 (IC Development Phase) - Threats:

The below threats are required by PP/9806 Version 2.0 on phase 2 (IC Development Phase) and have to be countered by the development environment, as shown per the table 3.1 “Threats and phases” in PP/9806 Version 2.0, page 19/54:

T.CLON:
This threat as per PP/9806 is standing for the cloning of the smartcard product and will have the following explanations in the configuration of this evaluated TOE.
T.CLON is covered by the threat T.T_PRODUCT.

T.DIS_DESIGN:
This threat covering the disclosure can be made possible by the disclosure of any of the electronic files and/or hard document that is related to the design of the smartcard microcontroller and to the component itself.
T.DIS_DESIGN is covered by the threats T.DIS_ELECFILES, T.DIS_HARDDOC, T.T_ELECFILES, T.T_HARDDOC, T.COPY_ELECFILES, T.PRINT_ELECFILES and T.T_PRODUCT.

T.DIS_SOFT:
This threat is about the disclosure of smartcard embedded software.
T.DIS_SOFT is covered by the threats T.DIS_ELECFILES, T.COPY_ELECFILES, T.PRINT_ELECFILES, T.T_ELECFILES and T.T_PRODUCT.

T.DIS_DSOFT:
This threat is about the disclosure of the IC dedicated software.
T.DIS_DSOFT is covered by the threats T.DIS_ELECFILES, T.DIS_HARDCOPY, T.COPY_ELECFILES, T.PRINT_ELECFILES, T.T_ELECFILES, T.T_HARDCOPY and T.T_PRODUCT.

T.DIS_TEST:
This threat is addressing the disclosure of test information, such as full results as of IC testing (as per the description within the version 2.0 of the PP/9806).
T.DIS_DSOFT is covered by the threats T.DIS_ELECFILES, T.DIS_HARDDOC, T.COPY_ELECFILES, T.PRINT_ELECFILES, T.T_ELECFILES and T.T_HARDDOC.

T. DIS_TOOLS:
This threat that is involving the development tools will be in the frame of the present TOE concerning the emulator and the simulator tools.
T.DIS_TOOLS is covered by the threats T.T_EMUL and T.T_SIMUL.

T.DIS_PHOTOMASK:
The photomasks in the “SmartCard IC Development Flow - Japan” are only existing under an electronic file format.
T.DIS_PHOTOMASK is covered by the threats T.DIS_ELECFILES, T.COPY_ELECFILES, T.PRINT_ELECFILES and T.T_PRODUCT.

T.T_SAMPLE:
This threat addressing the theft of sample (product) is covered by T.T_PRODUCT.

T.T_PHOTOMASK:
This threat, as understood from the version 2.0 of the PP/9806, is addressing the physical photomasks. Within the “SmartCard IC Development Flow - Japan”, photomasks are only existing under an electronic file format.
T.T_PHOTOMASK itself is not applicable.

T.T_PRODUCT:
This threat is addressing the theft of product and therefore is covered by the threat T.T_PRODUCT.

T.MOD_DESIGN:
The modification of IC design is considered as a threat when this modification is made under an unauthorized way and for malicious purpose.
T.MOD_DESIGN is covered by the threats T.MOD_ELECFILES and T.COPY_ELECFILES.

T.MOD_PHOTOMASK:
The modification of IC photomasks is considered as a threat when this modification is made under an unauthorized way and for malicious purpose.
T.MOD_PHOTOMASK is covered by the threats T.MOD_ELECFILES and T.COPY_ELECFILES.

T.MOD_DSOFT:
This threat is about the modification of the IC dedicated software.
T.MOD_DSOFT is covered by the threats T.MOD_ELECFILES, T.MOD_HARDCOPY and T.COPY_ELECFILES.

T.MOD_SOFT:
This threat is about the modification of the IC smartcard embedded software.
T.MOD_SOFT is covered by the threats T.MOD_ELECFILES and T.COPY_ELECFILES.

3.7 Organizational Security Policies (OSP’ s)

Editorial Note about CC:

“Organizational Security Policies” identify and explain organizational security policy statements or rules that the TOE must comply with (cf: CC Part 1).

These policies are necessary for an operation of the TOE in a secure environment.

Editorial Note about Security System:

For the purpose of the evaluation and certification process of the “SmartCard IC Development Flow - Japan”, a number of security procedures have been developed. For a correct implementation they have been described into written documents, in order they can be followed and can remain in the time. The objective for these documents could be summarized with: “The procedures and practices that are used shall be documented and what is inside the written documents shall be applied”.

Like for quality, this concept will be used and applied to security, leading to the implementation of a “Security System”.

Therefore a “Security System” will be the set of procedures that defines the rules for security to be implemented and used in order the operations covered by these procedures can meet the security objectives defined for the involved operations.

The “Security System” is based on specifications describing the procedures to be followed and is made for the management of on-site security. This “Security System” is composed of three sets of document:

- The Manuals.
- The “Security Operating Policies” (SOP’ s).
- The Specifications.

The Manuals, the “SOP’ s” and the Specifications involved in the security implementation in the “SmartCard IC Development Flow - Japan”, the TOE, and its Environment are described into this Security Target.

A deeper definition and description of these Manuals, “SOP’ s” and Specifications can be given inside a procedure that is related to the “Smartcard Specification System” OSP.

3.7.1 “Smartcard Specification System” OSP

This policy defines the management rules to be used to write and release specifications (manual, other policy) related to components or operations dedicated to smartcard activity.

3.7.2 “Smartcard Master Security Audit” OSP

While an audit program on security exists and is carried out under the control of the “Local Security Manager”, a “master security audit” is performed on a yearly basis by the “SCAC Security Manager”.

3.7.3 “Smartcard Subcontractor Approval” OSP

This policy defines the procedure to approve a subcontractor for any activity that is related to the TOE that is used to design the smartcard microcontroller components.

3.7.4 “Smartcard Subcontractor Management” OSP

This policy defines the procedure to govern and control subcontractors activities in operations that are related to the TOE that is used to design the smartcard microcontroller components.

3.7.5 “Smartcard Security Failure Report & Corrective Actions” OSP

A “Failure Report and Corrective Actions” procedure exists to notify about any security failure and non-conformance that may occur within the TOE and within the Environment of the TOE. This procedure is also used to define and report the corrective actions to be taken in order to fix the issue and prevent re-occurrence.

3.7.6 “Smartcard Security Change Management” OSP

This policy defines the procedure to govern and control the changes required to the “Security System”, to the TOE itself and to the Environment of the TOE.

3.7.7 “Trusted Delivery & Verification Procedure” OSP

This policy defines the method that is used to secure and make trusted the delivery of computerized and non- computerized information and data, and is used to verify that no mal-function occurred in the delivery process.

3.8 Conformance to PP/9806 Version 2.0 - Phase 2 (IC Development Phase) Organizational Security Policies:

For conformance to PP/9806 Version 2.0 on phase 2, no additional Organizational Security Policy is required to those of the OSP’ s listed into the chapter 3.7 of the present ST.

Chapter 4

4. Security Objectives

<u>Editorial Note about CC:</u>

The security objectives for the TOE shall be clearly stated and traced back to aspects of identified threats to be countered by the TOE and/or organizational security policies to be met by the TOE (cf: CC Part 1).

The security objectives for the environment shall be clearly stated and traced back to aspects of identified threats not completely countered by the TOE and/or organizational security policies or assumptions not completely met by the TOE (cf: CC Part 1).

The security objectives cover principally the following aspects:

- **Confidentiality, Integrity and availability of assets,**
- **Protection of the TOE and associated material and documentation during the design operation of the microcontrollers for the smartcard market.**

4.1 IT Security Objective for the TOE

O.ACS_PRT: The TOE IT shall give an access only to authorized personnel and shall protect its security critical parts and “computerized assets” against unauthorized access and operations.

4.2 NON-IT Security Objectives for the TOE

O.ASSETS_TRACK: The TOE NON-IT must track the “non-computerized” assets.

O.ASSETS_PRT: The TOE NON-IT must protect the “non-computerized” assets against theft and unauthorized access or use.

4.3 Security Objectives for the TOE Environment

O.TOE_PRT: The TOE is operated in a secure environment. It is required to the Environment of the TOE to bring a physical protection and an “Information System” protection to the TOE. The TOE shall be made accessible only by the authorized personnel (“Need To Know” personnel).

O.SEC_DEL: The Environment of the TOE shall guarantee that the delivery of any of the “computerized” or “non- computerized” assets (as listed in paragraph 3.2 of this Security Target) is secure. The delivery process shall maintain and verify the confidentiality and the integrity of the assets when they are delivered from or to the TOE.

4.4 <u>Conformance to PP/9806 Version 2.0 - Phase 2 (IC Development Phase) – Security Objectives</u>:

The below objectives for the environment are required by PP/9806 Version 2.0 on phase 2 (IC Development Phase), as shown per paragraph 4.2.2 in PP/9806 Version 2.0, page 23/54:

O.SOFT_ACS: Is the security objective requiring that the smartcard embedded software is only accessible by the authorized personnel within the IC designer on the need to know basis.
O.SOFT_ACS is covered by the security objectives O.ACS_PRT and O.TOE_PRT.

O.DESIGN_ACS: Is the security objective requiring that the IC specifications, detailed design, IC data-bases, schematic/lay-out or any further design information is only accessible by the authorized personnel within the IC designer on the need to know basis.
O.DESIGN_ACS is covered by the security objectives O.ACS_PRT, O.ASSETS_PRT and O.TOE_PRT.

O.DSOFT_ACS: Is the security objective requiring that IC dedicated software specification, detailed design, source code or any further information is only accessible by the authorized personnel within the IC designer on the need to know basis.
O.DSOFT_ACS is covered by the security objectives O.ACS_PRT, O.ASSETS_PRT and O.TOE_PRT.

O.MASK_FAB: Is the security objective requiring that physical, personnel, organizational, technical procedures during photomask fabrication, including deliveries between photomasks manufacturer and IC manufacturer, is ensuring the integrity and the confidentiality of the TOE (the product in this case).
In the case of the TOE, the photomasks are not physically fabricated in the way it is described within the version 2.0 of the PP/9806. Any of the security objectives that is requiring to ensure the integrity and the confidentiality of the electronic files, will cover this security objective from the version 2.0 of PP/9806.
O.MASK_FAB is covered by the security objectives O.ACS_PRT, O.TOE_PRT and O.SEC_DEL.

O.MECH_ACS: Is the security objective requiring that details of hardware security mechanism specifications are only accessible by the authorized personnel within the IC designer on the need to know basis.
O.MECH_ACS is covered by the security objectives O.ACS_PRT, O.ASSETS_PRT and O.TOE_PRT.

O.TI_ACS: Is the security objective requiring that security relevant technology information is only accessible by the authorized personnel within the IC designer on the need to know basis.
O.TI_ACS is covered by the security objectives O.ACS_PRT, O.ASSETS_PRT and O.TOE_PRT.

Chapter 5

5. Security Requirements

5.1 TOE IT Security Requirements

5.1.1 TOE IT Security Functional Requirements

<u>Editorial Note about CC:</u>

The statement of TOE security functional requirements should define the functional requirements for the TOE as functional components drawn from the Common Criteria part 2 (cf: CC Part 1).

5.1.1.1 User Identification before any Action (FIA_UID.2)

Hierarchical to: FIA_UID.1 Timing of Identification.
It is applied in the TOE that no actions are allowed before the user is identified. Therefore, the "FIA_UID.1" security functional requirement is not relevant and will not be used.

FIA_UID.2.1: The TOE security functions shall require each user to identify itself before allowing any other TOE security functions-mediated actions on behalf of that user.

<u>Iteration 1:</u>
The TOE security functions of [refinement: "Windows"] shall require each user to identify itself before allowing any other TOE security functions-mediated actions on behalf of that user.
The "Windows" operating system, for identification of each user, requires each user to enter the User Identifier (User Identifier may be the Logon Name). This is required before any other TOE security functions-mediated actions, on behalf of that user, is allowed.

<u>Iteration 2:</u>
The TOE security functions of [refinement: "Unix"] shall require each user to identify itself before allowing any other TOE security functions-mediated actions on behalf of that user.
The "Unix" operating system, for identification of each user, requires each user to enter its Login Name (Login Name may be the Identification Number). This is required before any other TOE security functions-mediated actions, on behalf of that user, is allowed.

<u>Iteration 3:</u>
The TOE security functions of [refinement: "Windows"] shall require each user to identify itself before allowing any other TOE security functions-mediated actions on behalf of that user.
The "Windows" operating system, for identification of each user, requires each user to enter the User Identifier (User Identifier may be the Logon Name). This is required before any other TOE security functions-mediated actions, on behalf of that user, is allowed.
Dependencies: No dependencies.

5.1.1.2 User Authentication before any Action (FIA_UAU.2)

Hierarchical to: FIA_UAU.1 Timing of Authentication.
It is applied in the TOE that no actions are allowed before the user is authenticated. Identification and authentication of user is the first action run by the TOE and at the same time. Therefore, “FIA_UAU.1” is not relevant and will not be used.

FIA_UAU2.1: The TOE security functions shall require each user to be successfully authenticated before allowing any other TOE security functions-mediated actions on behalf of that user.

Iteration 1:
The TOE security functions of [refinement: “Windows”] shall require each user to be successfully authenticated before allowing any other TOE security functions-mediated actions on behalf of that user.
The “Windows” operating system, for authentication of each user, requires each user to enter its password. The authentication of the user is the first action performed before any other TOE security function-mediated action is taking place. The authentication is in fact performed at the same time than the identification and is the first action of the TOE security functions.

Iteration 2:
The TOE security functions of [refinement: “Unix”] shall require each user to be successfully authenticated before allowing any other TOE security functions-mediated actions on behalf of that user.
The “Unix” operating system, for authentication of each user, requires each user to enter its password. The authentication of the user is the first action performed before any other TOE security function-mediated action is taking place. The authentication is in fact performed at the same time than the identification and is the first action of the TOE security functions.

Iteration 3:
The TOE security functions of [refinement: “Windows”] shall require each user to be successfully authenticated before allowing any other TOE security functions-mediated actions on behalf of that user.
The “Windows” operating system, for authentication of each user, requires each user to enter its password. The authentication of the user is the first action performed before any other TOE security function-mediated action is taking place. The authentication is in fact performed at the same time than the identification and is the first action of the TOE security functions.

Dependencies: FIA_UID.1 Timing of identification.
It is applied in the TOE that no actions are allowed before the user is identified and authenticated. Therefore, the dependency to FIA_UID.1 is not relevant.

5.1.1.3 User Attribute Definition (FIA_ATD.1)

Hierarchical to: No other components.

FIA_ATD.1.1: The TOE security functions shall maintain the following list of security attributes belonging to individual users: [assignment: list of security attributes].

Iteration 1:
The TOE security functions of [refinement: “Windows”] shall maintain the following list of security attributes belonging to individual users: [assignment:

- User Identifier.
- Password.
- User Roles.
- User Rights].

Iteration 2:
The TOE security functions of [refinement: “Unix”] shall maintain the following list of security attributes belonging to individual users: [assignment:

- Login Name (Root for Administrator and other name for other users).
- Password.
- Property (Owner or Non-owner).
- User Roles.
- User Rights].

Iteration 3:
The TOE security functions of [refinement: “Windows”] shall maintain the following list of security attributes belonging to individual users: [assignment:

- User Identifier.
- Password.
- User Roles.
- User Rights].

Dependencies: No dependencies.

5.1.1.4 Security Roles (FMT_SMR.1)

Hierarchical to: No other components.

FMT_SMR.1.1: The TOE security functions shall maintain the roles [assignment: the authorized identified roles].

Iteration 1:
The TOE security functions of [refinement: “Windows”] shall maintain the roles [assignment:

- Administrator Role.
- User Role].

The “Windows” operating system, for its secure operation and to protect its own secured assets (files,…), recognizes and maintains the two roles, and only these two roles, administrator role and user role.

Iteration 2:
The TOE security functions of [refinement: “Unix”] shall maintain the roles [assignment:

- Administrator Role.
- User Role].

The “Unix” operating system, for its secure operation and to protect its own secured assets (files,…), recognizes and maintains the two roles, and only these two roles, administrator role and user role.

Iteration 3:
The TOE security functions of [refinement: “Windows”] shall maintain the roles [assignment:

- Administrator Role.
- User Role].

The “Windows” operating system, for its secure operation and to protect its own secured assets (files,…), recognizes and maintains the two roles, and only these two roles, administrator role and user role.

FMT_SMR.1.2: The TOE security functions shall be able to associate users with roles.

Iteration 1:
The TOE security functions of [refinement: “Windows”] shall be able to associate users with roles.
“Administrator” and “Users” are the two roles recognized by the “Windows” operating system. Therefore, attributes are also used by the TOE IT to make the difference between these two roles and to give the exact rights to the users, depending on the identity claimed by these users (“Administrator” and “Users”).
This association of users with roles, within “Windows” is made by the User Identifier and confirmed with the Password entered.

Iteration 2:
The TOE security functions of [refinement: “Unix”] shall be able to associate users with roles.
“Administrator” and “Users” are the two roles recognized by the “Unix” operating system. Therefore, attributes are also used by the TOE IT to make the difference between these two roles and to give the exact rights to the users, depending on the identity claimed by these users (“Administrator” and “Users”).
This association of users with roles, within “Unix”, is made by the use of the Login Name and confirmed with the Password entered.

Iteration 3:
The TOE security functions of [refinement: “Windows”] shall be able to associate users with roles.
“Administrator” and “Users” are the two roles recognized by the “Windows” operating system. Therefore, attributes are also used by the TOE IT to make the difference between these two roles

and to give the exact rights to the users, depending on the identity claimed by these users (“Administrator” and “Users”).
This association of users with roles, within “Windows” is made by the User Identifier and confirmed with the Password entered.

Dependencies: FIA_UID.1 Timing of identification.
As it was earlier explained “Timing of identification” is not relevant to this TOE, because it is applied that no actions are allowed before the user is identified. Therefore, the dependency to FIA_UID.1 is also not relevant.

5.1.1.5 Complete Access Control (FDP_ACC.2)

Hierarchical to: FDP_ACC.1 Subset Access Control
The FDP_ACC.1 component is not reported into this ST, as the FDP_ACC.2 component is encompassing FDP_ACC.1 and is hierarchical to FDP_ACC.1.

FDP_ACC.2.1: The TOE security functions shall enforce the [assignment: access control security functions policy] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the Security Function Policy.

Iteration 1:
The TOE security functions of [refinement: “Windows”] shall enforce the [assignment: “Windows” access control security functions policy] on [assignment: administrator and users, on administrator electronic files, users electronic files, administration rights and user rights] and all operations among subjects and objects covered by the Security Function Policy.

Iteration 2:
The TOE security functions of [refinement: “Unix”] shall enforce the [assignment: “Unix” access control security functions policy] on [assignment: administrator and users, administrator electronic files, user electronic files, administrator rights and user rights] and all operations among subjects and objects covered by the Security Function Policy.

Iteration 3:
The TOE security functions of [refinement: “Windows”] shall enforce the [assignment: “Windows” access control security functions policy] on [assignment: administrator and users, on administrator electronic files, users electronic files, administration rights and user rights] and all operations among subjects and objects covered by the Security Function Policy.

FDP_ACC2.2: 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 Function Policy.

Iteration 1:
The TOE security functions of [refinement: “Windows”] 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 Function Policy.

Iteration 2:
The TOE security functions of [refinement: “Unix”] 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 Function Policy.

Iteration 3:
The TOE security functions of [refinement: “Windows”] 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 Function Policy.

Dependencies: FDP_ACF.1 Security Attribute Based Access Control
Dependency is satisfied. See paragraph 5.1.1.6.

5.1.1.6 Security Attribute Based Access Control (FDP_ACF.1)

Hierarchical to: No other components.

FDP_ACF.1.1: The TOE security functions shall enforce the [assignment: access control security functions policy] to objects based on [assignment: security attributes, named groups of security attributes].

Iteration 1:
The TOE security functions of [refinement: “Windows”] shall enforce the [assignment: “Windows” access control security functions policy] to objects based on [assignment: security attributes that are User Roles and User Rights].

Iteration 2:
The TOE security functions of [refinement: “Unix”] shall enforce the [assignment: “Unix” access control security functions policy] to objects based on [assignment: security attributes that are User Roles, Property (Owner or Non-Owner) and User Rights].

Iteration 3:
The TOE security functions of [refinement: “Windows”] shall enforce the [assignment: “Windows” access control security functions policy] to objects based on [assignment: security attributes that are User Roles and User Rights].
FDP_ACF.1.2: The TOE security functions shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

Iteration 1:
The TOE security functions of [refinement: “Windows”] shall enforce the following rule to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: the rule is the verification of the attributes that are Role, User Rights as explained in the table hereafter.

. Controlled subjects are:

- Administrator.
- Users.

. Controlled objects are:

- Administrator electronic files.
- Users electronic files.
- Administration rights.
- User rights.

* Table showing authorized operation among controlled subjects and controlled objects:

		OBJECTS					
		Admin. Elec. Files	Admin. Rights	Own User Elec. Files*	Other Users Elec. Files**	Own User Rights	Other Users Rights
SUBJECTS	Administrator	R, W, X	R, W, X	R, W, X	R, W, X	R, W, X	R, W, X
	User	No Operation	No Operation	R, W, X	O	R, W, X	No Operation

* Authorized operations of that user on its own Electronic Files, depending on its own user role (User, Administrator).
** Operations authorized to that user (Subject) on the Electronic Files of the other users, depending on its own user role (User, Administrator) and depending on the rights authorized by the other users that are the owners of the Electronic Files.

R: Read
W: Write
X: Execute
O: depending on the rights authorized by the owners of the Electronic Files (they are the other users) to that user (Subject). This can be R, W, X (or any combination) or No Operation.

Iteration 2:
The TOE security functions of [refinement: “Unix”] shall enforce the following rule to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: the rule

is the verification of the attributes that are Role, Property and User Rights as explained in the table hereafter.

. Controlled subjects are:

- Administrator.
- Users.

. Controlled objects are:

- Administrator electronic files.
- Users electronic files.
- Administration rights.
- User rights.

* Table showing authorized operation among controlled subjects and controlled objects:

		OBJECTS					
		Admin. Elec. Files	Admin. Rights	Own User Elec. Files*	Other Users Elec. Files**	Own User Rights	Other Users Rights
SUBJECTS	Administrator	R, W, X	R, W, X	R, W, X	R, W, X	R, W, X	R, W, X
	User	No Operation	No Operation	R, W, X	O	R, W, X	No Operation

* Authorized operations of that user on its own Electronic Files, depending on its own user role (User, Administrator).
** Operations authorized to that user (Subject) on the Electronic Files of the other users, depending on its own user role (User, Administrator) and depending on the rights authorized by the other users that are the owners of the Electronic Files.

R: Read
W: Write
X: Execute
O: depending on the rights authorized by the owners of the Electronic Files (they are the other users) to that user (Subject). This can be R, W, X (or any combination) or No Operation.

Iteration 3:
The TOE security functions of [refinement: “Windows”] shall enforce the following rule to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: the rule is the verification of the attributes that are Role, User Rights as explained in the table hereafter.

. Controlled subjects are:

- Administrator.
- Users.

. Controlled objects are:

- Administrator electronic files.
- Users electronic files.
- Administration rights.
- User rights.

* Table showing authorized operation among controlled subjects and controlled objects:

		OBJECTS					
		Admin. Elec. Files	Admin. Rights	Own User Elec. Files*	Other Users Elec. Files**	Own User Rights	Other Users Rights
SUBJECTS	Administrator	R, W, X	R, W, X	R, W, X	R, W, X	R, W, X	R, W, X
	User	No Operation	No Operation	R, W, X	O	R, W, X	No Operation

* Authorized operations of that user on its own Electronic Files, depending on its own user role (User, Administrator).
** Operations authorized to that user (Subject) on the Electronic Files of the other users, depending on its own user role (User, Administrator) and depending on the rights authorized by the other users that are the owners of the Electronic Files.

R: Read
W: Write
X: Execute
O: depending on the rights authorized by the owners of the Electronic Files (they are the other users) to that user (Subject). This can be R, W, X (or any combination) or No Operation.

FDP_ACF.1.3: The TOE security functions shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].

Iteration 1:
The TOE security functions of [refinement: “Windows”] shall explicitly authorize access of subjects to objects based on the following additional rule: [assignment: Control of User Identifier and of User Password].

Iteration 2:
The TOE security functions of [refinement: “Unix”] shall explicitly authorize access of subjects to objects based on the following additional rule: [assignment: Control of user Login Name and of User Password].

Iteration 3:
The TOE security functions of [refinement: “Windows”] shall explicitly authorize access of subjects to objects based on the following additional rule: [assignment: Control of User Identifier and of User Password].

FDP_ACF.1.4: The TOE security functions shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

Iteration 1:
The TOE security functions of [refinement: “Windows”] shall explicitly deny access of subjects to objects based on the [assignment: rule that is Control of User Identifier and of User Password].

Iteration 2:
The TOE security functions of [refinement: “Unix”] shall explicitly deny access of subjects to objects based on the [assignment: rule that is Control of Login Name and of User Password].

Iteration 3:
The TOE security functions of [refinement: “Windows”] shall explicitly deny access of subjects to objects based on the [assignment: rule that is Control of User Identifier and of User Password].

Dependencies: FDP_ACC.1 Subset Access Control.
FMT_MSA.3 Static Attribute Initialization.
The dependency to FDP_ACC.1 is satisfied by the component FDP_ACC.2 Complete Access Control that is hierarchical to FDP_ACC.1.
The dependency to FMT_MSA.3 has not been chosen because the FMT_MSA.3 is asking for the availability of default values for the security attributes, in order to compliant with the requirements, while in the case of the present TOE no default values are defined for these security attributes. Therefore FMT_MSA.3 is considered to not be relevant.

5.1.1.7 Management of Security Attributes (FMT_MSA.1)

Hierarchical: No other components:

FMT_MSA.1.1: The TOE security functions shall enforce the [assignment: access control security functions policy, information flow control security functions policy] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorized identified roles].

Iteration 1:

The TOE security functions of [refinement: “Windows”] shall enforce the [assignment: “Windows” access control security functions policy] to restrict the ability to [selection: modify, delete, [assignment: set]] the security attributes [assignment: User Identifier, Password and User Rights] to [assignment: the authorized identified roles], as shown per the below table:

	Windows					
	User Identifier		**Password**		**User Rights**	
	Own	Other	Own	Other	Own	Other
Administrator	S M D	S M D	S M D	S M D	S M D	S M D
User	No Op.	No Op.	M	No Op.	S M D	No Op.

S: Set.
M: Modify.
D: Delete.
No Op.: No operation possible.

Iteration 2:

The TOE security functions of [refinement: “Unix”] shall enforce the [assignment: “Unix” access control security functions policy] to restrict the ability to [selection: modify, delete, [assignment: set]] the security attributes [assignment: Login Name, Password, Property and User Rights] to [assignment: the authorized identified roles], as shown per the below table:

	Unix							
	Password		**Login Name**		**Property**		**User Rights**	
	Own	Other	Own	Other	Own	Other	Own	Other
Administrator	S M D	S M D	No Op.	S M D	S M D	S M D	S M D	S M D
User	M	No Op.	No Op.	No Op.	M	No Op.	S M D	No Op.

S: Set.
M: Modify.

D: Delete.
No Op.: No operation possible.

<u>Iteration 3:</u>
The TOE security functions of [refinement: “Windows”] shall enforce the [assignment: “Windows” access control security functions policy] to restrict the ability to [selection: modify, delete, [assignment: set]] the security attributes [assignment: User Identifier, Password and User Rights] to [assignment: the authorized identified roles], as shown per the below table:

	Windows					
	User Identifier		**Password**		**User Rights**	
	Own	Other	Own	Other	Own	Other
Administrator	S M D	S M D	S M D	S M D	S M D	S M D
User	No Op.	No Op.	M	No Op.	S M D	No Op.

S: Set.
M: Modify.
D: Delete.
No Op.: No operation possible.

Dependencies: FDP_ACC.1 Subset Access Control or FDP_IFC.1 Subset Information Flow Control.
FMT_SMR.1 Security Roles.
The dependency to FDP_ACC.1 or FDP_IFC.1 is satisfied by the component FDP_ACC.2 Complete Access Control that is hierarchical to FDP_ACC.1.
The dependency to FMT_SMR.1 is satisfied.

5.1.1.8 Management of Security Functions Behavior (FMT_MOF.1)

Hierarchical to: No other components.

FMT_MOF.1.1: The TOE security functions shall restrict the ability to [selection: determine the behavior of, disable, enable, modify the behavior of] the functions [assignment: list of functions] to [assignment: the authorized identified roles].

<u>Iteration 1</u>
The TOE security functions of [refinement: “Windows”] shall restrict the ability to [selection: determine, disable, enable, modify the behavior of] the functions [assignment: as shown per the

table hereunder] to [assignment: the authorized identified roles], as shown per the table hereunder:

		Authorized Identified Roles	
		Administrator	**Users**
Security Functions	SF9	Determine, Modify	No ability
	SF10	No ability	No ability
	SF11	Determine, Modify	No ability
	SF12	Modify	Modify
	SF13	Determine, Enable, Disable, Modify	Modify

Iteration 2:

The TOE security functions of [refinement: “Unix”] shall restrict the ability to [selection: determine, disable, enable, modify the behavior of] the functions [assignment: as shown per the table hereunder] to [assignment: the authorized identified roles], as shown per the table hereunder:

		Authorized Identified Roles	
		Administrator	**Users**
Security Functions	SF1	No ability	Determine, Enable, Disable, Modify
	SF3	Determine, Enable, Disable, Modify	Determine, Enable, Disable, Modify
	SF4	No ability	No ability
	SF5	Determine, Modify	Determine, Modify
	SF6	Determine, Enable, Disable, Modify	Determine, Enable, Disable, Modify
	SF7	Determine, Enable, Disable, Modify	Determine, Enable, Disable, Modify

SF2: Not represented Security Function.
SF8: Not represented Security Function.

Iteration 3:

The TOE security functions of [refinement: “Windows”] shall restrict the ability to [selection: determine, disable, enable, modify the behavior of] the functions [assignment: as shown per the table hereunder] to [assignment: the authorized identified roles], as shown per the table hereunder:

		Authorized Identified Roles	
		Administrator	**Users**
Security Function	SF14	Determine, Modify	No ability
	SF15	No ability	No ability
	SF16	Determine, Modify	No ability
	SF17	Modify	Modify

	SF18	Determine, Enable, Disable, Modify	Modify

Dependencies: FMT_SMR.1 Security Roles.
Dependency is satisfied.

5.1.2 TOE IT Security Assurance Requirements

Editorial Note about CC:

The statement of TOE security assurance requirements should state the assurance requirements as one of the EAL' s optionally augmented by Common Criteria Part 3 assurance components for the TOE as functional components (cf: CC Part 1).

The assurance requirements correspond to those of EAL1 augmented with assurance components as listed below.

EAL1 Assurance Components:

5.1.2.1 Version Numbers (ACM_CAP.1)

Dependencies: No dependencies.

Developer action elements:

- ACM_CAP.1.1D: The developer shall provide a reference for the TOE.

Content and presentation of evidence elements:

- ACM_CAP.1.1C: The reference for the TOE shall be unique to each version of the TOE.
- ACM_CAP.1.2C: The TOE shall be labeled with its reference.

Evaluator action elements:

- ACM_CAP.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.2.2 Installation, Generation and Start-up Procedures (ADO_IGS.1)

Dependencies: AGD_ADM.1 Administrator Guidance.

Developer action elements:

- ADO_IGS.1.1D: The developer shall document procedures necessary for the secure installation, generation and start-up of the TOE.

Content and presentation of evidence elements:

- ADO_IGS.1.1C: The documentation shall describe the steps necessary for secure installation, generation and start-up of the TOE.

Evaluator action elements:

- ADO_IGS.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- ADO_IGS.1.2E: The evaluator shall determine that the installation, generation and start-up procedures result in a secure configuration.

5.1.2.3 Informal Functional Specification (ADV_FSP.1)

Dependencies: ADV_RCR.1 Informal Correspondence Demonstration.

Developer action elements:

- ADV_FSP.1.1D: The developer shall provide a functional specification.

Content and presentation of evidence elements:

- ADV_FSP.1.1C: The functional specification shall describe the TOE security functions and its external interfaces using an informal style.
- ADV_FSP.1.2C: The functional specification shall be internally consistent.
- ADV_FSP.1.3C: The functional specification shall describe the purpose and method of use of all external TOE security functions interfaces, providing details of effects, exceptions and error message, as appropriate.
- ADV_FSP.1.4C: The functional specification shall completely represent the TOE security functions.

Evaluator action elements:

- ADV_FSP.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- ADV_FSP.1.2E: The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.1.2.4 Representation Correspondence (ADV_RCR.1)

Dependencies: No dependencies.

Developer action elements:

- ADV_RCR.1.1D: The developer shall provide an analysis of correspondence between all adjacent pairs of TOE security functions representations that are provided.

Content and presentation of evidence elements:

- ADV_RCR.1.1C: For each adjacent pair of provided TOE security functions representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TOE security functions representation is correctly and completely refined in the less abstract TOE security functions representation.

Evaluator action elements:

- ADV_RCR.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.2.5 Administrator Guidance (AGD_ADM.1)

Dependencies: ADV_FSP.1 Informal Functional Specification.

Developer action elements:

- AGD_ADM.1.1D: The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

- AGD_ADM.1.1C: The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.
- AGD_ADM.1.2C: The administrator guidance shall describe how to administer the TOE in a secure manner.
- AGD_ADM.1.3C: The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
- AGD_ADM.1.4C: The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.
- AGD_ADM.1.5C: The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.
- AGD_ADM.1.6C: The administrator guidance shall describe each type of security relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TOE security functions.
- AGD_ADM.1.7C: The administrator guidance shall be consistent with all other documentation supplied for evaluation.
- AGD_ADM.1.8C: The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

- AGD_ADM.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.2.6 User Guidance (AGD_USR.1)

Dependencies: ADV_FSP.1 Informal Functional Specification.

Developer action elements:

- AGD_USR.1.1D: The developer shall provide user guidance.

Content and presentation of evidence elements:

- AGD_USR.1.1C: The user guidance shall describe the functions and interfaces available to the non-administrative user of the TOE.
- AGD_USR.1.2C: The user guidance shall describe the use of user-accessible security functions provided by the TOE.
- AGD_USR.1.3C: The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
- AGD_USR.1.4C: The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.
- AGD_USR.1.5C: The user guidance shall be consistent with all other documentation supplied for evaluation.
- AGD_USR.1.6C: The user guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

- AGD_USR.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.2.7 Independent Testing - Conformance (ATE_IND.1)

Dependencies: ADV_FSP.1 Informal Functional Specification.
AGD_ADM.1 Administrator Guidance.
AGD_USR.1 User Guidance.

Developer action elements:

- ATE_IND.1.1D: The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

- ATE_IND.1.1C: The TOE shall be suitable for testing

Evaluator action elements:

- ATE_IND.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- ATE_IND.1.2E: The evaluator shall test a subset of the TOE security functions as appropriate to confirm that the TOE operates as specified.

Augmentation Assurance Component:

5.1.2.8 Independent Vulnerability Analysis (AVA_VLA.2)

Dependencies: ADV_FSP.1 Informal Functional Specification.
ADV_HLD.2 Security Enforcing High-Level Design.

ADV_IMP.1 Subset of the Implementation of the TSF.
ADV_LLD.1 Descriptive Low-Level Design.
AGD_ADM.1 Administrator Guidance.
AGD_USR.1 User Guidance.

Developer action elements:

- AVA_VLA.2.1D: The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TOE security policy
- AVA_VLA.2.2D: The developer shall document the disposition of identified vulnerabilities.

Content and presentation of evidence elements:

- AVA_VLA.2.1C: The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.
- AVA_VLA.2.2C: The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

Evaluator action elements:

- AVA_VLA.2.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- AVA_VLA.2.2E: The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.
- AVA_VLA.2.3E: The evaluator shall perform an independent vulnerability analysis.
- AVA_VLA.2.4E: The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.
- AVA_VLA.2.5E: The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential.

5.2 TOE NON-IT Security Requirements

This paragraph defines statement of security requirements for the Non-IT part of the TOE.

5.2.1 Secure Storage

It is required to have implemented a secure storage for “Non-Computerized” Assets:

- Assets under hard document format, under hard copy format.
- Product samples.
- Emulator.
- Simulator.

It is required to have implemented a secure storage for the “Computerized” Assets:

- Electronic Files.

5.2.2 Material Asset Identification

It is required unique identification (reference and version number) for “Non-Computerized” Assets:

- Assets under hard document format, under hard copy format.
- Product samples.
- Emulator.
- Simulator.

5.2.3 Non Permanence

It is required that the test program and the evaluation program are not resident on test equipment and are erased after the completion of:

- Development operation for test program and for evaluation program.
- Evaluation operation of product samples for evaluation program.

It is required that the evaluation results are also not resident on the pieces of equipment used for evaluation and are erased after the completion of the evaluation operation.

5.2.4 End of Life

It is required that an “end of life” procedure exists for the hard copy of evaluation program and for the test program, and for the files under an electronic format (Electronic Files).

5.2.5 Transfer of Test Program - Hand-Carry – Secure Delivery

It is required that for transfer of test program, to the site for test production, an hand-carry transportation is used.

5.2.6 Data Back-up

It is required that data “back-up” exists for the evaluation results.

5.2.7 Material Asset Configuration Management

It is required to control the identification and manage configuration for:

- Assets under hard document format, under hard copy format,
- Product samples,
- Emulator,
- Simulator,

and to control any change that may be applied to them.

5.2.8 Access Control Management

It is required to have implemented the access rights and rules in order to control access and give access only to authorized personnel to the TOE, to its associated pieces of equipment (computers, locked shelves, safes,...), to the assets.

5.2.9 Passwords Management

It is required to securely create, control and manage all the passwords used to control the access to the TOE, to its associated pieces of equipment (computers, locked shelves, safes,...), to the assets.

5.2.10 Security Failure Report & Corrective Actions

It is required to notify about any failure or non-conformance occurring in the TOE, and to define and implement corrective actions in order to fix the issue and prevent its re-occurrence.

5.2.11 Security Change Management

It is required to govern and control the changes required to the TOE.

5.2.12 Information/Material Protection Management

It is required to securely classify, identify, manage, store, handle, pack and deliver the:

- Assets under hard document format, under hard copy format.
- Product samples.
- Emulator.
- Simulator.

5.2.13 Scrap Management

It is required that a “Scrap Management” procedure exists for the product samples (wafer samples, packaged samples), for the Test Program and Evaluation Program – both under “Hard Copy” format - and for the Hard Document of smartcard confidential information.

5.3 TOE Environment Security Requirements

This paragraph defines statement of security requirements for the Environment of the TOE.

5.3.1 Individual Non Disclosure Agreement

Each employee working in operations related to the TOE, used to design the smartcard microcontroller components, has in advance signed a Non Disclosure Agreement (Individual NDA).

5.3.2 New Employee Enrolment

Each new employee before working in operations related to the TOE, used to design the smartcard microcontroller components, has in advance followed the process used to enlist such new personnel.

5.3.3 Security Employee Separation

Each employee when under resignation status and who was working in operations related to the TOE, used to design the smartcard microcontroller components is compliant with the smartcard employee separation process.

5.3.4 Individual Identification and Authentication

Each employee, working in operations related to the TOE, used to design the smartcard microcontroller components, is individually identified and authenticated to give or deny access to smartcard controlled areas, storage shelves, files, evaluation program, test program, evaluation results and customer data, when applicable.

5.3.5 Access Control Management

It is required to have implemented the access rights and rules in order to control access and give access only to authorized personnel to areas where the TOE is taking place, and to the "SmartCard IC Development Information System".

5.3.6 Passwords Management

It is required to securely create, control and manage all the passwords used to control the access to the areas where the TOE is taking place and to the "SmartCard IC Development Information System".

5.3.7 Security Failure Report & Corrective Actions

It is required to notify about any failure or non-conformance occurring in the TOE Environment, and to define and implement corrective actions in order to fix the issue and prevent its re-occurrence.

5.3.8 Security Change Management

It is required to govern and control the changes required to the TOE Environment.

5.3.9 Secure "SmartCard IC Development Information System"

It is required that the "SmartCard IC Development Information System" provides protection to the TOE Information Technology, against any external attack or intrusion.

5.3.10 Secure Delivery and Verification

It is required to have implemented secure and trustable delivery of computerized and non-computerized information and data, and to verify that no mal-function occurred during the delivery process.

5.3.11 Photomasks Ordering

It is required that ordering of photomasks to maskshop (“photomasks maker”) is ensuring secure identification, traceability and is following ordering security rules to detect or prevent potential theft.

5.3.12 Subcontractor Approval

It is required to have implemented a procedure for approving a subcontractor whose activity will be related to the TOE, to the “SmartCard IC Development Information System” and to the assets, prior to this activity is started.

5.3.13 Subcontractor Management

It is required to have implemented a procedure for the management of a subcontractor whose activity is related to the TOE, to the “SmartCard IC Development Information System” and to the assets, after this subcontractor has been approved.

5.3.14 Security Check and Security

It is required to have implemented procedures, rules and usage methods to be applied within the TOE, in the “field of security”, in order to guarantee that the TOE and its Environment are operated in a “secure way”.

Chapter 6

6. TOE Summary Specification

6.1 Statement of TOE Security Functions

<u>Editorial Note:</u>

SF2 and SF8 Security Functions are not represented security functions.

6.1.1 SF1: Login

The “Unix” **Login** security function requires administrator and users to enter, first the Login Name and second the password, before any action is allowed by “Unix” operating system to administrator and users.

6.1.2 SF3: Attribute Manager

The “Unix” **Attribute Manager** security function are tables embedded into the operating system used to maintain the list of attributes belonging to users in order to operate the “Unix” operating system.

6.1.3 SF4: Admin

The “Unix” **Admin** security function is capable to associate roles to users and to manage the users role (administrator and user) based on the information provided by the **Login** security function.

6.1.4 SF5: File/Command Property

Embedded in the low level layers of “Unix” operating system, the **File/Command Property** security function associates property of file and/or command to the user (administrator or user) which was previously identified and authenticated.

6.1.5 SF6: File Configuration

The **File Configuration** security function of “Unix” is enforcing that any operation run by the administrator or the users is executed as a file with the attributes associated to the administrator or users.

6.1.6 SF7: Rights Manager

The **Rights Manager** security function of the “Unix” operating system is enforcing the management of rights for administrator and/or users depending on the identification and authentication previously made during the **Login** security function.

6.1.7 SF9: Logon

The “Windows” **Logon** security function requires administrator and users to enter, first the User Identifier and second the Password, before any action is allowed by “Windows” operating system to administrator and users.

6.1.8 SF10: Security Identifier (SID)

The “Windows” **SID** security function are tables embedded into the operating system used to maintain the list of attributes belonging to users in order to securely operate both the “Windows” operating system and its associated applications.

6.1.9 SF11: User Account Manager

The “Windows” **User Account Manager** security function is capable to associate roles to users and to manage the users role (administrator and user) based on the information provided by the **Logon** security function.

6.1.10 SF12: Owner

Embedded in the low level layers of “Windows” operating system, the **Owner** security function associates property of file and/or command to the user (administrator or user) which was previously identified and authenticated.

6.1.11 SF13: Security Account Manager (SAM)

The **SAM** security function of the “Windows” operating system is enforcing the management of rights for administrator and/or users depending on the identification and authentication previously made during the **Logon** security function.

6.1.12 SF14: Logon

The “Windows” **Logon** security function requires administrator and users to enter, first the User Identifier and second the Password, before any action is allowed by “Windows” operating system to administrator and users.

6.1.13 SF15: Security Identifier (SID)

The “Windows” **SID** security function are tables embedded into the operating system used to maintain the list of attributes belonging to users in order to securely operate both the “Windows” operating system and its associated applications.

6.1.14 SF16: User Account Manager

The “Windows” **User Account Manager** security function is capable to associate roles to users and to manage the users role (administrator and user) based on the information provided by the **Logon** security function.

6.1.15 SF17: Owner

Embedded in the low level layers of “Windows” operating system, the **Owner** security function associates property of file and/or command to the user (administrator or user) which was previously identified and authenticated.

6.1.16 SF18: Security Account Manager (SAM)

The **SAM** security function of the “Windows” operating system is enforcing the management of rights for administrator and/or users depending on the identification and authentication previously made during the **Logon** security function.

Table of Statement of TOE Security Functions

		TOE Security Functional Requirements							
		FIA_UID.2	FIA_UAU.2	FIA_ATD.1	FMT_SMR.1	FDP_ACC.2	FDP_ACF.1	FMT_MSA.1	FMT_MOF.1
TOE Security Functions	SF1	X	X		X	X	X	X	X
	SF3	X	X	X	X	X	X	X	X
	SF4				X	X	X	X	X
	SF5					X	X	X	X
	SF6							X	X
	SF7					X	X	X	X
	SF9	X	X		X	X	X	X	X
	SF10	X	X	X	X	X	X	X	X
	SF11				X	X	X	X	X
	SF12					X	X	X	X
	SF13					X	X	X	X
	SF14	X	X		X	X	X	X	X
	SF15	X	X	X	X	X	X	X	X
	SF16				X	X	X	X	X
	SF17					X	X	X	X
	SF18					X	X	X	X

6.2 Statement of TOE Assurance Measures (from CC part 3)

6.2.1 Assurance Measures to Version Numbers

Dependencies: No dependencies.

Developer action elements:

- ACM_CAP.1.1D: Security Target Statement (**ST Statement**). The TOE is referenced as being the “SmartCard IC Development Flow - Japan” taking place in the “SmartCard IC Development Section” - Japan. The present version of this development flow is 1.0.

Content and presentation of evidence elements:

- ACM_CAP.1.1C: The reference for the TOE is unique. Here applied to the “SmartCard IC Development Flow - Japan” identified and configuration managed (version number) by:
    - “Reference and Version Number to the “SmartCard IC Development Flow - Japan” – ACM_CAP.1” Manual – (**AM 1**).

- ACM_CAP.1.2C: The TOE is labeled, identified with the reference “SmartCard IC Development Flow - Japan”:
    - “Reference and Version Number to the “SmartCard IC Development Flow - Japan” – ACM_CAP.1” Manual – (**AM 1**).

6.2.2 Assurance Measures to Installation, Generation and Start-up

Dependencies: AGD_ADM.1 Administrator Guidance. Dependency is satisfied.

Developer action elements:

- ADO_IGS.1.1D: The procedures necessary to the secure installation, generation and start-up of the TOE are:

    - OS Install Procedure for [Unix] – (**AM 2**).

    - OS Installation Procedure for [Windows/Server] – (**AM 3**).

    - OS Installation Procedure for [Windows/Client] – (**AM4**).

Content and presentation of evidence elements:

- ADO_IGS.1.1C: The documentation, as explained above, describes the steps necessary for a secure installation, generation and start-up of the TOE IT.

6.2.3 Assurance Measure to Informal Specification

Dependencies: ADV_RCR.1 Informal Correspondence Demonstration. Dependency is satisfied.

Developer action elements:

- ADV_FSP.1.1D: The functional specifications are:

    - Functional Specification “Unix” Network – (**AM 5**).
    - “Windows” Functional Specification – (**AM 6** & **AM 7**).

Content and presentation of evidence elements:

- ADV_FSP.1.1C: The functional specifications describe the TOE security functions and its external interfaces using an informal style.
- ADV_FSP.1.2C: The functional specifications are internally consistent.
- ADV_FSP.1.3C: The functional specifications describe the purpose and method of use of all external TOE security functions interfaces, providing details of effects, exceptions and error message, as appropriate.
- ADV_FSP.1.4C: The functional specifications completely represent the TOE security functions.

6.2.4 Assurance Measure to Representation Correspondence

A representation correspondence exists for the pair "Security Target – Functional Specification".

Dependencies: No dependencies.

Developer action elements:

- ADV_RCR.1.1D: The analysis of correspondence between the adjacent pair "Security Target – Functional Specification" is described in:

  - "Representation Correspondence Unix Network" Manual – (**AM 8**).
  - "Windows " Representation Correspondence – (**AM 9** & **AM 10**).

Content and presentation of evidence elements:

- ADV_RCR.1.1C: For the "Security Target – Functional Specification" pair of provided TOE security functions representations, the analysis demonstrates that all relevant security functionality of the more abstract TOE security functions representation is correctly and completely refined in the less abstract TOE security functions representation.

Evaluator action elements:

- ADV_RCR.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.5 Assurance Measures to Administrator Guidance

Dependencies: ADV_FSP.1 Informal Functional Specification. Dependency is satisfied.

Developer action elements:

- AGD_ADM.1.1D: Administrator guidance, addressed to system administrative personnel, is:

  - Daily Management Procedure for [Unix] – (**AM 16**).
  - Administration Guidance for [Windows] – (**AM 17** & **AM 18**).

Content and presentation of evidence elements:

- AGD_ADM.1.1C: The administrator guidance describes the administrative functions and interfaces available to the administrator of the TOE.
- AGD_ADM.1.2C: The administrator guidance describes how to administer the TOE in a secure manner.
- AGD_ADM.1.3C: The administrator guidance contains warnings about functions and privileges that should be controlled in a secure processing environment.
- AGD_ADM.1.4C: The administrator guidance describes all assumptions regarding user behavior that are relevant to secure operation of the TOE.
- AGD_ADM.1.5C: The administrator guidance describes all security parameters under the control of the administrator, indicating secure values as appropriate.
- AGD_ADM.1.6C: The administrator guidance describes each type of security relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TOE security functions.
- AGD_ADM.1.7C: The administrator guidance is consistent with all other documentation supplied for evaluation.
- AGD_ADM.1.8C: The administrator guidance describes all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

- AGD_ADM.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.6 Assurance Measures to User Guidance

Dependencies: ADV_FSP.1 Informal Functional Specification. Dependency is satisfied.

Developer action elements:

- AGD_USR.1.1D: User guidance is:

  - Using Users Environment Procedure [for Unix] – (**AM 11**).
  - User Guidance for [Windows] is as per the generic information delivered with the software by the software manufacturer (**AM19**).
  - User Environment Guidance [for Windows]– (**AM 12**).

Content and presentation of evidence elements:

- AGD_USR.1.1C: The user guidance describes the functions and interfaces available to the non-administrative user of the TOE.
- AGD_USR.1.2C: The user guidance describes the use of user-accessible security functions provided by the TOE.
- AGD_USR.1.3C: The user guidance contains warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
- AGD_USR.1.4C: The user guidance clearly presents all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

- AGD_USR.1.5C: The user guidance is consistent with all other documentation supplied for evaluation.
- AGD_USR.1.6C: The user guidance describes all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

- AGD_USR.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.7 Assurance Measure to Independent Testing – Conformance

Dependencies: ADV_FSP.1 Informal Functional Specification.
AGD_ADM.1 Administrator Guidance.
AGD_USR.1 User Guidance.

Dependencies are satisfied.

Developer action elements: **ST Statement:**

- ATE_IND.1.1D: The TOE is made available for testing.

Content and presentation of evidence elements: **ST Statement:**

- ATE_IND.1.1C: The TOE is made suitable for testing

Evaluator action elements:

- ATE_IND.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- ATE_IND.1.2E: The evaluator

shall test a subset of the TOE security functions as appropriate to confirm that the TOE operates as specified.

6.2.8 Assurance Measure to Independent Vulnerability Analysis

Dependencies: ADV_FSP.1 Informal Functional Specification. Dependency is satisfied.

ADV_HLD.2 Security Enforcing High-Level Design.
ADV_IMP.1 Subset of the Implementation of the TSF.

ADV_LLD.1 Descriptive Low-Level Design.

AGD_ADM.1 Administrator Guidance. Dependency is satisfied.

AGD_USR.1 User Guidance. Dependency is satisfied.

Developer action elements:

- AVA_VLA.2.1D: Performed and documented analysis, searching for ways in which a user can violate the TOE security policy, is within the below deliverables.
- AVA_VLA.2.2D: Documented disposition of identified vulnerabilities is within the below deliverables:

  - "Vulnerability Analysis Unix Network" Smartcard Manual **–** (**AM 13**).
  - "Vulnerability Analysis Windows Network" **–** (**AM 14** & **AM 15**).

Content and presentation of evidence elements:

- AVA_VLA.2.1C: The documentation shows, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.
- AVA_VLA.2.2C: The documentation justifies that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

Table of Statement of TOE Assurance Measures:

		EAL1+ Security Assurance Requirements							
		ACM_CAP.1	**ADO_IGS.1**	**ADV_FSP.1**	**ADV_RCR.1**	**AGD_ADM.1**	**AGD_USR.1**	**ATE_IND.1**	**AVA_VLA.2**
TOE	**ST S***	**X**						**X**	
	AM1	**X**							
	AM2		**X**						
	AM3		**X**						
	AM4		**X**						

	AM5			X					
	AM6			X					
	AM7			X					
	AM8				X				
	AM9				X				
	AM10				X				
	AM11						X		
	AM12						X		
	AM13								X
	AM14								X
	AM15								X
	AM16					X			
	AM17					X			
	AM18					X			
	AM19						X		

* ST Statement

6.3 Statement of Non-IT Security Measures for the TOE

The Non-IT Security Measures for the TOE are specified with procedures. These procedures are detailed into manuals, specifications and SOP' s (Security Operating Policy).
The applicable manuals, specifications and SOP' s are listed, with their reference number and revision number, inside the below "list" sections. The reference number in bold represents the "chore" manual or specification or SOP, that is dedicated to the related security measure.

6.3.1 Secure Storage Procedure

Smartcard Manuals and specifications exist to define the procedure to be used for the secure storage of:

- "Non-Computerized " Assets:
  - Assets under hard document format, under hard copy format.
  - Product samples.
  - Emulator.
  - Simulator.
- "Computerized " Assets:
  - Electronic Files.

6.3.2 Material Asset Identification Procedure

Smartcard Manuals and specifications exist to define the procedure for the unique identification (reference and version number) for "Non-Computerized" Assets:

- Assets under hard document format, under hard copy format.
- Product samples.
- Emulator.

- Simulator.

6.3.3 Non Permanence Procedure

Smartcard Manual exists, requiring:

. That the test program and that the evaluation program are not resident on the test equipment and are electrically erased after the completion of:

- Development operation for evaluation program.
- Development operation for test program.
- Evaluation operation of product samples for evaluation program.

. That the evaluation results are not resident on pieces of equipment used for evaluation purpose and are erased after the completion of the evaluation operation.

6.3.4 End of Life Procedure

Smartcard Manuals exist, requiring “end of life” rules to be applied for the hard copy of evaluation program and for the test program, and for the files under an electronic format (Electronic Files).

6.3.5 Transfer of Test Program – Hand-Carry – Secure Delivery Procedure

Smartcard Manual exists, requiring hand-carry transportation of the test program to the site used for test production.

6.3.6 Data Back-up Procedure

Smartcard Manual exists, requiring data back-up for the evaluation results.

6.3.7 Material Asset Configuration Management Procedure

Smartcard Manuals and specification exist, requiring the control of the identification and the management of configuration for:

- Assets under hard document format, under hard copy format.
- Product samples.
- Emulator.
- Simulator.

And to control any change that may be applied to them.

6.3.8 Access Control Management Procedure

Smartcard Manuals and specification exist, requiring the implementation of access rights and rules in order to control the access and give access only to authorized personnel to the TOE, to its associated pieces of equipment (computers, locked shelves, safes,…), to the assets.

6.3.9 Passwords Management Procedure

Smartcard Manual and specifications exist, requiring to securely create, control and manage all the passwords used for controlling the access to the TOE, to its associated pieces of equipment (examples: computers, locked shelves, safes,…), to the assets.

6.3.10 Security Failure Report & Corrective Actions Procedure

Security Operating Policy and specification exist, requiring notification about any failure or non-conformance occurring in the TOE, and asking to define and to implement corrective actions in order to fix the issue and prevent its re-occurrence.

6.3.11 Security Change Management Procedure

Security Operating Policy and specification exist, requiring to govern and control the changes to be applied to the TOE.

6.3.12 Information/Material Protection Management Procedure

Smartcard Manual and specifications exist, requiring to securely classify, identify, manage, store, handle, pack and deliver the:

- Assets under hard document format, under hard copy format.
- Product samples.
- Emulator.
- Simulator.

6.3.13 Scrap Management Procedure

Smartcard Manuals and specification exist, requiring scrap management for the product samples (wafer samples, packaged samples), for the Test Program and the Evaluation Program – both under “Hard Copy” format - and for the Hard Document of smartcard confidential information.

6.4 Statement of Security Measures for the Environment

The Security Measures for the TOE Environment are specified with procedures. These procedures are detailed into manuals, specifications and SOP’ s (Security Operating Policy). The applicable manuals, specifications and SOP’ s are listed, with their reference number and revision number, inside the below “list” sections. The reference number in bold represents the “chore” manual or specification or SOP, that is dedicated to the related security measure.

6.4.1 Individual Non Disclosure Agreement Procedure

Smartcard Manual exists, requiring that every employee working in operations related to the TOE, used to develop the smartcard microcontroller components, has in advance signed a Non Disclosure Agreement (Individual NDA).

6.4.2 New Employee Enrolment Procedure

Smartcard Manual exists, requiring that every new employee, before working in operations related to the TOE, used to develop the smartcard microcontroller components, has in advance followed the process used to enlist such new personnel.

6.4.3 Security Employee Separation Procedure

Smartcard Manual and specification exist, requiring that every employee, when under resignation, transfer or retirement status and who was working in operations related to the TOE, used to develop the smartcard microcontroller components is compliant with the smartcard employee separation process.

6.4.4 Individual Identification and Authentication Procedure

Smartcard Manual exists, requiring that each employee working in operations related to the TOE, used to design the smartcard microcontroller components, is individually identified and authenticated to give or deny access to smartcard controlled areas, storage shelves, files, evaluation program, test program, evaluation results and customer data, when applicable.

6.4.5 Access Control Management Procedure

Smartcard Manual and specification exist, requiring that access rights and rules are implemented in order to control access and give access only to authorized personnel to areas where the TOE is taking place (Security Room and Tester Room), and to the "SmartCard IC Development Information System".

6.4.6 Passwords Management Procedure

Specification exists, requiring secure creation, control and management of all the passwords used to access to the areas where the TOE is taking place (Security Room and Tester Room), and to the "SmartCard IC Development Information System".

6.4.7 Security Failure Report & Corrective Actions Procedure

Security Operating Policy and specification exist, requiring notification about any occurring failure or non-conformance in the TOE Environment, and requiring definition and implementation of corrective actions in order to fix the issue and prevent re-occurrence.

6.4.8 Security Change Management Procedure

Security Operating Policy and specification exist, requiring to govern and control the changes to be applied to the Environment of the TOE.

6.4.9 Secure Smartcard IC Development Information System Procedure

Security Measures, within the "SmartCard IC Development Information System" exist to provide protection, against external attack or intrusion, to the TOE Information Technology.

6.4.10 Secure Delivery and Verification Procedure

Smartcard Manuals, specification and measure exist, requiring the implementation and the usage of secure and trustable delivery procedures for computerized and non- computerized information and data, and the verification that no mal-function occurred during the delivery process.

6.4.11 Photomasks Ordering Procedure

Smartcard Manual exists, requiring implementation of rules to order new photomasks to maskshop, also ensuring a secure identification traceability and delivery of photomasks, in order to prevent potential theft or at least to detect theft.

6.4.12 Subcontractor Approval Procedure

Smartcard Manual exists for approving a subcontractor whose activity will be related to the TOE or to the assets and prior to this activity is started.

6.4.13 Subcontractor Management Procedure

Smartcard Manual exists for managing, after approval, a subcontractor whose activity is related to the TOE or to the assets.

6.4.14 Security Check and Security Procedure

Specifications exist defining all the procedures and rules that are applicable to the "SmartCard IC Development Section", in the "field of security", in order to guarantee that the TOE and its Environment are operated in a "secure way". This is starting with the definition of the Security Organization, and followed by the Education Process to employees on security, by security checks and usage methods to send offsite the pieces of Information System equipment for repair, to use dedicated security related pieces of equipment and material.

Chapter 7

7. PP Claims

No specific PP claims are made for this Security Target.

However, in order to satisfy any future Evaluation/Certification of NEC product claiming for conformance to PP/9806 Version 2.0, the present Security Target is made fully compliant to all the requirements from PP/9806 involving the Environment of product under development. This Environment for development phase (phase 2), described in PP/9806, corresponds to the TOE of this Security Target.

The compliance and coverage of the present Security Target to the requirements of PP/9806 are explained in the section of the Security Target chapters entitled “Conformance to PP/9806 phase 2 (IC Development Phase)”.

Definitions & Acronyms:

IT: Information Technology
OSP: Organizational Security Policy
SCAC: SmartCard Application Center
SOP: Security Operating Policy
ST: Security Target
TOE: Target of Evaluation