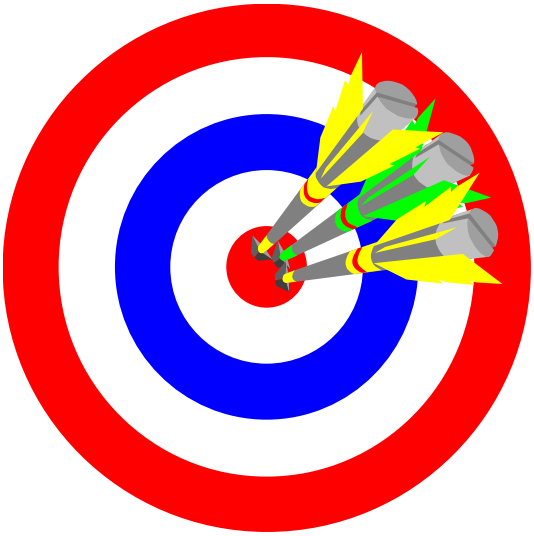
NEC

SmartCard

Application Center

PUBLIC SECURITY TARGET

NEC WAFER PRODUCTION -



JAPAN

NEC SmartCard Application Center

Version 1.0 Issue 13 May 2001

PUBLIC SECURITY TARGET			
Version Number	**Comments/Modifications**	**Prepared by/Signature**	**Date**
V 1.0	Original.	Le Bihan J.	13 May 01

Table of contents

Chapter 1

1. Security Target Introduction

1.1 ST Identification

Title: Public Security Target for NEC Wafer Production - Japan.
Version number: V1.0, issue May 2001.

This Public Security Target (ST) has been built with Common Criteria Version 2.1. It is a summary from the NEC Proprietary Security Target developed by NEC in the frame, and for the certification of a Wafer Production Line located in Japan.

Author of this ST was: IT & Project Security Manager of NEC SmartCard Application Center.

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

This ST is referring to the environment of production used in a NEC plant located in Japan to produce silicon wafers of microcontroller components dedicated to smartcard applications. This environment of production encompasses the “Production Flow”, that is the TOE, the associated “Information Technology” and the “Physical Environment” in which the TOE is operated.

The TOE (“Production Flow”) is identified with a dedicated name. Within this dedicated name, a number is used as a version number of this “Production Flow”. This number is incremented when a change in the “Production Flow” occurs.

1.2 ST Overview

1.2.1 General

This ST was conducted under the French IT Security Evaluation and Certification Scheme, managed by DCSSI, and with the AQL – Silicomp Group company, as the ITSEF.
This ST is, within NEC, the result of the work of a group composed of several departments from the plant where this “Production Flow” is taking place, such as:

- Manufacturing (Wafer Fabrication and Wafer Sort),
- Quality,
- Information System,
- Facilities,
- Administration,
- Planning,
- Process Engineering,
- Assembly & Test Engineering,

and with the help and sponsoring from the Security Organization in NEC SmartCard Application Center.

This ST was developed in the frame of the Common Criteria Evaluation and Certification of a “Production Flow”, with its associated “Information Technology” and “Environment”, used to produce the semiconductor components, which in this case are the micro-controller components, to be served on the worldwide integrated circuits market for the smartcard business.

Evaluation and Certification were run in order to demonstrate and to offer guarantee to NEC’ s customers and/or potential customers, in the level of security in place. In addition, a forecasted continuous improvement methodology will maintain the security level of this “Production Flow” at the state of the art level of the industry. A continuous improvement methodology will be supported by the implementation of a “Certification Maintenance Program”. This “Certification Maintenance Program” will include the security components from the “AMA” class (Maintenance of Assurance).

1.2.2 Need for Security

A smartcard (contact or contact-less smartcard or a combination of both) is usually seen as a credit card sized card having a non-volatile memory and a processing unit (microcontroller) embedded within it.

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.

The integrity and the confidentiality are built during the development phase of the product and then consolidated during its production phase. This production phase is used to transform, by the means of ultra microscopic metallurgy processes, raw silicon wafers into finished silicon chips, also named integrated circuits (microcontroller components). In the case of this present ST, the production phase is involving the “Production Flow” and its associated “Information Technology”, plus the “Environment” in which this “Production Flow” and “Information Technology” are operated.

Therefore, it became relevant that the “Production Flow”, its “Environment”, and the “Information Technology” are able to maintain their own integrity and confidentiality in order to ensure the protection of the above described elements.

The integrated circuit resulting from the production flow is a single chip security microcontroller based on the NEC submicron technology using the NEC 8 bit CISC and 32 bit RISC CPU cores, and including on-chip memories (EEPROM, RAM, ROM) of different size depending on the product version. These microcontrollers are used to be commercially known under 2 families:

8 bit Family:

µPD7898XX

32 bit Family:

µPD7039XX

These integrated circuits will be then mounted onto a smartcard frame to finally become the smartcard that everyone knows and that everyone is more and more often using in his day to day life for banking, transportation, portable phone, etc…

1.2.3 Certification Process

The intent of this ST is to specify the functional and assurance requirements applicable to the "Production Flow" used in the manufacturing, the testing and packing operations of the microcontroller components.

This 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 production phase.
- 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 the continuous improvement plan and "Maintenance Program" of the certification, any other product could be added in future to the list of these commercial names without any in depth change to security and to this ST, as soon as the added product is resulting from the same "Production Flow" and is belonging to one of the 2 product families previously listed.

1.3 Common Criteria Conformance Claim

The conformance claimed for this Security Target is:

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

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

- AVA_VLA.2 "Independent vulnerability analysis".

1.4 Control of "Security Target" Document

This Security Target is used by NEC and is a description of the in place security rules.

This ST Document is owned by NEC and is controlled by the NEC Smartcard Application Center (SCAC). This ST is being provided by NEC to the industry as an help, therefore NEC will not be responsible for any change that may be made to this document without its approval or not made by NEC itself.

Chapter 2

2. TOE Description

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

The security strategy defined by NEC SCAC Security Management was expecting, from this Evaluation/Certification process, the implementation of the basic security requirements, rules and practices for the **"Production Flow"**, its **"Information Technology"**, its **"Environment"** used to produce the microcontroller wafers dedicated to smartcard applications.

That is to say that the security emphasis will be stressed to this **"Production Flow"**, the TOE, to the Information Technology and to the environment of the TOE. However for consistency into the stated security strategy, and in order to achieve the protection of all the assets that have been identified, it is also asked that the TOE itself realize those of the necessary security measures that are required to it.
It was also foreseen that the "Production Flow" could be part of a smartcard product security Evaluation/Certification, performed in accordance with PP/9806 Version 2.0 and its claimed Evaluation Assurance Level (EAL4 augmented). Therefore, the present ST is taking into account the security requirements from PP/9806 Version 2.0 that the production environment needs to be compliant with. This is explained in the following content of the ST, by the chapters: "Conformance to PP/9806 Version 2.0 Phase 3 (Manufacturing Phase)".

However, the conformance to the EAL4 augmented assurance components, related to the production environment, of a PP/9806 Version 2.0 conformant evaluated product, are going to be covered during the "Maintenance Program" of the present certification.

As a summary this Security Target is covering the "Development Security" and the "Delivery" aspects.
"Configuration Management" aspects, for conformance to the EAL4, will be covered during the "Maintenance Program" of the present certification.

2.1.3 TOE Definition Statement

The TOE is the "**Production Flow**" used to manufacture, to test, to pack and to ship the microcontroller components to a logistic die-bank.

N.B: The above mentioned logistic die-bank is not under the responsibility and the control of Yamaguchi plant. Therefore the die-bank is out of the scope of this ST.

The usual production unit sent through the "Production Flow" is a wafer lot.

The "Production Flow" is encompassing three different flows:

- A "Product Manufacturing Flow", where the production unit is physically moved from one manufacturing step to the next one. This could be summarized, for the purpose of this ST, to the physical handling of the material all along the production steps in order to manufacture the product.
  Computerized operations are run in parallel to the sequential order of these

production steps. They are used for the computerized management of the production (Computer Aided Production Management) and are defined as performing the traceability of the production unit through the "Product Manufacturing Flow". The link between the computerized management of the production and the physical handling of the material (production unit) all along the production steps, is made by the wafer lot number which is the production unit identification number.

- A "Photomasks Flow" used to provide to the "Product Manufacturing Flow" the adequate product photomasks in order the photolithography operations of the numerous product layers, as per the component design and lay-out, can take place.
- A "Test Program Flow" used to provide to the "Product Manufacturing Flow" the adequate material to correctly perform the electrical test of each wafer of the lots in accordance with the targeted device electrical and security characteristics. This electrical test is sorting-out the dice that are not compliant to these characteristics. Those non-conformant dice (rejected dice) are marked, for visual identification, with a colored ink dot on their top face.

2.1.3.1 "Product Manufacturing Flow"

During the production operations, the ultra microscopic metallurgy processes will give to each dice of the wafers their electrical characteristics and build their security functions and behavior.

In the last operation of the manufacturing of wafers, each dice is electrically tested and sorted. At that time some security functions of the component may be activated and some customer data can be also entered into the memories of the component. After this electrical test, the wafers are packed and shipped to a die-bank.

This "Product Manufacturing Flow" is following the manufacturing steps as described within the chapter 2.2.1 of this ST.

In order to be operational and to ensure its production function, the "Product Manufacturing Flow" is using material as described hereafter:

- The production unit (or wafer lot) gathering the wafers (also named product). The manufacturing process operations are changing these wafers from raw wafers to finish good which are the wafers ready to be delivered to the customers.

- Equipment used to perform the manufacturing operations that are required to transform the wafers from raw material to end product and to test and pack them for shipment.
- Test tools (probe card, test board) are tools used to test the wafers.
- "On-line computer terminals" used to enable the acquisition of wafer lot identification data and production data.
- "Local host computer" used to store the results from electrical test of the wafers.
- Information Technology used to ensure data acquisition, traceability and management of wafer production. At first step of the flow, a wafer lot is created into the computerized system for production management and this wafer lot is identified with a unique identification number. This number, that is also physically printed on wafer lot labeling, will be used to track the wafer lot all along the flow in order to ensure its traceability.

2.1.3.2 "Photomasks Flow"

To be operational and to ensure the production function of the "Product Manufacturing Flow", it is required that the pieces of equipment involved in the manufacturing operations are well supplied with the photomasks. These photomasks are managed by the "Photomasks Flow".

The "Photomasks Flow" is following the steps as described within the chapter 2.2.2 of this ST.

To ensure its function, this "Photomasks Flow" is using material as described hereafter:

- Photomasks (or reticles) are used during the photolithography operations to print on the wafers the required patterns to give its electrical structure to each die of the wafers.

2.1.3.3 "Test Programs Flow"

To be operational and to ensure the production function of the "Product Manufacturing Flow", it is required that the pieces of equipment involved in the test operations are well supplied with the product test programs. The test programs are managed by the "Test Programs Flow".

The "Test Programs Flow" is following the steps as described within the chapter 2.2.3 of this ST.

To ensure its function, this "Test Programs Flow" is using material as described hereafter:

- Test program is used to perform the electrical sorting of the wafers and to reject dice not meeting the electrical specification targeted for the device by inking the rejected dice.

2.2 Phases of the TOE

2.2.1 TOE "Product Manufacturing Flow"

This flow, as shown hereafter, is composed of sequential operations (noted from 1 to 6).

While the packing operation of the wafer lots is the last step in the "Product Manufacturing Flow", it can be considered that the last operation in the construction of the smartcard product is taking place during the wafer testing. All during the "Product Manufacturing Flow" the key data controlled by the TOE has been the product traceability, but when at the end of the construction, like with the wafer testing, another key data is occurring. This data is the results from the electrical test of the wafers.

The physical and logical change from one production step to the next one is under the control of the TOE.

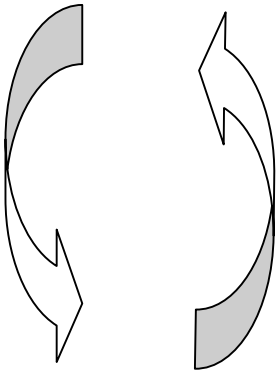
1- Lot preparation	The wafer lot is receiving a unique identification number. Lot traveler sheet is generated and data is entered into the production control computer system. Traceability is generated.
2- Oxidation	The silicon wafer is processed in a high temperature oxygen atmosphere to form a silicon dioxide (SiO2) film on the wafer.
2.1- Deposition	With gas reaction at high temperature, a silicon film is grown-up.
2.2- Photolithography	Photoresist is applied on the silicon wafer & the required pattern is printed on the wafer through a glass mask.
2.3- Ion Implantation	Impurities are ionized & implanted selectively into silicon while being accelerated by use of a strong electric field.
2.4- Deposition	An insulation film (SiO2) is grown-up.
2.5- Metalization	Wafer is sputtered by a metal film. Then the circuit is printed on the wafer through the photolithography.
3- Glassivation	Wafer is protected by a glass film.
4- Back Grinding	Wafers thickness is put at the required value.
5- Wafer Testing	Each wafer & each dice are electrically tested (wafer sorting). Rejected dice are inked. Some security functions are triggered. Customer data can be entered into the device memory. Output data: Test results.
6- Wafer Pack/Ship	Wafer lot is prepared & shipped to a wafer stock.

2.2.2 TOE "Photomasks Flow"

This flow, as shown hereafter, is composed of sequential operations (noted from 1 to 4).

The photomasks are used into the sequences numbered 2, 2.1, 2.2, 2.3, 2.4, 2.5 and 3 of the "Product Manufacturing Flow", previously shown.

The arrows are showing the loop that exists in the usage of the photomasks within this "Photomasks Flow".
The physical change from one step to the next one is under the control of the TOE.

1- Receipt from Photomask Owner	The photomasks are received by production line. They are identified and entered in a data-base for management and traceability.
2- Secure Storage	When not in use the photomasks are securely stored.
	
3- In Use	Photomasks are in use at wafer manufacturing equipment. When operation is completed, photomasks are back to secure Storage.
4- End of Life/Return to Owner	When arrived at their end of life, photomasks are returned to their owner.

2.2.3 TOE "Test Programs Flow"

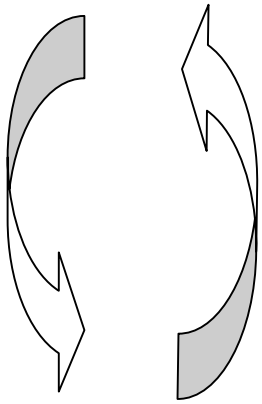
This flow, as shown hereafter, is composed of sequential operations (noted from 1 to 5).

The test programs are used into the sequence numbered 5 of the "Product Manufacturing Flow", previously shown.

The arrows are showing the loop that exists in the usage of a test program within this "Test Programs Flow".

The physical change from one step to the next one is under the control of the TOE.

1- Receipt from Test Program Owner	The test program is received by production line. It is identified and entered in a data-base for management and traceability.
2- Secure Storage of Test Program	When not in use the test program is securely stored.
3- Loading of Test Program on Test equipment	Test program is loaded into the test equipment.
4- Return of Test Program in Secure Storage	Test program is back to secure storage after loading and before test operation of wafer lot is started.
5- End of Life/Return to Owner	When arrived at their end of life, test program is returned to the owner.



2.3 Boundaries of the TOE

The TOE, as the "Production Flow", is including:

- The "Product Manufacturing Flow".
- The "Photomasks Flow".
- The "Test Program Flow".
- The pieces of equipment used for the manufacturing and testing operations.
- Photomasks.
- Test programs.

- Test tools (probe card, test board) used for the testing operation.
- "On-line computer terminals", that are located inside the Wafer Fabrication area and inside the Wafer Sort area, used for acquisition of wafer lot identification data and production data.
- The UNIX server (host computer).
- "Local host computer" used for storage of test results and the tester control console.
- Test results.
- The Information Technology of the "Product Manufacturing Flow" that includes:
  - ➔ A server application, of production management software, operated on the UNIX server under the "HP-UX" operating system.
  - ➔ A client application, of "Production Management Software", operated on the "On-line computer terminals" under Windows NT operating system.
  - ➔ Windows NT operating system operated on the "Local host computer" and on the "Tester Control Console".

Any other element to the above listed is considered to be out of the TOE and therefore is part of the environment of the TOE.

2.4 Environment of the TOE

Considering the TOE, the below elements are viewed as the environment for the TOE:

- The physical areas where the TOE is located.
- The site Information System features, other than those listed and described inside the paragraph 2.3 and the paragraph 2.5 of this ST.
- The personnel.

2.4.1 Physical Areas

Physical Areas are:

- The site itself.
- The areas where the TOE is located and operated in order a secure manufacturing, testing and packing of wafer lots can be achieved and a secure usage of photomasks and test program can be carried out.

2.4.2 Site Information System

The Information System of such site is huge and its main roles are to ensure the correct operations in manufacturing, stock control, finance and accountability, documentation, electronic mail, data-bases, personnel management, access to networks,... The Information System is using several software applications to run the above listed roles.

Such software applications, used to perform the above listed roles, are considered to be part of the environment of the TOE.

For a deeper description of the Information Technology of the TOE (IT), please refer to the paragraph 2.3 and to the paragraph 2.5 of this ST.

2.4.3 Personnel

The personnel are the people employed and/or contracted. It is required to this personnel to have the right skills and knowledge to be able to correctly perform the operations of the plant, that means in accordance with the objectives of the company and in accordance with the policies and procedures defining the rules to be executed in order to run the job accordingly.

The personnel working in the operations involving the microcontroller components dedicated to smartcard applications (the TOE), is also asked to meet the additional specific policies required by this domain of application. These policies are those which are later reported into the chapters of this ST.

2.5 General IT Features of the TOE

Among the TOE, the Information Technology (IT) is concerning the “Product Manufacturing Flow” and the “Test Program Flow”:

The “Photomasks Flow” is irrelevant to the IT features of the TOE.

The Information Technology of the TOE is made of:

- A “HP-UX” Unix server and of a server application, run for the “Production Management Software”, operated by the “HP-UX” Operating System. The production management software is used to control the manufacturing operations and to track the wafer lots all along the sequence of the operations within the flow of product manufacturing.

- A client application of “Production Management Software”, operated under “Windows NT”, used to enter the traceability data of the production unit. The data entry is made by the means of “on-line computer terminals” that are located within the Wafer Fabrication and the Wafer Sort areas where the “Product Manufacturing Flow” and the “Test Program Flow” are taking place.

- A “Windows NT” Operating System used in the Wafer Sort area to operate the “Local Host Computer” on wafer lot traceability data and test results, and to operate the “Tester Control Console” on test equipment command.

Chapter 3

3. TOE Security Environment

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 (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

The TOE, as being the “Production Flow”, is physically located into the wafer fabrication area and into the wafer sort area.

The TOE is used to:

- Get raw material prepared, microcontroller components manufactured, tested and packed. As a summary, by the use of the TOE, the goal is to transform raw silicon wafers into finished secure silicon chips under a configuration to enable the shipment to customers through the die-bank.
- Launch, control and track the wafer lots within the above areas. The objective of that usage is to control and manage the product moves during the sequential phases of the TOE, to gather and maintain the traceability data and the test data (test results) entered into files by the means of its associated Information Technology (see paragraph 2.5 “General IT Features of the TOE”).
- In addition, and with a global approach, it is also considered that the TOE and the assets need to be protected from outside attacks and that the TOE itself has to protect the assets against such attacks.

In order to strengthen such usage, the TOE is made accessible strictly under a “Need To Know” basis to authorized personnel. A full control and management of this authorized access is insured by the TOE itself, by the “Security Functional Requirements” of the Information Technology associated to the TOE, and also by the environmental security aspects of the TOE which are supported by the “Security System” of the plant.

3.2 Assets

Assets have to be protected in terms of confidentiality and of integrity by the TOE and/or by the TOE security environment.

Assets are:

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

3.2.1 Asset from the TOE

- Traceability data.
  Traceability data is including:
  . Identification (Lot number + product name) of product all along the production flow. This identification is unique.
  . Wafer lot status (in process, waiting, stop, scrap).
  . Physical location and destination (present, next operation).
  . Quantity.

- Test Results.

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 asset from the TOE will be mainly ensured by the TOE itself and by its Information Technology.

3.2.2 Assets used by the TOE

- Product (Wafer lot, wafer, dice).
- Photomasks.
  The photomasks taken into account are the security relevant photomasks.
- Test Programs.

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 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 Assumptions

Hereafter are listed the assumptions relative to information about the intended usage of the TOE and information about the environment of use of the TOE (CC Part 1).

These assumptions have to be met by the Environment of the TOE in order for the TOE to be considered secure (CC Part 1).

In the present case of this certification process, which main focus is the security offered by the “Production Environment” implemented on site during the manufacturing of the smartcard microcontoller components, the Non-IT part of the TOE and the Environment of the TOE are subject to several security objectives and requirements in order to protect assets against threats. These security objectives and requirements are deeply described and covered later into this ST.

However, it is necessary here to make assumptions about the processes that are not under the control of this TOE but which processes contributes to the security and protection of the assets. These assumptions are stated in order to get an additional level of barrier against potential attack from outside.

A.SEC_DEL: It is assumed that secure delivery occurred between supplier of photomasks and the “Production Flow” and between supplier of test programs and the “Production Flow”.

A.TRUST_PHOTOMASKS: It is assumed that photomasks, that are supplied to the “Production Flow”, can be trusted on security aspects.

A.TRUST_TPROG: It is assumed that test programs that are supplied to the “Production Flow”, can be trusted on security aspects.

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

3.4 Conformance to PP/9806 Version 2.0 - Phase 3 (Manufacturing Phase) - Assumptions:

No additional assumption is required to the above listed for conformance to PP/9806 Version 2.0 on phase 3.

3.5 Threats

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

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 that 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:

This type of threat covers unauthorized disclosure of assets by outside “attackers” who may possess a wide range of technical skills, resources and motivation. Such attackers may also have technical awareness of the product.

T.DIS_TPROG: Unauthorized disclosure of test program.

T.DIS_TDATA: Unauthorized disclosure of test results.

Unauthorized modification of assets:

The TOE and assets may be subjected to different types of logical or physical attacks that may compromise security.
Due to the intended usage of the TOE and assets (for example the TOE environment may be hostile), the security parts may be bypassed or compromised reducing the integrity of the TOE or assets security mechanisms and disabling their ability to manage the security.

T.MOD_TRACEDATA: Unauthorized modification or erase of traceability data.
T.MOD_TDATA: Unauthorized modification or erase of test results.

T.MOD_TPROG: Unauthorized modification or erase of test program.

Theft or unauthorized use of assets:

Potential attackers may gain access to the TOE and perform operations for which they are not authorized. For example, such attackers may personalize the TOE or assets in an unauthorized manner, or try to gain fraudulous access to the smartcard system, to assets.

T.T_TDATA: Theft or unauthorized use of test results.

T.T_PHOTOMASK: Theft or unauthorized use of wafer photomasks.

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

T.T_TPROG: Theft or unauthorized use of test program.

3.6 Conformance to PP/9806 Version 2.0 - Phase 3 (Manufacturing Phase) - Threats:

The below threats are required by PP/9806 Version 2.0 on phase 3 (Manufacturing Phase) and have to be countered by the manufacturing 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 the configuration of the evaluated “Production Flow” can be made possible by the theft of photomask or by the theft of product. The theft of photomask or product can be a direct theft that takes place in the manufacturing area or in the test area but the theft can be also made after modification of the traceability data (modification of quantity) to allow future theft of product. Therefore T.CLON is covered by the threats T.T_PHOTOMASK, T.T_PRODUCT and T.MOD_TRACEDATA.

T.DIS_SOFT:
This threat, as no unit related to the software is available in the evaluated “Production Flow” can only be made possible by the modification of traceability data (modification of quantity) to allow future theft of product, or by direct theft of product. Therefore T.DIS_SOFT is covered by the threats T.MOD_TRACEDATA, and T.T_PRODUCT.

T.DIS_DSOFT:
This threat, as no unit related to dedicated software is available in the evaluated “Production Flow” can only be made possible by the modification of traceability data (modification of quantity) to allow future theft of product, by the disclosure or theft of

test program or direct theft of product. Therefore T.DIS_SOFT is covered by the threats T.MOD_TRACEDATA, T.DIS_TPROG, T.T_TPROG and T.T_PRODUCT.

T.DIS_DESIGN:
This threat, as no information or data or document on design is made available in the "Production Flow" can only be made possible by the modification of traceability data (modification of quantity) to allow future theft of product, by the direct theft of photomask or by the direct theft of product. Therefore T.DIS_DESIGN is covered by the threats T.MOD_TRACEDATA, T.T_PHOTOMASK and T.T_PRODUCT.

T. DIS_TOOLS:
No development tools are available in "Production Flow". So the material involved by this threat will be only the testing tools. However in the configuration of the present "Production Flow", the testing tools are not an asset to be protected because they are fully standard for smartcard and non-smartcard products. Therefore T.DIS_TOOLS is not, in this case, a threat to be taken into account.

T.DIS_PHOTOMASK:
This threat mainly applies to photomask data or tape. But, no photomask data or tape is available in "Production Flow". Only the physical photomasks are available. They were securely delivered from another facility and then securely controlled within the "Production Flow". Therefore T.DIS_PHOTOMASK is not, in this case, a threat to be taken into account.

T.DIS_TEST:
This threat addressing the disclosure of test results is covered by T.DIS_TDATA.

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

T.T_PHOTOMASK:
This threat addressing the theft of photomask is covered by T.T_PHOTOMASK.

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

T.MOD_SOFT:
In "Production Flow", the only stage estimated to allow access to software for a "large scale" modification is at the testing operation, by the modification or theft of the test program itself. For a modification on a unit basis, it will require the theft of product (after modification of traceability data or direct theft of product). Therefore T.MOD_SOFT is covered by the threats T.MOD_TPROG, T.T_TPROG, T.MOD_TRACEDATA and T.T_PRODUCT.

T.MOD_DSOFT:

In “Production Flow”, the only stage estimated to allow access to dedicated software for a “large scale” modification is at the testing operation. For a modification on a unit basis, it will require the theft of product (after modification of traceability data or direct theft of product). Therefore T.MOD_DSOFT is covered by the threats T.MOD_TPROG, T.MOD_TRACEDATA and T.T_PRODUCT.

T.MOD_DESIGN:
This threat, as no information or data or document on design is made available in the “Production Flow”, is not really applicable in this way. Only physical representations of the design exists, with the product and with the photomasks. They are not allowing reusable modification of design. Therefore T.MOD_DESIGN is covered by the fact that in the case of the assets used by the TOE (photomask, product), this threat cannot be applied.

T.MOD_PHOTOMASK:
This threat, as no information or data or document on photomask is made available in the “Production Flow”, is not really applicable in this way. Only physical representation of the photomasks exists, making any modification, for reuse, of photomask not possible. Therefore T.MOD_PHOTOMASK is covered by the fact that in the case of the asset used by the TOE, this threat cannot be applied.

3.7 Organizational Security Policies (OSP’ s)

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

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

Editorial Note about Security System:

The “Security System” is 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 in-site management of security. This “Security System” is composed of two sets of specifications:

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

The “Manuals” and the “SOP’ s”, involved in the security implementation are described into this Security Target.

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 and controlled by the local "Smartcard Security Agent", a "master audit" is performed on a yearly basis by SCAC Security Manager.

3.7.3 "Smartcard Subcontractor Approval" OSP

This policy defines the procedure to approve a subcontractor for any activity related to the "Production Flow" used to manufacture the smartcard microcontroller components.

3.7.4 "Smartcard Subcontractor Management" OSP

This policy defines the procedure to govern and control subcontractors activities in operations related to the "Production Flow" used to manufacture 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 security failure, non-conformance and to define 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 Smartcard Security System.

3.8 Conformance to PP/9806 Version 2.0 - Phase 3 (Manufacturing Phase) Organizational Security Policies:

For conformance to PP/9806 Version 2.0 on phase 3, no additional Organizational Security Policy is required to the OSP' s listed into the chapter 3.7 of this ST.

Chapter 4

4. Security Objectives

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 (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 (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 construction, the electrical testing and packing of the wafers to be shipped to the smartcard market.

4.1 IT Security Objectives for the TOE

O.TRACE: The TOE IT must protect computerized traceability data against unauthorized modification or erase.

O.ACS_PRT: The TOE IT must give access only to authorized personnel.

O.ISSUE_INFO: The TOE IT shall inform personnel in case of any product transfer issue occurring all along the “Product Manufacturing Flow”.

4.2 NON-IT Security Objectives for the TOE

O.PRODUCT_TRACK: The TOE NON-IT must track product inside the wafer manufacturing area and inside the wafer test area.

O.IC_PRT: Product shall be protected against theft when used all along the “Production Flow”.

O.PHOTOMASK_TRACK: The TOE NON-IT must track photomasks inside the wafer manufacturing area.

O.PHOTOMASK_PRT: Photomasks shall be protected against theft when used all along the “Production Flow”.
O.TPROG_TRACK: The TOE NON-IT must track Test Program inside the wafer test area.

O.TPROG_PRT: Test program shall be accessible only by authorized personnel.

O.TDATA_PRT: Test results shall be accessible only by authorized personnel.

4.3 Security Objectives for the TOE Environment

4.3.1 TOE Environment Security Objective that is going to be refined into Security Requirements

O.AREA_PRT: The TOE is operated in a secure environment and shall be accessible only by authorized personnel.

4.3.2 TOE Environment Security Objectives that are not going to be refined into Security Requirements

O.SEC_DEL: The Environment of use of the TOE shall be able to guarantee that the confidentiality and the integrity of any material/information, when under delivery to the "Production Flow", is maintained.

O.TRUST_PHOTOMASK: The Environment of use of the TOE shall be able to guarantee that the trust given to the photomasks, delivered to the "Production Flow", is maintained.

O.TRUST_TPROG: The Environment of use of the TOE shall be able to guarantee that the trust given to the test program delivered to the "Production Flow", is maintained.

4.4 Conformance to PP/9806 Version 2.0 - Phase 3 (Manufacturing Phase) – Security Objectives:

The below objectives for the environment are required by PP/9806 Version 2.0 on phase 3 (Manufacturing Phase), as shown per paragraph 4.2.3 in PP/9806 Version 2.0, page 24/54:

O.TOE_PRT:
In the case of PP/9806 Version 2.0, the target of evaluation is the product. Therefore the security objective "O.TOE_PRT" is applicable to the protection of the product during the manufacturing phase.
Therefore, the objective of "TOE protection" and associated security procedures, as defined in PP/9806 Version 2.0, are covered in the present ST by:

- The set of security objectives for the "Production Flow" itself (TOE of this Security Target), but also by the security objectives for the Environment of the TOE.
- All the Organizational Security Policies as explained into the paragraph 3.7 of this Security Target.

O.IC_DLV:
In the case of PP/9806 Version 2.0, the target of evaluation is the product. Therefore the security objective "O.IC_DLV" requires procedures for the protection (to maintain integrity and confidentiality) of the product (which is the TOE and its assets in PP/9806 Version 2.0) during delivery from the manufacturing phase.
Therefore, in the Environment of the "Production Flow" (the TOE), a security functional requirement (5.2.6 "Hand-Carry"), dealing with secure delivery procedure, is answering to the O.IC_PRT security objective.
Therefore O.IC_DLV is covered by O.IC_PRT.

Chapter 5

5. Security Requirements

5.1 TOE IT Security Requirements

5.1.1 TOE IT Security Functional Requirements

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 (CC Part 1).

The TOE Security Functional Requirements will be issued for these relevant pieces of software of the TOE.

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.

Iteration 1:
The security functions of [refinement: “HP-UX”] shall require each user to identify itself before allowing any other TOE security functions-mediated actions on behalf of that user.
The “HP-UX” operating system, for identification of each user, requires each user to enter its Login Name. This is required before any other TOE security functions-mediated actions, on behalf of that user, is allowed.

Iteration 2:
The security functions of [refinement: “Production Management Software”] shall require each user to identify itself before allowing any other TOE security functions-mediated actions on behalf of that user.
The “Production Management Software”, for identification of each user, requires each user to enter its Identification Number. This is required before any other TOE security functions-mediated actions, on behalf of that user, is allowed.

Iteration 3:

The security functions of [refinement: “Windows NT”] shall require each user to identify itself before allowing any other TOE security functions-mediated actions on behalf of that user.
The “Windows NT” operating system, for identification of each user, requires each user to enter its User Identifier. 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 security functions of [refinement: “HP-UX”] shall require each user to be successfully authenticated before allowing any other TOE security functions-mediated actions on behalf of that user.
The “HP-UX” 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 security functions of [refinement: “Production Management Software”] shall require each user to be successfully authenticated before allowing any other TOE security functions-mediated actions on behalf of that user.
The “Production Management Software”, 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 security functions of [refinement: “Windows NT”] shall require each user to be successfully authenticated before allowing any other TOE security functions-mediated actions on behalf of that user.

The “Windows NT” 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 security functions of [refinement: “HP-UX”] shall maintain the following list of security attributes belonging to individual users: [assignment:

- Identification Number.
- Password.
- Login Name (Root or other name).
- Property (Owner or Non-owner).
- User Rights].

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

- Identification Number.
- Password.
- Employee Class.
- User Rights].

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

- User Identifier.
- Password.
- 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 security functions of [refinement: "HP-UX"] shall maintain the roles [assignment:
- Administrator role.
- User role].

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

Iteration 2:
The security functions of [refinement: "Production Management Software"] shall maintain the roles [assignment:
- Administrator role.
- User role].

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

Iteration 3:
The security functions of [refinement: "Windows NT"] shall maintain the roles [assignment:
- Administrator role.
- User role].

The "Windows NT" operating system, for its secure operation and to protect its own secured assets (files,…), recognizes and maintains the two roles, and only these two, 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: "HP-UX"] shall be able to associate users with roles.
"Administrator" and "Users" are the two roles recognized by the "HP-UX" 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 "HP-UX", is made by the use of the Login Name and confirmed with the Password entered.

Iteration 2:
The TOE security functions of [refinement: "Production Management Software"] shall be able to associate users with roles.
"Administrator" and "Users" are the two roles recognized by the operating system of the "Production Management Software". 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 the "Production Management Software", is made by the Identification Number and confirmed with the Password entered.

Iteration 3:
The TOE security functions of [refinement: "Windows NT"] shall be able to associate users with roles.
"Administrator" and "Users" are the two roles recognized by the "Windows NT" 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 NT" 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 has the FDP_ACC.2 is encompassing it and is hierarchical to it.

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: "HP-UX"] shall enforce the [assignment: "HP-UX" 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: “Production Management Software”] shall enforce the [assignment: “Production Management Software” access control security functions policy] on [assignment: administrator and users, on product identification (Lot number + product name), wafer lot status (in process, waiting, stop, scrap), physical location and destination (present, next operation) and quantity] and all operations among subjects and objects covered by the Security Function Policy.

Iteration 3:
The TOE security functions of [refinement: “Windows NT”] shall enforce the [assignment: “Windows NT” access control security functions policy on operations using the “client function” (GPC) of the “Production Management Software”, for “on-line computer terminals”, for “local host” and for “tester control console”] on [assignment: administrators and users, 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: “HP-UX”] 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: “Production Management Software”] 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 NT”] 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: "HP-UX"] shall enforce the [assignment: "HP-UX" access control security functions policy] to objects based on [assignment: security attributes that are Role, Property (Owner or Non-Owner) and User Rights].

Iteration 2:

The TOE security functions of [refinement: "Production Management Software"] shall enforce the [assignment: "Production Management Software" access control security functions policy] to objects based on [assignment: security attributes that are Identification Number and Employee Class].

Iteration 3:

The TOE security functions of [refinement: "Windows NT"] shall enforce the [assignment: "Windows NT" access control security functions policy] to objects based on [assignment: security attributes that are Role 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: "HP-UX"] 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

R: Read
W: Write
X: Execute
O: depending on the rights authorized by the user to the other users. This can be R, W, X and No Operation].

Iteration 2:
The TOE security functions of [refinement: "Production Management Software"] 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 Identification Number, Employee Class, User Rights, Location in production flow, and operation approval for authorized passwords.

. Controlled subjects are:
- Users.

. Controlled objects are:
- Identification (Lot number + product name).
- Wafer lot status (in process, waiting, stop, scrap).
- Physical location and destination (present, next operation).
- Quantity.

* Table showing Employee Class versus Employee:

		EMPLOYEE
EN	0	Operator

	1	Sub-group Leader & Process Maintenance
	2	Group Leader
	3	Sub-shift Manager
	4	Shift Manager
	5	Assistant Manager or above & Engineer

* Table showing authorized operation among controlled subjects and controlled objects for wafer fabrication:

		OBJECTS				
		Identification	Wafer lot status	Physical Location	Quantity	
					Inspection Step	Other Steps
USERS	0	No Operation	No Operation	Modification	Modification	No Operation
	1	Modification	Modification	Modification	Modification	Modification
	2	Modification	Modification	Modification	Modification	Modification
	3	Modification	Modification	Modification	Modification	Modification
	4	Modification	Modification	Modification	Modification	Modification
	5	Modification	Modification	Modification	Modification	Modification

* Table showing authorized operation among controlled subjects and controlled objects for wafer sort:

		OBJECTS				
		Identification	Wafer lot status	Physical Location	Quantity	
					Inspection Step	Other Steps
USERS	0	Modification	No Operation	Modification	Modification	No Operation
	1	Modification	Modification	Modification	Modification	Modification
	2	Modification	Modification	Modification	Modification	Modification
	3	Modification	Modification	Modification	Modification	Modification
	4	Modification	Modification	Modification	Modification	Modification
	5	Modification	Modification	Modification	Modification	Modification

].

Iteration 3:

The TOE security functions of [refinement: “Windows NT”] 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

R: Read
W: Write
X: Execute
O: depending on the rights authorized by the user to the other users. This can be R, W, X and 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: “HP-UX”] 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 2:
The TOE security functions of [refinement: “Production Management Software”] shall explicitly authorize access of subjects to objects based on the following additional rule: [assignment: Control of Identification Number and of User Password].

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

Iteration 2:
The TOE security functions of [refinement: "Production Management Software"] shall explicitly deny access of subjects to objects based on the [assignment: rule that is Control of Identification Number and of User Password].

Iteration 3:
The TOE security functions of [refinement: "Windows NT"] 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 any default values are defined for the security attributes. Therefore FMT_MSA.3 is not 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: "HP-UX"] shall enforce the [assignment: "HP-UX" access control security functions policy] to restrict the ability to [selection: modify, delete, [assignment: set]] the security attributes [assignment: Identification

Number, Password, Login Name, Property and User Rights] to [assignment: the authorized identified roles], as shown per the below table:

	HP-UX									
	Id Number		Password		Login Name		Property		User Rights	
	Own	Other	Own	Other	Own	Other	Own	Other	Own	Other
Administrator	S M D	S M D	S M D	S M D	No Op.	S M D	S M D	S M D	S M D	S M D
User	No Op.	No Op.	M	No Op.	No Op.	No Op.	No Op.	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: "Production Management Software"] shall enforce the [assignment: "Production Management Software" access control security functions policy] to restrict the ability to [selection: modify, delete, [assignment: set]] the security attributes [assignment: Identification Number, Password, Employee Class and User Rights] to [assignment: the authorized identified roles], as shown per the below table:

	Production Management Software							
	Id Number		Password		Emp. Class		User Rights	
	Own	Other	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	S M D	S M D
User	No Op.	No Op.	M	No Op.	No Op.	No Op.	S M D	No Op.

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

Iteration 3:
The TOE security functions of [refinement: "Windows NT"] shall enforce the [assignment: "Windows NT" 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 NT					
	User Id		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].

Iteration 1:
The TOE security functions of [refinement: "HP-UX"] shall restrict the ability to [selection: determine, 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	Determine, Modify	No ability
	SF3	No ability	No ability
	SF4	No ability	No ability
	SF5	No ability	No ability
	SF6	No ability	No ability
	SF7	No ability	No ability

Iteration 2:

The TOE security functions of [refinement: "Production Management Software"] 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	SF2	Determine, Modify	No ability
	SF3	No ability	No ability
	SF8	Determine, Disable, Enable, Modify	No ability

Iteration 3:

The TOE security functions of [refinement: "Windows NT"] shall restrict the ability to [selection: determine, 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	No ability	No ability
	SF12	No ability	No ability
	SF13	No ability	No ability

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

5.1.1.9 Security Alarms (FAU_ARP.1)

Hierarchical to: No other components.

FAU_ARP.1.1: The TOE security functions shall take [assignment: list of the least disruptive actions] upon a detection of a potential security violation.

The TOE security functions of [refinement: “Production Management Software”] shall take [assignment: an alarm action], towards employee, upon a detection of a potential security violation related to out of time limit for product transfer between two adjacent manufacturing steps. Employee is then able to start investigations to retrieve wafer lot and to identify root cause of non-compliant transfer time in order corrective actions can be implemented.

Dependencies: FAU_SAA.1 Potential Violation Analysis.
Dependency is satisfied.

5.1.1.10 Potential Violation Analysis (FAU_SAA.1)

Hierarchical to: No other components.

FAU_SAA.1.1: The TOE security functions shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TOE security policy.
The TOE security functions of [refinement: “Production Management Software”] shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TOE security policy. The audited event is the transfer time between two adjacent manufacturing steps. The rule is to count time since the release of product from previous manufacturing step occurred and if this transfer time is out of time limit, the “non-compliant” lot information is printed out.

FAU_SAA.1.2: The TOE security functions shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [assignment: subset of defined auditable events] known to indicate potential security violation;
b) [assignment: any other rules].

The TOE security functions of [refinement: “Production Management Software”] shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [assignment: Transfer time “out of limit”] known to indicate a potential security violation;
b) [assignment: no other rule].

Dependencies: FAU_GEN.1 Audit Data Generation.
Dependency is satisfied.

5.1.1.11 Audit Data Generation (FAU_GEN.1)

Hierarchical to: No other components.

FAU_GEN.1.1: The TOE security functions shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [selection: minimum, basic, detailed, not specified] level of audit; and
c) [assignment: other specifically defined auditable events].

The TOE security functions of [refinement: “Production Management Software”] shall be able to generate an audit record of the following auditable events:
a) Start-up and shut down of wafer lot transfer time;
   In the “Product Manufacturing Flow”, start-up of the audit function is the release of a wafer lot from one manufacturing step (step “n”) and shutdown of the audit function is the receipt of the same wafer lot at the next manufacturing step (step “n+1”). This audit function takes place from the first step up to the last step in the construction of the product.
b) All auditable events for the [selection: not specified] level of audit; Within the “Product Manufacturing Flow”, the correctness for a transfer of wafer lot, from one manufacturing step to the next one in order to inform about a potential violation (theft of wafer lot), is a transfer made within the allowed transfer time limit; and
c) [assignment: There is no other specifically defined auditable events].

FAU_GEN.1.2: The TOE security functions shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: other audit relevant information].

The TOE security functions of [refinement: “Production Management Software”] shall record within each audit record at least the following information:

a) - Date and time of the event.
   - Type of event is by definition, within the “Product Manufacturing Flow”, the correctness (transfer made within the allowed transfer time limit) of the transfer of a wafer lot from one manufacturing step to the next one.
   - Subject identity is the wafer lot with its associated identification number.
   - And the outcome of the event is a success when the wafer lot is received, at next manufacturing step, within the time limit. The outcome is a failure when the wafer lot is either not arrived at the next manufacturing step or is arrived at the next manufacturing step but out of the time limit; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: the other audit relevant information is, within the “Product Manufacturing Flow”, the manufacturing steps (step “n” and step “n+1”) which were involved (transfer from step “n” to step “n+1”)].

Dependencies: FPT_STM.1 Reliable Time Stamps.
Dependency is satisfied.

5.1.1.12 Reliable Time Stamps (FPT_STM.1)

Hierarchical to: No other components.

FPT_STM.1.1: The TOE security functions shall be able to provide reliable time stamps for its own use.

The TOE security functions of [refinement: “HP-UX”] shall be able to provide reliable time stamps for its own use. “HP-UX” that is the Operating System used to operate the “Production Management Software”, by providing its internal clock as a time base, shall be able to provide reliable time stamps for its own use and also for the use of the “Production Management Software”.

Dependencies: No dependencies.

5.1.2 TOE IT Security Assurance Requirements

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 (CC Part 1).

The assurance requirements are 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 of smartcard product, photomasks, test program, and test results.

5.2.2 Material Asset Identification

It is required that product, photomasks and test program are uniquely identified

5.2.3 Access Control

It is required that, access to test equipment and to local host, used for test results storage, is controlled with identification number and password entry of authorized employee before any actions is allowed to the employee.

5.2.4 Non Permanence
It is required that, test program is not resident on test equipment and electrically erased after test operation is completed.

5.2.5 End of Life
It is required that, for photomasks and test program, end of life procedure exists.

5.2.6 Hand-Carry
It is required that for transfer of smartcard wafer lots from wafer manufacturing area to wafer test area, of photomasks and of test program, hand carry transportation is used.

5.2.7 Data Back-up
It is required that, data back-up for test results exists.

5.2.8 Photomasks Ordering
It is required that ordering of new photomasks is ensuring secure identification, traceability and is following ordering security rules to detect or prevent potential thefts.

5.2.9 Configuration Management
It is required to control the identification of product, photomasks, test tools and test programs and to control any change that may be applied to them.

5.2.10 Scrap Management
It is required to securely control, collect, transport and destroy scrapped wafers and scrapped photomasks, during the application of “Production Flow”.

5.2.11 Passwords Management
It is required to securely create, control and manage all the passwords for access control to computers (software), files, test results.

5.2.12 Information/Material Protection Management
It is required to securely classify, identify, manage, store, handle, pack and deliver any smartcard related material (product, test program, photomasks), test results and customer data, when applicable.

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 “Production Flow”, used to manufacture 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 “Production Flow”, used to manufacture the smartcard microcontroller components, has in advance followed the process used to enlist such new personnel.

5.3.3 “Smartcard Employee Separation”

Each employee when under resignation status and who was working in operations related to the “Production Flow” used to manufacture 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 “Production Flow” used to manufacture the smartcard microcontroller components, is individually identified and authenticated to give or deny access to smartcard controlled areas, storage shelfes, files, test programs, photomasks, test 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 site, areas, storage shelves, files, test programs, photomasks, test results and customer data, when applicable.

5.3.6 “Passwords Management”

It is required to securely create, control and manage all the passwords for access control to areas.

5.3.7 “Smartcard Security Failure Report & Corrective Actions”

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

5.3.8 Secure Site Information System

It is required that, site Information System provides protection to the TOE Information Technology, against external attack or intrusion.

Chapter 6

6. TOE Summary Specification

6.1 Statement of TOE Security Functions

6.1.1 SF1: Login

The “HP-UX” **Login** security function requires administrator and users to enter, first the login –id and second the password, before any action is allowed by “HP-UX” operating system to administrator and users.

6.1.2 SF2: Access Control

The “Production Management Software” **Access Control** security function requires, first the identification of users and second the users to enter the password, before any action is allowed by the “Production Management Software” to users.

6.1.3 SF3: Attribute Manager

The “HP-UX” **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 both the “HP-UX” operating system and the “Production Management Software”.

6.1.4 SF4: Admin

The “HP-UX” **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** and the **Access Control** security functions.

6.1.5 SF5: File/Command Property

Embedded in the low level layers of “HP-UX” 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.

6.1.6 SF6: File Configuration

The **File Configuration** security function 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.

6.1.7 SF7: Rights Manager

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

6.1.8 SF8: Transfer Time Alarm

The **Transfer Time Alarm** security function of the “Production Management Software” is measuring transfer time settled for transfer of products between two adjacent manufacturing steps and warning employee when transfer time is out of standard time limit.

6.1.9 SF9: Logon

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

6.1.10 SF10: Security Identifier (SID)

The “Windows NT” **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 NT” operating system and its associated applications.

6.1.11 SF11: User Account Manager

The “Windows NT” **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.

6.1.12 SF12: Owner

Embedded in the low level layers of “Windows NT” 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.

6.1.13 SF13: Security Account Manager (SAM)

The **SAM** security function of the "Windows NT" 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	FAU_ARP.1	FAU_SAA.1	FAU_GEN.1	FPT_STM.1
TOE Security Functions	SF1	X	X		X	X	X	X	X				
	SF2	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				
	SF8									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				

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: Security Target Statement (**ST Statement**):

- ACM_CAP.1.1D: The TOE is referenced with a dedicated proprietary name. Within the name, a number is used as a version number for notification of change. This number is incremented when change occurs to the "Production Flow".

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

- ACM_CAP.1.1C: The reference for the TOE is unique and is here applied to the NEC submicron technology with its name. The TOE is used to produce the smartcard microcontroller components. Each version of the TOE is identified with an increase of the number within the name of the TOE.
  The Information Technology of the TOE is also uniquely referenced and is using the uniquely identified version of "HP-UX" operating system, of "Production Management Software" and of "Windows NT" operating system.
- ACM_CAP.1.2C: The TOE is labeled with this reference.

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:

  - ➔ "Production Management Software" installation, generation and start-up Manual – Version 1.0 (**AM 1**).
  - ➔ "Production Management Software" General Purpose Client Set-Up & User Manual – Version 6.0 (**AM 10**).
  - ➔ "HP-UX" Manual – Version 10.2 (**AM 2**).
  - ➔ First Step Guide of "Windows NT" Workstation – Version 4.0 (**AM 11**).
  - ➔ Supplement for Better Security – Version 1.0 (**AM 12**).

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.

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 specification for "HP-UX", "Production Management Software" and for "Windows NT" are:

  - ➔ "HP-UX" Functional Specification – Version 1.0 (**AM 3**).
  - ➔ "Production Management Software" Functional Specification – Version 1.0 (**AM 4**).

➔ "Windows NT" Functional Specification – Version 1.0 (**AM 14**).

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:

  ➔ "HP-UX" Representation Correspondence – Version 1.0 (**AM 5**).
  ➔ "Production Management Software" Representation Correspondence – Version 1.0 (**AM 6**).
  ➔ "Windows NT" Representation Correspondence – Version 1.0 (**AM 15**).

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:

  - ➔ "HP-UX" Manual – Version 10.2 (**AM 2**).
  - ➔ "Production Management Software" Administration & User Manual – Version 1.0 (**AM 7**).
  - ➔ "Windows NT" Server 4 Security, Troubleshooting and Optimization – Version Japan 1997 (**AM 13**).

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:

  - ➔ "HP-UX" Manual – Version 10.2 (**AM 2**).
  - ➔ "Production Management Software" Administration & User Manual – Version 1.0 (**AM 7**).
  - ➔ "Production Management Software" General Purpose Client Set-Up & User Manual – Version 6.0 (**AM 10**).

➔ First Step Guide of "Windows NT" Workstation – Version 4.0 (**AM 11**).

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. Dependency is not applicable.
ADV_IMP.1 Subset of the Implementation of the TSF. Dependency is not applicable.
ADV_LLD.1 Descriptive Low-Level Design. Dependency is not applicable.
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.

  ➔ "HP-UX" Vulnerability Analysis Specification – Version 1.0 (**AM 8**).
  ➔ "Production Management Software" Vulnerability Analysis Specification – Version 1.0 (**AM 9**).

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 Measures:							
		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 Secu	ST Statement	X						X	
	AM1		X						
	AM2		X			X	X		

	AM3			**X**					
	AM4			**X**					
	AM5				**X**				
	AM6				**X**				
	AM7					**X**	**X**		
	AM8								**X**
	AM9								**X**
	AM10		**X**				**X**		
	AM11		**X**				**X**		
	AM12		**X**						
	AM13					**X**			
	AM14			**X**					
	AM15				**X**				

6.3 Statement of Non-IT Security Measures for the TOE

6.3.1 Secure Storage Procedure

Manual or SOP (Security Operating Policy) shall exist to define the procedures to be used for the secure storage in locked shelves of smartcard product, photomasks, test program and storage in local host computer of test results.

6.3.2 Material Asset Identification Procedure

Manual or SOP (Security Operating Policy) shall exist to define the procedure for the unique identification of product, photomasks and test program.

6.3.3 Access Control Procedure

Manual or SOP (Security Operating Policy) shall exist to define the procedure for the control of the access to the test equipment and to the local host (test results storage), using the identification number and password of authorized employee, before any actions is allowed to the employee.

6.3.4 Non Permanence Procedure

Manual or SOP (Security Operating Policy) shall exist, requiring that the test program is not resident on test equipment and electrically erased when test operation is completed.

6.3.5 End of Life Procedure

Manual or SOP (Security Operating Policy) shall exist, requiring “end of life rules” for photomasks and test programs.

6.3.6 Hand-Carry Procedure

Manual or SOP (Security Operating Policy) shall exist, requiring "hand-carry transportation" for transfer of smartcard wafer lots, from wafer manufacturing area to wafer test area, of photomasks and of test programs.

6.3.7 Data Back-up Procedure

Manual or SOP (Security Operating Policy) shall exist, requiring data back-up for test results.

6.3.8 Photomasks Ordering Procedure

Manual or SOP (Security Operating Policy) shall exist, requiring rules to order new photomasks, ensuring a secure identification and traceability, and allowing to detect or prevent potential theft, are implemented.

6.3.9 Configuration Management Procedure

Manual or SOP (Security Operating Policy) shall exist, requiring the control of identification for product, photomasks, test tools and test programs, and allowing to control any change that may be applied to them.

6.3.10 Scrap Management Procedure

Manual or SOP (Security Operating Policy) shall exist, requiring a secure control, collection, transportation and destruction of scrapped wafers and scrapped photomasks.

6.3.11 Passwords Management Procedure

Manual or SOP (Security Operating Policy) shall exist, requiring to securely create, control and manage all the passwords for access control to computers (software), files and test results.

6.3.12 Information/Material Protection Management Procedure

Manual or SOP (Security Operating Policy) shall exist, requiring to securely classify, identify, manage, store, handle, pack and deliver any smartcard related material (product, test programs, photomasks), test results and customer data, when applicable.

6.4 Statement of Security Measures for the Environment

6.4.1 "Individual Non Disclosure Agreement" Procedure

Manual or SOP (Security Operating Policy) shall exist, requiring that every employee, working in operations related to the "Production Flow" used to manufacture the smartcard microcontroller components, has in advance signed a Non Disclosure Agreement (Individual NDA).

6.4.2 "New Employee Enrolment" Procedure

Manual or SOP (Security Operating Policy) shall exist, requiring that every new employee, before working in operations related to the “Production Flow, used to manufacture the smartcard microcontroller components, has in advance followed the process used to enlist such new personnel.

6.4.3 “Smartcard Employee Separation” Procedure

Manual or SOP (Security Operating Policy) shall exist, requiring that every employee, when under resignation status and who was working in operations related to the “Production Flow” used to manufacture the smartcard microcontroller components, is compliant with the smartcard employee separation process.

6.4.4 “Individual Identification and Authentication” Procedure

Manual or SOP (Security Operating Policy) shall exist, requiring that, in order to give or deny access to smartcard controlled areas, storage shelves, files, test programs, photomasks, test results and customer data, when applicable, every employee who is working in operations related to the “Production Flow”, used to manufacture the smartcard microcontroller components, is individually identified and authenticated.

6.4.5 “Access Control Management” Procedure

Manual or SOP (Security Operating Policy) shall exist, requiring that access rights and rules are implemented in order to control access and give access only to authorized personnel to site, areas, storage shelves, files, test programs, photomasks, test results and customer data, when applicable.

6.4.6 “Passwords Management” Procedure

Manual or SOP (Security Operating Policy) shall exist, requiring secure creation, control and management of all the passwords used to access the controlled areas.

6.4.7 “Smartcard Security Failure Report & Corrective Actions” Procedure

Manual or SOP (Security Operating Policy) shall exist, requiring notification about any occurring failure or non-conformance, definition and implementation of corrective actions in order to fix the issue and prevent its re-occurrence.

6.4.8 Secure Site Information System Procedure

Manual or SOP (Security Operating Policy) shall exist, requiring that the site Information System is providing protection, against external attack or intrusion, to the TOE Information Technology.

Chapter 7

7. PP Claims

No specific PP claims are made for this Security Target.

However, in order to satisfy any 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 manufacturing. This Environment for manufacturing phase (phase 3), 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 3 (Manufacturing Phase)”.

Chapter 8

8. Rationale

8.1 Introduction

This chapter presents the evidences used in the ST evaluation.
These evidences support the claims that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment.

8.2 Security Objectives Rationale

This section demonstrates that the stated security objectives address all of the security environment aspects identified.

8.2.1 Assets and Threats

The assets to be protected are:

- Traceability data.
- Test Results.
- Product (Wafer lot, wafer, dice).
- Photomasks (The photomasks taken into account are the security relevant photomasks, that includes those containing proprietary confidential information related to product security features data and to customer data).
- Test programs.

During the operation of the different phases of the “Production Flow”, as shown per the paragraph 2.2, the below threats have been identified. They are hereafter addressed to the assets as explained in the table.

Such threats are described in paragraph 3.5 of this ST.

		THREATS								
		T.DIS_TPROG	T.DIS_TDATA	T.MOD_TRACEDATA	T.MOD_TDATA	T.MOD_TPROG	T.T_TDATA	T.T_PHOTOMASK	T.T_PRODUCT	T.T_TPROG
ASSETS	Traceability data			**X**						
	Test Results		**X**		**X**		**X**			
	Product								**X**	
	Photomask							**X**		
	Test Programs	**X**				**X**				**X**

Table: Assets versus Threats.

8.2.2 Threats and Objectives Rationale

Security objectives have been identified to protect the identified assets against the identified threats.

These security objectives are covered by the TOE itself and by its Environment as described in the chapters 4.1, 4.2 and 4.3 of this ST.

The security objectives have been traced to these threats as shown per the table hereafter.

		SECURITY OBJECTIVES										
		O.TRACE	O.ACS_PRT	O.ISSUE_INFO	O.PRODUCT_TRACK	O.IC_PRT	O.PHOTOMASK_TRACK	O.PHOTOMASK_PRT	O.TPROG_TRACK	O.TPROG_PRT	O.TDATA_PRT	O.AREA_PRT
THREATS	T.DIS_TPROG									X		X
	T.DIS_TDATA										X	X
	T.MOD_TRACEDATA	X	X									X
	T.MOD_TDATA										X	X
	T.MOD_TPROG									X		X
	T.T_TDATA										X	X
	T.T_PHOTOMASK						X	X				X
	T.T_PRODUCT			X	X	X						X
	T.T_TPROG								X	X		X

Table: Threats versus Security Objectives.

T.DIS_TPROG is countered by the security objectives O.TPROG_PRT and O.AREA_PRT.

T.DIS_TDATA is countered by the security objectives O.TDATA_PRT and O.AREA_PRT.

T.MOD_TRACEDATA is countered by the security objectives O.TRACE, O.ACS_PRT and O.AREA_PRT.

T.MOD_TDATA is countered by the security objectives O.TDATA_PRT and O.AREA_PRT.

T.MOD_TPROG is countered by the security objectives O.TPROG_PRT and O.AREA_PRT.

T.T_TDATA is countered by the security objectives O.TDATA_PRT and O.AREA_PRT.

T.T_PHOTOMASK is countered by the security objectives O.PHOTOMASK_TRACK, O.PHOTOMASK_PRT and O.AREA_PRT.
T.T_PRODUCT is countered by the security objectives O.ISSUE_INFO, O.PRODUCT_TRACK, O.IC_PRT and O.AREA_PRT.

T.T_TPROG is countered by the security objectives O.TPROG_TRACK, O.TPROG_PRT and O.AREA_PRT.

8.2.3 Assumptions, Organizational Security Policies and Security Objectives Rationale

The security objectives have been traced to these assumptions and to these organizational security policies as shown per the table hereafter.

		TOE NON-IT SECURITY OBJECTIVES & TOE ENVIRONMENT SECURITY OBJECTIVES										
		O.PRODUCT_TRACK	O.IC_PRT	O.PHOTOMASK_TRACK	O.PHOTOMASK_PRT	O.TPROG_TRACK	O.TPROG_PRT	O.TDATA_PRT	O.SEC_DEL	O.TRUST_PHOTOMASK	O.TRUST_TPROG	O.AREA_PRT
ASSUMPTIONS	A.SEC_DEL								***X***			
	A.TRUST_PHOTOMASKS									***X***		
	A.TRUST_TPROG										***X***	
	A.SKL_PERSONNEL											**X**
	"Smartcard Specification System" OSP	**X**	**X**	**X**	**X**	**X**	**X**	**X**				**X**
	"Smartcard Master Security Audit" OSP	**X**	**X**	**X**	**X**	**X**	**X**	**X**				**X**
	"Smartcard Subcontractor Approval" OSP			**X**	**X**	**X**	**X**					

S & OSP, S	"Smartcard Subcontractor Management" OSP			**X**	**X**	**X**	**X**					
	"Smartcard Security Failure Report & Corrective Actions" OSP	**X**	**X**	**X**	**X**	**X**	**X**	**X**				**X**
	"Smartcard Security Change Management" OSP	**X**	**X**	**X**	**X**	**X**	**X**	**X**				**X**

Table: Assumptions and Organizational Security Policies versus Security Objectives.

8.2.3.1 TOE Environment Security Objective that is going to be refined into Security Requirements

O.PRODUCT_TRACK is the security objective requiring tracking of the product:

- This objective is covering the "Smartcard Specification System" OSP.
- This objective is covering the "Smartcard Master Security Audit" OSP.
- This objective is covering the "Smartcard Security Failure Report & Corrective Actions" OSP.
- This objective is covering the "Smartcard Security Change Management" OSP.

O.IC_PRT is the security objective asking for protection of the product against theft:

- This objective is covering the "Smartcard Specification System" OSP.
- This objective is covering the "Smartcard Master Security Audit" OSP.
- This objective is covering the "Smartcard Security Failure Report & Corrective Actions" OSP.
- This objective is covering the "Smartcard Security Change Management" OSP.

O.PHOTOMASK_TRACK is the security objective requiring tracking of the photomasks:

- This objective is covering the "Smartcard Specification System SOP" OSP.

- This objective is covering the “Smartcard Master Security Audit” OSP.
- This objective is covering the “Smartcard Subcontractor Approval” OSP.
- This objective is covering the “Smartcard Subcontractor Management” OSP.
- This objective is covering the “Smartcard Security Failure Report & Corrective Actions” OSP.
- This objective is covering the “Smartcard Security Change Management” OSP.

O.PHOTOMASK_PRT is the security objective requiring protection of the photomasks against theft:

- This objective is covering the “Smartcard Specification System” OSP.
- This objective is covering the “Smartcard Master Security Audit” OSP.
- This objective is covering the “Smartcard Subcontractor Approval” OSP.
- This objective is covering the “Smartcard Subcontractor Management” OSP.
- This objective is covering the “Smartcard Security Failure Report & Corrective Actions” OSP.
- This objective is covering the “Smartcard Security Change Management” OSP.

O.TPROG_TRACK is the security objective requiring tracking of the test program:

- This objective is covering the “Smartcard Specification System” OSP.
- This objective is covering the “Smartcard Master Security Audit” OSP.
- This objective is covering the “Smartcard Subcontractor Approval” OSP.
- This objective is covering the “Smartcard Subcontractor Management” OSP.
- This objective is covering the “Smartcard Security Failure Report & Corrective Actions” OSP.
- This objective is covering the “Smartcard Security Change Management” OSP.

O.TPROG_PRT is the security objective requiring the test program to be only accessible by authorized personnel:

- This objective is covering the “Smartcard Specification System” OSP.
- This objective is covering the “Smartcard Master Security Audit” OSP.
- This objective is covering the “Smartcard Subcontractor Approval” OSP.
- This objective is covering the “Smartcard Subcontractor Management” OSP.
- This objective is covering the “Smartcard Security Failure Report & Corrective Actions” OSP.
- This objective is covering the “Smartcard Security Change Management” OSP.

O.TDATA_PRT is the security objective requiring the test results to be only accessible by authorized personnel:

- This objective is covering the “Smartcard Specification System” OSP.
- This objective is covering the “Smartcard Master Security Audit” OSP.
- This objective is covering the “Smartcard Security Failure Report & Corrective Actions” OSP.
- This objective is covering the “Smartcard Security Change Management” OSP.

O.AREA_PRT is the security objective requiring that the TOE is operated in a secure environment and made only accessible to authorized personnel:

- This objective is covering A.SKL_PERSONNEL.
- This objective is covering the “Smartcard Specification System” OSP.
- This objective is covering the “Smartcard Master Security Audit” OSP.
- This objective is covering the “Smartcard Security Failure Report & Corrective Actions” OSP.

- This objective is covering the “Smartcard Security Change Management” OSP.

8.2.3.2 TOE Environment Security Objectives that are not going to be refined into Security Requirements

O.SEC_DEL is the security objective requiring that the Environment of use of the TOE is able to guarantee that confidentiality and integrity of material/information is maintained during delivery process to the “Production Flow”:

- This objective is covering A.SEC_DEL.

O.TRUST_PHOTOMASK is the security objective requiring that the Environment of use of the TOE is able to guarantee that the trust given to the photomasks delivered to the “Production Flow” is maintained:

- This objective is covering A.TRUST_PHOTOMASKS.

O.TRUST_TPROG is the security objective requiring that the Environment of use of the TOE is able to guarantee that the trust given to the test program delivered to the “Production Flow” is maintained:

- This objective is covering A.TRUST_TPROG.

8.3 Security Requirements Rationale

The security requirements rationale shall demonstrate that the set of security requirements (TOE and Environment) is suitable to meet the security objectives.

This section demonstrates that the combination of the security functional requirements is suitable to satisfy the identified security objectives for the TOE and for the Environment.

The security objectives have been traced to these functional requirements as shown per the tables hereafter:

- TOE IT Security Functional Requirements versus TOE IT Security Objectives.
- TOE NON-IT Security Requirements versus TOE NON-IT Security Objectives.
- TOE Environment Security Requirements versus TOE Environment Security Objectives.

8.3.1 TOE IT Security Functional Requirements Rationale

		TOE IT SECURITY OBJECTIVES		
		O.TRACE	O.ACS_PRT	O.ISSUE_INFO
TOE IT SECURITY FUNCTIONAL REQUIREMENTS	FIA_UID.2	X	X	
	FIA_UAU.2	X	X	
	FIA_ATD.1	X	X	
	FMT_SMR.1	X		
	FDP_ACC.2	X	X	
	FDP_ACF.1	X	X	
	FMT_MSA.1	X		
	FMT_MOF.1	X		
	FAU_ARP.1			X
	FAU_SAA.1			X
	FAU_GEN.1			X
	FPT_STM.1			X

Table: TOE IT Security Functional Requirements versus TOE IT Security Objectives.

O.TRACE is the security objective for protection of the computerized traceability data against unauthorized modification or erase.

In first case above, this objective needs to control the access to the IT in order to reject non-authorized person:

- This is performed by FIA_UID.2, FIA_UAU.2.
- This is performed by FIA_ATD.1.

In the second case, this objective needs to control and manage the rights of users and to protect these rights:

- This is performed by FIA_ATD.1.
- This is performed by FMT_SMR.1.
- This is also performed by the combination of:
  - . FDP_ACC.2 and FDP_ACF.1,
  - . FMT_MSA.1,
  - . and of FMT_MOF.1.
- This is also covered by the assumption A.SKL_PERSONNEL.

O.ACS_PRT is the security objective implemented for the control of the access to the TOE IT by the authorized personnel only. To meet this objective it is required:

- This is performed by FIA_UID.2 and by FIA_UAU.2.
- This is performed by the combination of security attributes to the users, as per FIA_ATD.1, with the access control policy of the IT, as per FDP_ACC.2 and FDP_ACF.1.

O.ISSUE_INFO is the security objective implemented to inform the personnel that wafer lot was not arriving to next manufacturing step within the defined time limit, possibly highlighting a potential theft, or at least a loss, of the wafer lot during transfer from the previous manufacturing step. To be fully met, this objective needs:

- This is performed by FAU_ARP.1.
- This is performed by FAU_SAA.1.
- This is performed by FAU_GEN.1.
- This is performed by FPT_STM.1.

8.3.2 TOE NON-IT Security Requirements Rationale

		TOE NON-IT SECURITY OBJECTIVES						
		O.PRODUCT_TRACK	O.IC_PRT	O.PHOTOMASK_TRACK	O.PHOTOMASK_PRT	O.TPROG_TRACK	O.TPROG_PRT	O.TDATA_PRT
TOE NON-IT SECURITY REQUIREMENTS	**Secure Storage 5.2.1**		X		X		X	X
	Material Asset Identification 5.2.2	X		X		X		
	Access Control 5.2.3						X	X
	Non Permanence 5.2.4						X	
	End Of Life 5.2.5				X		X	
	Hand-Carry 5.2.6		X		X		X	
	Data Back-Up 5.2.7							X
	Photomask Ordering 5.2.8				X	X		
	Configuration Management 5.2.9	X		X		X		
	Scrap Management 5.2.10		X		X			
	Passwords management 5.2.11		X		X		X	X
	Information/Material Protection Management 5.2.12	X	X	X	X	X	X	X

Table: TOE NON-IT Security Requirements versus TOE NON-IT Security Objectives.

O.PRODUCT_TRACK is the security objective implemented for the tracking of physical product (wafer lot) inside the wafer manufacturing area and inside the wafer test area. This security objective is requiring:

- 5.2.9 “Configuration Management” and 5.2.2 “Material Asset Identification”.
- 5.2.12 “Information/Material Protection Management”.

O.IC_PRT is the security objective implemented for protection of product (IC) against theft during all the manufacturing steps of the “Product Manufacturing Flow”. This security objective is covered by:

- 5.2.10 “Scrap Management”.
- 5.2.6 “Hand-Carry”.
- 5.2.11 “Password Management”.
- 5.2.1 “Secure Storage”.
- 5.2.12 “Information/Material Protection Management”.

O.PHOTOMASK_TRACK is the security objective implemented for the tracking of photomasks inside the wafer manufacturing area (“Product Manufacturing Flow” and “Photomasks Flow”). This security objective is requiring:

- 5.2.9 “Configuration Management” and 5.2.2 “Material Asset Identification”.
- 5.2.12“Information/Material Protection Management”.

O.PHOTOMASK_PRT is the security objective implemented for protection of photomasks against theft during all the manufacturing steps of the “Product Manufacturing Flow”. This security objective is covered by:

- 5.2.8 “Photomak Ordering”.
- 5.2.1 “Secure Storage” and by 5.2.5 “End Of Life”.
- 5.2.11 “Password Management” is also participating to this objective.
- 5.2.6 “Hand-Carry”.
- 5.2.10 “Scrap Management”.
- 5.2.12 “Information/Material Protection Management”.

O.TPROG_TRACK is the security objective implemented for the tracking of test program inside the wafer test area (“Product Manufacturing Flow” and “Test Program Flow”). This security objective is requiring:

- 5.2.9 “Configuration Management” and 5.2.2 “Material Asset Identification”.
- 5.2.12 “Information/Material Protection Management”.

O.TPROG_PRT is the security objective implemented for protection of test program against not authorized access during "Product Manufacturing Flow" and "Test Program Flow". This security objective is covered by:

- 5.2.1 "Secure Storage" and by 5.2.5 "End Of Life".
- 5.2.3 "Access Control".
- 5.2.4 "Non Permanence".
- 5.2.6 "Hand-Carry".
- 5.2.11 "Password Management".
- 5.2.12 "Information/Material Protection Management".

O.TDATA_PRT is the security objective implemented for protection of test results against not authorized access during "Product Manufacturing Flow". This security objective is covered by:

- 5.2.1 "Secure Storage".
- 5.2.3 "Access Control".
- 5.2.11 "Password Management".
- 5.2.7 "Data Back-Up".
- 5.2.12 "Information/Material Protection Management".

8.3.3 TOE Environment Security Requirements Rationale

		TOE ENVIRONMENT SECURITY OBJECTIVES
		O.AREA_PRT
TOE ENVIRONMENT SECURITY REQUIREMENTS	"Individual Non-Disclosure Agreement" 5.3.1	X
	"New Employee Enrolment" 5.3.2	X
	"Smartcard Employee Separation" 5.3.3	X
	"Individual Identification & Authentication" 5.3.4	X
	"Access Control Management" 5.3.5	X
	"Passwords management" 5.3.6	X
	"Smartcard Security Failure Report & Corrective Actions" 5.3.7	X
	Secure Site Information System 5.3.8	X

Table: TOE Environment Security Requirements versus TOE Environment Security Objectives.

O.AREA_PRT is the security objective requiring the TOE to be operated in a secure environment and area where the TOE is located to be accessible only to authorized personnel. The area where the TOE ("Production Flow") is located are the wafer manufacturing area and the wafer test area. This objective is covered by:

- 5.3.2 "New Employee Enrolment" Manual, 5.3.1 "Individual Non-Disclosure Agreement" Manual, 5.3.3 "Smartcard Employee Separation" Manual and by 5.3.8 "Secure Information System".
- 5.3.4 "Individual Identification & Authentication" Manual, 5.3.5 "Access Control Management" Manual and by 5.3.6 "Passwords Management" Manual.
- 5.3.7 "Smartcard Security Failure Report & Corrective Actions" SOP.

8.4 Organizational Security Policies Rationale

The Organizational Security Policies have been traced to the TOE NON-IT security requirements and to the TOE Environment security requirements as shown per the table hereafter:

This Table is also the result of the composition of the table from paragraph 8.2.3 "Assumptions, Organizational Security Policies and Objectives Rationale" (Except for the TOE IT Security Objectives), paragraph 8.3.2 "TOE Non-IT Security Requirements Rationale" and from paragraph 8.3.3 "TOE Environment Security Requirements Rationale".

This table is also showing the security requirements (TOE Non-IT and Environment) that shall be implemented to support security to the TOE. It is also showing the security requirements, and only these requirements were kept, needed to be managed at subcontractor' s to allow to later maintain the security to the TOE, when the contracted material is in place in the "Production Flow".

		ORGANIZATIONAL SECURITY POLICIES					
		"Smartcard Specification System" OSP	"Smartcard Master Security Audit" OSP	"Smartcard Subcontractor Approval" OSP	"Smartcard Subcontractor Mangement" OSP	"Smartcard Security Failure Report & Corrective Actions" OSP	"Smartcard Security Change Management" OSP
TOE NON-IT & ENVIRONMENT	**Secure Storage 5.2.1**	X	X			X	X
	Material Asset Identification 5.2.2	X	X	X	X	X	X
	Access Control 5.2.3	X	X			X	X
	Non Permanence 5.2.4	X	X			X	X
	End Of Life 5.2.5	X	X			X	X
	Hand-Carry 5.2.6	X	X			X	X
	Data Back-Up 5.2.7	X	X			X	X
	Photomask Ordering 5.2.8	X	X			X	X
	Configuration Management 5.2.9	X	X	X	X	X	X
	Scrap Management 5.2.10	X	X			X	X

	Passwords management 5.2.11	X	X			X	X
	Information/Material Protection Management 5.2.12	X	X	X	X	X	X
	"Individual Non Disclosure Agreement" 5.3.1	X	X			X	X
	"New Employee Enrolment" 5.3.2	X	X			X	X
	"Smartcard Employee Separation" 5.3.3	X	X			X	X
	"Individual Identification & Authentication" 5.3.4	X	X			X	X
	"Access Control Management" 5.3.5	X	X			X	X
	"Passwords Management" 5.3.6	X	X			X	X
	"Smartcard Security Failure Report & Corrective Actions" 5.3.7	X	X			X	X
	Secure Site Information System 5.3.8	X	X			X	X

Table: TOE NON-IT Security Requirements and TOE Environment Security Requirements versus Organizational Security Policies.

"Smartcard Specification System" is the Organizational Security Policy defining the rules to be used to write and release specifications (Manual, Other policy):

- "Smartcard Specification System" OSP is covering 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.5, 5.2.6, 5.2.7, 5.2.8, 5.2.9, 5.2.10, 5.2.11, 5.2.12, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 5.3.5, 5.3.6, 5.3.7 and 5.3.8.

"Smartcard Master Security Audit" is the Organizational Security Policy asking for the completion of a yearly security audit:

- Therefore the "Smartcard Master Security Audit" OSP is covering 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.5, 5.2.6, 5.2.7, 5.2.8, 5.2.9, 5.2.10, 5.2.11, 5.2.12, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 5.3.5, 5.3.6, 5.3.7 and 5.3.8.

"Smartcard Subcontractor Approval" is the Organizational Security Policy defining the procedure to approve a subcontractor:

- Therefore the "Smartcard Subcontractor Approval" OSP is covering 5.2.2, 5.2.9 and 5.2.12.

"Smartcard Subcontractor Management" is the Organizational Security Policy defining the procedure to control and govern the approved subcontractors:

- Therefore the "Smartcard Subcontractor Management" OSP is covering 5.2.2, 5.2.9 and 5.2.12.

"Smartcard Security Failure Report & Corrective Actions" is the Organizational Security Policy asking for notification of failure to security and requiring implementation of corrective actions:

- Therefore the "Smartcard Security Failure Report & Corrective Actions" OSP is covering 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.5, 5.2.6, 5.2.7, 5.2.8, 5.2.9, 5.2.10, 5.2.11, 5.2.12, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 5.3.5, 5.3.6, 5.3.7 and 5.3.8.

"Smartcard Security Change Management" is the Organizational Security Policy defining the procedure to govern and control the changes to the Smartcard Security System:

- Therefore the "Smartcard Security Change Management" OSP is covering 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.5, 5.2.6, 5.2.7, 5.2.8, 5.2.9, 5.2.10, 5.2.11, 5.2.12, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 5.3.5, 5.3.6, 5.3.7 and 5.3.8.

8.5 Security Assurance Requirements Rationale, Evaluation Assurance Level Rationale and Assurance Augmentation Rationale

The assurance requirements of this ST are summarized hereunder:

Requirement	**Name**	**Type**
EAL1	Functionally tested	Assurance level
AVA_VLA.2	Vulnerability Analysis	Independent

EAL1 assurance level has been chosen for this ST to meet the security objectives required to the TOE and its Environment by the type of application to which the TOE and its Environment are dedicated to.

It has been asked for an EAL1 level, because some confidence in correct operation of the TOE and its associated Environment was required to protect the assets manipulated and to maintain a level of security that is compatible with the required security level and that is needed to be guaranteed by the smartcard microcontroller components fabricated within this TOE and its Environment.

An evaluation at this level provides evidence that the TOE and its Environment security functions are in a manner consistent with its documentation and that it provides useful protection against the identified threats.

While the EAL1 level provides an evaluation of the TOE and of its Environment available to NEC customers and/or potential customers, the evaluation level which includes conformance to independent testing was also augmented of an independent vulnerability analysis (AVA_VLA.2) to confirm that any potential security vulnerabilities cannot be exploited in the intended environment of the TOE.

8.6 Mutually Supportive and Internally Consistent Security Requirements

FIA_UID.2 has no dependencies.

FIA_UAU.2 has dependency with FIA_UID.1 “Timing of identification”. The FIA_UID.1 component has not been selected because it is considered that no mediated actions relative to security shall be performed by the user before he is identified.
FIA_ATD.1 has no dependencies.

FMT_SMR.1 has dependency with FIA_UID.1 “Timing of identification”. The FIA_UID.1 component has not been selected because it is considered that no mediated actions relative to security shall be performed by the user before he is identified.

FDP_ACC.2 has dependency with FDP_ACF.1 “Security attribute based access control”. Dependency is satisfied.

FDP_ACF.1 has dependency with FDP_ACC.1 “Subset access control” and with FMT_MSA.3 “Static attribute initialization”.
Dependency with FDP_ACC.1 is considered to be satisfied, because component FDP_ACC.2 “Complete access control”, hierarchical to FDP_ACC.1, has been chosen. FMT_MSA.3 component has not been selected because it is considered that within the information system used by the TOE no default value is being used for the security attributes. However, component FMT_MSA.1 is used for a security attribute management purpose where the access control security function policy is always enforced and where the responsibility of attributes management is allowed only to an identified role (the administrator). Therefore, FMT_MSA.3 will not have any value added.

FMT_MSA.1 has dependency with FDP_ACC.1 “Subset access control” and with FMT_SMR.1 “Security roles”.

Dependency with FDP_ACC.1 is considered to be satisfied, because component FDP_ACC.2 “Complete access control”, hierarchical to FDP_ACC.1, has been chosen. Dependency with FMT_SMR.1 is satisfied.

FMT_MOF.1 has dependency with FMT_SMR.1 “Security Roles”. Dependency is satisfied.

FAU_ARP.1 has dependency with FAU_SAA.1 “Potential violation analysis”. Dependency is satisfied.

FAU_SAA.1 has dependency with FAU_GEN.1 “Audit data generation”. Dependency is satisfied.

FAU_GEN.1 has dependency with FPT_STM.1 “Reliable Time Stamps”. Dependency is satisfied.

FPT_STM.1 has no dependency.

Therefore the above dependencies analysis for the functional requirements demonstrates mutual support and internal consistency between these functional requirements.

EAL1 is an established set of mutually supportive and internally consistent assurance requirements.
The dependencies analysis for the additional assurance component AVA_VLA.2 “Independent vulnerability analysis” is showing mutually supportive and internally consistency because satisfied by EAL1 level for:

- ADV_FSP.1 “Informal functional specification”.
- AGD_ADM.1 “Administrator guidance”.
- AGD_USR.1 “User guidance”.

For dependencies with components ADV_HLD.2 “Security enforcing high level design”, ADV_IMP.1 “Subset of the implementation of the TSF” and ADV_LLD.1 “Descriptive low level design”, these components have not been selected because the aim of AVA_VLA.2 is to provide an independent vulnerability analysis to confirm the resistance of the TOE, which is a production flow, to penetration attacks performed by attackers possessing a basic attack potential.

In addition, AVA_VLA.2 is relevant for an evaluation assurance level claiming 4 (EAL4), while this ST is only claiming conformance to level EAL1 (augmented with AVA_VLA.2) of CC. This is another reason for not taking into account the above set of assurance components ADV_HLD.2, ADV_IMP.1 and ADV_LLD.1.

8.7 Assumptions Rationale

A.SEC_DEL: It has been assumed that secure delivery occurred between supplier of photomasks and “Production Flow” and between supplier of test program and “Production Flow”.

A.TRUST_PHOTOMASKS: It has been assumed that photomasks, that are supplied to the “Production Flow”, can be trusted on security aspects.

A.TRUST_TPROG: It has been assumed that test program that is supplied to the “Test Program Flow”, can be trusted on security aspects.

A.SKL_PERSONNEL: It has been assumed that personnel involved in the smartcard production operations have got the required skills and have been educated to the security rules to be used and that they are following these rules.

8.8 TOE Summary Specification Rationale

8.8.1 TOE Security Functions Rationale

		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	FAU_ARP.1	FAU_SAA.1	FAU_GEN.1	FPT_STM.1
TOE	SF1	X	X		X	X	X	X	X				
	SF2	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**				
	SF8									**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**				

Table: Statement of TOE Security Functions

FIA_UID.2: User Identification before any Action

FIA_UID.2 security functional requirement is covered by the “HP-UX” **Login** security function (SF1).

FIA_UID.2 security functional requirement is covered by the “Production Management Software” **Access Control** security function (SF2).

FIA_UID.2 security functional requirement is covered by the “HP-UX” **Attribute Manager** security function (SF3).

FIA_UID.2 security functional requirement is covered by the “Windows NT” **Logon** security function (SF9).

FIA_UID.2 security functional requirement is covered by the “Windows NT” **Security Identifier (SID)** security function (SF10).

FIA_UAU.2: User Authentication before any Action

FIA_UAU.2 security functional requirement is covered by the “HP-UX” **Login** security function (SF1).

FIA_UAU.2 security functional requirement is covered by the “Production Management Software” **Access Control** security function (SF2).

FIA_UAU.2 security functional requirement is covered by the “HP-UX” **Attribute Manager** security function (SF3).

FIA_UAU.2 security functional requirement is covered by the “Windows NT” **Logon** security function (SF9).

FIA_UAU.2 security functional requirement is covered by the “Windows NT” **Security Identifier (SID)** security function (SF10).

FIA_ATD.1: User Attribute Definition

FIA_ATD.1 security functional requirement is covered by the “HP-UX” **Attribute Manager** security function (SF3).

FIA_ATD.1 security functional requirement is covered by the “Windows NT” **Security Identifier (SID)** security function (SF10).

FMT_SMR.1: Security Roles

FMT_SMR.1 security functional requirement is covered by the “HP-UX” **Login** security function (SF1).

FMT_SMR.1 security functional requirement is covered by the “HP-UX” **Attribute Manager** security function (SF3).

FMT_SMR.1 security functional requirement is covered by the “HP-UX” **Admin** security function (SF4).

FMT_SMR.1 security functional requirement is covered by the “Windows NT” **Logon** security function (SF9).

FMT_SMR.1 security functional requirement is covered by the “Windows NT” **Security Identifier (SID)** security function (SF10).

FMT_SMR.1 security functional requirement is covered by the “Windows NT” **User Account Manager** security function (SF11).

FDP_ACC.2: Complete Access Control

FDP_ACC.2 security functional requirement is covered by the “HP-UX” **Login** security function (SF1).

FDP_ACC.2 security functional requirement is covered by the “Production Management Software” **Access Control** security function (SF2).

FDP_ACC.2 security functional requirement is covered by the “HP-UX” **Attribute Manager** security function (SF3).

FDP_ACC.2 security functional requirement is covered by the “HP-UX” **Admin** security function (SF4).

FDP_ACC.2 security functional requirement is covered by the “HP-UX” **File/Command Property** security function (SF5).

FDP_ACC.2 security functional requirement is covered by the “HP-UX” **Rights Manager** security function (SF7).

FDP_ACC.2 security functional requirement is covered by the “Windows NT” **Logon** security function (SF9).

FDP_ACC.2 security functional requirement is covered by the “Windows NT” **Security Identifier (SID)** security function (SF10).

FDP_ACC.2 security functional requirement is covered by the “Windows NT” **User Account Manager** security function (SF11).

FDP_ACC.2 security functional requirement is covered by the “Windows NT” **Owner** security function (SF12).

FDP_ACC.2 security functional requirement is covered by the “Windows NT” **Security Account Manager** security function (SF13).

FDP_ACF.1: Security Attribute Based Access Control

FDP_ACF.1 security functional requirement is covered by the “HP-UX” Login security function (SF1).

FDP_ACF.1 security functional requirement is covered by the “Production Management Software” **Access Control** security function (SF2).

FDP_ACF.1 security functional requirement is covered by the “HP-UX” **Attribute Manager** security function (SF3).
FDP_ACF.1 security functional requirement is covered by the “HP-UX” **Admin** security function (SF4).

FDP_ACF.1 security functional requirement is covered by the “HP-UX” **File/Command Property** security function (SF5).

FDP_ACF.1 security functional requirement is covered by the “HP-UX” **Rights Manager** security function (SF7).

FDP_ACF.1 security functional requirement is covered by the “Windows NT” **Logon** security function (SF9).

FDP_ACF.1 security functional requirement is covered by the “Windows NT” **Security Identifier (SID)** security function (SF10).

FDP_ACF.1 security functional requirement is covered by the “Windows NT” **User Manager** security function (SF11).

FDP_ACF.1 security functional requirement is covered by the “Windows NT” **Owner** security function (SF12).

FDP_ACF.1 security functional requirement is covered by the “Windows NT” **Security Account Manager (SAM)** security function (SF13).

FMT_MSA.1: Management of Security Attributes

FMT_MSA.1 security functional requirement is covered by the “HP-UX” **Login** security function (SF1).

FMT_MSA.1 security functional requirement is covered by the “Production Management Software” **Access Control** security function (SF2).

FMT_MSA.1 security functional requirement is covered by the “HP-UX” **Attribute Manager** security function (SF3).

FMT_MSA.1 security functional requirement is covered by the “HP-UX” **Admin** security function (SF4).

FMT_MSA.1 security functional requirement is covered by the “HP-UX” **File/Command Property** security function (SF5).

FMT_MSA.1 security functional requirement is covered by the “HP-UX” **File Configuration** security function (SF6).
FMT_MSA.1 security functional requirement is covered by the “HP-UX” **Rights Manager** security function (SF7).

FMT_MSA.1 security functional requirement is covered by the “Windows NT” **Logon** security function (SF9).

FMT_MSA.1 security functional requirement is covered by the “Windows NT” **Security Identifier (SID)** security function (SF10).

FMT_MSA.1 security functional requirement is covered by the “Windows NT” **User Account** security function (SF11).

FMT_MSA.1 security functional requirement is covered by the “Windows NT” **Owner** security function (SF12).

FMT_MSA.1 security functional requirement is covered by the “Windows NT” **Security Account Manager (SAM)** security function (SF13).

FMT_MOF.1: Management of Security Functions Behavior

FMT_MOF.1 security functional requirement is covered by the “HP-UX” **Login** security function (SF1).

FMT_MOF.1 security functional requirement is covered by the “HP-UX” **Attribute Manager** security function (SF3).

FMT_MOF.1 security functional requirement is covered by the “HP-UX” **Admin** security function (SF4).

FMT_MOF.1 security functional requirement is covered by the “HP-UX” **File/Command Property** security function (SF5).

FMT_MOF.1 security functional requirement is covered by the “HP-UX” **File Configuration** security function (SF6).

FMT_MOF.1 security functional requirement is covered by the “HP-UX” **Rights Manager** security function (SF7).

FMT_MOF.1 security functional requirement is covered by the “Windows NT” **Logon** security function (SF9).

FMT_MOF.1 security functional requirement is covered by the “Windows NT” **Security Identifier (SID)** security function (SF10).

FMT_MOF.1 security functional requirement is covered by the “Windows NT” **User Account Manager** security function (SF11).

FMT_MOF.1 security functional requirement is covered by the “Windows NT” **Owner** security function (SF12).

FMT_MOF.1 security functional requirement is covered by the “Windows NT” **Security Account Manager (SAM)** security function (SF13).

FAU_ARP.1: Security Alarms

FAU_ARP.1 security functional requirement is covered by the "Production Management Software" **Transfer Time Alarm** security function (SF8).

FAU_SAA.1: Security Audit Analysis

FAU_SAA.1 security functional requirement is covered by the "Production Management Software" **Transfer Time Alarm** security function (SF8).

FAU_GEN.1: Audit Data Generation

FAU_GEN.1 security functional requirement is covered by the "Production management Software" **Transfer Time Alarm** security function (SF8).

FPT_STM.1: Reliable Time Stamp

FPT_STM.1 security functional requirement is covered by the "Production Management Software" **Transfer Time Alarm** security function (SF8).

8.8.2 TOE Security Assurance Measures Rationale

		EAL1+ Security Assurance Measures:							
		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 Securit	ST Statement	X						X	
	AM1		X						
	AM2		X			X	X		
	AM3			X					

	AM4			**X**					
	AM5				**X**				
	AM6				**X**				
	AM7					**X**	**X**		
	AM8								**X**
	AM9								**X**
	AM10		**X**				**X**		
	AM11		**X**				**X**		
	AM12		**X**						
	AM13					**X**			
	AM14			**X**					
	AM15				**X**				

Table: Statement of TOE Assurance measures

ACM_CAP.1: Version Numbers

ACM_CAP.1 security assurance requirement is covered by the **Security Target Statement** assurance measure.

ADO_IGS.1: Installation, Generation and Start-up Procedures

ADO_IGS.1 security assurance requirement is covered by:

- **AM1**.
- **AM2**.
- **AM10**.
- **AM11**.
- **AM12**.

ADV_FSP.1: Informal Functional Specification

ADV_FSP.1 security assurance requirement is covered by:

- **AM3**.
- **AM4**.
- **AM14**.

ADV_RCR.1: Representation Correspondence

ADV_RCR.1 security assurance requirement is covered by:

- **AM5**.
- **AM6**.
- **AM15**.

AGD_ADM.1: Administrator Guidance

AGD_ADM.1 security assurance requirement is covered by:

- **AM2**.
- **AM7**.
- **AM13**.

AGD_USR.1: User Guidance

AGD_USR.1 security assurance requirement is covered by:

- **AM2**.
- **AM7**.
- **AM10**.
- **AM11**.

ATE_IND.1: Independent Testing - Conformance

ATE_IND.1 security assurance requirement is covered by the Security Target Statement assurance measure.

Augmentation Assurance Component

AVA_VLA.2: Independent Vulnerability Analysis

AVA_VLA.2 security assurance requirement is covered by:

- **AM8**.
- **AM9**.

8.8.3 Non-IT Security Assurance Measures for the TOE Rationale

Secure Storage Procedure (6.3.1)

Is the security measure corresponding to the **"Secure Storage (5.2.1)"** security requirement.
This is a Manual or SOP (Security Operating Policy) that defines the procedure requiring the secure storage in locked shelves of smartcard product, photomasks, test programs and the storage in local host computer of test results.

Material Asset Identification Procedure (6.3.2)

Is the security measure corresponding to the **"Material Asset Identification (5.2.2)"** security requirement.
This is a Manual or SOP (Security Operating Policy) that defines the procedure requiring the unique identification of product, photomasks and test programs.

Access Control Procedure (6.3.3)

Is the security measure corresponding to the **"Access Control (5.2.3)"** security requirement.
This is a Manual or SOP (Security Operating Policy) that defines the procedure requiring the control of the access to the test equipment and to the local host (test results storage), using the identification number and password of authorized employee, before any actions is allowed to the employee.

Non Permanence Procedure (6.3.4)

Is the security measure corresponding to the **"Non Permanence (5.2.4)"** security requirement.
This is a Manual or SOP (Security Operating Policy) that defines the procedure requiring that the test programs shall not resident on test equipment and electrically erased when test operation is completed.

End of Life Procedure (6.3.5)

Is the security measure corresponding to the **"End of Life (5.2.5)"** security requirement.
This is a Manual or SOP (Security Operating Policy) that defines the procedure requiring "end of life rules" for photomasks and test programs.

Hand-Carry Procedure (6.3.6)

Is the security measure corresponding to the **"Hand-Carry (5.2.6)"** security requirement.

This is a Manual or SOP (Security Operating Policy) that defines the procedure requiring "hand-carry transportation" for transfer of smartcard wafer lots, from wafer manufacturing area to wafer test area, of photomasks and of test programs.

Data Back-up Procedure (6.3.7)

Is the security measure corresponding to the **"Data Back-Up (5.2.7)"** security requirement.
This is a Manual or SOP (Security Operating Policy) that defines the procedure requiring data back-up for test results.

Photomasks Ordering Procedure (6.3.8)

Is the security measure corresponding to the **"Photomasks Ordering (5.2.8)"** security requirement.
This is a Manual or SOP (Security Operating Procedure) that defines the procedure requiring the implementation of rules to order new photomasks, ensuring a secure identification and traceability, and allowing detection or prevention of potential theft.

Configuration Management Procedure (6.3.9)

Is the security measure corresponding to the **"Configuration Management (5.2.9)"** security requirement.
This is a Manual or SOP (Security Operating Procedure) defining the procedure that requires the control of identification for product, photomasks, test tools and test programs, and allowing to control any change that may be applied to them.

Scrap Management Procedure (6.3.10)

Is the security measure corresponding to the **"Scrap Management (5.2.10)"** security requirement.
This is a Manual or SOP (Security Operating Procedure) that defines the procedure requiring a secure control, collection, transportation and destruction of scrapped wafers and scrapped photomasks.

Passwords Management Procedure (6.3.11)

Is the security measure corresponding to the **"Passwords Management (5.2.11)"** security requirement.
This is a Manual or SOP (Security Operating Policy) that defines the procedure requiring to securely create, control and manage all the passwords for access control to computers (software), files and test results.

Information/Material Protection Management Procedure (6.3.12)

Is the security measure corresponding to the **"Information/Material Protection Management (5.2.12)"** security requirement.
This is a Manual or SOP (Security Operating Policy) that defines the procedure requiring to securely classify, identify, manage, store, handle, pack and deliver any smartcard related material (product, test programs, photomasks), test results and customer data, when applicable.

8.8.4 Security Assurance Measures for the Environment Rationale

"Individual Non Disclosure Agreement" Procedure (6.4.1)

Is the security measure corresponding to **the "Individual Non Disclosure Agreement (5.3.1)"** security requirement.
This is a Manual or SOP (Security Operating Policy) that defines the procedure requiring that every employee, working in operations related to the "Production Flow" used to manufacture the smartcard microcontroller components, has in advance signed a Non Disclosure Agreement (Individual NDA).

"New Employee Enrolment" Procedure (6.4.2)

Is the security measure corresponding to the **"New Employee Enrolment (5.3.2)"** security requirement.
This is a Manual or SOP (Security Operating Policy) that defines the procedure requiring that every new employee, before working in operations related to the "Production Flow used to manufacture the smartcard microcontroller components, has in advance followed the process in place to enlist such new personnel.

"Smartcard Employee Separation" Procedure (6.4.3)

Is the security measure corresponding to the **"Smartcard Employee Separation (5.3.3)"** security requirement.
This is a Manual or SOP (Security Operating Policy) that defines the procedure requiring that every employee, when under resignation status and who was working in operations related to the "Production Flow" used to manufacture the smartcard microcontroller components, is compliant with the smartcard employee separation process.

"Individual Identification and Authentication" Procedure (6.4.4)

Is the security measure corresponding to the **"Individual Identification and Authentication (5.3.4)"** security requirement.

This is a Manual or SOP (Security Operating Policy) that defines the procedure requiring that, in order to give or deny access to smartcard controlled areas, storage shelves, files, test programs, photomasks, test results and customer data, when applicable, every employee who is working in operations related to the "Production Flow" used to manufacture the smartcard microcontroller components, is individually identified and authenticated.

"Access Control Management" Procedure (6.4.5)

Is the security measure corresponding to the **"Access Control Management (5.3.5)"** security requirement.
This is a Manual or SOP (Security Operating Policy) that defines the procedure requiring that access rights and rules are implemented in order to control access and give access only to authorized personnel to site, areas, storage shelves, files, test programs, photomasks, test results and customer data, when applicable.

"Passwords Management" Procedure (6.4.6)

Is the security measure corresponding to the **"Passwords Management (5.3.6)"** security requirement.
This is a Manual or SOP (Security Operating Policy) that defines the procedure requiring secure creation, control and management of all the passwords used to access the controlled areas.

"Smartcard Security Failure Report & Corrective Actions" Procedure (6.4.7)

Is the security measure corresponding to the **"Smartcard Security Failure Report & Corrective Actions (5.3.7)"** security requirement.
This is a Manual or SOP (Security Operating Policy) that defines the procedure requiring notification about any occurring failure or non-conformance, definition and implementation of corrective actions in order to fix the issue and prevent its re-occurrence.

Secure Site Information System Procedure (6.4.8)

Is the security measure corresponding to the **"Secure Site Information System (5.3.8)"** security requirement.
This is a Manual or SOP (Security Operating Policy) that defines the procedure requiring that the site Information System is providing protection, against external attack or intrusion, to the TOE Information Technology.

8.9 PP Claims Rationale

No specific PP claims are made for this Security Target.

However, in order to satisfy Evaluation/Certification of product in accordance with PP/9806 Version 2.0 and its claimed Evaluation Assurance Level (EAL4 augmented), the present Security Target is made fully compliant with all the requirements from PP/9806 Version 2.0, involving the Environment of product under manufacturing. This Environment for manufacturing phase (phase 3), described in PP/9806 Version 2.0, corresponds to the content of this Security Target.

The compliance and coverage of the present Security Target to the requirements of PP/9806 Version 2.0 are explained into the section of this Security Target with the chapters entitled “Conformance to PP/9806 Version 2.0 - Phase 3 (Manufacturing Phase)”:

- Assumptions of present Security Target are compliant to Assumptions of PP/9806 Version 2.0. See paragraph 3.4 of this Security Target.
- Threats of present Security Target are compliant to Threats of PP/9806 Version 2.0. See paragraph 3.6 of this Security Target.
- Organizational Security policies of present Security Target are compliant to Organizational Security Policies of PP/9806 Version 2.0. See paragraph 3.8 of this Security Target.
- Security Objectives of present Security Target are compliant to Security Objectives of PP/9806 Version 2.0. See paragraph 4.4 of this Security Target.

ANNEX A: DEFINITIONS AND ACRONYMS

AMx: Assurance Measure number x.
CC: Common Criteria.
CISC: Complex Instruction Set Computer.
CPU: Central Processor Unit.
DMP: Data Management Platform.
EAL: Evaluation Assurance Level.
EEPROM: Electrically Erasable Programmable Read Only Memory.
GPC: General Purpose Client.
IT: Information Technology.
OS: Operating System.
PC: Personal Computer.
PP: Protection Profile.
RAM: Random Access Memory.
RISC: Reduced Instruction Set Computer.
ROM: Read Only Memory.
SCAC: SmartCard Application Center.
SFR: Security Functional Requirement.
SFx: Security Function number x.
SiO2: Silicon Dioxide.
SOP: Security Operating Policy.
ST: Security Target.
TOE: Target Of Evaluation.