JICSAP ver.2.0 Protection Profile part 1

Multi-Application Secure System LSI Chip

Protection Profile

Version: **2.5**

Date: **June 6, 2003**

Issuers: **Japan IC Card System Application Council**

Authors: **Electronic Commerce Security Technology Research Association**

Table of contents

1. PP introduction 4
   1.1 PP identification 4
   1.2 PP overview 5
   1.3 Assurance level and SOF 5
   1.4 Related standards and documents 6
   1.5 Related protection Profiles 6
   1.6 Organisation of this document 6
2. TOE Description 8
   2.1 Configuration of the TOE 8
   2.2 Areas of application of the IC (Example) 10
3. TOE Security Environment 12
   3.1 Assets 12
   3.2 Assumptions 13
   3.3 Threats 13
   3.4 Organisational security policies 15
4. Security Objectives 16
   4.1 Security objectives for the TOE 16
   4.2 Security objectives for the environment 17
5. IT Security Requirements 18
   5.1 TOE security requirements 18
      5.1.1 TOE security functional requirements 18
      5.1.2 Explicitly stated security functional requirements 23
      5.1.3 TOE security assurance requirements 23
      5.1.4 Minimum strength of function (SOF) Claim 25
   5.2 Security requirements for the IT environment 25
6. Rationale 26
   6.1 Security objectives rationale 26
   6.2 Security requirements rationale 27
   6.3 Rationale on IT security requirements that do not satisfy dependency 30

6.4 Suitability of minimum strength of function (SOF) level 30

6.5 Appropriateness of TOE assurance requirements 30

6.6 Mutual support of security requirements 31

6.7 Rational for explicitly stated IT security requirements 31

7. Annex 33

7.1 Glossary 33

7.2 The process of design and manufacture to completion of a smart card 35

7.3 PP application note 37

7.3.1 Handling of the software used for quality test 37

7.3.2 Handling of i/o Ports 38

7.3.3 ST of products coated with package resin 38

7.3.4 Comments on the ADV Class 40

7.3.5 Reliability of memories 42

7.3.6 Comments on the ATE Class 42

Table 6-1 Security objectives rationale 26

Table 6-2 Objectives-Functional Requirements rationale 27

Table 6-3 Dependencies 29

Table 6-4 The mutually supportive functional requirements for each objective 31

Figure 2-1 Longitudinal Cross Section of an IC Package 8

Figure 2-2 Conceptual Block Diagram of an IC 9

Figure 2-3 Hardware/ Software Structure of an IC card 10

Figure 2-4 Example of the Use of IC: Smart Card 11

Figure 7-1 From Manufacturing to Use of a Smart Card 35

Figure 7-2 Picture of Packaging 36

Figure 7-3 Picture of Card Production 36

Figure 7-4 i/o Ports and Lead Frame Contacts 38

Figure 7-5 Relationship among PP, ST and ADV Class 41

1. PP introduction

1.1 PP identification

Title:	JICSAP ver2.0 Protection Profile part1, Multi-Application Secure System LSI Chip Protection Profile
Date:	June 6, 2003
Version:	2.5
Issuers:	Japan IC Card System Application Council
Authors:	Electronic Commerce Security Technology Research Association
TOE:	LSI chip
Registration:	TBD

This PP is English version of "Multi-Application Secure System LSI Chip Protection Profile" issued by Information Technology Promotion Agency in Japanese on August 29, 2002.

The issuer of this PP, Japan IC Card System Application Council got the right to translate and modify original PP from Information Technology Promotion Agency, and added necessary modification to let the original PP adapt to JICSAP ver2.0 smartcard specification in English. So, the title of this PP is named as JICSAP ver2.0 Protection Profile. Besides, Japan IC Card System Application Council is planning to make PP for IC Card OS conforms to JICSAP ver2.0 smartcard specification may be named as JICSAP ver2.0 Protection Profile part 2. So, the title of this PP is named as JICSAP ver2.0 Protection Profile part 1.

All responsibility for above translation and modification will be taken by the issuer, Japan IC Card System Application Council.

This PP is in conformance with Common Criteria for Information Technology Security Evaluation; Version 2.1 (hereafter referred to as [CC])

Which comprises

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.1 (hereafter referred to as [CC part1])

Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.1 (hereafter referred to as [CC part2])

Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.1 (hereafter referred to as [CC part3])

And, the

Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology; Version 1.0, August 1999 (hereafter referred to as [CEM])

has been taken into account.

Application note (for Japanese user):

This PP is in compliant to Japanese Industrial Standard JIS X 5070 (validated on July 20, 2000).

Although JIS X 5070 is the Japanese translation of ISO/IEC 15408, ISO/IEC 15408 Part 2 (Security Functional Requirements) and Part 3 (Security Assurance Requirements) are just summarized in Japanese and thus the details are referenced in English from ISO/IEC 15408 Part 2 and Part 3.

For this reason, as with the JIS standard, this PP references the English version of ISO/IEC 15408 with respect to such parts described in ISO/IEC 15408 but not in JISX5070. However, giving for the user convenience, Japanese translations by the Information Technology Promotion Agency are attached to the parts referenced in English explained above, in Japanese version of this PP.

1.2 PP overview

This PP describes the security requirements for system LSI chips (hereafter referred to as IC) which have processing unit (CPU: Central Processing Unit), memories (EEPROM, ROM, FeRAM, SRAM, DRAM, etc.), co-processor and others. The IC could include various libraries such as crypto library and test software.

IC is applied widely from home electronics to industrial machines but the software incorporated into the memories and the circuit configuration (wiring between the memories and processing unit, signal wires for external linkage, etc.) differ by the area of application. The ICs that are targeted by this PP are chips with memories and the circuit configuration equipped with security mechanisms in order to enhance the security of the IC application.

The following are some examples of security mechanisms implemented on the IC.

- Identity authentication
- Encryption of data, digital signature
- Access control to stored data

These ICs are incorporated into various products. Examples of applications ICs targeted by this PP include smart cards and mobile phones incorporating a security mechanism.

1.3 Assurance level and SOF

The assurance level for this PP is EAL4 augmented. Augmentation results from the selection of:

AVA_CCA.1: Covert channel analysis

AVA_VLA.4: Vulnerability Assessment – Vulnerability Analysis –Highly resistant

The minimum strength of security functions for the TOE is SOF-high (Strength of Functions High).

1.4 Related standards and documents

- [CC]
- [CEM]
- JIS X 5070 Security Technology – Evaluation Criteria for Information Technology Security
- JIS X 6300 Series IC Cards with Contacts
- JIS X 6322 Series Contactless IC Cards, Proximity Cards
- 3GPP TS Series Subscriber Identity Module (SIM)
- ISO/IEC 15408 – Information Technology – Security Techniques – Evaluation Criteria for IT Security
- ISO/IEC 7810 – Identification Cards – Physical Characteristics
- ISO/IEC 7816 – Identification Cards – Integrated Circuit Cards with Contacts
- ISO/IEC 14443 (draft) – Contactless Integrated Circuit Cards, Proximity Cards

1.5 Related protection Profiles

- Protection Profile Smartcard Integrated Circuit; Version 2.0, Sep 1998 (PP/9806)
- Protection Profile Smartcard IC with Embedded Software; Version 2.0, Jun 1999 (PP/9911)
- Protection Profile Smartcard IC with Multi-Application Secure Platform; Version 2.0, Nov 2000 (PP/0010)
- Smartcard IC Platform Protection Profile; Version 1.0, Jul 2001-10-17 (BSI-PP-0002)
- Smart Card Security User Group Smart Card Protection Profile; Draft Version 2.1d, Mar 21 2001
- ICCS Smart Card Protection Profile V1.0 (not yet certified)

1.6 Organisation of this document

Chapter 1, PP Introduction, describes an overview of this PP, the assurance level and related documents.

Chapter 2, TOE Description, provides the hardware structure of the IC that is the TOE of this PP and the smart card that is an application of the IC and states the importance of security.

Chapter 3, TOE Security Environment, describes the assets and four threats defined in this PP.

Chapter 4, Security Objectives, describes the four security objectives for the TOE.

Chapter 5, Security Requirements, describes the thirteen security functional requirements, one explicitly stated security functional requirements and the EAL4 augmented assurance requirements as the security requirements of the TOE.

Chapter 6 , Rationale, describes the security objectives rationale, functional requirements rationale and the rationale with respect to functional requirements that do not satisfy dependency, and PP Application Notes, describes matters to be noted upon production of the ST and preparing deliverables, and so on.

Chapter 7, Annex, describes glossary, the process of design and manufacture to completion of a smart card and efficiency of product evaluation.

2. TOE Description

2.1 Configuration of the TOE

The TOE for this PP is IC. In that case, only the hardware and the hardware dedicated software will be evaluated, all other software / algorithm is out of the scope. The hardware dedicated software may be composed of test software and/or various libraries such as crypto-library. Figure 2-1 shows a cross section of an IC. The TOE seen from the longitudinal cross section is comprised of the lowermost layer and middle layer and does not include the topmost layer. The IT functions of the TOE are data storing and data processing function.

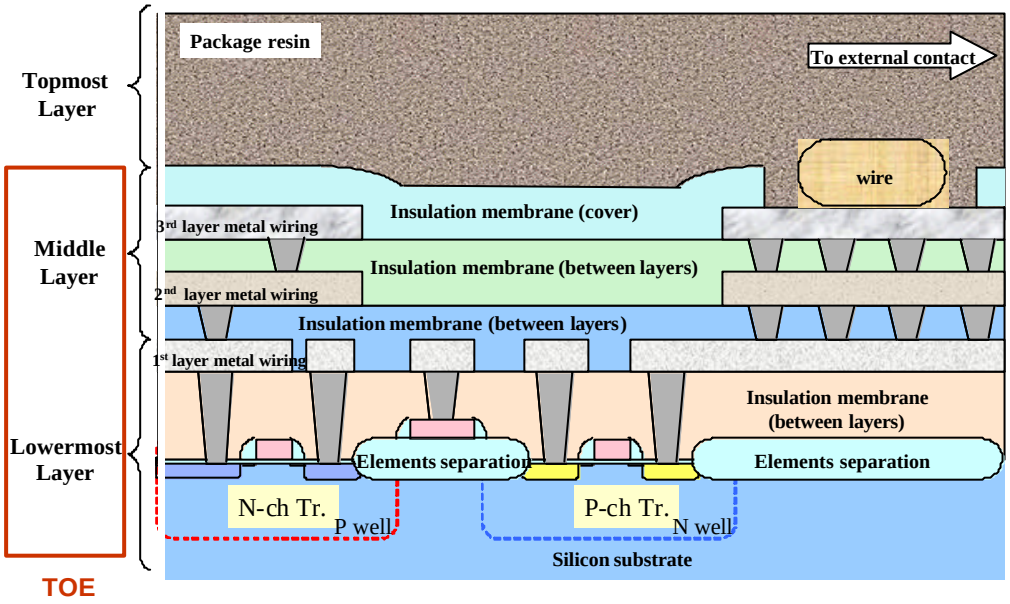

Figure 2-1 Longitudinal Cross Section of an IC Package

As describe above, the topmost layers are not included in the TOE. In that case, the resin could not be include as a part of the TOE.

The conceptual representation of a block diagram when the TOE is seen from above is shown in Figure 2-2. The size is several millimetres high and several millimetres wide (Note). The major electronic elements that comprise an IC are as follows.

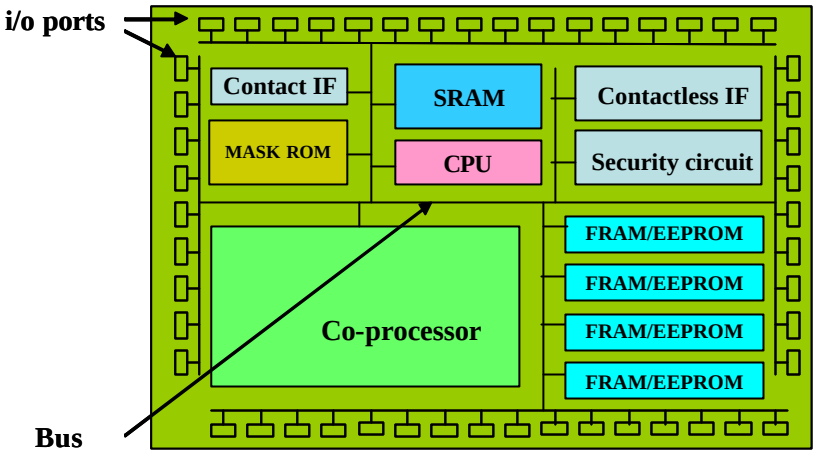

Figure 2-2 Conceptual Block Diagram of an IC

1. Processing unit that processes the data (CPU)
2. MASK ROM that is used for reading only, basic software or basic data that is written upon manufacture of the IC
3. Non-volatile memory to which data may be electronically written after manufacture of the IC (FeRAM, EEPROM, etc.)
4. Volatile memory that is used as work area for data processing, and loses stored data when power is no longer supplied(SRAM, DRAM, etc.).
5. Security circuit (Random number generator, Sensors, Tampering function, etc.)
6. Co-processor used for encryption, digital signatures, etc.

Such as security function 5, 6 are used for secure IT functions to protect data in the usage phase.

Contact interface/ Contactless interface that converts external data to data for internal processing

These elements given as examples are connected by various bus wires. Moreover, they are connected to i/o ports for exchanging data externally. The TOE of this PP is composed of these processing unit, memories, electronic circuits, and the hardware dedicated software (may be composed of test software and/or various libraries such as crypto-library).

Note) Figure 2-2 provides an example of the electronic circuit of an IC in order to deepen knowledge on the TOE. The processing units, memories, electronic circuits and other devices mounted on an IC are multiple layered and are composed of various elements.

Basic software (OS: Operating System) that is common to the area of application of the IC or application programs unique to the area of application are stored in the memories. Figure 2-3 shows the relationship among hardware (memories, processing units, etc.), software and application. The TOE of this PP is the hardware and the hardware dedicated software, and does not include basic software or application programs. In other words, the security requirements of this PP centre on measures having to do with hardware to respond to physical attacks (probing, attacks as light based and/or temperature, frequency, etc.) on the IC.

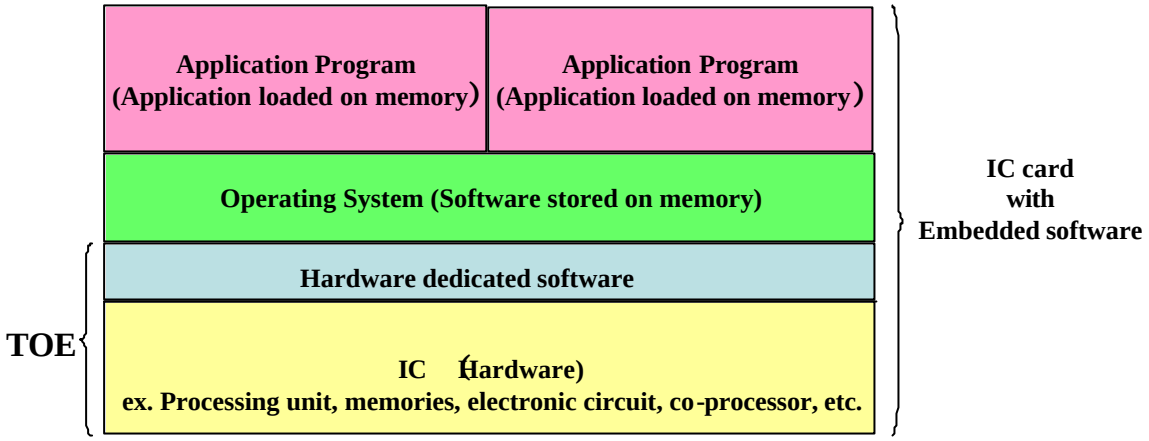

Figure 2-3 Hardware/ Software Structure of an IC card

2.2 Areas of application of the IC (Example)

The areas of application of IC are diverse and the basic software and application programs stored differ by the area of application. In particular, in the event the product incorporating the IC is to be delivered and used by consumers, it is difficult to manage the environment of use for both the manufacturer of the IC and the party procuring the IC. In other words, the environment is one that may be open to various threats. With respect to the IC targeted by this PP, the application programs or data themselves have value and in addition to this, the area of application is one in which tampering or theft of the programs or data can be expected to lead to enormous loss. An example of such an area of application is the smart card.

However, the fact that appropriate hardware protection is implemented for the IC is a condition precedent for ensuring that the OS, application program and data are not physically tampered with or stolen in order that these services may be provided safely.

It is possible to equip the IC incorporated into a smart card with a security function that confirms the validity of the card user or terminal, integrity of the data exchanged between the smart card and a terminal, confidentiality, access control to the stored data and other such functions. (Refer to Figure 2-4.)

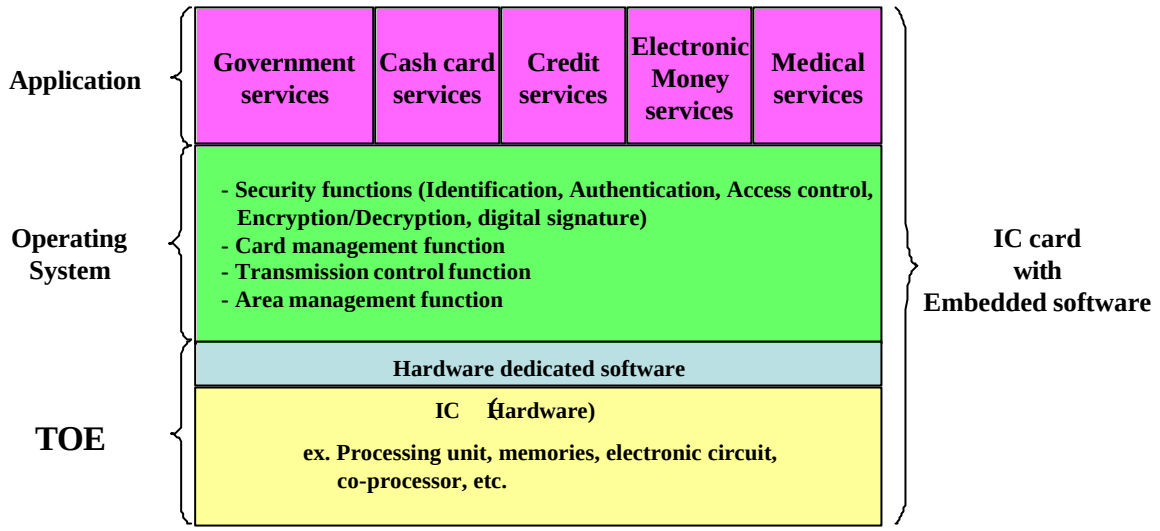

Figure 2-4 Example of the Use of IC: Smart Card

As a result of such security functions, the following services may be provided with greater security.

- Resident's card: Provision of various government services to the resident (such as issue of official seal certification)
- Bank card: Provision of services related to withdrawal from accounts and real time settlement to the account holders
- Credit card: Provision of services related to cashing, shopping and deferred payment to the credit card holders
- Electronic purse: A safe storage medium for electronic money
- Medical card: A storage medium for clinical information that can control access by function to physicians, nurses and patients

3. TOE Security Environment

3.1 Assets

The TOE of this PP is, as stated in Chapter 2, composed of such hardware as processing unit, memories and electronic circuit, and the hardware dedicated software. All other software stored in the memories is outside the scope of the TOE. This PP considers the assets that the TOE must protect to be user data, TSF data, and program code of hardware dedicated software. Abovementioned user data is the user data for TOE, so the user data specified in this PP contains user data for basic software or application programs, TSF data for basic software or application programs, program code of basic software, and program code of application programs. (Note)

Note) The term assets as used in this PP refers to the target of attack in the event an attacker launches a physical attack (probing, attacks as light based and/or temperature, frequency, etc.) on the IC. Depending on the design and manufacturing technology of an IC, electronic parts other than those stated in this document may be mounted. In the event such parts may become the target of physical attack, they are considered assets in this PP.

The following is a list of major processing unit and memories.

- CPU (Central Processing Unit) / Co-processor
- EEPROM (Electrically Erasable Programmable Read Only Memory)
- ROM (Read Only Memory)
- Flash memory
- FeRAM (Ferroelectric Random Access Memory)
- SRAM (Static Random Access Memory)
- DRAM (Dynamic Random Access Memory)

Bus wires may be data bus, address bus, clock bus and control bus (chip select and R/W). Moreover, i/o ports may be power/GND., clock and data input output contacts and are used, in addition to the input and output of application data, for such processes as testing, maintenance, input of keys and program loading.

Application note:

The fundamental stand of this PP toward the life cycle is as follows. It is sufficient to get the TOE which is guaranteed security at the end user phase regardless of phase such as development phase and manufacturing phase. So, it is not necessary to describe the detailed life cycle in this PP. And, critical interfaces (e.g. ES delivery, Module assembly, etc.) properly covered by security assurance requirements.

3.2 Assumptions

As mentioned in chapter 2.2, the areas of application of TOE(IC) are diverse and the basic software and application programs stored differ by the area of application. In particular, in the event the product incorporating the TOE(IC) is to be delivered and used by consumers, it is difficult to manage the environment of use for both the manufacturer of the IC and the party procuring the IC. In other words, the environment is one that may be open to various threats. With respect to the TOE(IC) targeted by this PP, the application programs or data themselves have value and in addition to this, the area of application is one in which tampering or theft of the programs or data can be expected to lead to enormous loss.

And, as mentioned in chapter 2.1, security functions are used for secure IT functions to protect data in the usage phase.

Therefore, security aspects related to development phase and manufacturing phase are properly covered by security assurance requirements. And, as the security aspects related to usage phase are properly covered by those security functions regardless of any using manner, assumptions related to usage phase is none.

So, no assumption has been defined in the scope of this PP.

3.3 Threats

Physical attacks on an IC are not isolated and in many cases, multiple methods are repeated on a trial and error basis in order to access the internal information (that is the data in the memories that store user data, TSF data, program code of software, and the data which are transmitted for processing flowing through the route). Moreover, in the event the data that are the target of attack comprise the encryption keys, the IC may be subjected to destructive attack but when the data consist of electronic money that itself has value, and the objective of the attack is modification of such data, the attack is not destructive. These electronic money and value are attractive for attacker, so this will be a motivation for the attacker who performs the following attacks.

1. T.Micro_attack

   The expert attacker who knows the semiconductor knowledge may perform physical attack on an IC from which the package resin or insulation coating has been removed to investigate the internal information or modify the internal information or cut the bus wires or reconnect the bus wires, using bespoke equipments.

   Application note:

   Two types of attack are conceivable with respect to IC from which the package resin or insulation coating has been removed.

   FIB (Focused Ion Beam) workstation, EBP (Electronic Beam Prober), AFM (Atomic Force Microscope) and other such methods are used for reverse engineering to infer the IC design information (circuit information, etc.) or the content of the storage elements or to steal the data flowing through the various bus wires. Also, at least, systems based on mechanical probes, Lasers, and photos could be used in the same way.

The other type is to expose an ion beam using, as examples, a FIB workstation, a Laser, a SEM, to alter the content of the memories or change specific circuits (recovery of the test circuit used for quality check and/or disablement of the security circuit).

2. T. Covert_channel

The proficient attacker who knows the cryptographic knowledge and circuit knowledge may analyse the internal processing information of the IC that is output from the covert channel in order to attempt to infer the data in the memory that are meaningful from the perspective of security, using standard equipments.

Application note:

From the design perspective of an IC, the external interfaces are called i/o ports. On the other hand, the route for information that may be used to infer internal processing is called hidden channel (covert channel or side channel). In the case of an IC, the following are conceivable methods of attack on such a covert channel.

- SPA (Simple Power Analysis) / DPA (Differential Power Analysis) attack:
  This method infers the encryption keys by statistically analysing the power consumption of the IC.
- Timing attack:
  This method infers the encryption keys by comparing and analysing the processing time of various input data within the IC.
- Leaked electromagnetic wave attack:
  This method infers the decrypted data by analysing the leak electromagnetic wave of the IC.

3. T.Fault_generation

An proficient attacker who knows the cryptographic knowledge and circuit knowledge can infer the data in the memory by causing the IC to operate in an abnormal environment and making the operation of the memories and/or circuit unstable, using specialised equipments.

Application note:

The methods of generating an abnormal environment are the following:

- DFA (Differential Fault Analysis) attack:
  The CPU in the IC is exposed to a low level of radiation to forcibly change the bit being processed and the encryption key is inferred by the difference from the normal processing. The Bell Core-Lenstra's attack on RSA that utilises the Chinese Remainder Theorem is an example of this type of attack.
- The voltage supply or clock of the IC is suddenly changed (Glitch attack) or the IC is operated at an abnormal temperature in order to utilise the electrical characteristics (such as time delay) of the memories.

4. T.Interface_attack

The proficient attacker who knows the circuit knowledge may utilize the unnecessary i/o ports to leak and tamper with data in the memory, using specialised equipments.

Application note:

The IC targeted by this PP incorporates a processing unit and various memories and has more than ten i/o ports. These i/o ports may be used for quality testing, software loading and/or setting the encryption key at the manufacturing stage or used for maintenance purposes after shipment as a product. Normally, the circuits of the i/o ports for the IC manufacturer are shut down prior to shipment and/or covered with the package resin in order to render them useless. However, there is the possibility that an attacker will overcome these obstacles to misuse the i/o ports.

3.4 Organisational security policies

No organizational security policy has been defined in the scope of this PP.

4. Security Objectives

4.1 Security objectives for the TOE

1. O.Micro_attack:

   The TOE shall assure the security of the processing unit, memories and electronic circuits from physical attack (probing, attacks as light based and/or temperature, frequency, etc.).

   Application note:

   As defense against physical attack, the TOE needs to implement design and manufacturing schemes. For example, use of multiple layers of circuits and a structure that makes physical access to important data difficult constitute such measures.

   Moreover, ensuring confidentiality of the data in the internal data bus wire through encryption and ensuring data integrity through use of digital signature are effective for defense and detection.

2. O.Covert_channel:

   The TOE shall have a mechanism to prevent inference of the internal processing of the IC.

   Application note:

   In order to prevent inference of the internal processing, the covert channel may be discarded or analysis of the covert channel may be made difficult. Adoption of package material that absorbs electromagnetic waves is an example of the former while schemes with respect to the architecture of the processing unit or co-processor, shift in the process timing and ensuring redundancy in the signal to noise ratio through incorporation of a dummy (noise) circuit are examples of the latter.

3. O.Fault_generation:

   The TOE must be capable of maintaining security even in a physically abnormal environment or condition.

   Application note:

   With respect to the DFA, confirming the results by dual implementation of the algorithm or making changes to the algorithm to insert check points during processing are conceivable measures. Covering 100% of the DFA would be difficult.

   Moreover, with respect to the Glitch attack, prevention through various sensor technologies that detect changes in the environment and circuit design that is able to withstand a Glitch attack (circuit design that is not impacted by changes in the environment that will be a hard challenge for the IC designers) are conceivable measures.

4. O.Interface_attack:

   The TOE must be capable of preventing abuse by any person except developer (such as maintenance person) of i/o ports not required in the environment of use of the IC.

   Application note:

   In the environment of use of an IC, unnecessary i/o ports are rendered unusable by cutting the circuit or covering with the package resin, and so on. However, when doing this, consideration must be given to intentional threats such as A. Physical_resist or T. Micro_attack.

   Moreover, i/o ports that are not required in use but need to be maintained for maintenance purposes need to have incorporated a function (authentication function) with respect to the user of the IC functions available at such i/o ports. Use of specific voltage, clock and data that are input from i/o ports as scheme for authentication is an example of a hardware oriented authentication system.

4.2 Security objectives for the environment

No security objectives for the environment has been defined in the scope of this PP.

5. IT Security Requirements

5.1 TOE security requirements

5.1.1 TOE security functional requirements

The security functional requirements stated in [CC part2] are difficult to apply to TOE composed of almost all hardware in this PP. For this reason, matters that the ST authors should note in assignment operations will be explained in the application note.

The security functional requirements for this TOE are the following 13. These requirements perform the following with respect to the definition of [CC part2]:

- Selection with respect to FDP_ITT.1.1, FPT_ITT.1.1
- Refinement with respect to FMT_MSA.1.1

The ST author needs to operate appropriate assignment, selection refinement and iteration with respect to the developed TOE.

FDP_ACC.1 that is a dependency of FDP_ITT.1 is not required by this PP. Please refer to the rationale for the reason this is so.

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist **[assignment: physical tampering scenarios]** to the **[assignment: list of TSF devices/elements]** by responding automatically such that the TSP is not violated.

Dependencies: No dependencies

Application note：

Threats (T. Micro_attack, T. Fault_generation, T. Interface_attack) that the security objectives for the TOE (O. Micro_attack, O. Fault_generation, O. Interface_attack) can counter are concretely stated in **[assignment: physical tampering scenarios]**.

The elements that comprise the TOE (assets) are stated in **[assignment: list of TSF devices/ elements]**.

What is important here is, by the assignment, what part of the TOE is protected from what kind of threats is concretely stated in a comprehensible manner and this may be undertaken in the form of a table.

FDP_ITT.1 Basic internal transfer protection

FDP_ITT.1.1 The TSF shall enforce the **[assignment: access control SFP(s) and/or information flow control SFP(s)]** to prevent the **[disclosure, modification]** of user data when it is transmitted between physically-separated parts of the TOE.

(Underline means completion of operations.)

Dependencies: **[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]**

Application note：

The security policy requirements of this PP have primarily to do with measures against physical attacks and for this reason, access control is subordinated. Accordingly, only the security policy name of the product will be entered in **[assignment: access control SFP(s) and/ or information flow control SFP(s)]**.

Moreover, “transmitted between physically-separated parts of the TOE” is considered the bus wires between the co-processor, processing unit, memories, and other such devices in this PP.

As the definition of user data, refer to chapter 3.1.

FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from **[disclosure, modification]** when it is transmitted between separate parts of the TOE.

(Underline means completion of operations.)

Dependencies: No dependencies

Application note:

As the definition of TSF data, refer to chapter 3.1.

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: **[assignment: list of types of failures in the TSF]**.

Dependencies: **ADV_SPM.1 Informal TOE security policy model**

Application note：

The threats stated in T. Fault_generation shall be described in **[assignment: list of types of failures in the TSF]**.

FRU_FLT.2 Limited fault tolerance

FRU_FLT.2.1 The TSF shall ensure the operation of **all the TOE’s capabilities** when the following failures occur: **[assignment: list of type of failures]**.

Dependencies: **FPT_FLS.1 Failure with preservation of secure state**

Application note：

The threats stated in T. Fault_generation shall be described in **[assignment: list of types of failures]**.

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **[assignment: access control SFP]** on **[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]**.

Dependencies: **FDP_ACF.1 Security attribute based access control**

Application note：

The name of the security policy for the external interfaces (i/o ports) of the IC shall be stated in **[assignment: access control SFP]**. In the event an interface for a particular purpose (such as i/o ports used for DC parametric test in the manufacturing process or pre/final wafer test, etc.) is to be disabled prior to shipment of the IC to the customer, this shall be stated in the policy.

In **[assignment: list of subjects, objects and operations among subjects and objects covered by the SFP]**, maintenance staff in addition to general IC users shall be stated under subjects, the target (such as assets) that can be accessed from the i/o ports shall be stated under objects and operations that can be performed upon access shall be stated under operations.

Note) Access control of general IC users is performed not by hardware but by upper tier software. With respect to this functional requirement, roles that cannot be controlled by software (such as maintenance staff) and the i/o ports, operations and assets utilized by such a role need to be clearly identified.

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **[assignment: access control SFP]** to objects based on **[assignment: security attributes, named groups of security attributes]**.

FDP_ACF.1.2 The TSF 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]**.

FDP_ACF.1.3 The TSF 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]**.

FDP_ACF.1.4 The TSF 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]**.

Dependencies: **FDP_ACC.1 Subset access control**
FMT_MSA.3 Static attribute initialization

Application note:

In **[assignment: security attributes, named groups of security attributes]**, signals that authenticate the subjects (such as voltage, current, clock and other such factors in the case of

authentication by pattern recognition) shall be stated. The concrete method of authentication of subjects shall be stated in FIA_UAU.5.

In the rules of **[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]**, the framework of the rules shall be stated. The actualization of these rules in the IC constitutes operations.

If there are exceptional access rules with respect to FDP_ACF.1.1 and FDP_ACF.1.2, these shall be stated in FDP_ACF.1.3 and FDP_ACF.1.4.

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **[assignment: access control SFP, ~~information flow control SFP~~]** 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]**.

Dependencies: **[FDP_ACC.1 Subset access control or ~~FDP_IFC.1 Subset information flow control~~]**
FMT_SMR.1 Security roles

Application note:

In the event designation and changing of security attributes used in authentication are enabled, the roles that may be changed shall be clearly identified.

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **[assignment: access control SFP, information flow control SFP]** to provide **[selection: restrictive, permissive, other property]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **[assignment: the authorized identified roles]** to specify alternative initial values to override the default values when an object or information is created.

Dependencies: **FMT_MSA.1 Management of security attributes**
FMT_SMR.1 Security roles

Application note:

The definition of the initial setting of security attributes shall be provided. In the case of hardware oriented access control, the initial setting value may be determined as a fixed value upon design. In such a case, this fact shall be clearly identified in the security policy.

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **[assignment: the authorized identified roles]**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: **FIA_UID.1 Timing of identification**

Application note:

Roles that are supported by the TOE shall be listed in **[assignment: the authorized identified roles].**

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow **[assignment: list of TSF-mediated actions]** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow **[assignment: list of TSF mediated actions]** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: **FIA_UID.1 Timing of identification**

Application note:

If there is signal information from the TOE that relates to authentication, this shall be stated in **[assignment: list of TSF mediated actions]** of FIA_UID.1 and FIA_UAU.1.

However, i/o ports that are not normally used are targeted for access control in this PP. The user identification and user authentication functions that these i/o ports have shall be stated.

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide **[assignment: list of multiple authentication mechanisms]** to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the **[assignment: rules describing how the multiple authentication mechanisms provide authentication]**.

Dependencies: No dependencies

Application note:

The names of mechanisms of the i/o ports shall be listed in **[assignment: list of multiple authentication mechanisms]**.

The authentication rules of the mechanisms shall be stated in **[assignment: rules describing how the multiple authentication mechanisms provide authentication]**.

5.1.2 Explicitly stated security functional requirements

The explicitly stated IT security requirements required for the TOE are the following requirement. This requirement has been added in accordance with [CC]. Refinement operation must be undertaken with respect to these requirements in accordance with the TOE developed.

FDP_RIL.1 Reduce the information leakage

FDP_RIL.1.1 The TSF shall provide mechanism(s) to reduce information leakage that could compromise user data.

Dependencies: **AVA_CCA.1 Covert Channel Analysis**

5.1.3 TOE security assurance requirements

The assurance requirements of this TOE are EAL4 augmented by adding AVA_CCA.1 and AVA_VLA.4 to EAL4. These have been selected from [CC part 3]. The ST authors shall perform appropriate refinement and iteration with respect to these requirements in line with the developed TOE.

Class ACM: Configuration management

ACM_AUT.1 Partial CM automation

ACM_CAP.4 Generation support and acceptance procedures

ACM_SCP.2 Problem tracking CM coverage

Class ADO: Delivery and operation

ADO_DEL.2 Detection of modification

ADO_IGS.1 Installation, generation, and start-up procedures

Class ADV: Development

ADV_FSP.2 Fully defined external interfaces

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

ADV_RCR.1 Informal correspondence demonstration

ADV_SPM.1 Informal TOE security policy model

Application note:

Please refer to “7.3.4 Comments on the ADV Class”, Matters to be Noted upon Production of the ST, with respect to the evidences that the product developer should prepare at ADV_FSP.2, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, and ADV_RCR.1.

Moreover, the TSP model required in this PP is the following functional requirement.

FPT_FLS.1 Failure with preservation of secure state.

The ST authors need to create a model for actualizing FPT_FLS.1 and to indicate this in ADV_SPM.1. Moreover, in stating the access control SFP with respect to i/o ports, the following requirements need to be satisfied.

FDP_ACC.1 Subset access control

FDP_ACF.1 Security attribute based access control

FMT_MSA.1 Management of security attributes

FMT_MSA.3 Static attribute initialization

Class AGD: Guidance documents

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

Class ALC: Life cycle support

ALC_DVS.1 Identification of security measures

ALC_LCD.1 Developer defined life-cycle model

ALC_TAT.1 Well-defined development tools

Class ATE: Tests

ATE_COV.2 Analysis of coverage

ATE_DPT.1 Testing: high-level design

ATE_FUN.1 Functional testing

ATE_IND.2 Independent testing – sample

Application note:

Please refer to the matters to be noted in the production of the ST in "7.3.6 Comments on the ATE Class".

Class AVA: Vulnerability assessment

AVA_CCA.1 Covert Channel Analysis

Application note:

In the [CC], analysis of channels other than normal channels as covert channel is required for the system that performs access control based on information flow control. This PP considers i/o ports other than the normal ports to be covert channels and requires covert channel analysis by the ST authors. The leaked information assumed in T. Covert_channel of this PP is all considered covert channel. The ST authors must prepare analysis of the leakage route and measures with respect to such leakage as evidences in **AVA_CCA.1**.

AVA_MSU.2 Validation of analysis

AVA_SOF.1 Strength of TOE security function evaluation

AVA_VLA.4 Highly resistant

Application note:

Already various physical attacks against the IC have occurred and various materials that point to vulnerability have been publicly available. Since these can be considered obvious vulnerability, systematic analysis needs to be undertaken and the ST authors need to prepare evidences that appropriate measures with respect to the TOE have been undertaken.

5.1.4 Minimum strength of function (SOF) Claim

The minimum strength of security functions for the TOE is SOF-high (Strength of Functions High). The TOE security functional requirements that are related to SOF is **FIA_UAU.5**.

In addition, as some encryption mechanism may be used, the proficient attacker who knows the cryptographic knowledge is supported as an attack agent in this PP (see chapter 3.3).

Even if no SOF claim applies to cryptographic mechanisms, the strength of these mechanism would be analysed during the VLA analysis by the same kind of approach.

5.2 Security requirements for the IT environment

There are no security requirements for the IT environment defined in this PP.

6. Rationale

6.1 Security objectives rationale

Table 6-1 shows the relationship among threats, assumption and objectives for the TOE and objectives for the environment.

Table 6-1 Security objectives rationale

Threats/Objectives		O.Micro_attack	O.Covert_channel	O.Fault_generation	O.Interface_attack
Threats	1. T.Micro_attack	○			
	2. T.Covert_channel		○		
	3. T.Fault_generation			○	
	4. T.Interface attack				○

Protecting an IC against an attacker with unlimited funding merely raises technical development cost and manufacturing cost and is thus unrealistic, in addition to over-specifications for AVA-VLA.4. So, the rationale for objectives with respect to four threats is given below and these are all objectives that are designed to make an attack more difficult (such as raising the cost of an attack, increasing the time required for an attack or necessitating high level specialised knowledge.)

1) T. Micro_attack is countered by O. Micro_attack.

   Through O. Micro_attack, the security of the processing unit, memories and electronic circuit of an IC is assured against attacks.

2) T. Covert_channel is countered by O. Covert_channel.

   Through O. Covert_channel, the TOE shall have a mechanism to prevent inference of the internal processing of the IC.

3) T. Fault_generation is countered by O. Fault_generation.

   Through O. Fault_generation, the TOE shall be capable of maintaining security even in a physically abnormal condition.

4) T. Interface_attack is countered by O. Interface_attack.

   Through O. Interface_attack, measures to prevent misuse of i/o ports not required in the environment of use of the IC.

6.2 Security requirements rationale

Table 6-2 shows the security objectives for the TOE and security objectives for environment as the vertical axis and security functional requirements as the horizontal axis and indicates the relationship between these.

Table 6-2 Objectives-Functional Requirements rationale

Objectives/Requirements		FPT_PHP.3	FDP_ITT.1	FPT_ITT.1	FPT_FLS.1	FRU_FLT.2	FDP_ACC.1	FDP_ACF.1	FMT_MSA.1.	FMT_MSA.3	FMT_SMR.1	FIA_UID.1	FIA_UAU.1	FIA_UAU.5	FDP_RIL.1
TOE	1. O.Micro_attack	○	○	○											
	2. O.Covert_channel														○
	3. O.Fault_generation	○			○	○									
	4. O.Interface_attack	○					○	○	○	○	○	○	○	○	

The following constitutes the rationale for the four security objectives for the TOE. (Note)

Note) FPT_PHP.3 is a functional requirement to guarantee the security of the TSF against physical attack. But in case of IC, to put in place a foolproof defence raises the cost of IC. So, it is acceptable the measures to remove or reduce the threat.

1) O. Micro_attack is realized through the following three functional requirements.

   FPT_PHP.3 Resistance to physical attack

   FDP_ITT.1 Basic internal transfer protection

   FPT_ITT.1 Basic internal TSF data transfer protection

   Through FPT_PHP.3, the processing unit and memories of the IC are designed and manufactured structural features that make physical attack difficult. Moreover, through FDP_ITT.1 and FPT_ITT.1, the confidentiality and integrity of user data and the TSF data that flow through the bus wire that connect the processing unit or memories are assured.

2) O. Covert_channel is realized through the following functional requirement.

   FDP_RIL.1 Reduce the information leakage

   Through FDP_RIL.1, the covert channels themselves, that are the target of attackers, are reduced in number and since the ratio of signal to noise on the covert channel is low, analysis of information is difficult.

3) O. Fault_generation is realized through the following three functional requirements.

   FPT_PHP.3 Resistance to physical attack

   FPT_FLS.1 Failure with preservation of secure state

FRU_FLT.2 Limited fault tolerance

Through FPT_PHP.3, physical abnormality (voltage, clock, etc.) and abnormality during processing of the algorithm due to a physical attack are detected and the operation of the TOE during abnormality is assured through FRU_FLT.2 and return to a secure state maintained by FPT_FLS.1.

4) O. Interface_attack is realized by:

FPT_PHP.3 Resistance to physical attack or,

FDP_ACC.1 Subset access control

FDP_ACF.1 Security attribute based access control

Those i/o ports that are not required in the environment of use of the IC are either physically removed by FPT_PHP.3 or are targeted for logical access control through FDP_ACC.1 and FDP_ACF.1.

In the event a logical measure (FDP_ACC.1 and FDP_ACF.1) is to be employed, the principle of use of the i/o is determined by [assignment: access control SFP] and the type of i/o ports, subjects that may utilize such ports and what can be done by such ports (operations, objects) are clearly identified. The following are requirements that support the logical measures.

FMT_MSA.1 Management of security attributes

FMT_MSA.3 Static attribute initialisation

FMT_SMR.1 Security roles

FIA_UID.1 Timing of identification

FIA_UAU.1 Timing of authentication

FIA_UAU.5 Multiple authentication mechanisms

The roles that may utilize i/o ports are clarified through FMT_SMR.1 and the method of authenticating such roles is clarified through FIA_UAU.5. Moreover, the default value and roles with authority to change the value with respect to the security attributes used in authentication are clarified through FMT_MSA.1 and FMT_MSA.3. Furthermore, TOE action allowable prior to identification and authentication is clarified through FIA_UID.1 and FIA_UAU.1.

Application note:

The functional requirement that actualizes O. Interface_attack is selected from among FPT_PHP.3 or FDP_ACC.1 and FDP_ACF.1 from the perspective of the functions of the IC. The ST authors must state the measures that correspond to the i/o ports for each function of the IC in the ST. Moreover, if the TOE consists of only one of the measures, there will be no SF (Security Function) to actualize the other. This fact should also be stated in the ST.

Table 6-3 shows the all dependencies derived by security requirements in this PP. This PP satisfies all dependencies except for number2 (FDP_ITT.1) and number15 (AVA_CCA.1). Please refer to 6.3 about the dependencies of FDP_ITT.1 and AVA_CCA.1.

Table. 6-3 Dependencies

Number	Requirement	Dependencies	Refer to
1	FPT_PHP.3	No	-
2	FDP_ITT.1	FDP_ACC.1	Section 6.3
3	FPT_ITT.1	No	-
4	FPT_FLS.1	ADV_SPM.1	Section 5.1.3
5	FRU_FLT.2	FPT_FLS.1	Number 4
6	FDP_ACC.1	FDP_ACF.1	Number 7
7	FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	Number 6, 9
8	FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1, FMT_SMR.1	Number 6 (choose FDP_ACC.1), Number 10
9	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	Number 8, Number 10
10	FMT_SMR.1	FIA_UID.1	Number 11
11	FIA_UID.1	No	-
12	FIA_UAU.1	FIA_UID.1	Number 11
13	FIA_UAU.5	No	-
14	FDP_RIL.1	AVA_CCA.1	Number 15
15	AVA_CCA.1	ADV_FSP.2, AGD_ADM.1, AGD_USR.1	Section 5.1.3
		ADV_IMP.2	Section 6.3
16	AVA_VLA.4	ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, AGD_ADM.1, AGD_USR.1	Section 5.1.3

6.3 Rationale on IT security requirements that do not satisfy dependency

1) FDP_ACC.1 of the dependency of FDP_ITT.1

This requirement (FDP_ITT.1) requires measures with respect to physical attacks (Micro_attack) on the bus wires in the IC and does not require an access control policy FDP_ACC.1 for the bus circuit.

However, the i/o ports of the IC require hardware based access control and this PP requires FDP_ACC.1.

2) ADV_IMP.2 of the dependency of AVA_CCA.1

The main target of covert channel analysis (AVA_CCA) in CC is a requirement about information flow control, but the requirement (AVA_CCA) in this PP requires the analysis of the leakage route and measures with respect to the leakage information of the internal processing of the IC. Processing unit, security circuit and co-processor are elements concern with the internal processing, but memories are not be included. Therefore, all representation of TSF required by ADV_IMP.2 are not be needed. It is sufficient to satisfy ADV_IMP.1 which requires the subset of ADV_IMP.2.

6.4 Suitability of minimum strength of function (SOF) level

As described in chapter 2 (TOE Description), the TOE of this PP (IC) will be applied to various areas. In particular, in the event the product incorporating the IC is to be delivered and used by consumers, it is difficult to manage the environment of use for both the manufacturer of the IC and the party procuring the IC. In other words, the environment is one that may be open to various threats externally. With respect to the IC targeted by this PP, the application programs or data themselves have value and in addition to this, the area of application is one in which tampering or theft of the programs or data can be expected to lead to enormous loss. An example of such an area of application is the smart card.

So, the claimed SOF should be high since the security mechanisms have to protect high level attack.

6.5 Appropriateness of TOE assurance requirements

As the integration of IC becomes higher and downsizing progresses, the areas in which the IC may be applied expands further. This spiral expansion can be expected to continue into the future as long as appropriate security can be maintained. However, counterfeit crimes have already occurred with respect to the smart card that is one such application of the IC. While the method employed in such crime cannot be said to focus on weaknesses in the latest IC (hardware) technology, there is no question that the methods have become more advanced and for attackers, ICs are attractive targets for counterfeiting. When consideration is given to these circumstances, the IC must incorporate advanced security measures in a highly reliable manner. On the other hand, realising a high level of assurance involves proportionate cost and it is a fact that this impacts the price of products. When consideration

is given to these facts, EAL4 can be considered an appropriate choice as it contains evaluation of details of the TOE (evaluation on lower tier design document).

In the environment of use of an IC, it must be assumed that attacks will be made by various people with a high level of know-how. In order to counter this, it is necessary to review the TOE from various angles to ensure that there are no vulnerability and for this reason AVA_VLA.4 was added. Moreover, methods of analysing leaked information are disclosed on the Internet and through meetings of specialised academic societies. As IC developers need to access such information in the development work, AVA_CCA.1 was also added.

6.6 Mutual support of security requirements

Table 6-4 shows the mutually supportive functional requirements for each objective.

Table 6-4 The mutually supportive functional requirements for each objective

Objectives for TOE	Mutual support requirements
1. O.Micro_attack	FPT_PHP.3, FDP_ITT.1, FPT_ITT.1
2. O.Covert_channel	None
3. O.Fault_generation	FPT_PHP.3, FPT_FLS.1, FRU_FLT.2
4. O.Interface_attack	FPT_PHP.3, FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.5

The external interface is only pad interface which cannot modify after the delivery of TOE, so the TOE will not be bypassed. All of the hardware are included in TOE and TOE don't have any extra function, so the TOE will not be tampered or deactivated by extra functions.

6.7 Rational for explicitly stated IT security requirements

Some attack methods to presume the TSF data for basic software or application programs (such as encryption key) by analyzing the information which leaked from TOE (such as variations in power consumption, execution time, transmitted electromagnetic wave, etc.), are disclosed on the Internet and through meetings of specialised academic societies.

Note) As the relationship between user data for TOE and TSF data for basic software or application programs, refer to chapter 3.1.

The examples of the technical mechanism used in the TOE to address above-mentioned attacks are to reduce the variations in power consumption and/or reduce the variations in execution time and/or reduce the variations in transmitted electromagnetic wave. Another examples of the technical mechanism used in the TOE are to hide the real variations in power consumption and/or hide the real variations in execution time and/or hide the real variations in transmitted electromagnetic wave by randomizing.

The examples of the technical mechanism used in the TOE are countermeasure which completed by TOE itself, but countermeasure against active attack from outside. However, the security functional components defined in [CC] are appropriate to address the technical mechanism against active attack from outside. So, the security functional component **Reduce the information leakage (FDP_RIL.1)** has been newly created to address the specific issues of preventing the above-mentioned attacks by reduce the information leakage.

The leaked information from TOE (such as variations in power consumption, execution time, transmitted electromagnetic wave, etc.) are transmitted for processing flowing through the route for example the bus wires between the memories and a processing unit, between the memories and co-processors, and i/o ports that extend from the memories or a processing unit for external interface. The bus wires between the memories and a processing unit, between the memories and co-processors, are called hidden channel (covert channel or side channel). So, the ST authors are required to do covert channel analysis. This is a reason why **Covert Channel Analysis (AVA_CCA.1)** is defined as dependencies of **Reduce the information leakage (FDP_RIL.1)**.

7. Annex

7.1 Glossary

- ST (Security Target): A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
- TOE (Target of Evaluation): An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
- TSF (TOE Security Functions): A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
- TSC (TSF Scope of Control): The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.
- ROM (Read-only Memory) :general term of non-volatility memory(even if it disconnects a power supply, the contents of memory are held) only f or read-out of data
- RAM (Random Access Memory) :general term of the memory that writing and read-out of data are possible.
- EEPROM (Electrically Erasable Programmable ROM) :memory which can eliminate / write data in the contents of it electrically.
- FeRAM (Ferroelectric RAM) :RAM using the ferroelectric. Data can be held even if it disconnects a power supply.
- DRAM (Dynamic Ram) :RAM which memorizes data by refreshing a memory data at every fixed time. Cell area can be reduced and high accumulation and large scale RAM is made.
- SRAM (Static Random Access Memory) :RAM which does not need refreshment operation like DRAM.
- Co-processor :The additional processor which strengthens specific processings (cryptographic operation etc.) in order to strengthen the performance of CPU.
- Bus line :the transmission way for each circuit exchanging data within IC. There is the inside bus within CPU and the exterior bus which connects CPU to co-processor and a memory module, etc.
- RE (Reverse Engineering) :technology of analyzing the internal structure and the functions of IC.
- Covert_channel :the secret channel of information estimated internal processing without going via formal interface of a product. It is also called side channel. Examples are power consumption, processing time, a disclosure electromagnetic wave, etc.
- SPA(Simple Power Analysis) :how to observe the power consumption at the time of input-and-output data processing of the plurality (comparatively small number) for an attack, and to guess the key of encryption.
- DPA(Differential Power Analysis) :Differential Power Analysis. The measurement of current drawn by the IC during cryptographic operation, which can then be used to infer computational paths taken by the algorithm, and hence secrets being operated on.
- DFA(Differential Fault Analysis) :Differential Fault Analysis. The running of the IC in a hostile environment (e.g. strong electric field) to induce errors in cryptographic calculations.

- Chinese Remainder Theorem：
- RSA (Rivest, Shamir, Adleman) :a kind of the asymmetrical cryptographic algorithm whose key can be public.
- DES (Data Encryption Standard) :A kind of the symmetrical cryptographic algorithm using the same key as encryption and decryption.
- i/o ports :real external interfaces on IC. In a using environment, even when they are unnecessary, they include the ports used by the quality test etc. They are also called PAD.

7.2 The process of design and manufacture to completion of a smart card

The areas of LS chip applications are diverse and in general, prior to development, market research is undertaken in order to determine the overall requirements of the IC. In the sections that follow, an overview of the work after the development decision taken, from the design and manufacturing of the IC to completion of the application product as well as the relationship of these steps to the requirements of this PP are explained taking the example of smart cards that constitute one area of application.

Figure 7-1 shows a rough overall figure of the work involved and may be called the life cycle of a smart card.

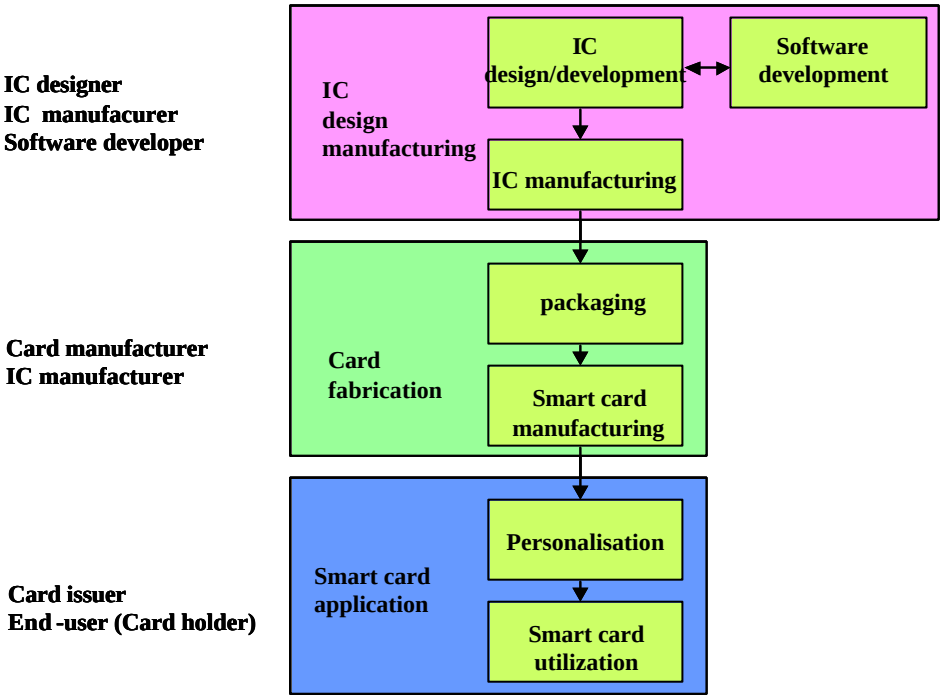

Figure 7-1 From Manufacturing to Use of a Smart Card

(1) Design and manufacture of the IC

After the logical design of an IC and the manufacturing process (photomask fabrication) are decided and development of software that will be masked in the ROM of the IC is completed, the IC is manufactured (wafer manufacturing, wafer processing). The IC that is the result of this series of tasks involved is the TOE of this PP and the form is comprised of extremely minute pieces aligned in a mesh pattern on a wafer measuring several tens of centimetres on each side. Security functional requirements and assurance requirements for the TOE pertain to this design and manufacturing process but threats assume attacks upon use of the IC in smart cards.

(2) Card Fabrication

The LSI packaging process involves cutting out the individual IC from the wafers completed after the design and manufacturing processes and bonding this onto a lead frame, connecting the contacts on the lead frame to the electrode contacts on the IC, covering the exterior with package resin and the product that is the result of these processes (Figure 7-2) is called an IC package (note). In the case of IC for smart cards, in many cases the electrode contacts on the IC that are

connected to the lead frame are limited to 6 contacts (VDD, GND, CLK, I/O, RST, VPP) under ISO regulations. Moreover, the process of coating with the package resin is performed as part of the process of card production (Figure 7-3).

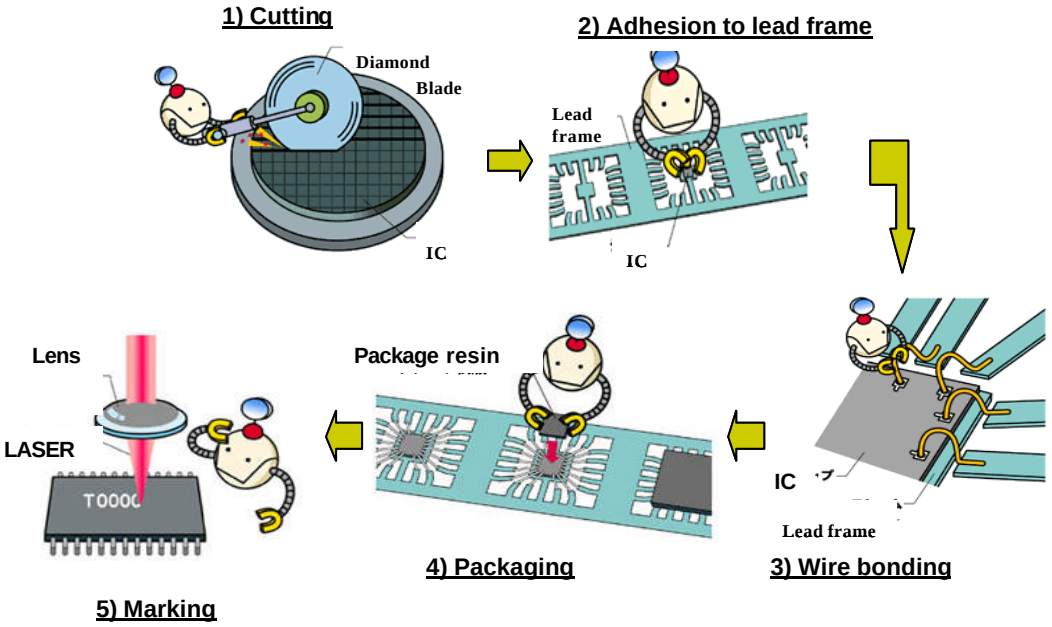

Figure 7-2 Picture of Packaging

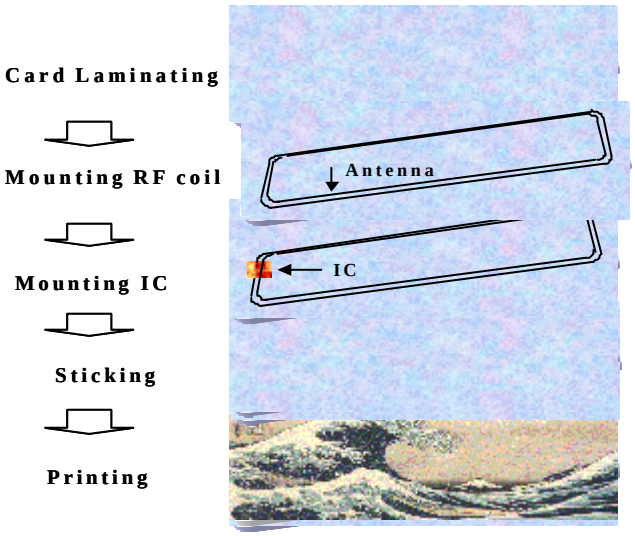

Figure 7-3 Picture of Card Production

In card fabrication, the lead frame is embedded in a plastic card in the case of the contact type card and in the case of a contactless type card, the lead frame is sandwiched between cards. In addition to such external tasks, the software used in common by smart card applications is loaded on the memories (non-volatile memories such as FRAM and EEPROM) and the logical layout of the memories is undertaken.

Note) An IC package is sometimes referred to simply as IC. In the case of such products, the A. Physical_breaking of this PP is considered a threat for the TOE and ST needs to be produced.

(3) Applications of the smart card

The completed smart card is delivered to the card issuer that is the operator of the application and information for the cardholder, the final user of the card, is input by the card issuer. The main types of information input are application programs/ data set in the IC, the TSF data required by the application, personal information of the cardholder (PIN, etc.) and the name, address, photo of the cardholder, name of the issuer, term of validity, and other such information that is printed on the front surface of the card.

7.3 PP application note

This PP describes the minimum security requirements for IC. The developer will implement some additional security functions, and will make evidences adding these minimum security requirements at developing the TOE and ST. The following are some information will be useful for developer.

7.3.1 Handling of the software used for quality test

In the IC manufacturing process and in particular in the wafer inspection process, inspection on whether or not the wafer prior to individual IC being cut is defective and the electric characteristics of the IC is performed. The software used in this process is called hardware dedicated software in this PP. This inspection includes reading and writing 0, 1 on the memories. This function is highly convenient for an attacker. When consideration is given to the objectives and the timing of use of this function, rather than demand strict access control (FDP class), the function should be disabled prior to shipment. That is to say, following development and manufacturing policy shall be established.

DP.Disable_D_software

IC manufacturer shall guaranty the software (Hardware Dedicated Software) used for quality test in the manufacturing process of an IC is removed or disabled prior to shipment.

Software for investigating hardware problems needs full-fledged access control and this is believed to be achievable through the operating system shown in Figure 2-3.

7.3.2 Handling of i/o Ports

This PP assumes that attacks on the i/o ports (T. Interface_attack) constitute a threat. The TOE of this PP(IC) is, as shown in Figure 7-4, several millimetres wide and high and the i/o ports (externally visible interfaces) indicate the electrode contact (Pad) of the IC. Normal IC's pad have all lines connected to a terminal on the substrate called the lead frame, but even if such connection is not in place, contacts used in quality testing in the manufacturing process are considered to be included within the meaning of i/o ports (contacts a and b in Figure 7-4).

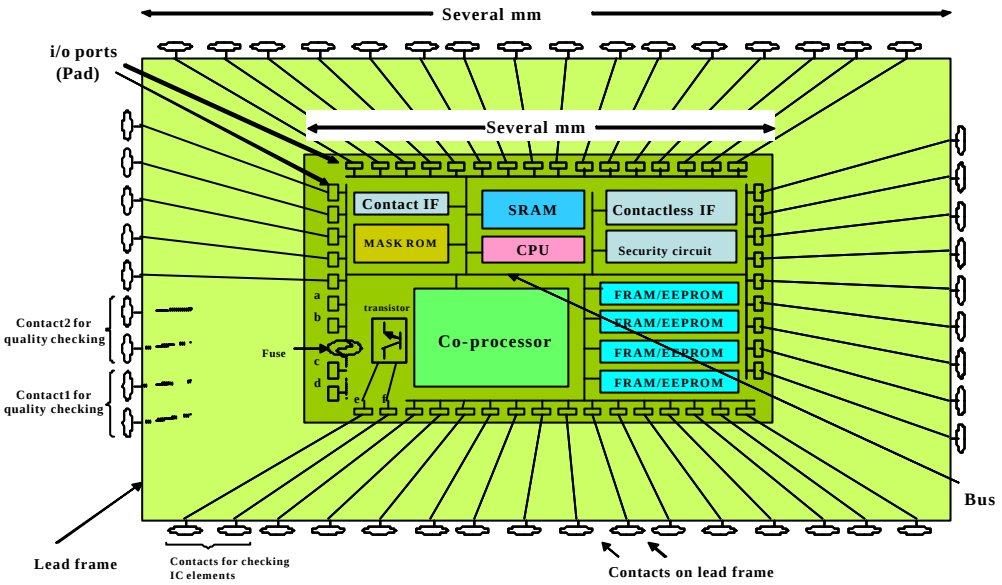

Figure 7-4 i/o Ports and Lead Frame Contacts

On the other hand, contacts with respect to which the wires to the electrode contacts have been physically and logically cut (for example, by cutting the fuse) (contacts c and d in Figure 7-4) in the manufacturing process are not considered i/o ports. Moreover, contacts are sometimes installed on the lead frame in order to confirm the condition of the IC transistors (contacts e and f in Figure 7-4). These contacts are not connected to the processing unit or memories of the IC and are thus not included within the meaning of i/o ports.

7.3.3 ST of products coated with package resin

In this PP, the package resin (Figure 2-1) is excluded from the scope of the TOE. However, it can be assumed that some manufacturers of IC ship the products after coating the package resin. In such cases, the package resin is included in the scope of the TOE. When this is so, the intentions of this PP with respect to the threats (T. Physical_resist), objectives (O. Physical_resist), and TOE security requirements (FPT_PHP.3) are added in the ST.

T.Physical_resist

In order to enhance the quality of the TOE (the processing unit and memories of the IC), the package resin or insulation coating (topmost layer in Figure 2-1) that covers the IC must have both physical and chemical strength in the face of an attack.

Application note:

In preparing for a physical attack, the attacker must first remove the package resin or insulation coating without impairing the functions of the IC.

While on the one hand, the package resin or insulation coating is necessary in order to prevent infiltration of water or ion to the processing unit or memories of the IC and to enhance physical resistance to bending, measures for removing such covering without impairing the functions of the processing unit or memories such as:

- Physical removal using a knife in the case of plastic
- Dissolution using special chemicals under specific environmental conditions in the case of epoxy resin

are also required for purposes of troubleshooting with respect to the IC.

Troubleshooting work will be facilitated if as a quality enhancement measure, removal of the package resin or insulation coating is facilitated. Concurrently, however, this will facilitate the preparatory work of an attacker. In other words, an appropriate balance must be in place.

By adopting this threat, it is expected that threat to the TOE will decrease. Moreover, this is a threat that needs to be addressed in the IC package products.

O.Physical_resist:

Physical and chemical means of removal are in place with respect to the package resin or insulation coating that covers the TOE.

Application note:

Package resin or insulation coating has been used to stabilize the electrical characteristic in order to enhance the quality of the IC but as the applications of IC increase, it is necessary to include measures having to do with counterfeiting among the uses of such covering.

The IC targeted by this PP is assumed to have an encryption function. In the case of an encryption device realised through the device unit, measures need to be in place to ensure that the device body cannot readily be opened and that internal information will be erased in the event of unauthorised opening of the device body. If the same requirement is applied to an IC, the package resin should not be readily removable or, even if removable, should require significant know-how and cost.

Measures such as considering the material of the package resin with these issues in mind are required.

The security functional requirements needed are as following measures against T.Physical_resist:

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist **[assignment: physical tampering scenarios]** to the **[assignment: list of TSF devices/elements]** by responding automatically such that the TSP is not violated.

Dependencies: No dependencies

Application note:

T.Physical_resist adopted by the ST authors shall be stated in **[assignment: physical tampering scenarios].**

7.3.4 Comments on the ADV Class

The TOE targeted by this PP is IC comprised of hardware. Design related evidences (ADV_FSP, ADV_HLD, ADV_LLD, ADV_IMP, ADV_RCR) required for the ADV class in [CC part 3] are produced in the design and manufacturing process of the IC shown in Figure 7-1. The following sections will deal with matters that will be of reference in preparing such evidences.

Figure 6-2 shows the relationship among PP, ST and ADV. The ST authors realise the PP security requirements (SFRs) in the product and indicates an overview of such requirements as security functions (SFs) in the TSS (TOE Summary Specification) of the ST. The requirements of the ADV class require evidence that the functional specification (ADV_FSP), high level design (ADV_HLD), low level design (ADV_LLD) and implement (ADV_IMP) produced in the design process of the product, fully actualise the SFs and evidence (ADV_RCR) that these are concretely realised in stages (indicate the relationship of correspondence).

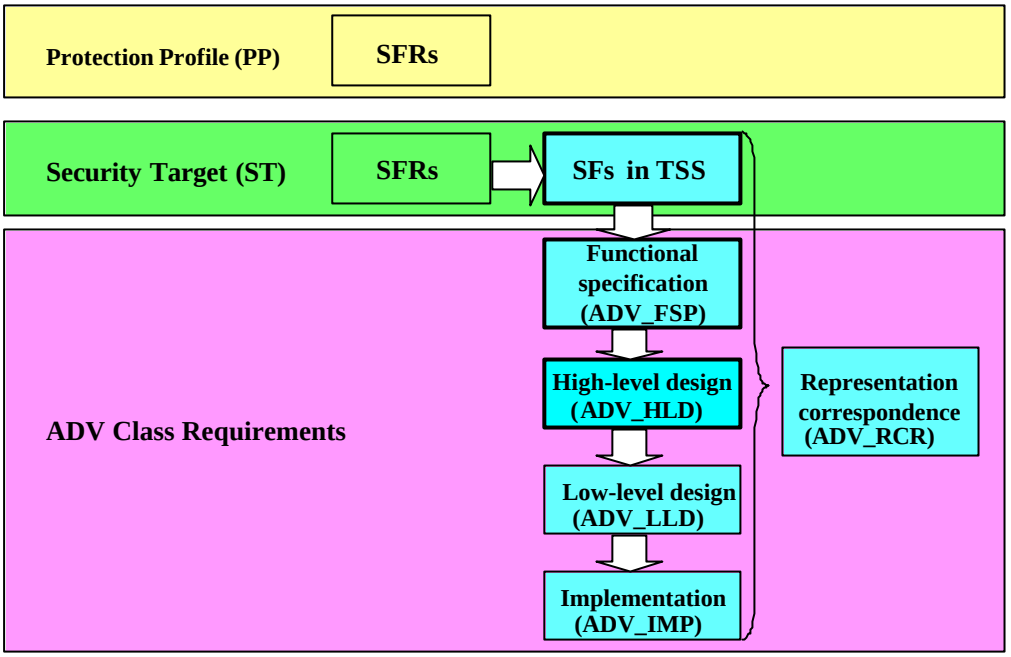

Figure 7-5 Relationship among PP, ST and ADV Class

On the other hand, the core functional requirement of this PP is FPT_PHP.3 and in the design and development of this, there are many cases in which application of the tiered design approach as in the CC expressed in compact functional units (subsystem, module) is difficult.(Note) At the very least, the following information should be prepared and the intentions of the CC respected.

Note) The requirements of the ADV class are means of actualising the TOE and not of actualising the semiconductor chip. In fact, the TOE is a part of the means of actualising the semiconductor chip.

First of all, the ST (Security Target) is developed at the IC design / development stages of Fig 7-1. The followings describe the products (evidences) as examples which are needed for assurance requirements at each work process of a planning, a designing, and a production evaluation.

1) At the planning work, the outline specification documents of a product are drawn up. These outline specification documents describe the functional outline of a product, an outline block diagram, external interfaces (a user interface, physical conditions) about a product and the large frame (layout information (the layer/width of wiring), element size), etc. about manufacture. In order to consider as CC conformity, it is desirable to make clear the correspondence between the outline specifications and SFs (Security functions) described in TSS (TOE Summary Specification) of ST.

2) At the designing work, the system block diagram documents of a product are drawn up based on various kinds of specifications at the planning work. This block diagram states CPU cell, memory cell, which are the composition element of IC, the wiring (bus line) information between composition elements, external interfaces (i/o ports), and the CPU functions(a command set, interruption, memory map, etc).Moreover, the specifications for quality control / maintenance of CPU cell, memory cell are

also drawn up. ST developers have to make clear the correspondence between SFs and these documents.

Next, the system block diagram is translated into information for manufacturing and function testing. However, in the case of using an automatic design tool like Verilog, the source list described by HDL (Hardware Description Language), simulation results and netlists, etc. are evidences. In the case of not using an automatic design tool, schematic information, which is input-and-output data for a schematic editor, netlists, test results, etc. are evidences. The correspondences between SFs and these evidences are also required for evaluations. Moreover, layout data and mask data may also be needed for detailed evaluation of SFs.

3) At the trial production / evaluation work, function evaluations of sample chip which is producted by using mask data designed at the designing stage are performed and it is also important to evaluate SFs and leave evidences of them in addition to doing function evaluations.

As mentioned above, the evidences are required at the development / design work, besides, the using method of dedicated software and Vulnerability assessment-related work results, etc. are added. ST developers have to respond to the requirements for assurance requirements according to each actual conditions of TOE development.

7.3.5 Reliability of memories

The IC targeted by this PP will be applied to various field. The memories used in an IC must have sufficient durability to the number of data reading and writing in the assumed environment of use.

7.3.6 Comments on the ATE Class

(1) ATE_FUN.1

It is necessary to prepare the test plan, test procedures, test results and other such elements.

Since this PP has to do with the security function of the IC, functions related to encryption are also included. In particular, while the algorithm for encryption or the appropriateness of the random number generation mechanism is outside the scope of the CC, it is desirable that the results of verification of these be prepared as evidences for ATE_FUN.1.

(2) ATE_COV.2

The scope of the test shall cover the content of ADV_FSP.2.

With respect to each SF, test environment, method, results, and other such factors shall be clearly identified.

(3) ATE_DPT.1

The depth of the test shall be to the content of ADV_HLD.2.

With respect to each subsystem, the test environment, method, results and other such factors shall be clearly identified.