JICSAP ver.2.0 Protection Profile part 2

Protection Profile for Smart Cards with the Application Program Loading Function

Version: **1.7e**

Date: **September 4, 2003**

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

Authors: **Electronic Commerce Se curity Technology Research Association**

English translation **27 June, 2002**

English proofreading 1st **19th Dec., 2002**

English proofreading 2nd **25th Dec., 2002**

Dealing with observations from the evaluator	
ver 1.1e	11th March, 2003
ver 1.2e	22nd March, 2003
ver 1.3e	1st April, 2003
Ver 1.4e	13th May, 2003
ver 1.5e	8th July, 2003
ver 1.6e	27th August, 2003
ver 1.7e	4th September, 2003

Table of contents

1. PP Introduction

1.1 PP Identification

Title: JICSAP ver.2.0 Protection Profile part 2, Protection Profile for Smart cards with the Application Program Loading Function

Date:	September 4, 2003
Version:	1.7e
Issuers:	Japan IC Card System Application Council
Authors:	Electronic Commerce Security Technology Research Association
TOE:	Smart card software
Registration:	TBD

This PP is English version of "Protection Profile for Smart cards with the Application Program Loading Function" issued by New Media Development Association in Japanese on December 10th 2001.

The issuer of this PP, Japan IC Card System Application Council got the right to translate and modify original PP from New Media Development Association, and added necessary modification to let the original PP adapt to JICSAP ver2.0 smartcard specification in English.

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

This PP is in compliant to Common Criteria version 2.1.

For the user convenience, Japanese translations by the Information Technology Promotion Agency are attached to the parts referenced in English from CC, in Japanese version of this PP.

1.2 PP Overview

This PP is one of two PPs produced in order to uphold the IT security of the smart card system to be used in the Research Project on "Cities Equipped with Information Technologies", which the New Media Development Association is commissioned from the Ministry of Economy, Trade and Industry as a project under the fiscal 2000 supplementary budget.

However, the user may utilize this PP for purposes other than the Research Project on "Cities Equipped with Information Technologies"(Note 1).

Note 1) the author of the PP shall not be liable to the results of such use.

This PP describes the security requirements for the software in a smart card that is embedded with an IC chip in a plastic card.

The security requirements for the hardware of IC card are described in "1), 2) and 5) of section 1.5 the related protection profiles".

Note: It is desirable for Japanese government to procure the IC card based on a composite ST which is composed of ST for software and hardware. Detail explanation of composite ST is described in CC Supporting document– "ETR-lite for Composition".

The smart card incorporates a processing circuit (CPU: Central Processing Unit), memories (ROM, RAM, FeRAM, EEPROM, etc.), co-processor and other integrated circuits and provides high-level security functions through the software stored in the storage elements. Moreover, this PP also assumes that application programs will be downloaded to the card through a network and Reader/Writer before or after the card issuance. It is possible that some basic application programs may be masked in the ROM during the production phase of the IC chip.

Although this PP directly targets the smart card that is capable of loading such applications used by the Research project on "Cities Equipped with Information Technologies", the smart card system of the project does not specify any specific application.

Then, the examples of applications of Smart cards targeted by this PP are given below.

- Public services to the residents (e.g. official stamp certification) as residential card;
- Banking services such as deposit/withdrawal or debit payments as bank card
- Later payment services after shopping/services as credit card
- Secure storage media for electronic money as electronic purse
- Secure storage for medical information in advanced medical services.

This PP assumes that these applications will reside in a single card.

A smart card may be supplied with power externally or incorporate the power supply internally. This PP targets such cards that are supplied with power externally (contact type and contactless type).

1.3 Assurance Level and SOF

The assurance level of this PP claims EAL4 augmented. The assurance requirement augmented is:

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

And the strength of the probabilistic algorithm is SOF-High.

1.4 Related Standards and Documents

The related standards and documents are as follows:

- JIS X 5070 Security Technology – Evaluation Criteria for Information Technology Security
- JIS X 6300 Series, Identification cards -- Integrated circuit(s) cards with contacts
- JIS X 6322 Series, Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards
- ISO/IEC 15408 – Information Technology – Security Techniques – Evaluation Criteria for IT Security
- JICSAP Smart Card Specifications V2.0

- Smart Card Interface Specifications for the Research project on "Cities Equipped with Information Technologies" Version 1.0
- Residential Smart Card Specifications
- ISO/IEC 7810 – Identification Cards – Physical Characteristics
- ISO/IEC 7816 – Identification Cards – Integrated Circuit Cards with Contacts
- ISO/IEC 14443– Contactless Integrated Circuit Cards, Proximity Cards
- CC Supporting document– "ETR-lite for Composition", Version 1.1, July 2002

1.5 Related Protection Profiles

The related Protection Profiles are as follows:

-1) JICSAP ver.2.0 Protection Profile part1, Multi-Application Secure System LSI Chip Protection Profile; Version 2.5, June 6, 2003 (PP/0301)

-2) Protection Profile Smart card Integrated Circuit; Version 2.0, Sep 1998 (PP/9806)

-3) Protection Profile Smart card IC with Embedded Software; Version 2.0, Jun 1999 (PP/9911)

-4) Protection Profile Smart card IC with Multi-Application Secure Platform; Version 2.0, Nov 2000 (PP/0010)

-5) Smart card IC Platform Protection Profile; Version 1.0, Jul 2001-10-17 (BSI-PP-0002)

-6) Smart card Security User Group Smart card Protection Profile; Version 3.0, Sep 9 2001

-7) ICCS Smart card Protection Profile V1.0

1), 2) and 5) are used for the security requirement for hardware of the IC card.

1.6 Structure of this Document

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

Chapter 2, TOE Description, defines the TOE scope and explains the life cycle of smart card and the related threat agents.

Chapter 3, TOE Security Environment, describes the assets defined in this PP, three assumptions, seven threats, and two organizational security policies.

Chapter 4, Security Objectives, describes the eight security objectives for the TOE and the five security objectives for the environment.

Chapter 5, Security Requirements, states the twenty-seven security functional requirements and the assurance requirements that augment EAL4 as the security requirements of the TOE, SOF-High and the two functional requirements of the environment. Of the functional requirements of the TOE, two requirements are explicitly stated functional requirements.

Chapter 6, Rationale, demonstrates the rationale with respect to the security objectives, functional requirements, SOF and explicitly stated functional requirements.

Chapter 7 provides Application notes.

This PP contains application notes in various places to supplement the intent of the main descriptions. The issues explained in the application notes are examples of implementing the requirements in this PP but do not limit the method of implementation. The ST authors may refer to the information contained in the application notes.

2. TOE Description

2.1 Product Type

Figure 2-1 shows the logical relationship between the smart card system and the TOE. The smart card exchanges data with a higher layer application system (terminal or server) through the Reader/Writer. The smart card is consisted with hardware (e.g. processing circuit, memories (ROM, RAM, FeRAM, EEPROM, etc.), and co-processor), software (OS, CM, etc.) and application programs (Note 1) that are loaded in the memories. The TOE is the software portion of the product as shown in Figure 2-1 therefore the hardware and application programs are not within the TOE scope. Accordingly, the hardware-dedicated software or firmware that is designed to ensure the hardware reliability and tamper-resistance is also out of the TOE scope (Note 2).

Security measures on the smart card surface are also not targeted as TOE.

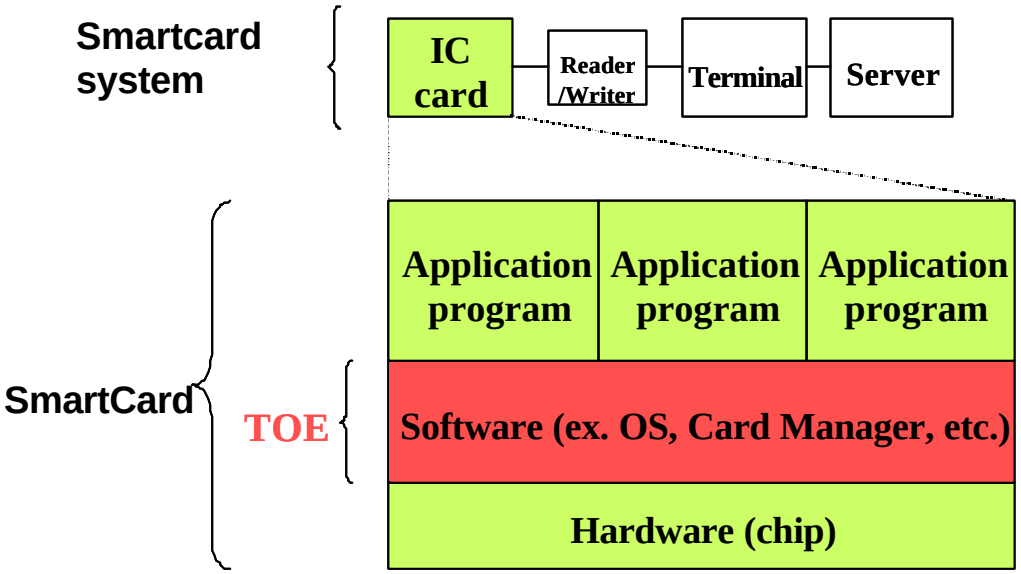


Figure 2-1 The Smart card System and TOE

Note 1) various structures may be applied to the product required by this PP. Since it is difficult to describe the TOE functions and scope in general terms and in detail without limiting the diversity of the structure, the TOE description in this PP is simplified. It is advisable that the ST authors describe the TOE functions and scope for specific products concretely. Sub section 7.5 provides an example of TOE description.

Note 2) the hardware and firmware defined as out of TOE scope in this PP are those used only to establish the hardware reliabilities and counter the tampering.

2.2 IC Manufacturing, Smart card Personalisation and End-Usage

Figure 2-2 shows the series of process (life cycle) and related personnel from development/production of the IC chip, IC packaging, card fabrication, delivery to the cardholder (end user), namely, the processes through preparing the operational environments to using the cards.

At the manufacturing stage, the OS, CM, libraries and other elements are masked in the IC chip based on design profiles. Moreover, the application programs may also be developed, debugged, and then masked at this stage. The users involved at this stage are collectively called 'manufacturer' in this PP.

At the issuance stage, dedicated personnel use a dedicated card-issuing terminal to personalise the card, load application programs and set the operational environment for such programs (setting the key for encryption or digital signature, initialising the application data, etc.). After these processes are completed, the smart card is delivered to the cardholder by post or other delivery services. Once the card is delivered, the management responsibility for the card is transferred from the card issuer to the cardholder. This PP assumes such application loading upon use of smart card and considers this loading operation as a part of the issuance process. The term 'issuer' in this PP collectively refers to all personnel involved in the issuance process.

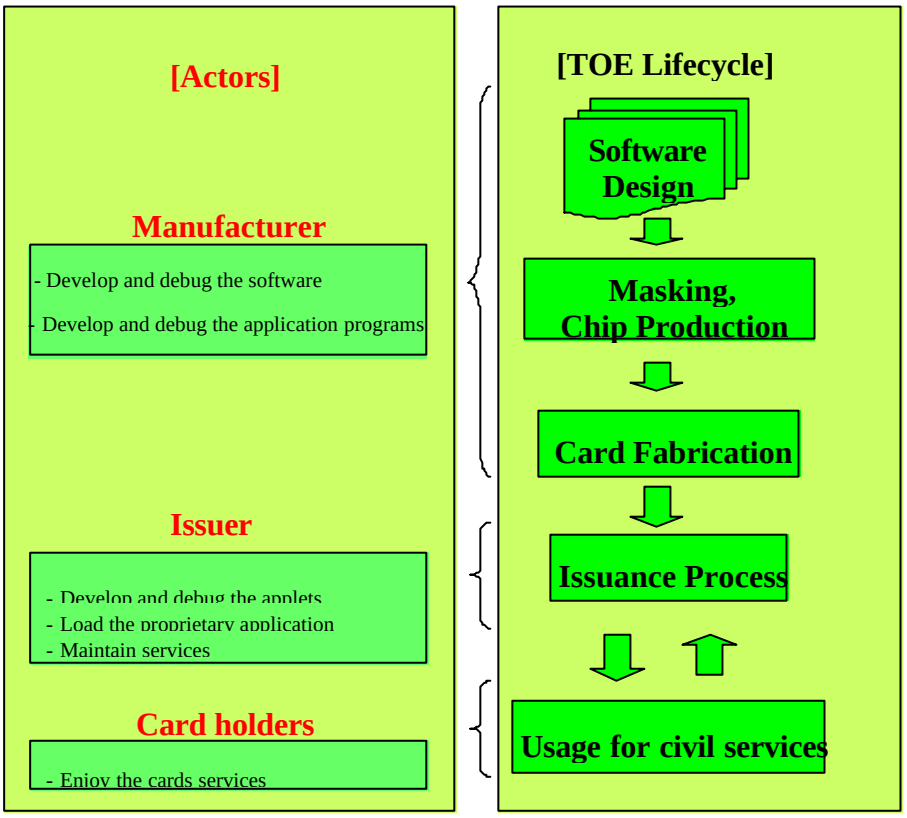


Figure 2-2 TOE Lifecycle and related personnel

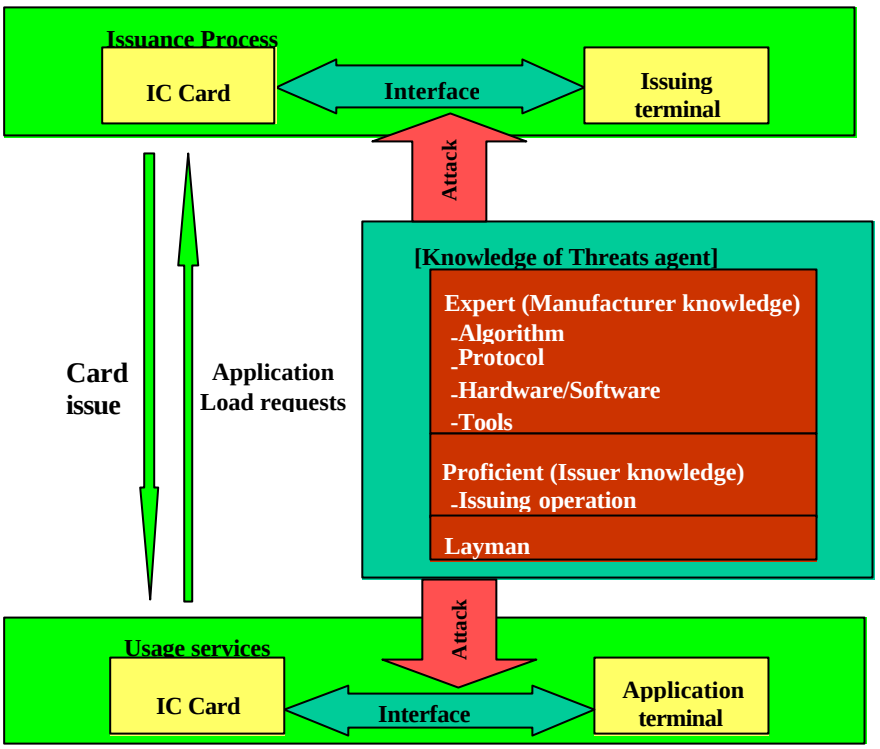


Figure 2-3 Knowledge of threats agent and attack method

At the end-usage stage, the cardholder enjoys the relevant services through a dedicated service terminal via the application program loaded in the card. At this stage, the management responsibility for the card belongs to the cardholder and various threats are assumed to exist with respect to the card.

This PP assumes the whole life cycle of a card as the threat objectives and classifies the primary threat agents as follows (expert, proficient, and layman).

Expert: These are experts with respect to cards who possess specialised knowledge (hardware or software designs, protocols between the card and the Reader/Writer, testing/maintenance tools used for testing, algorithm for encryption and digital signature, etc.) and who use such specialised knowledge to utilise various devices.

Proficient: People with knowledge of card issuances (issuance operations).

Layman: Cardholders, including those who can operate a personal computer and acquire standardised documents.

Some cardholders who have the expert or proficient knowledge are considered as 'Expert' or 'Proficient'.

Note: Although the user of this PP is assumed to be the issuer who intends to procure smart cards, the security requirements primarily exist at the end-usage stage.(Figure 2-3)

2.3 IT Features

If the product composed of the TOE is the IC Card with contact, when the card is inserted into (if the card is contactless type, when it is held to) the Reader/Writer equipped onto the card terminal, the power is turned on and the basic software is automatically invoked and enters into a stand-by mode in which it waits

for the data from the card terminal*. The TOE executes the following functions depending on the data received from the card terminal.

- ✧ The memory management function that provides memory area to the loaded applications and maintain firewalls between loaded applications;
- ✧ The communication function that allows data transmissions/receptions with the Reader/Writer using a standard protocol;
- ✧ Command requests that cannot be understood by the TOE are passed to the selected application program;
- ✧ The function that loads the application programs;

Notwithstanding the foregoing, the IC Card does not accept any new command until the on-process command is completely processed and the response is returned.

Moreover, the IC Card incorporates the following security functions in order to securely execute the above functions.

- ✧ Identification and authentication function for the card owner;
- ✧ Terminal authentication function to verify the terminal authenticity;
- ✧ File access control function based on the results from the above card owner and terminal authentication;
- ✧ Prevention function against such mutual interference or data competition between the loaded applications;
- ✧ Data recovery function upon such service interruption due to power disconnection.
- ✧ Secure messaging function between the IC Card and the Reader/Writer to ensure the confidentiality and integrity of data during communication.

*Note) the data from the terminal are called “commands” and those returned from the card are called “responses”.

3. TOE Security Environment

3.1 Assets

A smart card is manufactured via diverse manufacturing processes. In this PP, the data to be protected by the TOE and the data that constitute the means of protection are considered as 'primary assets' and all other data, such as various documents generated in the manufacturing process, are considered 'secondary assets'.

1) Primary assets:

The user data protected by the TOE are the data used by the downloaded applications or the application programs themselves. The following are examples of such data.

2) Residential card application: resident's address, name, etc.;

3) Bank card application: account number, account name, etc.;

4) Credit card application: credit card number, etc.;

5) Electronic purse application: electronic money, etc;

6) Clinical card application: medical information, etc.

In order to protect the above data, the TOE utilises the TSF data (authentication data or security attributes). The following are examples of such data.

7) User authentication (personal authentication): PIN, biometric information (fingerprint, retina, iris, handwriting, etc.), etc.

8) Terminal authentication: authentication keys, etc.

9) Authorisation data: digital certificate for application program loading, etc.

10) Service expiration, etc.

2) Secondary assets:

Information that is produced or used during the manufacturing process of the TOE impacts the integrity or confidentiality of the TOE itself significantly. This kind of information is called 'secondary assets' and the security of such information is established through the diverse assurance requirements that are required by EAL4 + AVA_VLA.4. The following is an overview.

11) ACM Class:
Evidence that unauthorised action has not been taken in the production and manufacturing process with respect to the TOE.

12) ADO Class:
Evidence that the delivery and installation of the TOE are correctly performed.

13) ADV Class:
Evidence that the TOE functional requirements have been correctly implemented in the design and development process of the TOE.

14) AGD Class:
Evidence that the TOE functions and intended usage have been correctly guided.

15) ALC Class:
Evidence that appropriate security measures have been implemented from the TOE development environment through card issuance process of figure 2-2.

16) ATE Class:
Evidence that the TOE has been appropriately tested.

17) AVA Class:
Evidence that there is no vulnerability in the TOE.

3.2 Assumptions

1) A. TSF_Data:

The TSF data to be set in the TOE is assumed to be securely managed out of the TOE.

Application note:

This assumption is concerned with the physical and personnel aspects.

Among the TSF data set in the TOE, the management of authentication data is of particular importance. In the life cycle of the TOE, smart card related people such as manufacturer, issuer and card holder are involved. It is assumed that these users securely manage the authentication data they use. In addition, the authentication data is assumed to be securely kept in the Reader/Writer or terminal existing on the channel to the TOE.

2) A. Education:

The operational education is assumed to be undertaken based on the role assigned by the TOE.

Application note:

This assumption is concerned with the personnel aspects.

In this PP, the clarification of roles of the manufacturer, issuer and card holder is required as an organizational security policy (details on this will be described in a later section). What is assumed here is that the consumer has been sufficiently educated based on information provided by the ST authors to ensure that the consumer will make no errors in initial setting or operational mistakes.

3) A. Application

Application programs loaded by authorised personnel are assumed not to maliciously behave.

Application note:

This assumption is concerned with the physical aspects.

It is assumed that application programs to be loaded are developed by various users for diverse purposes. With respect to user data that are intentionally shared among a plurality of applications, it is assumed that individual application program has been designed with consideration given to the user data security.

Conceivable examples of malicious behavior by an application program include access into other applications' areas and abuse of the TSF interface.

3.3 Threats

1) T. Logical_Atk:

Expert level attackers may abuse of the logical interface, in order to modify or steal the user data.

Application note:

The logical interface is the interface for data exchange between the TOE and Reader/Writer, and it is commonly referred as 'command/response'. T. Logical_Atk is an attack that focuses on this logical interface, and generally an expert level threat.

For example, the command/response format is determined by international standards (e.g. ISO), regional standards (e.g. JICSAP), industry standards (e.g. EMV) or proprietary specifications. As exploits of the logical interface, it is conceivable that the different interpretations of its format and meaning will be abused. Moreover, the commands provided on specific purposes (such as card issuance, debugging, maintenance, etc.) may also be abused. Furthermore, tampering or exposure of primary assets using a combination of such commands is also conceivable. The ST authors should recognize the relationship between the countermeasures by the TOE and relevant attacks.

2) T. Repeat:

Expert level attackers may perform the replay attack for the logical interface to expose the TSF data that is used to submit the authenticity of the TOE. The logical interface for submitting the authenticity of the TOE may be replayed with brute force.

Application note:

A feature of smart card is the fact that a smart card has the function of submitting the identity of the card to the counterpart of communication (Reader/Writer or terminal) for authentication purposes (the command determined as the internal authenticate command of ISO corresponds to this). In order to implement this function, an encryption key is required. While this key does not constitute data used to protect user data, it may be required the security in an assumption in the PP/ST of the Reader/Writer or terminal, therefore this type of attack is considered as an expert level threat in this PP.

3) T. Abort:

Tampering with or exposing user data or TSF data through the TSF service abort. The intentional interruption by expert attackers and the accidental interruption by layman may cause the threat.

Application note:

Two cases may be considered with respect to the TSF service abort. One case is when an expert level attacker exerts physical (voltage, frequency, and temperature) stress for the purpose of tampering with or exposing the data and thus the ST authors must define the physical stress and countermeasures to be taken by the TOE.

The other case is a threat that occurs when a general layman is using the card, including the removal of the card in operation, the power termination at the power supply and other such events. Although these may not be intentional threats, destruction of internal user data or TSF data due to such events must be avoided.

4) T. Apl:

Proficient level unauthorised persons may load application programs which tamper with or expose the user data or TSF data of other application programs.

Application note:

Since it is assumed that the application programs loaded by an authorized person will not maliciously behave, such application programs loaded by an unauthorised person may be considered as a threat. Access to other application areas and abuse of TSF interface are conceivable methods of malicious behavior.

This is a threat in which proficient level attackers are involved.

5) T. Term:

A proficient level person may abuse the special terminal to tamper with or expose the user data.

Application note:

A special terminal is a device that uses the specific commands (e.g. for card issuance, the debugging or maintenance, etc.). Normally, this kind of terminal must be implemented with the functions to authenticate the operator. However, even with a terminal implemented with the authentication function, if the TOE does not authenticate the operator, the TOE cannot counter abuse of the terminal. This is a proficient level attack by a person who can easily perform initial setting of the TOE without any knowledge of the TOE design.

6) T. Issue:

Unauthorised user may abuse the user data or TSF data in the TOE before the authorised end user activates the TOE.

Application note:

From completion of the TOE production to the delivery to the end user, there are the various processes shown in Figure 2-2. In the case of smart card, a variety of organizations assume a variety of scopes of responsibilities to undertake these processes. It is conceivable that theft and counterfeiting of TOE by experts may be performed during the transport of the TOE between such organisations with different scope of responsibility or between different departments within a single organisation. Such TOE counterfeit that appears like a finished product through malicious means and abuse must be prevented.

7) T. Chip:

The smart card including the TOE may be attacked by sophisticated attackers who are well versed in semiconductors and/or cryptographic technologies.

Application note:

- by use of FIB (Focused Ion Beam) workstation, EBP (Electron Beam Prober), AFM (Atomic Force Microscope), the attacker physically tampers or eavesdrops (i.e. by tampering the TOE itself or the TSF data, retrieving the TSF data) the processing units or memory elements;
- the attacker estimates the TSF data through the analysis of the leaked information during cryptographic process;
- the attacker estimates TSF data through the analysis of the results under fault injected operations.

3.4 Organizational Security Policies

1) P. Role:

The roles with respect to security management of the TOE shall be defined clearly.

Application note:

In producing this PP, several specification documents have been referenced. In these specifications the relationship between roles and commands is clearly described. However, it is unclear whether the TOE should be developed recognizing the roles described therein. In this PP, the TOE should recognize the role, and the role is considered as a core to the security of the TOE and is thus determined as an organizational security policy.

At least, the roles should be defined as the issuance, maintenance and debugging and service operations. The ST authors must clearly define the roles supported by TOE and the corresponding commands.

2) **P.Secure_Path:**

A secure communication path shall be established between the TOE and the Reader/Writer and terminal.

Application note:

A secure path refers to a path that ensures the confidentiality and integrity of data during communication. As a method of establishing a secure path, in addition to logical measures such as encryption or digital signature for the whole data (command/response) or one data field on the path, there is a physical protection on the path. In this PP, the method of implementing this requirement is left up to the discretion of the consumer or the ST authors.

4. Security Objectives

4.1 Security Objectives for the TOE

1) O. Identification

The TSF must clearly identify the logical interface, authorized user and accessible assets.

Application note:

The ST authors must indicate that the TSF is able to clearly identify the user accessing the TOE, the logical interface to be used and the accessible assets.

In the definition of the user accessing the TOE, the roles to be determined by the organizational security policy, namely issuance, maintenance and debugging and service operations must be included at least. The refinement of roles determined by the organizational security policy and the creation of new roles depending on the circumstances of the TOE are left up to the discretion of the ST authors. For example, using terminology of card operations, the general user who is the ultimate card owner and the other card owners involved in the process from chip manufacture to card issuance (chip vendor, card manufacturer, service provider, application program provider, card issuer, personalizer, etc.) correspond to this. Moreover, at the stage of card use, the administrator who utilizes the card service also is corresponding. In this objective, it is defined as a user to be identified by the TOE.

The logical interface generally is, as well as specified under ISO 7816, those specified in the regional standard, industrial standard and proprietary specification and the TSF must clearly identify them.

As for the assets, they must be identified. If the card does not support the application loading capabilities, the EF (Elementary File) should be the identifiable unit. However, for those cards targeted under this PP, the unit of asset may be significantly expanded. The ST authors must clearly define the assets of a smart card to be delivered to the card holder for the first time.

2) O. Authentication

The TSF must ensure that only authorized users can access the user data.

Application note:

Among the user data protected by the TOE are the data used by the downloaded applications or the application programs themselves. Access to the user data to be protected by the TOE should be limited to the users authenticated by the TOE.

The methods of user authentication are variable like PIN, terminal authentication using an algorithm (e.g. external authentication command), authenticated data (e.g. certificate for loading application data). The requirement in this objective is that an authentication method is in place but not the appropriateness of the authentication method.

3) O. Issuer_Wk

The TSF must clearly define operations in the issuance process and its completion, and ensure that only the administrator can perform these operations.

Application note:

In this objective, the administrator is defined as the personnel involved in the issuance operation who has the authority with respect to configuring the environment of an application (allocating the service domain and loading the application program) or with respect to setting or changing the TSF data. The ST authors should clearly identify not only these types of authority but also the logical interface required in the issuance operations and, in the event there is an sequential rule in the logical interfaces, must also identify the sequence. However, this information may be enticement to attackers and thus the ST authors should be careful in describing the sequence.

Generally, the issuance operations involve not only the data setting required by the issuer but also include information setting on the surface of the card. The ST authors must take all these processes into consideration to distinguish between the in-process TOE (unstable condition) and the completed TOE, in order to counter threats such as theft. Technically, the in-process TOE is deactivated, and when the TOE is activated, it represents that the issuance process is completed.

4) O. Trouble_Shoot

The TSF must ensure that only an authorized user can perform the troubleshooting.

Application note:

The TOE is provided with means of troubleshooting (using the logical interface) in the manufacturing stage or in the end-usage stage. The users who can perform the troubleshooting should be limited to authorized personnel in accordance with its role (manufacturer, issuer, etc.).

5) O. Secure_Mech

The TSF must provide secure authentication mechanism(s) to counter replay attacks on authentication.

Application note:

The authentication data are the primary targets of this kind of attack (brute force attack). Accordingly, the authentication mechanism must be implemented with the functions for withstanding replay attacks.

Moreover, since the clearance functions provided by the smart card may also be a target of replay attacks (for guessing the key), a similar security functions are required. The key used in internal authentication command may be an example.

Note) the key used in internal authentication command is not the TSF data. However, from the perspective of the Reader/Writer or terminal that is the communication counterpart for the TOE, the key will be required to be secure as an assumption in the PP of the Reader/Writer or terminal. Therefore this protection is included as a security objective for the TOE.

6) O. Separate

The TSF must ensure that the TSF prevent the TSF-itself from interference and tampering by the application programs. The TSF must ensure application programs against resource invasion by other application programs.

Application note:

The assumption **A.Application** states that application programs loaded by an authorized person will not take unauthorised action. However, for a smart card that supports the function to load various application programs of different origin, a function to segregate each application, namely a firewall function should be necessary. The firewall prevents unauthorized accesses into other application areas either directly or via the TSF interface. Moreover, in the event the resource collision occurs, the integrity of the resource must be ensured.

7) O. Recovery

The TSF must provide the mechanism to recover the user data and TSF data securely after interruption.

Application note:

The TSF services may be interrupted during the services are turned on for a variety of causes. The TOE must detect the interruption regardless of whether such interruption is intentional or erroneous, and it must recover the states prior to detection of the abnormality (TSF, TSF data and user data shall be recovered the states before the abnormality). Moreover, the TOE itself must not be in such unstable state, where some asset exposure or tampering may be undertaken.

8) O. Clear

The TSF must ensure that the user data or TSF data will not be retained in the work area used by the application programs.

Application note:

In the event selected application programs the work area when undertaking their services, regardless of whether the service is aborted or is completed successfully, the both user data or TSF data must not be retained in the work area in order to prevent any abuse during the next service. This security objective is independent on whether or not the logical interface accesses directly or indirectly to the work area.

4.2 Security Objectives for the Environment

The assumptions except OE.Secure_Path are themselves the objectives with respect to the environment and the expression is the same as for the assumptions.

1) OE. Secure_Path:

A secure communication path must be established between the TOE and the Reader/Writer and terminal.

2) OE. TSF_Data:

The TSF data to be set in the TOE is assumed to be securely managed out of the TOE.

Application note:

"out of the TOE" means Hardware of Smart Card, Reader/Writer, Terminal, and Server in Figure 2-1 and actors in Figure 2-2.

3) OE. Education:

The operational education is assumed to be undertaken based on the role assigned by the TOE.

4) OE. Chip:

The TOE is assumed to operate on a physically secure chip.

Application note:

The TOE developer should confirm that physical security measures implemented on the hardware. The followings are the protection profiles that require the hardware security:

- JICSAP ver.2.0 Protection Profile part1, Multi-Application Secure System LSI Chip Protection Profile; Version 2.5, June 6, 2003 (PP/0301)
- Smartcard IC Platform Protection Profile; Version 1.0, Jul 2001 (BSI-PP-0002)
- Protection Profile Smartcard Integrated Circuit; Version 2.0, Sep 1998 (PP/9806)

The TOE developer should pay attention to the design and implementation of the TOE so as to utilize security measures of the IC chip.

5) OE. Application

Application programs loaded by authorised personnel are assumed not to maliciously behave.

5. Security Requirements

5.1 TOE Security Requirements

5.1.1 TOE Security Functional Requirements

The security functional requirements for the TOE are the following twenty-five require requirements. These requirements are all drawn from Common criteria v2.1 and no refinement has been made. The ST authors must perform appropriate assignment, selection, refinement and iteration operations with respect to these requirements in accordance with the TOE developed.

FCS_CKM.1 **Cryptographic key generation**

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

Dependencies: **[FCS_CKM.2 Cryptographic key distribution**
or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.4 **Cryptographic key destruction**

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[assignment: cryptographic key destruction method]** that meets the following: **[assignment: list of standards]**.

Dependencies: **[FDP_ITC.1 Import of user data without security attributes**
or
FCS_CKM.1 Cryptographic key generation]
FMT_MSA.2 Secure security attributes

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[assignment: list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

Dependencies: **[FDP_ITC.1 Import of user data without security attributes**
or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

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**

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 authorise access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorise 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

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **[selection: allocation of the resource to, deallocation of the resource from]** the following objects: **[assignment: list of objects]**.

Dependencies: No dependencies

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **[assignment: number]** unsuccessful authentication attempts occur related to **[assignment: list of authentication events]**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[assignment: list of actions]**.

Dependencies: **FIA_UAU.1 Timing of authentication**

FIA_ATD.1 User attribute definition

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

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**

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to **[assignment: identified authentication mechanism(s)]**.

Dependencies: No dependencies

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

FIA_UAU.6 Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions **[assignment: list of conditions under which re-authentication is required]**.

Dependencies: No dependencies

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

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to **[selection: determine the behaviour of, disable, enable, modify the behaviour of]** the functions **[assignment: list of functions]** to **[assignment: the authorised identified roles]**.

Dependencies: **FMT_SMR.1 Security roles**

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 authorised identified roles]**.

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

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Dependencies: **ADV_SPM.1 Informal TOE security policy model**
[FDP_ACC.1 Subset access control
or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

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 authorised 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

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]** the **[assignment: list of TSF data]** to **[assignment: the authorised identified roles]**.

Dependencies: **FMT_SMR.1 Security roles**

FMT_SMR.1 Security roles

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

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

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

FPT_AMT.1 Abstract machine testing

FPT_AMT.1.1 The TSF shall run a suite of tests **[selection: during initial start-up, periodically during normal operation, at the request of an authorised user, other conditions]** to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Dependencies: No dependencies

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**

FPT_RCV.3 Automated recovery without undue loss

FPT_RCV.3.1 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

FPT_RCV.3.2 For **[assignment: list of failures/service discontinuities]**, the TSF shall ensure the return of the TOE to a secure state using automated procedures.

FPT_RCV.3.3 The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding **[assignment: quantification]** for loss of TSF data or objects within the TSC.

FPT_RCV.3.4 The TSF shall provide the capability to determine the objects that were or were not capable of being recovered.

Dependencies: **FPT_TST.1 TSF testing**
AGD_ADM.1 Administrator guidance
ADV_SPM.1 Informal TOE security policy model

FPT_RCV.4 Function recovery

FPT_RCV.4.1 The TSF shall ensure **that [assignment: list of SFs and failure scenarios]** have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

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

FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests **[selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]]** to demonstrate the correct operation of the TSF**.**

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

Dependencies: **FPT_AMT.1 Abstract machine testing**

5.1.2 Explicitly Stated IT Security Requirements

The explicitly stated IT security requirements required for the TOE are the following two requirements. These requirements have been added in accordance with the regulations of Common criteria v2.1. Assignment, refinement and iteration operations must be undertaken with respect to these requirements in accordance with the TOE developed.

FAU_CFG.1	**Configuration generation**
FAU_CFG.1.1	The TSF shall maintain the configuration file as an object.
FAU_CFG.1.2	The TSF shall record within the configuration file at least the following configuration data 1) TOE identification and release date 2) **[assignment: other configuration-related information]**
Dependencies:	No dependencies

FDP_IOA.1	**Attribute definition of Logical interface and object**
FDP_IOA.1.1	The TSF shall maintain the following list of security attributes belonging to individual logical interfaces and objects: **[assignment: list of security attributes]**.
Dependencies:	No dependencies

5.1.3 TOE Security Assurance Requirements

The assurance requirements of this TOE are comprised of EAL4 augmented with AVA_VLA.4. These requirements have been selected from CC part 3. The ST authors can perform appropriate refinement and iteration operations with respect to these requirements in conformance with the TOE developed.

5.1.4 Minimum Strength of Function (SOF) Claim

The minimum strength of function of this TOE is SOF-high.

5.2 Security Requirements for the IT Environment

The security functional requirements for the IT environment are the following two requirements. These requirements are drawn from Common criteria v2.1 part 2 and no refinement operation has been performed. The ST authors must perform appropriate assignment, selection, refinement and iteration operations with respect to these requirements in accordance with the TOE developed.

FDP_RIP.1 **Subset residual information protection**

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **[selection: allocation of the resource to, deallocation of the resource from]** the following objects: **[assignment: list of objects]**.

Dependencies: No dependencies

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

6. Rationale

6.1 Security Objectives Rationale

Table 6-1 shows that each threat, organisational security policy and assumption to be countered/satisfied are mapped to at least one security objective for the TOE and objectives for the environment.

Table 6-1 Security objectives rationale

Environment/ Objectives		for the TOE								for the environment				
		1 O.Identification	2 O.Authentication	3 O.Issuer_Wk	4 O.Trouble_Shoot	5 O.Secure_Mech	6 O.Separate	7 O.Recovery	8 O.Clear	1 OE.Secure_Path	2 OE.TSF_Data	3 OE.Education	4 OE.Chip	5 OE.Application
Threats	1) T.Logical_Atk	• ›	• ›	• ›	• ›									
	2) T.Repeat					• ›								
	3) T.Abort							• ›	• ›					
	4) T.Apl		• ›				• ›							
	5) T.Term		• ›	• ›	• ›									
	6) T.Issue			• ›										
	7) T.Chip												• ›	
Policy	1) P.Role	• ›	• ›	• ›	• ›							• ›		
	2) P.Secure_Path									• ›				
Assumptions	1) A.TSF_Data										• ›			
	2) A.Education											• ›		
	3) A.Application													• ›

The rationale for the seven threats is as given below.

1) T. Logical_Atk is countered by O. Identification, O. Authentication, O. Issuer_Wk and O. Trouble_Shoot

   Through O.Identification, the logical interface is clearly identified and commands with erroneous syntax or semantics are eradicated.

   Through O.Identification, the assets to be protected are clearly identified, and through O.Authentication, the users who can access such assets are limited to those authenticated.

   Commands for the issuance operation, debugging and maintenance are identified by O.Identification and the use of these commands is limited to users authenticated through O.Issuer_Wk and O. Trouble_Shoot accordingly.

2) T. Repeat is countered by O.Secure_Mech.

   Through O.Secure_Mech, the authentication mechanism is provided with a preventive mechanism against not only replay attacks onto the TSF data but also inference of the TSF data of Reader/Writer or terminal thus reducing the likelihood of threat.

   Application note:

   The mechanism provided by O.Secure_Mech prevents not only against attacks on the PIN or terminal authentication key but also attacks on the key used in the Reader/Writer or terminal for card authentication.

3) T. Abort is countered by O.Recovery and O.Clear

   Even if the TSF service is interrupted, O.Recovery recovers the user data and TSF data to the original (TSF, TSF data and user data shall be recovered the states before the occurrence of abnormality) in the secure state. Moreover, through O. Clear, the user data or TSF data used extracted within the work area is cleared so that they cannot be used in the next service.

4) T. Apl is countered by O. Authentication and O. Separate

   The users who can download application programs are authenticated through O.Authentication. Moreover, the accesses by the loaded application program are limited to the area allocated for that program by O.Separate thus preventing resource collision with other applications.

5) T. Term is countered by O. Authentication, O. Issuer_Wk, and O. Trouble_Shoot.

   Even if the special terminal (e.g. for card issuance, the debugging or maintenance, etc.) were abused, the users who can use the logical interface of that terminal are authenticated through O.Authentication and limited to a role dedicated to the issuance operations and maintenance/debug operations through O.Issuer_Wk and O.Trouble_Shoot.

6) T. Issue is countered by O. Issuer_Wk.

Through O. Issuer_Wk, the logical interfaces (including sequential rule) to proceed and complete the issuance operations are clearly identified and the in-process TOE is rendered unusable.

7) T.Chip is counterd by OE.Chip.

Through OE.Chip, the IC chip on which the TOE runs has security measures to counter physical attacks, logical attacks, and side channel attacks. The TOE developer also has to pay attention to utilizing those security measures in design and implementaion of the TOE.

The rationale regarding policy is as follows.

1) P. Role is countered by O. Identification, O. Authentication, O. Issuer_Wk, O. Trouble_Shoot and OE. Education.

Through O. Identification, the roles of users that are allowed accesses are identified and authenticated through O. Authentication. Moreover, the logical interfaces for issuance or maintenance/debugging operations are limited to that role and authenticated user. The role that can perform the issuance operation and its completion is clearly indicated through O.Issuer_Wk. Through O.Trouble_Shoot the role that can perform the troubleshooting is restricted to an authorized user. Furthermore, education is provided for the users with such roles through OE. Education.

2) P. Secure_Path is countered by OE.Secure_Path

Through OE.Secure_Path, the secure communication path between the TOE and the Reader/Writer to ensure the user data integrity and confidentiality is realised.

The assumptions themselves are described in the format of objectives and the objectives of the environment are represented in the same way as assumptions.

6.2 Security Requirements Rationale

Table 6-2 lists the security objectives for the TOE and security objectives for the environment in the vertical axis and the security functional requirements in the horizontal axis and shows the relationship between these. The primary requirements directly address to security objectives. The supportive requirements support for the security objectives. These two types of requirements support the security objectives directly.

Table 6-2 Objectives-Functional Requirements relation

	Objectives	FAU_CFG.1	FCS_CKM.1	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_RIP.1	FIA_AFL.1	FIA_ATD.1	FIA_IOA.1	FIA_UAU.1	FIA_UAU.4	FIA_UAU.5	FIA_UAU.6	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPT_AMT.1	FPT_FLS.1	FPT_PHP.3	FPT_RCV.3	FPT_RCV.4	FPT_SEP.1	FPT_TST.1	ADV_SPM.1	AGD_ADM.1
TOE	1) O.Identification									◎	◎																			
	2) O.Authentication		○	○	○	◎	◎			◎	◎	◎	○	○	○	◎			△	△										△	
	3) O.Issuer_Wk		○	○	○	◎	◎			◎	◎	◎	○	○	○	◎	○	○	○	○	○	○								△	
	4) O.Trouble_Shoot	◎	○	○	○	◎	◎			◎	◎	◎	○	○	○	◎			△	△										△	
	5) O.Secure_Mech								◎	◎		◎		◎		△															
	6) O.Separate																											◎			
	7) O.Recovery																						△	◎		◎	◎		△	△	△
	8) O.Clear							◎																							
Env.	2) OE.TSF_Data							◎																							
	4) OE.Chip																								◎						

Note 1) the double circle indicates primary requirements for the objectives, the single circle indicates the supportive requirements that strengthen the principal requirements and the triangle indicates dependencies.

6.2.1 Fulfilment of TOE Objectives by the TOE Functional Requirements

The rationale for the eight security objectives for the TOE is provided below.

In this PP, it is not desirable to describe the implementation details (security functional requirements). However, in order to establish the rationale, there are some cases where it is necessary to assume an implementation image. For such cases, an example of implementation is given as application note.

1) O.Identification is satisfied through

FIA_ATD.1 User attribute definition and;

FDP_IOA.1 Attribute definition of Logical interface and object

Through FIA_ATD.1, the user (subject) is clearly identified and through FDP_IOA.1, the logical interface and assets (objects) are clearly identified.

Application note:

The ST authors must specify the information for identifying the user, logical interface and assets to [list of security attributes] in FIA_ATD.1 and FDP_IOA.1.

2) O.Authentication is satisfied through the following six functional requirements.

FIA_ATD.1 User attribute definition;

FDP_IOA.1 Attribute definition of Logical interface and object;

FIA_UID.1 Timing of identification;

FIA_UAU.1 Timing of authentication;

FDP_ACC.1 Subset access control; and

FDP_ACF.1 Security attribute based access control

Through FIA_ATD.1 and FDP_IOA.1, the user (subjects), logical interface (operations) and assets are clearly identified, and the user is authenticated through FIA_UAU.1. The compliance with the rules determined by access control SFP in FDP_ACC.1 and FDP_ACF is ensured with respect to access by the authenticated subjects (authorized users). The information that the TOE can indicate to the user prior to user identification and authentication is clearly identified through FIA_UID.1 and FIA_UAU.1.

The following constitute the six supportive requirements to enforce O.Authentication.

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.6 Re-authenticating

FCS_CKM.1 Cryptographic key generation

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1 Cryptographic operation

Through FIA_UAU.4, the reuse of authentication data (e.g. Challenge data) is restricted, and therefore even if the authentication data were to be stolen in the path, such data are rendered useless. Through FIA_UAU.5, the authentication mechanisms supported by the TOE are clarified, and since these utilize the cryptographic algorithm and key length specified in components of FCS classes, they are able to counter external attacks. Moreover, through FIA_UAU.6, the timing of re-authentication is clearly specified and unauthorised access to the assets used in the work area is prevented.

Through FCS_CKM.1, FCS_CKM.4 and FCS_COP.1, the algorithm, generation, destruction, and length of the key used in authentication or encryption, which are able to counter external attacks, are clearly specified.

FMT_MSA.2, FMT_MSA.3 and ADV_SPM.1 are selected in order to satisfy the dependencies to be enforced.

Application note:

The ST authors must indicate the **[access control SFP]** name implemented by the TOE in FDP_ACC.1 and FDP_ACF.1 and clearly identify the subjects, operations and objects controlled by that SFP in **[list of subjects, objects and operations among subject and objects covered by the SFP]**. The ST authors must also specify the security attributes used in the access control in **[security attributes]** and rules in **[rules governing access among controlled subjects and controlled objects using controlled operations on controlled subjects]**.

In case that the security mechanism uses random numbers as the challenge data for the terminal authentication, the name of such mechanism must be specified in **[identified authentication mechanism(s)]** in FIA_UAU.4. Moreover, all authentication mechanisms supported by the TOE must be clearly specified in **[list of multiple authentication mechanism(s)]**, and specify the authentication mechanism with the applicable users or roles in **[rules describing how the multiple authentication mechanisms provide authentication]** of FIA_UAU.5. In FIA_UAU.6, the timing of re-authentication, e.g. normal completion of TSF service, TSF service abort and all such events, must be specified in **[list of conditions under which re-authentication is required]**.

In FCS_CKM.1, FCS_CKM.4 and FCS_COP.1, it is desirable that incorporation be concretely stated using refinement and iteration.

3) O. Issuer_Wk is satisfied with the following six functional requirements.

FIA_ATD.1 User attribute definition;

FDP_IOA.1 Attribute definition of Logical interface and object;

FIA_UID.1 Timing of identification;

FIA_UAU.1 Timing of authentication;

FDP_ACC.1 Subset access control; and

FDP_ACF.1 Security attribute based access control

Through FIA_ATD.1 and FDP_IOA.1, issue operator (subjects), logical interfaces for issuance (operations) and assets (objects) are clearly identified and with respect to issuance operations, authentication is performed through FIA_UAU.1.

The compliance to the rules led by the access control SFP in FDP_ACC.1 and FDP_ACF.1 is ensured with respect to access by an authenticated issuer.

The information that the TOE can indicate to the issuer prior to the identification and authentication is clearly specified in FIA_UID.1, FIA_UAU.1.

The following are the twelve supportive requirements that strengthen O. Issuer_Wk.

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.6 Re-authenticating

FMT_MOF.1 Management of security functions behaviour

FMT_MSA.1 Management of security attributes

FMT_MSA.2 Secure security attributes

FMT_MSA.3 Static attribute initialisation

FMT_MTD.1 Management of TSF data

FMT_SMR.1 Security roles

FCS_CKM.1 Cryptographic key generation

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1 Cryptographic operation

Through FIA_UAU.4, reuse of authentication data (e.g. Challenge data) used in authentication is restricted, and even if the authentication data were to be stolen in the path, such data are rendered useless. Through FIA_UAU.5, the authentication mechanisms supported by the TOE are clarified, and since these utilize the cryptographic algorithm and key length specified in components of FCS classes, they are able to counter external attacks. Moreover, through FIA_UAU.6, the timing of re-authentication is clearly specified and unauthorised access to the assets used in the work area is prevented.

Through FMT_SMR.1, the issuance operations are clearly identified as roles. The access to TSF data concerning issuance operations is limited to the issuance operation role through FMT_MTD.1. Moreover, the default value of TSF data is specified in FMT_MSA.3, and the appropriateness of the TSF data input by the issuer is checked in FMT_MSA.2. The modifications of security attributes are limited to the issuer through FMT_MSA.1. And furthermore, the modification of functions used by the issuer is limited to the Role specified in FMT_MOF.1.

Through FCS_CKM.1, FCS_CKM.4 and FCS_COP.1, the algorithm, generation, destruction, and length of the key used in authentication or encryption are clearly specified.

ADV_SPM.1 is selected in order to satisfy the dependency to be enforced.

Application note:

The ST authors must indicate the **[access control SFP]** name implemented by the TOE in FDP_ACC.1 and FDP_ACF.1 and clearly identify the subjects, operations and objects controlled by that SFP in **[list of subjects, objects and operations among subject and objects covered by the SFP]**. The ST authors must also specify the security attributes used in the access control in **[security attributes]** and rules in **[rules governing access among controlled subjects and controlled objects using controlled operations on controlled subjects]**. In the rule definition, if there is a sequential rule among the logical interfaces for issuance operations, that sequence must also be clearly specified. Moreover, the method of indicating completion of the issuance operations must be clearly described in FDP_ACC.1 and FDP_ACF.1

In case that the security mechanism uses random numbers as the challenge data for the terminal authentication, the name of such mechanism must be specified in **[identified authentication mechanism(s)]** in FIA_UAU.4. Moreover, all authentication mechanisms supported by the TOE must be clearly specified in **[list of multiple authentication mechanism(s)]**, and specify the authentication mechanism with the applicable users or roles in **[rules describing how the multiple authentication mechanisms provide authentication]** of FIA_UAU.5. In FIA_UAU.6, the timing of re-authentication, e.g. normal completion of TSF service, TSF service abort and all such events, must be specified in **[list of conditions under which re-authentication is required]**.

[The authorised identified roles] of FMT_SMR.1 must specify the issuer, and the TSF data to be operated by that issuer must be specified in FMT_MTD.1.

In FCS_CKM.1, FCS_CKM.4 and FCS_COP.1, it is desirable that incorporation be concretely stated using refinement and iteration.

4) O. Trouble_Shoot is satisfied with the following seven functional requirements.

FIA_ATD.1 User attribute definition

FDP_IOA.1 Attribute definition of Logical interface and object

FIA_UID.1 Timing of identification

FIA_UAU.1 Timing of authentication

FDP_ACC.1 Subset access control

FDP_ACF.1 Security attribute based access control

FAU_CFG.1 Configuration generation

Through FIA_ATD.1 and FDP_IOA.1, maintenance and debugging (subjects), logical interfaces for maintenance and debugging (operations) and assets (objects) are clearly identified and with respect to maintenance and debugging, authentication is performed through FIA_UAU.1.

The compliance to the rules led by the access control SFP in FDP_ACC.1 and FDP_ACF.1 is ensured with respect to the access by authenticated subjects. The TOE ID information and other information for maintenance and debugging may be obtained as specified in FAU_CFG.1.

Information that the TOE can provide for the maintenance and debugging operations prior to the identification and authentication is clearly identified in FIA_UID.1, FIA_UAU.1.

The following are the supportive requirements to enforce O. Trouble_Shoot.

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.6 Re-authenticating

FCS_CKM.1 Cryptographic key generation

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1 Cryptographic operation

Through FIA_UAU.4, reuse of authentication data (e.g. Challenge data) used in authentication is restricted, and even if the authentication data were to be stolen in the path, such data are rendered useless. Through FIA_UAU.5, the authentication mechanisms supported by the TOE are clarified, and since these utilize the cryptographic algorithm and key length specified in components of FCS classes, they are able to counter external attacks. Moreover, through FIA_UAU.6, the timing of authentication is clearly specified and unauthorised access to the assets used in the work area is prevented.

Through FCS_CKM.1, FCS_CKM.4 and FCS_COP.1, the algorithm, generation, destruction, and length of the key used in authentication or encryption are clearly specified.

FMT_MSA.2, FMT_MSA.3 and ADV_SPM.1 are selected in order to satisfy the dependencies to be enforced.

Application note:

The ST authors must indicate the **[access control SFP]** name implemented by the TOE in FDP_ACC.1 and FDP_ACF.1 and clearly identify the subjects, operations and objects controlled by the policy in **[list of subjects, objects and operations among subject and objects covered by the SFP]**. The ST authors must also designate the attributes used in access control in **[security attributes]** and rules in **[rules governing access among controlled subjects and controlled objects using controlled operations on controlled subjects]**.

In the event a mechanism whereby random numbers are used as challenge in terminal authentication is used, the name of such mechanism must be designated in **[identified authentication mechanism(s)]** in FIA_UAU.4. Moreover, all authentication mechanisms supported by the TOE must be clearly identified in **[list of multiple authentication mechanism(s)]** and the user or role subjected to the authentication mechanism **in [rules describing how the multiple authentication mechanisms provide authentication]** of FIA_UAU.5. In FIA_UAU.6, the timing of re-authentication, e.g. normal completion of TSF

service, TSF service abort and all such events, must be stated in **[list of conditions under which re-authentication is required]**.

In FCS_CKM.1, FCS_CKM.4 and FCS_COP.1, it is desirable that incorporation be concretely stated using refinement and iteration.

5) O. Secure_Mech is satisfied with the following four functional requirements.

FIA_ATD.1 User attribute definition

FIA_UAU.1 Timing of authentication

FIA_UAU.5 Multiple authentication mechanisms

FIA_AFL.1 Authentication failure handling

For the users defined with the security attribute in FIA_ATD.1, an authentication mechanism to prevent replay attacks is provided through FIA_UAU.5. If the event such abnormality supposed as a replay attack is detected, the action specified in FIA_AFL.1 is undertaken. The information visible to a user before the authentication is clearly identified in FIA_UAU.1.

FIA_UID.1 is selected in order to satisfy the dependencies to be enforced.

Application note:

The ST authors must describe the authentication mechanism resistant to replay attacks in **[rules describing how the multiple authentication mechanisms provide authentication]** of FIA_UAU.5.

The ST authors must describe the events concerned with authentication in the **[list of authentication events]**, and describe the TSF actions for authentication failures in **[assignment: list of actions]** in FIA_AFL.1. In the description of such TSF actions for authentication failures, the abnormality in the identification to the Reader/Writer or terminal must be included as well as failure with respect to the TSF data.

6) O. Separate is satisfied with:

FPT_SEP.1 TSF domain separation

FPT_SEP.1 allows the TSF is protected from the application programs. And by expanding domain concept to each application program, each loaded application program is restricted its direct or indirect accesses to other applications.

7) O. Recovery is satisfied with the following:

FPT_RCV.3 Automated recovery without undue loss

FPT_RCV.4 Function recovery

FPT_FLS.1 Failure with preservation of secure state

Through FPT_RCV.3 and FPT_RCV.4, service interruptions are detected and the integrity of TSF data used in the service and the TOE function are automatically recovered. FPT_FLS.1 ensures that the TOE returns to a secure state.

The following security functional requirements and security assurance requirements are necessary for the dependencies from FPT_RCV.3.

FPT_TST.1 TSF testing

FPT_AMT.1 Abstract machine testing

ADV_SPM.1

AGD_ADM.1

Application note:

The ST authors must specify the events to recognized by the TOE as a service abnormality in the **[list of failures/ service discontinuities]** in FPT_RCV.3 and the **[list of types of failures in the FSF]** in FPT_FLS.1 in a manner that covers T. Abort described in Section 3.3.

Moreover, in order to satisfy FPT_TST.1 and FPT_AMT.1 that are dependencies from FPT_RCV.3, it is necessary for the TOE to confirm the state of its own operational environment (hardware, resources, etc.) before commencing its operation.

8) O. Clear is satisfied through:

FDP_RIP.1 Subset residual information protection

The assets used in the work area cannot be reused by other services through FDP_RIP.1.

Application note:

The ST authors must specify the timing at which the asset is rendered unusable by other services in **[allocation of the resource to, deallocation of the resource from]** in FDP_RIP.1. The ST authors should be careful that only logical deletion of work area does not constitute what is meant by “rendered unusable”.

6.2.2 Fulfilment of the IT Environment Objectives by the Functional Requirements

Among the five security objectives for the environment described, there are two security objectives for the IT environment. The rationale is as follows.

2) OE TSF_Data is satisfied through:

FDP_RIP.1 Subset residual information protection

FDP_RIP.1 ensures that information is not retained in the IT devices external to the TOE.

4) OE. Chip is satisfied through:

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3 ensures that the hardware on which the TOE operates can withstand physical attacks.

6.2.3 Suitability of Minimum Strength of Function (SOF) Level

The TOE in this PP is a smart card that has security as its catch phrase and is used for diverse applications such as municipal, financial and medical services as explained in Section 3 "Security Environment". Moreover, the management of the card itself is entrusted to card users with varying levels of experience. In other words, while a large volume of proprietary data is stored on a smart card, the card is placed in an environment prone to attack. Moreover, the smart card specifications are gradually becoming standardized enhancing development efficiency for the developer but at the same time, creating a more convenient environment for attackers.

Due to these circumstances, the minimum strength of function in this PP should be **SOF-High** to prevent prolonged attack by expert-level attackers.

6.2.4 Appropriateness of the TOE Assurance Requirements

A variety of proprietary information stored in a smart card is attractive to criminals. While smart cards that replace the plastic cards have high level of security as its catch phrase, as such smart cards become more pervasive, instances of counterfeiting are arising. Due to these circumstances, the security function implemented in a smart card must be highly reliable. On the other hand, the evaluation for a high assurance level takes a considerable cost and thus this may impact the product. Consideration these facts, EAL4 may be considered as an appropriate level since it includes evaluation (evaluation of low-level designs and source codes) on the details of the TOE.

In the usage environment assumed in this PP, it is assumed that various people with a significant level of skill will undertake attacks. In order to counter such attacks, it is necessary to review the TOE from various angles to ensure that there are no exploitable vulnerabilities, and for this reason, AVA_VLA.4 is added.

6.2.5 Mutual Support and internal consistency of Security Requirements

The selected requirements are internally consistent. The PP includes no requirements that contradict another requirement in the PP. In the set of requirements where different requirements apply to the same types of events, operations, data, the requirements do not contradict each other.

Table 6-3 provides the mutually supportive functional requirements for each objective.

Table 6-3 Mutual Supportive Requirements for each Objective

Objectives		Mutual support requirements
TOE	1) O.Identification	FIA_ATD.1, FDP_IOA.1
	2) O.Authentication	FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FDP_ACC.1, FDP_ACF.1, FIA_ATD.1, FDP_IOA.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_UID.1, FMT_MSA.2, FMT_MSA.3, ADV_SPM.1
	3) O.Issuer_Wk	FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FDP_ACC.1, FDP_ACF.1, FIA_ATD.1, FDP_IOA.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_UID.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_SMR.1, ADV_SPM.1
	4) O.Trouble_Shoot	FAU_CFG.1, FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FDP_ACC.1, FDP_ACF.1, FIA_ATD.1, FDP_IOA.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_UID.1, FMT_MSA.2, FMT_MSA.3, ADV_SPM.1
	5) O.Secure_Mech	FIA_AFL.1, FIA_ATD.1, FIA_UAU.1, FIA_UAU.5, FIA_UID.1
	6) O.Separate	FPT_SEP.1
	7) O.Recovery	FPT_AMT.1, FPT_FLS.1, FPT_RCV.3, FPT_RCV.4, FPT_TST.1, ADV_SPM.1, ADV_ADM.1
	8) O.Clear	FDP_RIP.1

Table 6-3(cont.) Mutual Supportive Requirements for each Objective

Environment	2) OE.TSF_Data	FDP_RIP.1
	4) OE.Chip	FPT_PHP.3

As for Bypass/Tampering/Deactivation: The embedded software in the smart card of this PP consists of only basic software. As the external interface of the TOE is restricted to logical interfaces, there is no bypassing, tampering, de-activation of the mutually supportive security functions in Table. 6-3. Though proprietary applications might be loaded to the card after issuing the card, as the TOE operates on its own domain requested by FPT_SEP.1, the applications can't bypass, tamper and deactivate.

Rationale that dependencies are satisfied:

Table 6-4 indicates direct and indirect dependencies of functional requirements. All of these dependencies are satisfied.

Table 6-4 Security functional requirements dependencies

Functional requirements		Depend on:	Descriptions
TOE	1)FAU_CFG.1	No dependencies	not applicable
	2) FCS_CKM.1	[FCS_CKM.2 or	Section 5.1.1(FCS_COP.1)
		FCS_CKM.4	Section 5.1.1
		FMT_MSA.2	Section 5.1.1
	3) FCS_CKM.4	[FDP_ITC.1or FCS_CKM.1]	Section 5.1.1(FCS_CKM.1)
		FMT_MSA.2	Section 5.1.1
	4) FCS_COP.1	[FDP_ITC.1or FCS_CKM.1]	Section 5.1.1(FCS_CKM.1)
		FCS_CKM.4	Section 5.1.1
		FMT_MSA.2	Section 5.1.1
	5) FDP_ACC.1	FDP_ACF.1	Section 5.1.1
	6) FDP_ACF.1	FDP_ACC.1	Section 5.1.1
		FMT_MSA.3	Section 5.1.1
	7) FDP_RIP.1	No dependencies	not applicable
	8) FIA_AFL..1	FIA_UAU.1	Section 5.1.1
	9) FIA_ATD.1	No dependencies	not applicable
	10) FIA_IOA.1	No dependencies	not applicable
	11) FIA_UAU.1	FIA_UID.1	Section 5.1.1
	12) FIA_UAU.4	No dependencies	not applicable
	13) FIA_UAU.5	No dependencies	not applicable
	14) FIA_UAU.6	No dependencies	not applicable
	15) FIA_UID.1	No dependencies	not applicable
	16) FMT_MOF.1	FMT_SMR.1	Section 5.1.1
	17) FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	Section 5.1.1(FDP_ACC.1)
		FMT_SMR.1	Section 5.1.1
	18) FMT_MSA.2	ADV_SPM.1	Section 5.1.3
		[FDP_ACC.1or FDP_IFC.1]	Section 5.1.1(FDP_ACC.1)
		FMT_MSA.1	Section 5.1.1
		FMT_SMR.1	Section 5.1.1
	19) FMT_MSA.3	FMT_MSA.1	Section 5.1.1
		FMT_SMR.1	Section 5.1.1
	20) FMT_MTD.1	FMT_SMR.1	Section 5.1.1
	21) FMT_SMR.1	FIA_UID.1	Section 5.1.1
	22) FPT_AMT.1	No dependencies	not applicable
	23) FPT_FLS.1	ADV_SPM.1	Section 5.1.1
	24) FPT_RCV.3	FPT_TST.1	Section 5.1.1
		AGD_ADM.1	Section 5.1.3
		ADV_SPM.1	Section 5.1.3
	25) FPT_RCV.4	ADV_SPM.1	Section 5.1.3
	26) FPT_SEP.1	No dependencies	not applicable
	27) FPT_TST.1	FPT_AMT.1	Section 5.1.1
Environmer	1) FDP_RIP.1	No dependencies	not applicable
	2) FPT_PHP.3	No dependencies	not applicable

6.2.6 Rationale for Explicitly Stated IT Security Requirements

This PP defines two explicitly stated IT security requirements.

FAU_CFG.1	**Configuration generation**
FAU_CFG.1.1	The TSF shall maintain the configuration file as an object.
FAU_CFG.1.2	The TSF shall record within the configuration file at least the following configuration data 1) TOE identification and release date 2) **[assignment: other configuration-related information]**

Smart cards are manufactured through the diverse processes shown in Figure 2-2. Moreover, a plurality of competing firms is involved in each process. Accordingly, the completed TOE is a combination of parts produced by firms with differing scopes of responsibility. In order to perform maintenance and debugging efficiently at the end-usage stage of the TOE, the parts produced by organisations with different areas of responsibility should be clearly identified. FAU_CFG.1 is a requirement that satisfies this need and has been added as there is no similar requirement in CC part 2.

Moreover, the information concerning the manufacturer is meaningful for an attacker; as such that information is under access control as an object. As attack agents are supposed to be the proficient, it is appropriate that assurance level is EAL4.

Application notes (Operations)

For FAU_CFG.1.2 2) assignment, the ST authors should specify any other configuration-related information about the TOE manufacturing phases.

FDP_IOA.1	**Attribute definition of Logical interface and object**
FDP_IOA.1.1	The TSF shall maintain the following list of security attributes belonging to individual logical interfaces and objects: **[assignment: list of security attributes]**.

FDP_ACF and FDP_ACC determine the relationship among users (subjects), objects and operations as in the access control policy. However, CC part 2 targets only the user to be identified. The TOE in this PP is the software of a smart card, and is the entire software that comprises the base of the card unlike the personal computer operating system. Accordingly, clear identification of objects or operations is relatively easier, and through such clear identification, the TSP or TSF are easier to understand to reduce the vulnerability. Though Security Functional Requirements for identification are defined in FIA class of CC part 2, they address user and/or subject identification. Therefore FDP_IOA.1 that identifies object is stated explicitly in FDP class. As attack agents are supposed to be the proficient, it is appropriate that assurance level is EAL4.

Application notes (Operations)

In FDP_IOA.1.1 assignment, the ST authors should specify the security attributes that the access control functions will use in the specification of the access control policy For example, such attributes may be things such as command names, command execution conditions, or any other attribute specified by the ST authors.

7. Annex

7.1 Glossary / acronym

Glossary

Smart card related people:	This corresponds to the user defined in the CC and is an operational term related to the stages from the manufacture to the end-usage. The smart card manufacturer, the issuer and cardholder are included within the definition of this term.
Manufacturer:	This term refers to organisations or people involved in the manufacture of a smart card and includes the firms to manufacture IC chips, develop software, package the chip, and fabricate the cards from chip package, and the people involved in those tasks in these (manufacturing, testing, maintenance).
Issuer:	The issuer is the user to set the rights and service information (loading application programs and configuring the operation environment [key data, initial values] of the application) on the smart card. This user is a part of the company procuring smart cards in this PP. The terms primary issuer or secondary issuer are sometimes used collectively with respect to these tasks.
Cardholder:	This user is the person who obtains a smart card from the issuer and enjoys the services set in the card.
Expert:	An expert is a person with the same level of knowledge as the manufacturer and who is capable of utilising manufacturing level devices.
Proficient:	A proficient is a person who has the same level of knowledge as the issuer and in particular has knowledge concerning issuance operations and who can utilize the devices used for card issuance.
Layman:	A layman is the user including people capable of operating a personal computer and obtaining standardisation materials.
Assets:	Assets are comprised of primary assets to be protected by the TOE and secondary assets for protecting the integrity and confidentiality of the TOE in the manufacturing process.
Primary assets:	Primary assets are data to be protected by the TOE and are comprised of the user data and TSF data that protect user data. The TSF data are comprised of authentication data and security attributes.
Secondary assets:	Secondary assets are data produced and used during the manufacturing process of the TOE to protect the integrity and confidentiality of the TOE. The detailed are provided in Common criteria v2.1 part 3 assurance requirements.
Logical interface:	The logical interface is the interface for exchanging data between a smart card and the communication counterpart (Reader/Writer or terminal) and is generally called command/response. The syntax is standardised under international standards (e.g. ISO/IEC), regional standards (e.g. JICSAP), industrial standards (e.g. EMV) or proprietary standards.
Issuance commands:	Issuance commands are the commands in the logical interfaces that the issuer uses in the issuance operations.
Maintenance/Debug related commands:	Maintenance/debugging commands are the commands in the logical interfaces that are required in the maintenance or testing of a smart card.

Acronym

OS	Operating System
CM	Card Manager
IC	Integrated Circuit

7.2 Japanese Translation of Functional Requirements

The following terms have been translated into Japanese for reference purposes by the Information Technology Promotion Agency, Japan and are the functional requirements for the TOE and IT environment. FAU_CFG.1 and FDP_IOA.1, the functional requirements that have been added, were translated by ECSEC.

7.3 TOE Functional Requirements

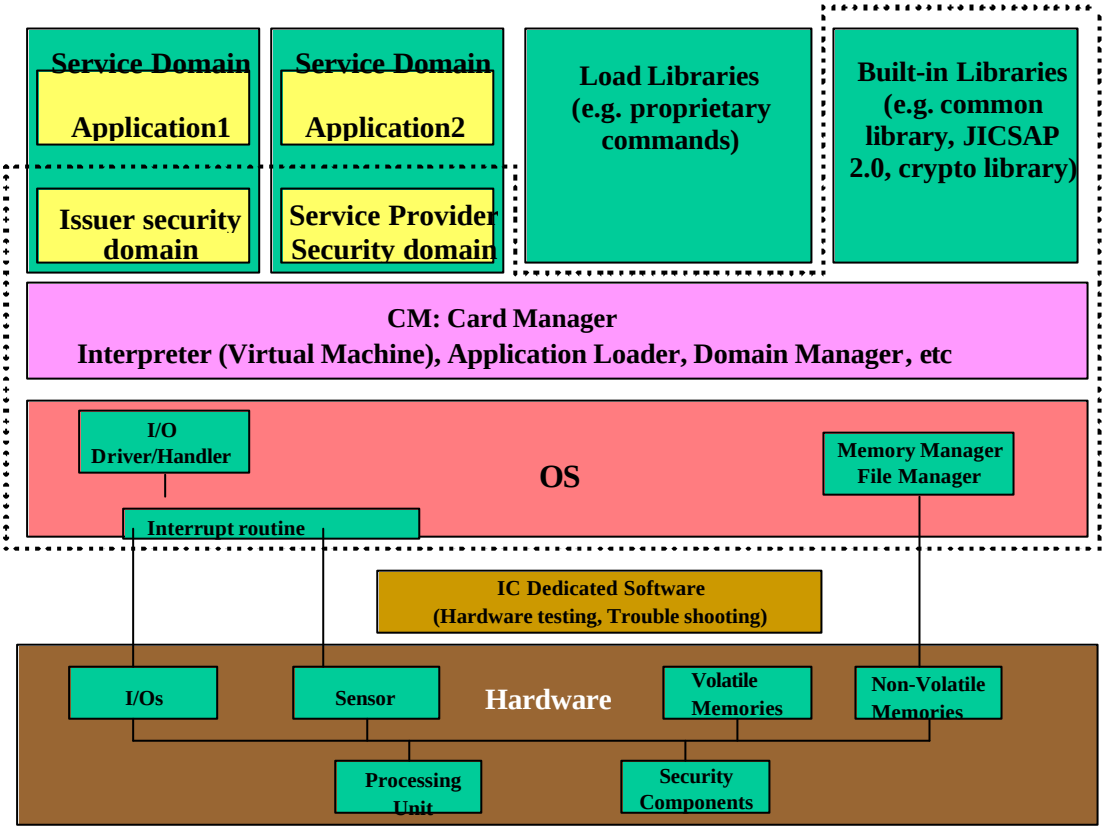
[This section is omitted, because it is same as section 5.1.]

7.4 Security Requirements for IT Environment

[This section is omitted, because it is same as section 5.2.]

7.5 Example of a TOE Structure

Smart cards that are capable of downloading a variety of application programs are already available on the market. This PP does not determine the structure or implementation method. It describes the security requirements to be implemented. Upon compiling the requirements of this document in the ST, it is desirable that the ST authors represents the functions of the TOE in a more detailed manner than this document and that defines the user interface and hardware boundaries. Figure 7-1 is an example of the expression of the TOE.



Sensor: temperature, frequency, electro-magnetic wave, instruction exception, timer, etc.

Figure 7-1 Example of TOE Configuration

In this figure, the TOE is consisting of OS comprised of I/O driver/handler that interfaces with the memory manager, file manager or Reader/Writer for managing hardware, card manager that controls application programs and operate on a higher tier and a group of libraries that support external logical interface. Moreover, the figure expresses the image of TSF data (issuer security domain, service provide service domain) under the control of the TOE.

Moreover, in order to clarify the boundary between the hardware and software, the software used for hardware debugging or reliability testing is represented as being outside the TSC.

7.6 Relationships with related Protection Profiles

In producing this PP, the PPs referenced are PP/9806, PP/9911, PP/0011, BSI-PP-0002 (SSVG), SCSUG and ICCS listed in Section 1.5. The following rationalize that some requirements that are adopted in other PP are not selected in this PP and that certain requirements are selected in this PP only.

7.6.1 FDP Class

Table 7-1 shows the FDP Class functional requirements for the FDP Class in the various PPs.

Table 7-1 Comparison of the FDP Class

FDP Class	9806 Phase3	9806 Phase3-7	9911	0010	SCSUG	ICCS	SSVG	JICSAP PP part2	0301 JICSAP PP part1
FDP_ACC.1 Subset access control					•	•		•	•
FDP_ACC.2 Complete Access Control		•	•	•				•	•
FDP_ACF.1 Security Attribute Based Access Control		•	•	•	•	•		•	•
FDP_IFC.1 Subset Information Flow Control		•			•	•	•	•	•
FDP_IFF.1 Simple Security Attributes		•			•	•		•	•
FDP_ITC.1 Import of User Data without Security Attributes			•	•	•	•		•	•
FDP_ETC.1 Export of User Data without Security Attributes			•	•	•			•	•
FDP_IOA.1 Attribute Definition of Logical interface and object								•	
FDP_ITT.1 Basic internal transfer protection					•		•	•	•
FDP_RIP.1 Subset residual information protection			•	•	•			•	•
FDP_RIP.2 Full residual information protection						•		•	•
FDP_ROL.1 Basic rollback				•				•	•
FDP_DAU.1 Basic Data Authentication			•	•				•	•
FDP_SDI.1 Stored Data Integrity Monitoring	•							•	•
FDP_SDI.2 Stored data integrity monitoring and action			•	•		•		•	•
FDP_UCT Inter-TSF user data confidentiality transfer								•	•
FDP_UIT.1 Data exchange integrity					•	•		•	•

1) FDP_ACC, FDP_ACF, FDP_RIP

The access control for the user data is mandatory in order to support O.Authentication, O.Issue_Wk and O.Trouble_Shoot. However, since if all objects in the smart card are targeted for access control, the load on the TOE would become excessive and thus FDP_ACC.1 and FDP_RIP.1 are selected.

2) FDP_IFC, FDP_IFF, FDP_ITC, FDP_ETC

The security attributes of user data or subjects that are stored in a smart card may be controlled. However, if such flow control as label control is introduced into the current logical interface,

extension of the logical interface or reworks of the existing cards will be required, and thus the supports for these requirements are abandoned in this PP.

3) FDP_ITT

It is desirable that the user data protection between the CPU and co-processor be implemented. However, as this would lead to excessive number of mandatory requirements, the supports for these requirements are left to the discretion the ST authors.

4) FDP_ROL

Existing smart cards do not have a logical interface that supports rollback. And, since extension of the logical interface or reworking of existing cards will be required, the support for this requirement is abandoned in this PP.

5) FDP_DAU.1, FDP_SDI

Based on the concept that maintaining the user data integrity is the responsibility of application programs, the support for these requirements are abandoned in this PP.

6) FDP_UCT, FDP_UIT

The user data integrity and confidentiality upon communication with an external TSF constitute an organizational security policy (P.Secure_Path) in this PP. However, in order to realize this OSP, the relevant mechanism is required in the smart card. The implementation of this mechanism is left to the discretion of the ST authors.

7) FDP_IOA

The identification of object and logical interface is necessary.

7.6.2 FIA Class

Table 7-2 shows the FIA Class functional requirements in the referenced PPs.

Table 7-2 Comparison of the FIA Class

FIA Class	9806 Phase3	9806 Phase3-7	9911	0010	SCSUG	ICCS	SSVG	JICSAP PP part2	0301 JICSAP PP part1
FIA_AFL.1 Authentication failure handling			•	•	•			•	•
FIA_ATD.1 User Attribute Definition	•		•	•	•	•		•	•
FIA_UAU.1 Timing of authentication			•	•	•	•		•	•
FIA_UAU.2 User authentication before any action	•							•	•
FIA_UAU.3 Unforgeable authentication			•					•	•
FIA_UAU.4 Single- use Authentication Mechanisms			•	•		•		•	•
FIA_UAU.5 Multiple authentication mechanisms								•	•
FIA_UAU.6 Re- authentication								•	•
FIA_UAU.7 Protected authentication feedback					•	•		•	•
FIA_UID.1 Timing of identification			•	•	•	•		•	•
FIA_UID.2 User Identification before any action	•		•	•				•	•

1) FIA_ATD

The identification for the user is same.

2) FIA_UID, FIA_UAU, AFL

As balance referrals may be necessary even without identification or authentication with respect to electronic money stored in a smart card, FIA_UID.1 and FIA_UAU.1 are selected. Moreover, clear identification of the authentication failure process (FIA_AFL.1), the authentication mechanism (FIA_UAU.5) and the timing of re-authentication (FIA_UAU.6) are considered mandatory. Assuming that a disposable token will be used to authenticate the counterpart of communication (Reader/Writer or terminal), FIA_UAU.4 is required. However, the requirement for user authentication using biometric (FIA_UAU.3) is left to the discretion of the ST authors.

7.6.3 FMT Class

Table 7-3 shows the FMT Class functional requirements in the various PPs.

Table 7-3 Comparison of the FMT Class

FMT Class	9806 Phase3	9806 Phase3-7	9911	0010	SCSUG	ICCS	SSVG	JICSAP PP part2	0301 JICSAP PP part1
FMT_LIM.1 Limited capabilities							•	•	•
FMT_LIM.2 Limited availability							•	•	•
FMT_MOF.1 Management of security functions behavior		•	•	•	•	•		•	•
FMT_MSA.1 Management of security attributes		•	•	•	•	•		•	•
FMT_MSA.2 Secure security attributes			•	•	•			•	•
FMT_MSA.3 Static Attribute Initialisation		•	•	•	•			•	•
FMT_MTD.1 Management of TSF data			•	•	•	•		•	•
FMT_SMR.1 Security roles		•	•	•				•	•
FMT_MTD.2 Management of limits on TSF data				•	•			•	•
FMT_MTD.3 Secure TSF data					•			•	•
FMT_REV.1 Revocation					•			•	•

1) FMT_LIM

Since this is a hardware requirement, it will be reviewed in the Chip PP.

2) FMT_MOF, FMT_MSA, FMT_MTD, FMT_SMR

The role of people involved in the processes leading to the issuance of a smart card, the security attributes of the role, operation of the security attributes, usable external interface (operation) and other such factors need to be clearly identified.

3) FMT_MTD, FMT_REV

For a smart card, the security attributes used commonly as limit or revocation are not clearly identified and this is left to the discretion of the ST authors.

7.6.4 FAU Class

Table 7-4 shows the FAU Class functional requirements in the referenced PPs.

Table 7-4 Comparison of the FAU Class

FAU Class	9806 Phase3	9806 Phase3-7	9911	0010	SCSUG	ICCS	SSVG	JICSAP PP part2	0301 JICSAP PP part1
FAU_LST.1 Audit list generation					•			•	•
FAU_SAS.1 Audit storage							•	•	•
FAU_CFG.1 Configuration Generation								•	•
FAU_ARP.1 Security Alarms				•	•			•	•
FAU_SAA.1 Potential Violation Analysis		•	•	•	•			•	•
FAU_SEL.1 Selective audit					•			•	•
FAU_STG.1 Protected audit trail storage					•			•	•
FAU_STG.3 Action in case of possible audit data loss					•			•	•

1) FAU_LST, FAU_SAS, FAU_CFG

These requirements to record identification data of software or hardware that comprise the TOE and the same requirements are covered in this PP through FAU_CFG.1.

2) FAU_ARP, FAU_SAA, FAU_SEL, FAU_STG

Due to the available resources to the smart card, it is difficult for a smart card itself effectively to maintain service records. Moreover, even were attack records and method of notification with regards such attacks to be maintained, since the smart card is in the hands of the attacker, such records cannot be effectively utilized.

7.6.5 FCS Class

Table 7-5 shows the FCS Class functional requirements for the referenced PPs.

Table 7-5 Comparison of the FCS Class

FCS Class	9806 Phase3	9806 Phase3-7	9911	0010	SCSUG	ICCS	SSVG	JICSAP PP part2	0301 JICSAP PP part1
FCS_CKM.1 Cryptographic key generation					•			•	•›
FCS_CKM.3 Cryptographic key access			•	•›	•›			•	•›
FCS_CKM.4 Cryptographic key destruction			•	•›				•	•›
FCS_COP.1 Cryptographic operations			•	•›	•›	•›		•	•›
FCS_RND.1 Quality metric for random numbers							•	•›	•›

1) FCS_CKM, FCS_COP

The algorithm and key length must be clearly specified with respect to the key generation and destruction. Since the access to the key by a user is not in the logical interface, this is left up to the discretion of the ST authors.

2) FCS_RND

This requires a generation metric for random numbers. Random number generation is supported by the hardware, but its metric is not suitable for assurance requirements rather than functional requirements.

7.6.6 FPT Class

Table 7-6 shows the FPT Class functional requirements of the referenced PPs.

Table 7-6 Comparison of the FPT Class

FPT Class	9806 Phase3	9806 Phase3-7	9911	0010	SCSUG	ICCS	SSVG	JICSAP PP part2	0301 JICSAP PP part1
FPT_SEP.1 TSF Domain separation			•	•	•		•	•	•
FPT_RCV.3 Automated recovery without undue loss					•	•		•	•
FPT_RCV.4 Function recovery				•	•	•		•	•
FPT_FLS.1 Failure with preservation of secure state			•	•	•	•	•	•	•
FPT_PHP.1 Passive detection of physical attack						•		•	•
FPT_PHP.2 Notification of Physical Attack		•						•	•
FPT_PHP.3 Resistance to Physical Attack		•	•	•	•	•	•	•	•
FPT_ITI.1 Inter-TSF detection of modification					•	•		•	•
FPT_TDC.1 Inter-TSF basic TSF data consistency			•	•				•	•
FPT_ITT.1 Basic internal TSF data transfer protection					•		•	•	•
FPT_RPL.1 Replay detection					•			•	•
FPT_RVM.1 Non- bypassability of the TSP				•	•			•	•
FPT_TST.1 TOE Security Functions Testing	•		•	•	•	•		•	•

1) FPT_PHP

The countermeasures against hardware attacks are addressed in the Chip PP.

2) FPT_RCV, FPT_FLS

It is mandatory that function recovery and secure state be acquired in the event of service abnormality.

3) FPT_SEP

A firewall function for loaded application programs is mandatory.

4) FPT_ITI, FPT_TDC, FPT_ITT, FPT_RPL, FPT_RVM, FPT_TST

No transmission of TSF data (FPT_ISI) takes place between the TSFs in a smart card, and there is no shared TSF data with a remote TSF (FPT_TDC).

The consistency of TSF data transmitted between the CPU and co-processor is addressed through the hardware.

As TOE is not capable of detecting replay attacks on user data in a smart card, this is dropped from the requirements (FPT_RPL).

It is assumed that in a smart card, all functions are enabled upon the power turned on (FPT_RVM).

7.6.7 Other Classes

Table 7-7 shows other class functional requirements for the referenced PPs.

Table 7-7 Comparison of Other Classes

Other Classes	9806 Phase3	9806 Phase3-7	9911	0010	SCSUG	ICCS	SSVG	JICSAP PP part2	0301 JICSAP PP part1
FRU_FLT.2 Limited fault tolerance							•	•	•
FRU_RSA.1 Maximum quotas				•				•	•
FPR_UNO.1 Unobservability		•	•	•				•	•
FTP_ITC.1 Inter-TSF trusted channel					•			•	•

1) FRU_FLT, FPR_UNO, FTP_ITC

FRU_FLT will be reviewed in the hardware.

FPR_UNO will be satisfied through FPT_SEP.

FTP_ITC is a requirement for a secure channel with remote IT products but this is not a requirement in this PP. This issue is left to the discretion of the ST authors.

2) FRU_RSA

The resource management for maximum allocation causes an excessive load on the TOE and this issue is left to the discretion of the ST authors.

7.7 Life Cycle Consideration

A variety of companies are involved in the processes leading to the end-usage of a smart card. Figure 7-2 is an example of this situation.

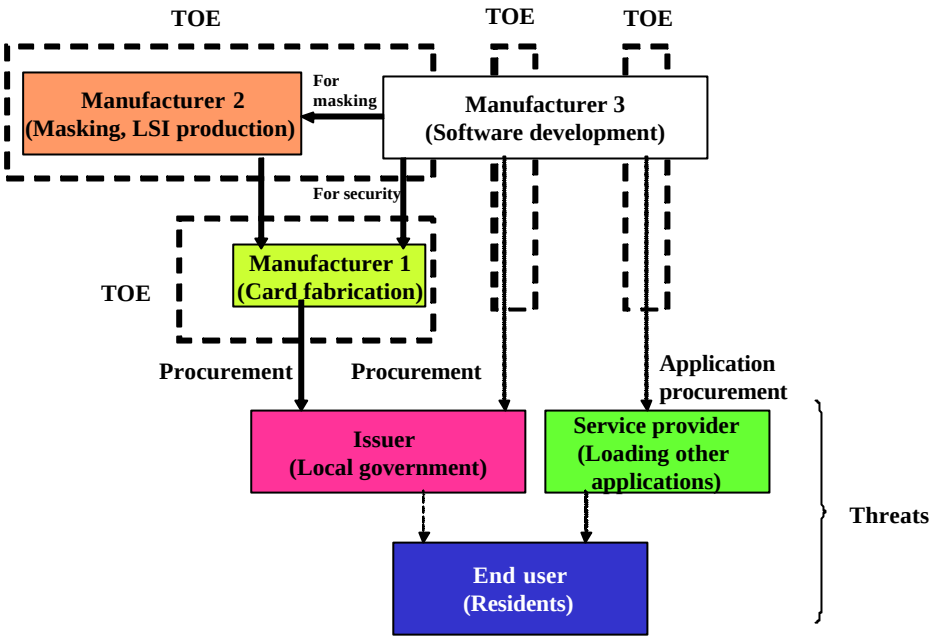


Figure 7-2 Example of Flow of Product Development

Manufacturer 2 that manufactures the chip is a semiconductor manufacturer that procures from Manufacturer 3 (a different organisation) the software (OS) to be masked onto the chip. The completed chip is packaged and fabricated to a card at Manufacturer 1. The reader of this PP is the issuer (consumer above Figure 7-2) who procures the smart card. The issuer loads the application program required to provide services onto the smart card and configures the environment to provide the services and delivers the card to the user. The user enjoys the services using the card provided and, at the same time, accesses to a service provider to add new services (load new application programs).

From the perspective of evaluation, the target of evaluation is the ST based on the PP prepared by the consumer with the various deliverables to satisfy the EAL referred in the ST. However, there is an issue of whether or not Manufacturer 1 is able to prepare all deliverables to undertake evaluation, or in other words, evidence regarding the masked software (a deliverable from Manufacturer 3) and evidence with respect to the chip and hardware (deliverables from Manufacturer 2), can be prepared.

Another issue is that the chips manufactured at Manufacturer 2 may be sold to various organisations and when each organisation subjects the product to evaluation, the chips are also evaluated despite the fact that the chips are the same and this not only inefficient but also may increase the workload of the chip manufacturer.

As an approach for resolving such issues, there is the method of subdividing the TOE into hardware (chip), software (OS), and application program and subjecting each of these separately to evaluation. This PP takes this approach. With this approach, the issue of efficiency mentioned above will be resolved. The pending issue is about the evidences. With respect to the evidences, some review are

being made of a system under which the organisation that evaluates the chip and the organisation that evaluates the smart card determining the contents of evidence required in the evaluation of a smart card and with the agreement of Manufacturer 1 and Manufacturer 2, providing such evidence. However, evaluation bodies and manufacturers exist in various countries and some time will conceivably be required before a resolution that can be applied internationally is found.