Smart Card Open Platform

Protection Profile V2.2

2010. 12. 20

(This page left blank on purpose for double-side printing)

Protection Profile Title

Smart Card Open Platform Protection Profile V2.2

Evaluation Criteria Version

This Protection Profile has been prepared in conformance to the Common Criteria V3.1r3 for Information Technology Security Evaluation

Developer

This Protection Profile has been developed by KISA(Korea Internet & Security Agency) and Sungkyunkwan University.

Tables of Contents

List of Tables

List of Figures

1 Protection Profile(PP) Introduction

1.1 PP Reference

1 Title: Smart Card Open Platform Protection Profile

2 Protection Profile Version: V2.2

3 Evaluation Criteria: Common Criteria for Information Security System (Ministry of Public Administration and Security Notice No. 2009-52)

4 Common Criteria Version: V3.1r3

5 Evaluation Assurance Level: EAL4+(ATE_DPT.2, AVA_VAN.4)

6 Authors: KISA, Sungkyunkwan University

7 Evaluation Authority: IT Security Certification Center

8 Certification Number : KECS-PP-0097a-2008, December 20, 2010

9 Validation Result: This Protection Profile is certified to be compatible with Common Criteria.

10 Keywords : Smart card, COS, IC chip, Terminal, Open Platform

1.2 TOE Overview

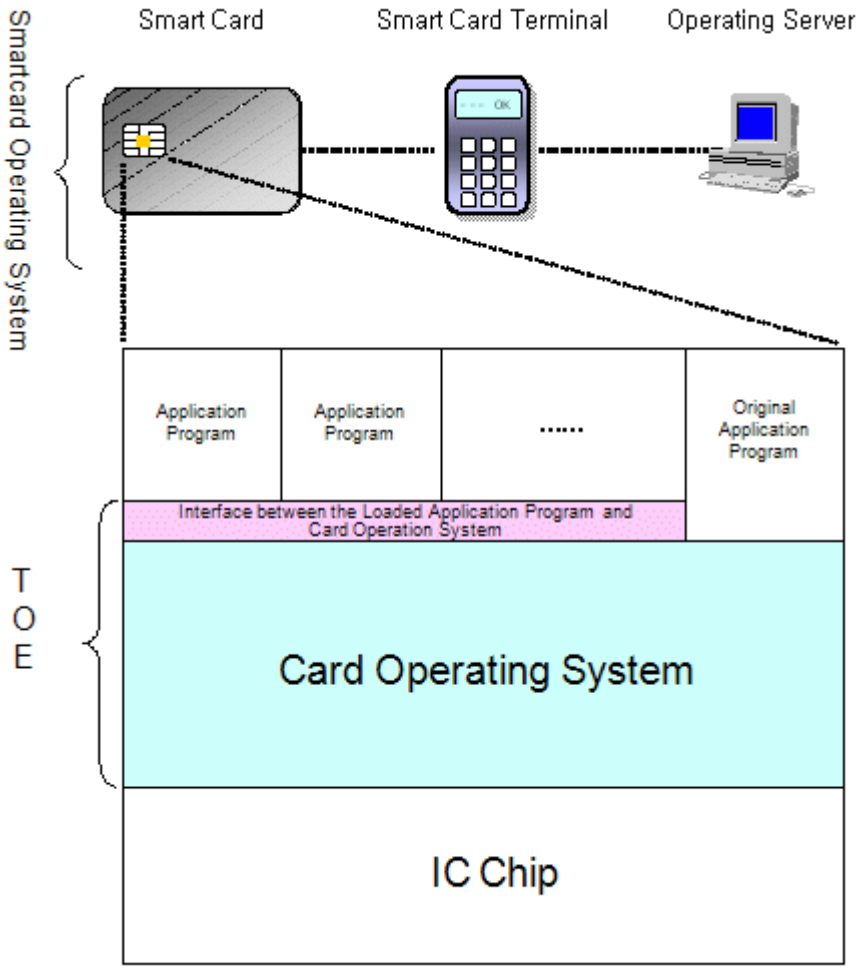
11 This Protection Profile defines security functional requirements and assurance requirements for Smart Card operating system, and interface between loaded application program and operating system except for IC chip which is hardware part of Smart Card and loaded application program.

12 In general, Smart Card is a device built in with central processing unit (CPU) and memory that is capable of information processing and storage. Supporting multiple functions, Smart Card mainly consists with the hardware element of IC chip, card operating system for resource and data management, interface between the loaded application program and card operating system, and application program to provide specific functions. IC chip, the hardware part of Smart Card, generally consists with central processing unit (CPU), coprocessor, input/ output port, RAM, ROM and EEPROM.

13 The Smart Card Operating System is designed for operation with the Smart Card terminal through bi-directional serial interface. The tasks include input/output data transmission, instruction execution management, file management, cryptographic function, etc.

1.2.1 TOE environment

14 (Figure 1) shows the environment in which Smart Card is actually operated and the scope of the TOE and hierarchy of Smart Card that provides multiple functions. The TOE is an open platform that includes the Smart Card operating system, execution environment and the management program, etc. with the exception of IC chip and the loaded application program. The IC chip, the software for the IC chip and the firmware are IT environment in which the TOE is operated.



(Figure1) TOE Configuration

15 Smart card holder and issuer generally execute operations through communication with Smart Card terminal. Issuer executes management operations of loading, deleting and modifying application by using Smart Card terminal. The holder uses Smart Card functions by using terminal. Here, Smart Card terminal and the operating server becomes the IT environment for the TOE operation.

16 This Protection Profile does not define detailed functions according to open platform (eg Java Card, Multos, etc.), so the developer shall include relevant security requirements in the ST.

[Table1] Stages of the Smart Card Manufacturing

Stage	Admin.	Description	Remarks
Design	Designer	- This is the stage of the software (card operating system, interface between the loaded the application program and the card operating system, the application program, etc.) and the IC chip design. - In general, the software and the IC chip can be designed by the different designers.	Design stage can be sequential or simultaneous.
Manufacturing	Manufacturer	- This is the stage of masking the designed operating system to the ROM. This includes the processes of the IC chip manufacturing, package and loading the packaged IC chip to card, etc. - The card is completed by loading coil in the Smart Card.	-
Issuance	**Issuer**	The completed card is delivered to the issuer. The issuer distributes card after loading the application program for final use.	Loading application program Defect repair
Use	**Holder**	After issuance, the Smart Card holder uses the card to suit the purpose.	-
	Issuer	Issuer additionally loads the application program in order to additionally expand the functions of the Smart Card.	Loading application program
End of Use	**Issuer**	When use of the card is ended, holder returns the card to issuer. The issuer makes the card ended of use to be completely useless.	Deleting application program, deleting data of each device

17 [Table 1] shows the processes through which the Smart Card passes through the stages of the design, the manufacturing and the issuance to reach the stages of use and end of use.

18 In the stage of the manufacturing, the basic software, such as the card operating system and the library, etc., is loaded in the IC chip on the basis of the design information. Also, the application program can be loaded. In the stage of issuance, the issuer executes Smart Card personalization, the application program loading and the environment configuration (cryptographic key setting and the environment configuration for the application program loaded, etc.), etc. When the card issuance is completed by the card issuer, the Smart Card is delivered to the cardholder. Then, responsibility for the Smart Card management is handed over to the cardholder. The application program can be loaded at the card manufacturing and the issuance or the during card use. The process

of the application loading is regarded as one of the processes of the issuance and the issuer refers to the person who takes a part in the issuing operation.

19 The card operating system and the interface between the loaded application program and the card operating system, etc. can be designed by different designers. Procedures must be established for the TOE distribution specific to each stage. Also, secure distribution procedures must be applied to the Smart Card distribution in each stage.

20 Major assets to be protected by the TOE in this Protection Profile are the data managed in the card. The TOE data are largely divided into 2 types, such as the user data and the TSF data necessary in the TOE operation. Also, documents created in the course of the TOE production are additional assets to be protected as they affect the integrity and the confidentiality of the TOE.

21 The user data to be protected by the TOE are the application program data that are to be installed at application by using the TOE or the application program itself.

22 The TOE manages and protects user data by using the TSF data.

23 The Smart Card is a product carried and used by user, therefore is the target to be stolen by the attackers. So, the IC chip itself is an asset to be protected from the physical threats.

24 Although not an asset directly protected by the TOE, information created or used in the course of the TOE production significantly affects integrity or confidentiality of the TOE itself. Such information is called additional asset and security of additional asset is satisfied with assurance requirement of EAL4+.

1.2.2 TOE Scope

25 TOE executes security violation analysis, cryptographic function, identification and authentication, security management, and other TSF security functions.

Security violation analysis

26 TOE detects security violation events security violation in relation to checksum value of internal data or incidents, such as the resource allocation error or the authentication failure, etc. and takes actions such as the card function disablement and memory data deletion, etc..

Cryptographic function

27 TOE executes cryptographic key generation/destruction. Also, it ensures that cryptographic-related information cannot be found out by exploiting physical state (changes of the electrical current, voltage and the electromagnetic, etc) that occurred in cryptographic operation.

Access Control

28 The TOE provides access control rules to ensure that only the authorized user can access data.

Identification and Authentication

29 TOE ensures that it identifies and authenticates the identity of user and provides action in case of the authentication failure.

Security management

30 TOE manages security capability, security attribute, TSF data and security role etc.

Other TSF security

31 TOE conducts self-test to verify the integrity of TSF data and executable code, provides capability to recover to secure state when the failure occurred.

32 TOE can require additional hardware, software or firmware for operation. This protection profile was developed to reflect TOE that implemented in various types and required for TOE execution when ST author accept this protection profile, but shall describe all non-TOE hardware, software or firmware.

1.3 Conventions

33 The notation, formatting and conventions used in this Protection Profile are consistent it the Common Criteria.

34 The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration. Each of these operations is used in this Protection Profile.

Iteration

It is used when a component is repeated with varying operations. The result of iteration is marked by iteration number in parenthesis following the component identifier, i.e., (Iteration No.).

Assignment

It is used to assign specific values to unspecified parameters (e.g. : password length). The result of assignment is indicated in square brackets, i.e., [assignment_Value].

Selection

It is used to select one or more options provided by the CC in stating a requirement. The result of selection is shown as *underlined and italicized*.

Refinement

It is used to add detail to a requirement, and thus further restricts a requirement. The result of refinement is shown in **bold text**.

Security target author

It is used to denote points in which final determination of attributes is left to the security target author. The security target author operation is indicated by the words { determined by the Security target author } in braces. In addition, operations of the security functional requirements that are not completely performed in the Protection Profile shall be performed fully by the security target author.

35 Application Notes are provided to help to clarify the intent of a requirement, identify implementation choices or to define "Pass/Fail" criteria for a requirement. Application Notes will follow relevant requirements where appropriate.

1.4 Terms and Definitions

36 Terms that are used herein and defined in the CC as well are to have the same meaning as in the CC.

Smart Card Terminal
Device mounted with Smart Card reader/ recorder function as well as keypad, display and security module, etc.

Authorized Issuer
Authorized user that securely operates and manages functions according to TOE security policies

Authentication Data
Information used to verify the claimed identity of a user.

EEPROM (Electrically Erasable Programmable Read-Only Memory)
This is non-volatile memory device that stably remembers memory over a long period of time without requiring power. As a modified version of EPROM (Electrically Programmable Read-only Memory), EEPROM can electrically erase and re-record data. Therefore, this can be conveniently used in application that requires to re-record program. Data are recorded and erased by electrically changing the electric charge of elements that consists a chip. As electric reading or recording is possible, reprogramming is possible while loaded inside system.

IC Chip (Integrated Circuit Chip)
As an important semiconductor to process the functions of Smart Card, IC chip is a processing device that includes the four functional units of mask ROM, EEPROM, RAM and I/O port.

RAM (Random Access Memory)
RAM is a storage that maintains operating system application program and the currently used data in order to enable quick access by computer processor. RAM if capable of reading and writing faster than any other computer storage devices, such as hard disk, floppy disk and CD-ROM, etc. However, data stored in RAM are maintained only during the computer is in operation. Data in RAM disappear when computer is turned off. When computer is turned on again, operating system or other files in hard disk are loaded in RAM again.

ROM (Read-Only Memory)
As a semiconductor memory device, ROM can read, but cannot change contents. This is compared with RAM, which is capable of both reading and writing. Since contents of data are maintained even when computer is turned off, ROM is generally used to load the basic operating system function or language interpreter in computer.

1.5 Protection Profile Organization

37 Section 1 provides the introductory material for the Protection Profile.

38 Section 2 provides the conformance claim that declares conformance for common criteria, protection profile, and packages, and describes rationale of conformance claim and the method of PP conformance.

39 Section 3 describes the TOE security environment and includes security problems of the TOE and its IT environment from such as threats, organisational security policies and assumptions,.

40 Section 4 defines the security objectives for the TOE and its IT environment to respond to identified threats, enforce organizational security policies, and support the assumptions.

41 Section 5 contains the IT security requirements including the functional and assurance requirements intended to satisfy security objectives.

42 Section 6 describes Application Notes which deserve notice in applying the PP herein.

43 References contain references to noteworthy background and/or supporting materials for prospective users of the PP who may be interested in knowing more than what is specified herein.

44 Acronym is an acronym list that defines frequently used acronyms.

2 Conformance Claim

45 Conformance claim contains common criteria, protection profile and package for this protection profile, and methods for other protection profiles and security targets to conform with this protection file.

2.1 Conformance to Common Criteria

46 This protection profile claims conformance to

- Common Criteria for Information Technology Security Evaluation, part 1 : Introduction and general model, Version 3.1r3, July. 2009, CCMB-2009-07-001
- Common Criteria for Information Technology Security Evaluation, part 2 : Security functional requirements, Version 3.1r3, July. 2009, CCMB-2009-07-002
- Common Criteria for Information Technology Security Evaluation, part 3 : Security assurance requirements, Version 3.1r3, July. 2009, CCMB-2009-07-003

as follows

- Part 2 Conformant
- Part 3 Conformant

2.2 Conformance to Protection Profile

47 This protection profile doesn't claims conformance to any other Protection Profiles.

2.3 Conformance to Package

48 This protection profile is conforming to assurance package as follows

- Assurance Package : EAL4+(ATE_DPT.2, AVA_VAN.4)

2.4 Rationale of Conformance Claim

49 Since this protection profile is not claiming conformance to any other protection profile, no rationale is necessary here.

2.5 Method of PP Conformance

50 This protection profile requires “demonstrable conformance of any ST or PP, which claims conformance to this PP”.

3 Security Problem Definition

51 Security Problem Definition defines threats, organizational policy and assumptions that intended to be processed by TOE and TOE environment.

3.1 Threats

52 Threat agents are generally IT entity or users that illegally accesses and abnormally damage TOE and security target system. Threat agents hold medium level of professional knowledge, resources and motives.

T. Logical_Attack

53 The threat agent may change or disclose the user data or the TSF data by exploiting logical interface.

Application Notes : The logical interface is the data exchange interface between the TOE and the Smart Card terminal. It mainly implies the instructions and the responses between the Smart Card and terminal. For the instruction and the response syntaxes, there are the international standards, the local standards, the company standards and the independent standards. The attacker may attack by exploiting syntaxes that exploit logical interface or interpretational difference, or by exploiting instructions for specific use.

T. Issuance_Misuse

54 The threat agents may exploit the TOE in the process issuing the Smart Card that includes the TOE.

T. Illegal_Terminal_Use

55 The threat agent may change and disclose the user data or the TSF data by using unauthorized the Smart Card terminal.

T. Illegal Program

56 The threat agent may change and disclose the user data or the TSF data by illegally installing the application program that includes malicious code in the TOE.

T. Unintentional_Failure

57 The threat agent may exploit disclosure of and damage to the user data and the TSF data caused by suspension of the power supply during the card use or incomplete ending of the TSF service due to impact, etc.

T. Continuous_Authentication_Attempt

58 The threat agent may access the TOE by continuously attempting authorization.

T. Intentional_Triggering_of_Failures

59 The threat agent may change and disclose the user data or the TSF data by incompletely ending the TSF service with attack using physical stress to the Smart Card.

Application Notes: This threat refers to the attack by attacker to exert physical stress of the voltage, the frequency and the temperature, etc., for the purpose of changing or disclosing the TSF data.

T. Residual_Information

60 In case the TOE reuses resources, the threat agent may illegally access information as information of the object is not properly removed.

T. Information Disclosure

61 The threat agent may exploit the information disclosed from the TOE during normal use of the TOE.

Application Notes : Information disclosed during normal use of the TOE refers to the electrical signals, such as the electrical power, the voltage and the current, etc. emitted from the IC circuit of the Smart Card. This threat implies the attack by the attacker to obtain cryptographic key or important the TSF data by analyzing electrical signals generated from the Smart Card with analysis devices. Types of this attack include the electric power analysis attack, the electric power difference analysis attack and the timing attack, etc.

3.2 Organizational Security Policies

62 The organizational security policies described in this section are handled by the TOE to accommodate this protection profile.

P. Open_Platform

63 The TOE must be developed as open platform that can be loaded with application programs.

P. Role_Division

64 The role is divided per each responsible person from the stage of the Smart Card manufacturing to the stage of use. The TOE must be manufactured and managed with secure method according to the role.

3.3 Assumptions

65 Following conditions are assumed to exist in the TOE security environment that conforms to this Protection Profile.

A.Trusted_Path

66 There is trusted path between the TOE and the Smart Card terminal, the communication target of the TOE.

A. Application_Program

67 The legitimately installed the application program does not contain malicious code.

A. Underlying_Hardware

68 The underlying hardware in which the TOE is operated provides cryptographic function to support security function and it is physically secure.

Application Notes: Hardware, the basis of the TOE operation, must be equipped with handling measures for the diverse physical attacks. On the assumption of this, the TOE is securely operated and security of the Smart Card is achieved. Also, cryptographic function can be provided from cryptographic processor in IC chip or cryptographic library which is loaded in IC chip.

A. TOE_Management

69 The stage from the TOE manufacturing to use is divided of the roles, such as the manufacturer, the issuer and the holder. Appropriate training is necessary according to

the regulations prescribed per each role. Also, repair and replacement due to defect of the TOE or the Smart Card are processed with secure method.

A. TSF_Data

70 The TSF data exported to the outside of the TOE, therefore handled in the course of the TOE operation are securely managed.

4 Security Objectives

71 This protection profile defines security objectives by categorizing them into the TOE security purpose and security purpose for the environment. The TOE security objective is directly handled by the TOE. Security objective for the environment is handled in relation to the IT fields or by the technical/process-related means.

4.1 Security Objectives for the TOE

72 The followings are security objectives to be directly handled by the TOE.

O. Data_Protection

73 The TOE must protect the TSF data stored in TOE against unauthorized disclosure, modification and deletion.

O. Issuance

74 The TOE must ensure that the authorized issuer can issue the Smart Card according to the prescribed procedures.

O. Identification

75 The TOE must clarify users capable of the using logical interface and the assets to be used according to the role.

Application Notes : The TOE must be able to clearly identity user and asset so that each user is connected to the asset that can be accessed with the logical interface.

O. Authorized_Failure_Repair

76 The TOE must ensure that only the authorized user can repair a breakdown.

Application Notes: Only the person capable of using the logical interface with the authorized terminal can repair defects. The logical interface can be implemented by using the international standards, the local standards, the company standards and the independent standards.

O. Authentication

77 User must complete authentication process when attempting to access the TOE user data and the TSF data.

O. Automated_Recovery

78 The TOE must be recovered to secure state when failure in the TSF occurs. Also, the TOE, by detecting failure in the TSF, must recommence the TSF service under the state prior to failure.

O. Residual_Information_Deletion

79 The TOE must ensure that the user data or the TSF data are not remaining when ending operation domain used by the TSF.

O. Information_Disclosure_Handling

80 The TOE must implement countermeasures to prevent misuse of the information disclosed during normal use of the TOE.

Application Notes : When handling measures are implemented in the IC chip of the Smart Card to satisfy this security objective, ST author shall specify this security objective as objective for environment.

O. Open_Platform

81 The TOE must support open platform to which the application programs can be loaded.

4.2 Security Objectives for Environment

82 The followings are security objectives to be addressed by the technical/procedural means that supported by environment to make TOE provides security functionality accurately.

OE. Trusted_Communication

83 The trusted path must be provided between the TOE and the Smart Card terminal as the communication target of the TOE.

OE. TSF_Data

84 The TSF data exported to the outside of the TOE, therefore handled in the course of the TOE operation must be securely managed.

OE. Training

85 Operation training must be administered according to the roles of each administrator in the course of the TOE manufacturing, issuance and use.

OE.Underlying_Hardware

86 The TOE must ensure operation in the physically secure the IC chip. The TOE underlying hardware must be equipped with countermeasures and cryptographic function for a variety of the physical attacks to support security function of TOE.

OE. Application_Program

87 The legitimately installed the application program in the TOE must not contain malicious code.

4.3 Rationale of Security Objectives

88 Rationale of the security objectives demonstrates that the specified security objectives are appropriate, sufficient to handle security problems and are essential, rather than excessive.

89 Rationale of the security objectives demonstrates the following.

- Each assumption, threat and organizational security policy is handled by at least one security objective.
- Each security objective handles at least one assumption, threat and organizational security policy.

[Table2] Handling of Security Problem Definition and Security Objectives

Security Objectives / Security Problem Definition	TOE Security Objective									Security Objective for Environment				
	O. Data_Protection	O. Issuance	O. Identification	O. Authorized_Failur_ Repair	O. Authentication	O. Automated_Recovery	O. Residual_Information_Deletion	O. Information_Disclosure_Handling	OE. Open_Platform	OE. Training	OE. Trusted_Communication	OE. Application_Program	OE. Underlying_Hardware	OE. TSF_Data
A. Trusted_Path											×			
A. Application_Program												×		
A. Underlying_Hardware													×	
A. TOE_Management										×				
A. TSF_Data														×
T. Logical_Attack	×	×	×	×	×									
T. Issuance_Misuse		×												
T.Illegal_Terminal_Use	×	×	×	×	×									
T. Illegal_Program			×		×									
T.Unintentional_Failure						×	×							
T.Continuous_Authentication_Attempt					×									
T.Intentional_Triggering_of_Failures													×	
T. Residual_Information							×						×	
T. Information_Disclosure								×						
P. Open_Platform									×					
P. Role_Division		×	×	×	×					×				

4.3.1 Rationale of TOE Security Objective

O. Data_Protection

90 This security objective ensures that only the authorized user can access and modify the asset of user data. This security objective handles the threats of T. Logical_attack and T. Illegal_terminal use to trigger attack by using of the Smart Card by unauthorized user.

O. Issuance

91 This security objective enables only the authorized person to execute issuing operation at the Smart Card issuance. This security objective handles the threat of T. Logical_attack to execute logical attack and the threats of T. Illegal_terminal use and T. Issuance_misuse of which unauthorized user illegally accesses terminal and executes issuing operation and executes the organization security policy of P. Role_division.

O. Identification

92 This security objective ensures to identify the roles of the TOE user and the issuer. The TOE must clarify users capable of using logical interface and the assets to be used accordingly. Therefore, this security objective handles the threats of T. Logical_attack, T. Illegal_terminal use and T. Illegal_program and executes P. Role_division.

O. Authorized_Defect_Repair

93 This security objective ensures that only the authorized issuer can access the management function of the Smart Card in case of defect occurrence in the TOE. This security objective handles the threats of T. Illegal_terminal use to illegally use terminal

and T. Logical_attack, the threat that executes logical attack, such as illegal instruction use, etc. and executes the organizational security policy of P. Role_division.

O. Authentication

94 This security objective ensures that the TOE provides the identified user with the means of authentication. Therefore, this security objective handles the threats of T. Logical_attack, T. Illegal_terminal use, T. Illegal_program and T. Continuous_authentication_attempt and executes the policies of P. Role_division.

O. Automated_Recovery

95 This security objective ensures that the TOE detects abnormalities during the TSF service, therefore recommences service under the state prior to abnormality detection. Therefore, this security objective handles the threat of T. Unintentional_Failure of which TSF service is suspended by unintentional failure during use.

O. Residual_Information_Deletion

96 This security objective also handles the threat of T. Unintentional_Failure as it ensures to remove information from resources after service is incompletely ended. Also, this security objective ensures that the user data or the TSF data are not remaining in the operation domain where the TSF service is used. This handles the threat of T. Residual_information, the threat of not appropriately removing information after the TSF records information in resources and ends the use.

O. Information_Disclosure_Handling

97 This security objective ensures to implement countermeasures of preventing exploitation of the sensitive TSF data by capturing the disclosed data with devices even during the normal use of the TOE. The TOE can be attacked in the environment in which it may be exploited by being exposed to physical vulnerability. Therefore, this security objective handles the attack of T. Information_disclosure.

O. Open_Platform

98 This security objective ensures that he TOE is an open platform that can be loaded with the application functions. Therefore, this security objective supports the organizational security policy of P. Open_Platform.

4.3.2 Rationale of Security Objective for Environment

OE. Training

99 This security objective for environment ensures that appropriate training is executed according to the roles divided in the processes of issuance and use during the stage of the TOE manufacturing. The Developer must specify to execute appropriate training in user manual and administrator manual and the evaluator must verify this. Therefore, this security objective supports the assumption of A. TOE_management and the organizational security policy of P. Role_division.

OE.Trusted_Communication

100 This security objective ensures to provide the trusted path between the TOE and theSmart Card terminal as the communication target of TOE. Therefore, this security objective supports the assumption of A. Trusted_path.

OE. Application_Program

101 This security objective ensures that the administrator will check that the application does not contain malicious code through appropriate validation of the application to be loaded. Therefore, this security objective supports the assumption of A. Application_program.

OE.Underlying_Hardware

102 This security objective ensures that the TOE is operated in the physically secure chip state and that the underlying hardware of the TOE is equipped with countermeasure and cryptographic function for a variety of physical attacks to support TOE security function. Therefore, this security objective supports A.Underlying_Hardware and handles the threat of T. Intentional_Triggering_of_Failures, and T. Residual_Information and supports the assumption of A. Underlying_Hardware.

OE. TSF_Data

103 This security objective ensures that the TSF data that escape the TOE in the environment in which the TOE is operated are securely managed even in the outside of the TOE control. To achieve this security objective, the developer must securely manage the TSF data stored in terminal, the environment where the TOE is used. Therefore, this security objective supports the assumption of A. TSF_data.

5 Definiton of Extended Component

104 This protection profile does not define extended component.

6 Security Requirements

105 This section provides functional and assurance requirements that must be satisfied by a Protection Profile-compliant the TOE.

106 This Protection Profile defines all subjects, objects, operation, security attributes, external entities employed in security requirements.

a) Subjects, objects and related security attributes, operation,

[Table3] Definition of Subjects/Objects and related Security Attributes, Operation

Subject(User)	Subject(User) Security Attribute	Object(Information)	Object(Information) Security Attribute	Operation
Active entity within TOE 1)	-	User data 2)	-	-All operations
Issuer, Holder	User identifier, Authentication data, Role	TSF Data	-	- Modification, deletion etc -Specify limits -Verify integrity
		Security Attribute	-	-Modification, deletion etc -Specify alternative initial values to override the default values

Application Note:1), 2) specified the types of subject/object, and ST author shall define the list of each subject/object.

b) External entity

- Smart Card terminal
- Smart Card IC chip

107 ST author should precisely define subjects, objects, operation, security attributes, external entities when they were not specifically explained in this Protection Profile.

6.1 Security Functional Requirements

108 The security functional requirements for this Protection Profile consist of the following components from Part2 of the CC in order to satisfy security requirements identified in chapter 4, summarized in the following [Table 4].

[Table4] Security Functional Requirements

Security Functional Classes	**Security Functional Components**	
Security Audit	FAU_ARP.1	Security Alarms
	FAU_SAA.1	Potential violation analysis
Cryptographic support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User Data Protection	FDP_ACC.2	Complete access control
	FDP_ACF.1	Security attribute based access control
	FDP_RIP.1	Subset residual information protection
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.6	Re-authenticating
	FIA_UID.1	Timing of identification
Security Management	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_MTD.2	Management of limits on TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Privacy	FPR_UNO.1	Unobservability
TSF Protection	FPT_FLS.1	Failure with preservation of secure state
	FPT_RCV.3	Automated recovery without undue loss
	FPT_RCV.4	Function recovery
	FPT_TST.1	TSF testing

6.1.1 Security Audit

FAU_ARP.1 Security Alarms

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

109 FAU_ARP.1.1 The TSF shall take [assignment: *list of the least actions*] upon detection of a potential security violation.

Application Notes: This functional requirement may define a variety of handling functions to protect data of Smart Card in case the TOE detects potential external security violation incident. The card function disablement and memory data deletion, etc. can be the handling measures when detecting external attack.

FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

110 FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

111 FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events :

a) Accumulation or combination of [assignment: *subset of defined auditable events*] known to indicate a potential security violation;

b) [assignment: *any other rules*].

Application Notes : The TOE does not analyze potential violation by using the audited incident and executes potential security violation analysis by using the processing state of internal incidents without executing audit record. Therefore, refinement operation was executed. The TSF may execute security warning function in FAU_ARP.1 by analyzing security violation in relation to checksum value of internal data or incidents, such as the resource allocation error or the authentication failure, etc.

6.1.2 Cryptographic Support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

112 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*].

Application Notes: This security functional requirement can support cryptographic key generation in Toe environment (cryptographic processor of Smart Card IC chip or cryptographic library loaded in IC chip) when it cannot be completely implemented to TOE security functional requirement.

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

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

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

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

114 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*].

Application Notes: This security functional requirement can support cryptographic key generation in Toe environment (cryptographic processor of Smart Card IC chip or cryptographic library loaded in IC chip) when it cannot be completely implemented to TOE security functional requirement.

6.1.3 User Data Protection

FDP_ACC.2 Complete access control

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

115 FDP_ACC.2.1 The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects and objects*] and all operations among subjects and objects covered by the SFP.

116 FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Application Notes: Access control policy executed by the Smart Card must be specified and described in detail when preparing security target specifications of product implemented by observing this Protection Profile. Here, access control policy refers to the rule of enforcing access control between a certain entity and a certain object in the Smart Card.

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

117 FDP_ACF.1.1 The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].

118 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*].

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

120 FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

121 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*].

6.1.4 Identification and authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

122 FIA_AFL.1.1 The TSF shall detect when [selection: [assignment*: positive integer number*], an administrator configurable positive integer within [assignment: *range of*

acceptable values]] unsuccessful authentication attempts occur related to [assignment*: list of authentication events*].

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

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

124 FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) user identifier;
b) authentication data;
c) roles;
d) { determined by the ST author }

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

125 FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: *a defined quality metric*].

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

126 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.

127 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.

Application Notes: In the Smart Card, authentication is used in a various ways. Types of authentication include user authentication using the PIN, authentication between the

Smart Card and the terminal and authentication between the Smart Card and the application program, etc. The ST author must describe all of the authentication mechanisms and the evaluator must check them.

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Application Notes: Single-use authentication mechanisms are applicable to all users including authenticated administrator, and can avoid using single-use mechanisms for available services within not violating security policy. The examples of authentication mechanisms that single-use is possible include single-use password and cryptographic timestamp.

FIA_UAU.6 Re-authenticating

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Application Notes: The ST developer must describe the conditions of re-authentication after normally or abnormally ending service during the Smart Card use.

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

130 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.

131 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.

Application Notes: Within the scope of the TOE, user is limited to the issuer and the holder. The Issuer and the holder must use the function to suit their roles by accessing the TOE after completing identification and authentication processes.

6.1.5 Security Management

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

132 FMT_MOF.1.1 The TSF shall restrict the ability to *disable, enable, [assignment: other operation]* the functions [assignment: *list of functions*] to [assignment: *the authorized identified roles*].

Application Notes: This security functional requirement must implement to the start Smart Card function by the issuer when commencing the Smart Card use and, at the same time, must hold the function to stop the Smart Card function by the issuer when destroying the Smart Card function. Also, In the stage of use after the Smart Card issuance, the issuer may load, delete and modify the application program, and the holder can also execute the role of the issuer. In this case, the holder can load and modify application program.

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

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

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

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

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

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

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

136 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 authorized identified roles*].

FMT_MTD.2 Management of limits on TSF data

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data
FMT_SMR.1 Security roles

137 FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].

138 FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [assignment: *actions to be taken*].

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

139 FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment: *list of security management functions to be provided by the TSF*].

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

140 FMT_SMR.1.1 The TSF shall maintain the roles [issuer, holder].

141 FMT_SMR.1.2 The TSF shall be able to associate users with **defined roles in FMT_SMR.1.1 .**

Application Notes: The Smart Card issuer executes the role of overall administrator for the Smart Card. The Issuer loads the application program before the Smart Card use and also serves the role of receiving defect occurrence during use to repair the defect and of destroying the Smart Card when card use is terminated. In this Protection Profile, the holder can play some of the roles of issuer in the stage of use. Also, the role of issuer can be entrusted to another issuer.

6.1.6 Privacy

FPR_UNO.1 Unobservability

Hierarchical to: No other components.

Dependencies: No dependencies.

142 FPR_UNO.1.1 The TSF shall ensure that [external entities] are unable to observe the operation [FCS_COP.1 cryptographic operation, [assignment: other *list of operations*] on [assignment: *list of objects*] by [TSF].

6.1.7 Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

143 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*].

FPT_RCV.3 Automated recovery without undue loss

Hierarchical to: FPT_RCV.2 Automated recovery

Dependencies: AGD_OPE.1 Operational user guidance

144 FPT_RCV.3.1 When automated recovery from [assignment: *list of failures/service discontinuities*] is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

145 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.

146 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.

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

FPT_RCV.4 Function recovery

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

149 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 authorized user, at the conditions* [assignment: *conditions under which self test should occur*]] to demonstrate the correct operation of the TSF. operation of [selection: [assignment: *parts of TSF*], *the TSF*].

150 FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of [selection: [assignment: *parts of TSF data*], *TSF data*].

151 FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of [selection: *[assignment: parts of TSF], TSF*].

6.2 Security Assurance Requirement

152 The security assurance requirements for this Protection Profile consist of the components from Part 3 of the CC, and added assurance components are follows. [Table 5] shows assurance components.

- ATE_DPT.2 Testing: security enforcing modules
- AVA_VAN.4 Methodical vulnerability analysis

[Table5] Security Assurance Requirements

Assurance Classes	Assurance Components	
Security Target Evaluation	ASE_INT.1	ST Introduction
	ASE_CCL.1	Conformance claims
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_ECD.1	Extended components definition
	ASE_REQ.2	Derived security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life Cycle Support	ALC_CMC.4	Generation support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: security enforcing modules
	ATE_FUN.1	Functional testing

	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.4	Methodical vulnerability analysis

6.2.1 Security Target Evaluation

ASE_INT.1 ST Introduction

Dependencies: No dependencies.

Developer action elements:

153 ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements:

154 ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

155 ASE_INT.1.2C The ST reference shall uniquely identify the ST.

156 ASE_INT.1.3C The TOE reference shall identify the TOE.

157 ASE_INT.1.4C The TOE overview shall summarize the usage and major security features of the TOE.

158 ASE_INT.1.5C The TOE overview shall identify the TOE type.

159 ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE

160 ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

161 ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements:

162 ASE_INT.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

163 ASE_INT.1.2E The evaluator *shall confirm* that theTOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_CCL.1 Conformance claims

Dependencies: ASE_INT.1 ST introduction
ASE_ECD.1 Extended components definition
ASE_REQ.1 Stated security requirements

Developer action elements:

164 ASE_CCL.1.1D The developer shall provide a conformance claim.

165 ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements:

166 ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

167 ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

168 ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

169 ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

170 ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

171 ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

172 ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

173 ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

174 ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

175 ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action elements:

176 ASE_CCL.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ASE_SPD.1 Security problem definition

Dependencies: No dependencies.

Developer action elements:

177 ASE_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements:

178 ASE_SPD.1.1C The security problem definition shall describe the threats.

179 ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

180 ASE_SPD.1.3C The security problem definition shall describe the OSPs.

181 ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements:

182 ASE_SPD.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ASE_OBJ.2 Security objectives

Dependencies: ASE_SPD.1 Security problem definition

Developer action elements:

183 ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

184 ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

Content and presentation elements:

185 ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

186 ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

187 ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

188 ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

189 ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

190 ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

Evaluator action elements:

191 ASE_OBJ.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

Developer action elements:

192 ASE_ECD.1.1D The developer shall provide a statement of security requirements.

193 ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements:

194 ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

195 ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

196 ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

197 ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

198 ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

Evaluator action elements:

199 ASE_ECD.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

200 ASE_ECD.1.2E The evaluator *shall confirm* that no extended component can be clearly expressed using existing components.

ASE_REQ.2 Derived security requirements

Dependencies: ASE_OBJ.2 Security objectives
ASE_ECD.1 Extended components definition

Developer action elements:

201 ASE_REQ.2.1D The developer shall provide a statement of security requirements.

202 ASE_REQ.2.2D The developer shall provide a security requirements rationale.

Content and presentation elements:

203 ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

204 ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

205 ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

206 ASE_REQ.2.4C All operations shall be performed correctly.

207 ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

208 ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

209 ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

210 ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

211 ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

Evaluator action elements:

212 ASE_REQ.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1 TOE summary specification

Dependencies: ASE_INT.1 ST introduction
ASE_REQ.1 Stated security requirements
ADV_FSP.1 Basic functional specification

Developer action elements:

213 ASE_TSS.1.1D The developer shall provide a TOE summary specification. Content and presentation elements:

214 ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR. Evaluator action elements:

215 ASE_TSS.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

216 ASE_TSS.1.2E The evaluator *shall confirm* that the TOE summary specification is consistent with the TOE overview and the TOE description.

6.2.2 Development

ADV_ARC.1 Security architecture description

Dependencies: ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design

Developer action elements:

217 ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

218 ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

219 ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF. Content and presentation elements:

220 ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

221 ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

222 ADV_ARC.1.3C The security architecture description shall describe how the TSF initialization process is secure.

223 ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

224 ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements:

225 ADV_ARC.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.4 Complete functional specification

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

226 ADV_FSP.4.1D The developer shall provide a functional specification.

227 ADV_FSP.4.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

228 ADV_FSP.4.1C The functional specification shall completely represent the TSF.

229 ADV_FSP.4.2C The functional specification shall describe the purpose and method of use for all TSFI.

230 ADV_FSP.4.3C The functional specification shall identify and describe all parameters associated with each TSFI.

231 ADV_FSP.4.4C The functional specification shall describe all actions associated with each TSFI.

232 ADV_FSP.4.5C The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

233 ADV_FSP.4.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

234 ADV_FSP.4.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

235 ADV_FSP.4.2E The evaluator *shall determine* that the functional specification is an accurate and complete instantiation of the SFRs.

ADV_IMP.1 Implementation representation of the TSF

Dependencies: ADV_TDS.3 Basic modular design
ALC_TAT.1 Well-defined development tools

Developer action elements:

236 ADV_IMP.1.1D The developer shall make available the implementation representation for the entire TSF.

237 ADV_IMP.1.2D The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.

Content and presentation elements:

238 ADV_IMP.1.1C The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.

239 ADV_IMP.1.2C The implementation representation shall be in the form used by the development personnel.

240 ADV_IMP.1.3C The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.

Evaluator action elements:

241 ADV_IMP.1.1E The evaluator *shall confirm* that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.3 Basic modular design

Dependencies: ADV_FSP.4 Complete functional specification

Developer action elements:

242 ADV_TDS.3.1D The developer shall provide the design of the TOE.

243 ADV_TDS.3.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

244 ADV_TDS.3.1C The design shall describe the structure of the TOE in terms of subsystems.

245 ADV_TDS.3.2C The design shall describe the TSF in terms of modules.

246 ADV_TDS.3.3C The design shall identify all subsystems of the TSF.

247 ADV_TDS.3.4C The design shall provide a description of each subsystem of the TSF.

248 ADV_TDS.3.5C The design shall provide a description of the interactions among all subsystems of the TSF.

249 ADV_TDS.3.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

250 ADV_TDS.3.7C The design shall describe each SFR-enforcing module in terms of its purpose and relationship with other modules.

251 ADV_TDS.3.8C The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing modules.

252 ADV_TDS.3.9C The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.

253 ADV_TDS.3.10C The mapping shall demonstrate that all TSFIs trace to the behavior described in the TOE design that they invoke.

Evaluator action elements:

254 ADV_TDS.3.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

255 ADV_TDS.3.2E The evaluator *shall determine* that the design is an accurate and complete instantiation of all security functional requirements.

6.2.3 Guidance Documents

AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

256 AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements:

257 AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

258 AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

259 AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

260 AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

261 AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

262 AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

263 AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

264 AGD_OPE.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

265 AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures. Content and presentation elements:

266 AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

267 AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

268 AGD_PRE.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

269 AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

6.2.4 Life cycle Support

ALC_CMC.4 Production support, acceptance procedures and automation

Dependencies: ALC_CMS.1 TOE CM coverage
ALC_DVS.1 Identification of security measures
ALC_LCD.1 Developer defined life-cycle model

Developer action elements:

270 ALC_CMC.4.1D The developer shall provide the TOE and a reference for the TOE.

271 ALC_CMC.4.2D The developer shall provide the CM documentation.

272 ALC_CMC.4.3D The developer shall use a CM system.

Content and presentation elements:

273 ALC_CMC.4.1C The TOE shall be labelled with its unique reference.

274 ALC_CMC.4.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

275 ALC_CMC.4.3C The CM system shall uniquely identify all configuration items.

276 ALC_CMC.4.4C The CM system shall provide automated measures such that only authorized changes are made to the configuration items.

277 ALC_CMC.4.5C The CM system shall support the production of the TOE by automated means.

278 ALC_CMC.4.6C The CM documentation shall include a CM plan.

279 ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the TOE.

280 ALC_CMC.4.8C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

281 ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

282 ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

Evaluator action elements:

283 ALC_CMC.4.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ALC_CMS.4 Problem tracking CM coverage

Dependencies: No dependencies.

Developer action elements:

284 ALC_CMS.4.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

285 ALC_CMS.4.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.

286 ALC_CMS.4.2C The configuration list shall uniquely identify the configuration items.

287 ALC_CMS.4.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

288 ALC_CMS.4.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ALC_DEL.1 Delivery procedures

Dependencies: No dependencies.

Developer action elements:

289 ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

290 ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements:

289 ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements:

291 ALC_DEL.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1 Identification of security measures

Dependencies: No dependencies.

Developer action elements:

292 ALC_DVS.1.1D The developer shall produce and provide development security documentation.

Content and presentation elements:

293 ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

Evaluator action elements:

294 ALC_DVS.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

295 ALC_DVS.1.2E The evaluator *shall confirm* that the security measures are being applied.

ALC_LCD.1 Developer defined life-cycle model

Dependencies: No dependencies.

Developer action elements:

296 ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

296 ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation elements:

297 ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

298 ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements:

299 ALC_LCD.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ALC_TAT.1 Well-defined development tools

Dependencies: ADV_IMP.1 Implementation representation of the TSF

Developer action elements:

299 ALC_TAT.1.1D The developer shall provide the documentation identifying each development tool being used for the TOE.

300 ALC_TAT.1.2D The developer shall document and provide the selected implementation-dependent options of each development tool.

Content and presentation elements:

301 ALC_TAT.1.1C Each development tool used for implementation shall be well-defined.

302 ALC_TAT.1.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

303 ALC_TAT.1.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

Evaluator action elements:

304 ALC_TAT.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

6.2.5 Tests

ATE_COV.2 Analysis of coverage

Dependencies:ADV_FSP.2Security-enforcing functional specification
ATE_FUN.1 Functional testing

Developer action elements:

305 ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation elements:

306 ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

307 ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

Evaluator action elements:

308 ATE_COV.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ATE_DPT.2 Testing: security enforcing modules

Dependencies: ADV_ARC.1 Security architecture description
ADV_TDS.3 Basic modular design
ATE_FUN.1 Functional testing

Developer action elements:

309 ATE_DPT.2.1D The developer shall provide the analysis of the depth of testing.

Content and presentation elements:

310 ATE_DPT.2.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and SFR-enforcing modules in the TOE design.

311 ATE_DPT.2.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

312 ATE_DPT.2.3C The analysis of the depth of testing shall demonstrate that the SFR-enforcing modules in the TOE design have been tested.

Evaluator action elements:

313 ATE_DPT.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements:

314 ATE_FUN.1.1D The developer shall test the TSF and document the results.

315 ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:

316 ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

317 ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

318 ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

319 ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements:

320 ATE_FUN.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent testing - sample

Dependencies:ADV_FSP.2 Security-enforcing functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures
ATE_COV.1 Evidence of coverage
ATE_FUN.1 Functional testing

Developer action elements:

321 ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

322 ATE_IND.2.1C The TOE shall be suitable for testing.

323 ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

324 ATE_IND.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

325 ATE_IND.2.2E The evaluator *shall execute* a sample of tests in the test documentation to verify the developer test results.

326 ATE_IND.2.3E The evaluator *shall test* a subset of the TSF to confirm that the TSF operates as specified.

6.2.6 Vulnerability assessment

AVA_VAN.4 Methodical vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description

ADV_FSP.4 Complete functional specification
ADV_TDS.3 Basic modular design
ADV_IMP.1 Implementation representation of the TSF
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures
ATE_DPT.1 Testing: basic design

Developer action elements:

327 AVA_VAN.4.1D The developer shall provide the TOE for testing.

Content and presentation elements:

328 AVA_VAN.4.1C The TOE shall be suitable for testing.

Evaluator action elements:

329 AVA_VAN.4.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

330 AVA_VAN.4.2E The evaluator *shall perform* a search of public domain sources to identify potential vulnerabilities in the TOE.

331 AVA_VAN.4.3E The evaluator *shall perform* an independent, methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

332 AVA_VAN.4.4E The evaluator *shall conduct* penetration testing based on the identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by an attacker possessing Moderate attack potential.

6.3 Rationale of Security Requirements

333 Rational of security requirements demonstrate that the described IT security requirements are suitable to satisfy security objectives and, as a result, appropriate to handle security problems.

6.3.1 Rationale of the TOE Security Functional Requirements

334 Rationale of the TOE security functional requirements demonstrates the followings.

- Each the TOE security objective is handled by at least one the TOE security functional requirement.
- Each the TOE security functional requirement handles at least one the TOE security objective.

[Table6] Handling Security Objectives and Security Functional Requirements

Security Objectives / Security Functional Requirements	TOE Security Objective								
	O. Data_Protection	O. Issuance	O. Identification	O. Authorized_Failure_Repair	O. Authentication	O. Automated_Recovery	O. Residual_Information_Deletion	O. Information_Disclosure_Handling	O.Open_Platform
FAU_ARP.1				×	×				
FAU_SAA.1				×	×				
FCS_CKM.1					×				
FCS_CKM.4					×		×		
FCS_COP.1					×				
FDP_ACC.2	×								×
FDP_ACF.1	×								×
FDP_RIP.1							×		
FIA_AFL.1		×		×	×				
FIA_ATD.1		×	×	×	×				
FIA_SOS.1					×				
FIA_UAU.1	×	×		×	×				
FIA_UAU.4		×		×	×				
FIA_UAU.6		×		×	×				
FIA_UID.1	×	×	×	×					
FMT_MOF.1	×								
FMT_MSA.1	×								×
FMT_MSA.3	×								×
FMT_MTD.1		×							

FMT_MTD.2		×							
FMT_SMF.1		×							
FMT_SMR.1		×	×	×	×				
FPR_UNO.1								×	
FPT_FLS.1						×			
FPT_RCV.3						×			
FPT_RVC.4						×			
FPT_TST.1	×					×			

FAU_ARP.1 Security Alarms

335 This component ensures handling ability in the event of detecting security violation, therefore satisfies TOE security objective of O. Authorized_Failure_Repair and O. Authentication.

FAU_SAA.1 Potential Violation Analysis

336 This component ensures the ability to point out security violation by inspecting the audited incident, therefore satisfies TOE security objective of O. Authorized_Failure_Repair and O. Authentication.

FCS_CKM.1 Cryptographic Key Generation

337 This component ensures that the cryptographic keys are generated in accordance with a specified algorithm and key sizes, therefore satisfies TOE security objective of O. Authentication.

FCS_CKM.4 Cryptographic Key Destruction

338 This component ensures that the cryptographic keys are destroyed in accordance with a specified destruction method, therefore satisfies TOE security objective of O.Authentication and O. Residual_Information_Deletion.

FCS_COP.1 Cryptographic Operation

339 This component ensures that the cryptographic operation performed in accordance with a specified algorithm and with a cryptographic key of specified sizes, therefore satisfies TOE security objective of O.Authentication.

FDP_ACC.2 Complete Access Control

340 This component ensures that the security policy for TOE access control is defined, and the coverage of security policy is defined, and it controls the loading of the application program, therefore satisfies TOE security objective of O. Data Protection and O.Open_Platform.

FDP_ACF.1 Security Attribute Based Access Control

341 This component ensures that the access control security is enforced, based upon security attributes, therefore satisfies TOE security objective of O. Data_Protection and O.Open_Platform.

FDP_RIP.1 Subset residual information protection

342 This component ensures that the TSF ensure that any residual information content of any resources is unavailable to a defined subset of the objects controlled by the TSF upon the resource's allocation or deallocation, therefore satisfies TOE security objective of O.Residual_Information_Deletion.

FIA_AFL.1 Authentication failure handling

343 This component ensures the ability to define number of unsuccessful authentication attempts and take actions when the defined number has been met or surpassed, therefore satisfies TOE security objective of O. Issuance, O. Authorized_Failure_Repair, and O.Authentication.

FIA_ATD.1 User Attribute Definition

344 This component defines the list of security attributes for each user, therefore satisfies TOE security objective of O. Issuance, O. identification, O. Authorized_Failure_Repair, and O.Authentication.

FIA_SOS.1 Verification of secrets

345 This component provides mechanisms that verify that secrets meet defined qualitymetric, therefore satisfies TOE security objective of O.Authentication.

FIA_UAU.1 Timing Of Authentication

346 This component ensures the ability to successfully authorize administrator, therefore satisfies TOE security objectives of O. Data_Protection, O. Issuance, O. Authorized_Failure_Repair, and O.Authentication.

FIA_UAU.4 Single-use authentication mechanisms

347 This component ensures the ability to prevent reuse of authentication data, therefore satisfies TOE security objectives of O. Issuance, O. Authorized_Failure_Repair, and O.Authentication.

FIA_UAU.6 Re-authenticating

348 This component ensures the ability to specify events for which the user needs to be re-authenticated, therefore satisfies TOE security objectives of O. Issuance, O. Authorized_Failure_Repair, and O. Authentication.

FIA_UID.1 Timing of identification

349 This component allows users to perform certain actions before being identified by the TSF, therefore satisfies TOE security objectives of O. Data_Protection, O. Issuance, O.Identification and O. Authorized_Failure_Repair.

FMT_MOF.1 Security Function Management

350 This component ensures the ability for authorized administrator to manage security function, therefore satisfies TOE security objectives of O.Data_Protection.

FMT_MSA.1 Management of Security Attributes

351 This component ensures that authorized administrator to manage security attributes that apply to the policy of access control, therefore satisfies TOE security objectives of O. Data_Protection and O.Open_Platform.

FMT_MSA.3 Static Attribute Initialization

352 This component provides an initial value of security attributes that apply to the policy of access control, therefore satisfies TOE security objectives of O.Data_Protection and O.Open_Platform.

FMT_MTD.1 Management of TSF Data(2)

353 This component provides the function for authorized administrator to manage TSF data, therefore satisfies TOE security objectives of O. Issuance.

FMT_MTD.2 TSF Data Limit Management

354 This component ensures that authorized administrator to manage limits of TSF data and to take handling actions when the designed limits are reached or exceeded, therefore satisfies TOE security objectives of O. Issuance.

FMT_SMF.1 Specification of Management Function

355 This component requires to specify management functions, such as security functions, security attributes, and TSF data, etc., to be enforced by TSF, therefore satisfies TOE security objectives of O. Issuance.

FMT_SMR.1 Role of Security

356 This component ensures that the role of TOE security administrator to be related to the role of administrator, therefore satisfies TOE security objectives of O. Issuance, O. Identification, O. Authorized_Failure_Repair, and O.Authentication.

FPR_UNO.1 Unobservability

357 This component ensures that external entity cannot find cryptograph related information by abusing physical phenomenon (electric current, electric power, electromagnetism change) occurred when TSF conducts cryptographic operation, therefore satisfies TOE security objectives of O. Information_Disclosure_Handling.

FPT_FLS.1 Failure with preservation of secure state

358 This component ensures that the TSF preserve a secure state in the face of the identified failures, therefore satisfies TOE security objectives of O. Automated_Recovery.

FPT_RCV.3 Automated recovery without undue loss

359 This component provides for automated recovery, but strengthens the requirements by disallowing undue loss of protected objects, therefore satisfies TOE security objectives of O. Automated_Recovery.

FPT_RCV.4 Function recovery

360 This component provides for recovery at the level of particular functions, ensuring either successful completion or rollback of TSF data to a secure state, therefore satisfies TOE security objectives of O.Automated_Recovery.

FPT_TST.1 Self-test of TSF

361 This component ensures the self-test of TSF for accurate operation and ability for authorized administrator to verify integrity of TSF data and TSF execution code, therefore satisfies TOE security objectives of O.TSF_Data_Protection and O.Automated_Recovery.

6.3.2 Rationale of TOE Security Assurance Requirements

362 The evaluation assurance level of this Protection Profile is EAL4 addition, and the added component is followed.

- ATE_DPT.2Testing : Testing: security enforcing modules
- AVA_VAN.4 Methodical vulnerability analysis

363 EAL4 is assurance package to require systematic design, test and review. And it permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices, which, though rigorous, do not require

substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

364 EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.

365 EAL4 provides configuration management including functional and complete interface specification, a description of the modular design, and implementation representation for the subset of TSF, test, and automation, to understand the security behavior.

366 The TOE is developed by using publicly available standard implementation specifications. Therefore, it is easy to obtain information related to design and operation of the TOE. Also, TOE is easily accessed as it is used in open environment and it is difficult to trace an attack. However, since the IC chip is not included in the scope of the TOE, it does not require understanding on hardware structure and advanced specialized equipments, etc. Therefore, considering the resources, motivation and expertise, the TOE must counter attackers possessing moderate attack potential. EAL4 includes AVA_VLA.3 that resistant the enhanced-basic attack potential. Therefore, AVA_VAN.4(Methodical vulnerability analysis) is augmented to execute resistance analysis to attackers possessing moderate attack potential, and systematic vulnerability analysis to module design of TOE and TSF implementation representation etc. And, ATE_DPT.2 is augmented to test the SFR-enforcing module to analyze vulnerability of the TOE module design. However, there still exists direct attack potential to the IC chip by threat agent possessing high attack potential and evaluation and verification for this may be assigned to the IC chip manufacturer.

6.3.3 Rationale of Dependency

6.3.3.1 Dependency of TOE Security Functional Requirements

367 FAU_GEN.1 in dependency with FAU_SAA.1 is not satisfied. The Smart card does not have sufficient storage space to record security incidents. Accordingly, excessive

security audit may cause risk to security of the card. So, security incidents are not recorded. Therefore, in this Protection Profile, requirements of FAU_GEN.1 are not defined.

368 FDP_ACF.1 and FMT_MSA.1 have dependency to FDP_ACC.1, and this is satisfied by FDP_ACC.2 that is in hierarchical relationship with FDP_ACC.1.

[Table7] Dependency of TOE Security Functional Components

No.	Security Functional Components	Dependency	Reference
1	FAU_ARP.1	FAU_SAA.1	2
2	FAU_SAA.1	FAU_GEN.1	None
3	FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	[- or 5] 4
4	FCK_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	[- or – or 3]
5	FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	[- or – or 3] , 4
6	FDP_ACC.2	FDP_ACF.1	7
7	FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	6, 18
8	FDP_RIP.1	-	-
9	FIA_AFL.1	FIA_UAU.1	12
10	FIA_ATD.1	-	-
11	FIA_SOS.1	-	-
12	FIA_UAU.1	FIA_UID.1	15
13	FIA_UAU.4	-	-
14	FIA_UAU.6	-	-
15	FIA_UID.1	-	-
16	FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	21, 22
17	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1, FMT_SMR.1	[6 or -] 21, 22
18	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	17, 22
19	FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	21, 22
20	FMT_MTD.2	FMT_MTD.1, FMT_SMR.1	19, 22
21	FMT_SMF.1	-	-
22	FMT_SMR.1	FIA_UID.1	15
23	FPR_UNO.1	-	-
24	FPT_FLS.1	-	-

25	FPT_RCV.3	AGD_OPE.1	EAL4
26	FPT_RVC.4	-	-
27	FPT_TST.1	-	-

6.3.3.2 Dependency of TOE Assurance Requirements

369 Dependency of EAL4 assurance package provided in Common Criteria of the information protection system is already satisfied. Therefore, rationale for this is omitted. Dependency of the added assurance requirements is as shown in [Table 8]. This Protection Profile satisfies all dependencies of assurance requirements.

[Table8] Dependency of the Added Assurance Components

No.	Assurance Components	Dependency	Ref. No.
1	ATE_DPT.2	ADV_ARC.1 ADV_TDS.3 ATE_FUN.1	EAL4 EAL4 EAL4
2	AVA_VAN.4	ADV_ARC.1 ADV_FSP.4 ADV_TDS.3 ADV_IMP.1 AGD_OPE.1 AGD_PRE.1 ATE_DPT.1	EAL4 EAL4 EAL4 EAL4 EAL4 EAL4 EAL4

7 Protection Profile Application Notes

370 This Protection Profile can be utilized as of the following. The product developer or the marketer can draw up the Security Targets by observing all contents defined in this Protection Profile and the user can utilize them for purchasing bases and operation management of the product intended for use.

371 This Protection Profile includes the minimum security requirements and does not make definition on implementation model of the TOE. In relation to security problems possible to occur according to the TOE implementation model, the developer shall define additional security problems, security objectives and security requirements.

372 When external entities(ex: DBMS etc for storing audit data) that interact with TOE are included in ST, the test for external entities shall be conducted by adding FPT_TEE.1(external entity test) requirement, and an action shall be ensured if the test failed.

REFERENCES

[1]Common Criteria for Information Technology Security Evaluation, Version 3.1r3, CCMB, 2009. 07.

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1r3, CCMB, 2009. 07.

[3] Smart Card Handbook third Edition, Wolfgang Rankl and Wolfgang Effing, John Wiley and Sons, Ltd, 2003.

[4] ISO/IEC 14443 Proximity Card

[5] ISO/IEC 7810 Identification cards : Physical Characteristics

[6] ISO/IEC 7816 Identification cards : Integrated Circuit Cards with Contacts

[7] ISO/IEC 10536 Close-coupled Cards

[8] Java Card™System Protection Profile Collection Version 1.0b, Sun Microsystems, August2003

[9] Protection Profile Smart Card IC with Multi-Application Secure Platform Version 2.0, European Smart Card Industry Association, November 2000

[10] Smart Card Protection Profile Version 3.0(SCSUG-SCPP), Smart Card Security User Group, September 2001