Firewall Protection Profile V2.0

2008. 4. 24

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

Protection Profile Title

Firewall Protection Profile for Government

Evaluation Criteria Version

This Protection Profile has been prepared in conformance to the Common Criteria for Information Technology Security Evaluation V3.1r2.

Developer

This Protection Profile has been developed by the following developers:

Gyeonggu Yi, Byunggyu No, Wan s. Yi, Gyumin Cho, Suntae Park

Taehun Kim, Taeseung Lee, Eunkyoung Yi , Kyeongho Son, Yungi Seong

Korea Information Security Agency (KISA)

Dongho Won, SeungJu Kim, Hyesuk Cho, Ungryeol Jun, Hanjae Jung, Jeongpil Lee, Yonguk Kim, Yunyoung Lee, Seongjin Lee

SungKyunKwan University

Revision History

Version	Date	Details
1.1	2003. 4. 30	- Firewall Protection Profile for Government V1.1
1.2	2006. 5. 17	- Reflected the CC V2.3 - Deleted assumption of A. Attacker level and listed the related contents in threat, modified attack level from medium to low in order to handle AVA_VLA.2 - Modified O. Access Control from 'control access to the internal and external networks' to 'access control to the TOE'. - Modified error in definition of auditable events in FAU_GEN.1 and reflected it in '[Table 2] auditable events' - Modified Application Notes so that reliable time stamp component of FPT_STM.1 can be implemented in IT environment of the TOE - Deleted the extension component of FPT_TST.2(extension) and listed the related contents in FAR_ARP.1, FAU_GEN.1 and FAU_SAA.1 - Others: Modified editing error and supplemented contents, etc.
2.0	2008. 4. 24	- Reflected the CCV3.1r2 - Modified the PP structure, terms and acronyms - Deleted FPT_SEP and RVM and the related O. Self-protection, T. Bypassing and T. New Attack. - Deleted TE. Poor Mangement(conflict with A. Trusted Administrator) and TE. Delivery and Installation(assurance requirements of ALC_DEL and AGD_PRE are covered) and the corresponding OE. Secure Management. - For FAU_SAR and FAU_STG, it is specified in the 'application notes' that they can be supported in IT environment in case where complete implementation with the TOE security functions is not possible. - Deleted O. Access Control as well as FDP_ACC and FDP_ACF since it is sufficiently satisfied with FDP_IFC and FDP_IFF. - Changed FPT_STM.1 to OE. Time Stamps - Deleted FPT_AMT.1. It is specified in '6. Protection Profile Application Notes' that FPT_TEE.1 should be included, according to the TOE implementation. - Changed the evaluation assurance level from EAL3+ to EAL4. - ADV_IMP.1 is included in EAL4. Therefore, T. Flaw Implementation and O. Flaw Implementation Inspection are deleted. - Modified the attack potential from low to Enhanced-Basic in order to handle AVA_VAN.3 required by EAL4. - Others: Modified editing error and supplemented contents, etc.

Table of Contents

List of Tables

List of Figures

1. PP Introduction

1.1 PP Reference

1 Title : Firewall Protection Profile

2 Protection Profile Version : V2.0

3 Evaluation Criteria : Common Criteria for Information Security Evaluation (Ministry of Information and Communication Public Notice No. 2005-25)

4 Common Criteria Version : V3.1r2

5 Evaluation Assurance Level : EAL4

6 Developer : IT Security Evaluation Division, Evaluation Planning Team, KISA
Information & Communication Engineering, SungKyunKwan University

7 Certification Body : IT Security Certification Center, National Intelligence Service

8 Registration Number : KECS-PP-0093-2008, April 24, 2008

9 Validation Result : Validated under the KECS(Korea IT Security Evaluation and Certification Scheme)

10 Keywords : Protection Profile, Information Flow Control, Firewall

1.2 TOE Overview

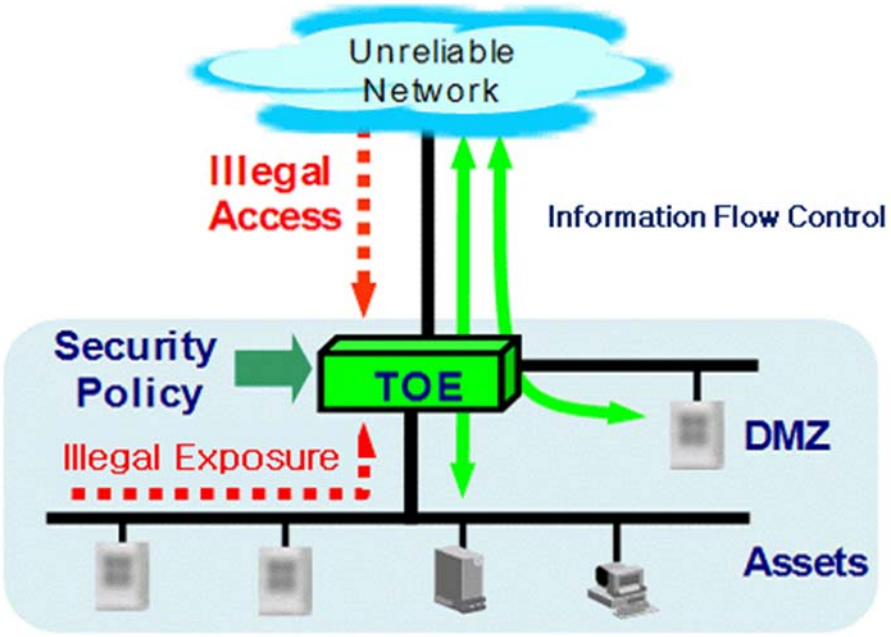
11 This PP defines security functional requirements and security assurance requirements of the firewall used as a means to protect internal information and the communications network of an organization.

12 The purpose of a firewall is to provide controlled accesses to service request to the network to be protected. A firewall is divided into various politic and technical categories, such as in terms of a configuration method, level of the applied the network and the access control method, etc. A firewall is categorized into packet-filtering, application-level gateway and hybrid types according to the network level. Per a configuration and operation method, it is also categorized into the dual network host, bastion host, screen subnet and screen host gateway firewall. This PP includes security requirements that are commonly applied regardless of the diverse configurations.

1.2.1 TOE Operational Environment

13 (Figure 1) shows the operational environment and the key security functions of the TOE.

14 The TOE is located where the external network, such as the Internet, and the internal network of Organization are connected and executes security functions, all information transferred between the internal and external networks shall pass through the TOE. A firewall can be configured in the forms of dual-homed, screened-host and screened-subnet, etc. Diverse installation types and operation methods of a firewall can be used.



(Figure 1) TOE Description

15 Assets to be protected by the TOE are the protected target system (network services and resources, etc., protected by the security policies of the firewall) that exist in the internal network of organization. Also, the TOE itself and the important data of the inside of the TOE (security attributes and TSF data, etc.) are assets to be protected by the TOE.

1.2.2 TOE Scope

16 The TOE executes the functions of security audit, information flow control, user identification and authentication, security management and other TSF protection, etc.

Security Audit

17 The TOE generates, records and reviews audit record of the security-related events in order to trace responsibilities for the security-related activities. Also, the TOE detects potential security violation of the audited events and takes the response actions

Information flow control

18 The TOE ensures that the related security policies are executed in order to mediate information flow.

Identification and Authentication

19 The TOE identifies and authenticates the user identity and defines TSF actions in cases of authentication failures.

Security Management

20 The TOE manages security functions, security attributes, TSF data and security roles, etc.

Other TSF Protection

21 The TOE executes self tests in order to verify integrity of TSF data and executable code. The TOE provides session management functions after time interval of user inactivity.

22 The TOE may be implemented to stand-alone type or require additional hardware, software or firmware for operation. This Protection Profile has been developed to reflect the TOE implemented in various types. In case where ST author conforms this Protection Profile, all non-TOE hardware, software or firmware that are necessary for the TOE execution shall be described.

1.3 Conventions

23 The notation, formatting and conventions used in this Protection Profile are consistent with the Common Criteria for Information Technology Security Evaluation.

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

Assignment

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].

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.).

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**.

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*.

Security target author operation

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.

25 "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

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

Assets

Entities that the owner of the TOE presumably places value upon.

Assignment

The specification of an identified parameter in a component (of the CC) or requirement.

Attack Potential

A measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources and motivation.

Authentication Data

Information used to verify the claimed identity of a user.

Authorized Administrator

An authorized user who may, in accordance with the SFRs, operation and manage Firewall.

Authorized User

A user who may, in accordance with the SFRs, perform an operation

Class

A grouping of CC families that share a common focus.

Component

The smallest selectable set of elements on which requirements may be based.

Dependency

A relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package.

Element

An indivisible statement of security need.

Evaluation Assurance Level (EAL)

An assurance package, consisting of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale.

External Entity

any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.

Family

A grouping of components that share a similar goal but may differ in emphasis or rigor.

Identity

A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Iteration

The use of the same component to express two or more distinct requirements.

Object

A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Operation (on a component of the CC)

Modifying or repeating that component. Allowed operations on components are assignment, iteration, refinement and selection.

Operation (on an object)

A specific type of action performed by a subject on an object.

Organizational security policy (OSP)

A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organization in the operational environment.

Protection Profile (PP)

An implementation-independent statement of security needs for a TOE type.

Refinement

The addition of details to a component.

Role

A predefined set of rules establishing the allowed interactions between a user and the TOE.

Security Function Policy (SFP)

A set of rules describing specific security behavior enforced by the TSF and expressible as a set of SFRs.

Security Target (ST)

An implementation-dependent statement of security needs for a specific identified TOE.

Selection

The specification of one or more items from a list in a component.

Subject

An active entity in the TOE that performs operations on objects.

Target Of Evaluation (TOE)

A set of software, firmware and/or hardware possibly accompanied by guidance.

Threat Agent

An unauthorized user that brings assets under such threats as illegal access, modification or deletion.

TOE Security Functionality (TSF)

A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs.

TSF data

Data created by and for the TOE, that might affect the operation of the TOE.

User

See external entity

1.5 PP Organization

27 Section 1 provides the PP reference and the TOE overview for the PP introduction.

28 Section 2 describes the conformance claim of the CC, PP, package, conformance rationale and PP conformance statement.

29 Section 3 describes the TOE security problem definition of the TOE and the TOE environment such as assumptions, threats and organizational security policies.

30 Section 4 defines the security objectives for the TOE and its environment to address threats, assumptions and organizational security policies.

31 Section 5 describes the security requirements including the functional and assurance requirements intended to satisfy security objectives.

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

33 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.

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

2. Conformance Claim

35 Conformance claim describes the CC, PP and package conformance claim, conformance rationale, PP conformance statement.

2.1 CC Conformance Claim

36 This protection profile claims conformance to

– Common Criteria reference

- Common Criteria for Information Technology Security Evaluation, part 1 : Introduction and general model, Version 3.1r1, Sep. 2006, CCMB-2006-09-001
- Common Criteria for Information Technology Security Evaluation, part 2 : Security functional requirements, Version 3.1r1, Sep. 2007, CCMB-2007-09-002
- Common Criteria for Information Technology Security Evaluation, part 3 : Security assurance requirements, Version 3.1r1, Sep. 2007, CCMB-2007-09-003

- Common Criteria Conformance

- Part 2 Conformant
- Part 3 Conformant

2.2 PP Conformance Claim

37 There is no PP conformed by this PP.

2.3 Package Conformance Claim

38 This PP conforms the following package of security assurance requirements.

- Assurance Package: EAL4 conformance

2.4 Conformance Rationale

39 This PP did not claim conformance of other PPs, therefore it is not necessary to describe the conformance rationale.

2.5 PP Conformance Statement

40 This PP requires " demonstrable-PP conformance".

Application Notes: The most basic rule for demonstrable-PP conformance is that the ST is considered to be "equivalent or more restrictive" than the PP.

Here, the concept of the 'equivalent' means that SFR A in the PP can be used the same as SFR A or can be replaced with SFR B of the equivalent level in the ST. For example, FTA_SSL.1 (TSF-initiated session locking) of the PP can be replaced with FTA_SSL.3 (TSF-initiated termination) in the ST in order to manage sessions after time interval of user inactivity.

Also, the concept of 'more restrictive' means that the TOE that meets the ST also meets the PP by specifying the addition of details(the rules of refinement apply) or applying stronger requirements.

3. Security Problem Definition

41 The security problem definition defines the intended threats, organizational security policies and assumptions so as to be handled by the TOE and the TOE operation environment.

3.1 Threats

42 The Threat agent is generally IT entities and human users who exert damage to the TOE and internal assets in abnormal methods or attempt illegal access to the TOE and internal assets from outside. The Threat agent has enhanced-basic level of expertise, resources and motivation

T. Address Spoofing

43 The threat agent of the external network may try to access the internal network by spoofing the source IP address as an the internal IP address.

T. Continuous Authentication Attempt

44 The threat agent can acquire the authorised user rights by attempting continuous authentication to access the TOE.

T. Illegal Information Inflow

45 The threat agent can violate the internal network with inflow of not allowed information from outside.

T. Illegal Information Outflow

46 The Internal user can have illegal information exposed to the outside through the network.

T. Impersonation

47 The threat agent can access the TOE by masquerading as an authorized user.

T. Recording Failure

48 The threat agent can disable recording of security-related events of the TOE by exhausting storage capacity.

T. Replay Attack

49 The threat agent can access the TOE by replaying the authentication data of an authorized user.

T. Stored Data Damage

50 The threat agent can expose, modify and delete TSF data stored in the TOE in an unauthorized method.

3.2 Organizational Security Policies

51 The TOE shall comply with the following Organizational Security Policies.

P. Audit

52 To trace responsibilities on all security-related activities, security-related events shall be recorded and maintained and reviewed.

P. Secure Management

53 The TOE shall provide management means for the authorised administrator to manage the TOE in a secure manner.

3.1 Assumptions

54 The following conditions are assumed to exist in the operational environment.

A. Operating System Reinforcement

55 Unnecessary services or means shall be removed from the operating system, and security shall be enhanced to better protect against vulnerabilities in the operating system thereby ensuring its reliability and stability.

A. Physical Security

56 The TOE shall be located in physically secure environment that can be accessed only by the authorized administrator.

A. Security Maintenance

57 When the internal network environment changes due to change in the network configuration, host increase/ decrease and service increase/ decrease, etc., the changed environment and security policy shall immediately be reflected in the TOE operation policy so that security level can be maintained to be the same as before.

A. Single Point of Connection

58 All communications between the external and internal networks are carried out only through the TOE.

A. Trusted Administrator

59 The authorized administrator of the TOE shall not have any malicious intention, receive proper training on the TOE management, and follow the administrator guidelines

4. Security Objectives

60 This PP defines security objectives by categorizing them into the TOE and the environment. Security objectives for the TOE are directly handled by the TOE. Security objectives for operation environment shall be handled by technical/procedural means supported by the operation environment in order for the TOE to accurately provide security functions.

4.1 Security Objectives for the TOE

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

O. Audit

62 The TOE shall record and maintain security-related events in order to enable tracing of responsibilities for security-related acts and shall provide means to review the recorded data.

O. Data Protection

63 The TOE shall protect TSF data stored in the TOE from unauthorized exposure, modify and deletion.

O. Identification and Authentication

64 The TOE shall uniquely identify user and authenticate identity of user.

O. Information Flow Control

65 The TOE shall control outflow and inflow of unauthorized information from inside to outside or from outside to inside.

O. Management

66 The TOE shall provide means for the authorized administrator of the TOE to efficiently manage the TOE in a secure manner.

4.2 Security Objectives for the Operational Environment

67 The followings are security objectives handled in relation to IT fields or by non-technical/procedure-related means.

OE. Operation System Reinforcement

68 Unnecessary services or means shall be removed from the operating system, and security shall be enhanced to better protect against vulnerabilities in the operating system thereby ensuring its reliability and stability.

OE. Physical Security

69 The TOE shall be located in physically secure environment that can be accessed only by the authorized administrator.

OE. Security Maintenance

70 When the internal network environment changes due to change in the network configuration, host increase/ decrease and service increase/ decrease, etc., the changed environment and security policy shall immediately be reflected in the TOE operation policy so that security level can be maintained to be the same as before.

OE. Single Point of Connection

71 All communications between the external and internal networks are carried out only through the TOE.

OE. Time Stamp

72 The TOE shall accurately record the security related events by using the reliable time stamps provided by the TOE operational environment.

OE. Trusted Administrator

73 The authorized administrator of the TOE shall not have any malicious intention, receive proper training on the TOE management, and follow the administrator guidelines.

4.3 Security Objectives rationale

74 The security objectives rationale demonstrates that the specified security objectives are appropriate, sufficient to trace security problems and are essential, rather than excessive.

75 The rationale of security objectives demonstrates the following.

- Each threat, organizational security policy and assumption has at least one security objective tracing to it.
- Each security objective traces to at least one threat, organizational security policy and assumption.

[Table 1] Summary of Mappings Between Security Problem Definition and Security Objectives

Security Objectives / Security Problem Definition	Security Objectives for the TOE					Security Objectives for the Operational Environment					
	O. Audit	O. Data Protection	O. Identification and Authentication	O. Information flow Control	O. Management	OE. Operation System Reinforcement	OE. Physical Security	OE. Security Maintenance	OE. Single point of Connection	OE. Time Stamp	OE. Trusted Administrator
T. Address Spoofing				X							
T. Continuous Authentication Attempt			X								
T. Illegal Information Inflow				X							
T. Illegal Information Outflow				X							
T. Impersonation			X								
T. Recording Failure	X										
T. Replay Attack			X								
T. Stored Data Damage		X	X								
P. Audit	X									X	
P. Secure Management					X						X
A. Operation System Reinforcement						X					
A. Physical Security							X				
A. Security Maintenance								X			
A. Single Point of Connection									X		
A. Trusted Administrator											X

4.3.1 Rationale of Security Objectives for the TOE

O. Audit

76 The TOE to provide means to accurately record, maintain and review security-related events in details, therefore is required to counter threat of T. Recording Failure and to enforcing organizational security policy of P. Audit.

O. Management

77 The TOE to provide means for the authorized administrator to manage the TOE in a secure manner, therefore is required to enforcing organizational security policy of P. Secure Management.

O. Data Protection

78 The TOE to ensure integrity of TSF data, therefore is required to counter threat of T. Stored Data Damage.

O. Identification and Authentication

79 The TOE to ensure uniquely identify and authorize user, therefore is required to counter threats of T. Impersonation, T. Continuous authentication attempt, T. Replay Attack and T. Stored Data Damage.

O. Information Flow Control

80 The TOE to ensure mediate information flow according to security policy, therefore is required to counter threats of T. Illegal information inflow, T. Illegal information outflow and T. Address spoofing.

4.3.2 Rationale of Security Objectives for the Operational Environment

OE. Physical Security

81 This security objective for the operational environments ensures physically secure environment of the TOE, therefore is required to support assumption of A. Physical Security.

OE. Security Maintenance

82 When the internal network environment changes due to change in the internal network configuration, increase/decrease of host and increase/decrease of service, etc., this security objective for the operational environments ensures to immediately reflect the changed environment and security policy to operation policy, therefore to maintain security in the same level as before. Therefore, this security objective is required to support assumption of A. Security Maintenance.

OE. Trusted Administrator

83 This security objective for the operational environments ensures that the authorized administrator of the TOE can be trusted. Therefore, this is required to enforcing organizational security policies of P. Secure Management and to support assumption of A. Trusted Administrator.

OE. Operation System Reinforcement

84 This security objective for the operational environments ensures for operation system to be reliability and stability by executing operation to remove all services or means in operation system not required and reinforcement on vulnerabilities of operation system. Therefore, this security objective is required to support assumption of A. Operation System Reinforcement .

OE. Single Point of Connection

85 This security objective for the operational environments ensures that all communications between the external and internal networks are carried out only through the TOE, therefore is required to support assumption of A. Single Point of Connection

OE. Time Stamp

86 Security objectives for this operational environment ensures to accurately record the security-related events by using reliable time stamps provided by the TOE operational environment, therefore is required to enforcing organizational security policies of P. Audit.

5. Security Requirements

87 Security requirements describe security functional and assurance requirements to be satisfied by the TOE that conforms this PP.

88 This PP defines all subjects, objects, operations, security attributes and external entities, etc. used in security requirements as follows.

a) Subjects, objects and the related security attributes, operations

[Table 2] Definition of Subjects, Objects and the Related Security Attributes, Operations

Subjects(User)	Security Attributes of Subjects(User)	Objects(Information)	Security Attributes of Objects(Information)	Operations
External entities that send and receive information through the TOE [1)]	-	Traffic (packet) sent through the TOE[2)]	-	. All operations
Authorized Administrator	-	Audit Data	-	. Read, etc.
		Identification and Authentication Data	-	. modify, delete
		Audit storage capacity, number of unsuccessful authentication attempts, time interval which self test occurs	-	. specify of the limits
		TSF data	-	. verify the Integrity
		Security attributes	-	. Change default, query, modify, delete . specify alternative initial values to override the default values

Application Notes: [1)] ,[2)] specify the types of subjects/information. Each subject/information list shall be defined by the ST author.

b) External entity

- No external entity explicitly specified in security functional and assurance requirements

89 The ST author shall clearly define all subjects, objects, operations, security attributes and external entities, etc. not explicitly specified in this PP.

5.1 Security Functional Requirements

90 The security functional requirements defined in this Protection Profile consist of the following components from Part 2 of the CC, summarized in the following [Table 3].

[Table 3] Security Functional Requirements

Security Functional Class	Security Functional Components	
Security Audit	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_SEL.1	Selective audit
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
User Data Protection	FDP_IFC.2	Complete information flow control
	FDP_IFF.1	Simple security attributes
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.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
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
Protection of the TSF	FPT_TST.1	TSF testing
TOE Access	FTA_SSL.1	TSF-initiated session locking

	FTA_SSL.3	TSF-initiated termination

5.1.1 Security Audit

FAU_ARP.1 Security alarms

Hierarchical to : No other components.

Dependencies : FAU_SAA.1 Potential violation analysis

91 FAU_ARP.1.1 The TSF shall take [{ determined by the Security target author } list of actions] upon detection of a potential security violation.

FAU_GEN.1 Audit data generation

Hierarchical to : No other components.

Dependencies : FPT_STM.1 Reliable time stamps

92 FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *not specified* level of audit; and

c) [Refer to “Auditable Events” of [Table 4], { determined by the Security target author } auditable events].

93 FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [Refer to “Additional audit record content” of [Table 4], { determined by the Security target author } other audit relevant information].

[Table 4] Auditable events

Functional Components	Auditable Events	Additional audit record content s
FAU_ARP.1	Actions taken due to imminent security violations.	Recipient identity of actions
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms, Automated responses performed by the tool.	-
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	-
FDP_IFF.1	Decisions to permit requested information flows.	Identified information of Object

FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state	-
FIA_SOS.1	Rejection by the TSF of any tested secret	-
FIA_UAU.1	All use of the authentication mechanism	-
FIA_UAU.4	Attempts to reuse authentication data.	-
FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identity provided	-
FMT_MOF.1	All modifications in the behavior of the functions in the TSF.	-
FMT_MSA.1	All modifications of the values of security attributes.	Modified values of the security attributes
FMT_MTD.1	All modifications to the values of TSF data.	Modified values of TSF data
FMT_MTD.2	All modifications to the limits on TSF data	Modified limit of TSF data
FMT_SMF.1	Use of the management functions.	-
FMT_SMR.1	Modifications to the group of users that are part of a role	-
FPT_TST.1	Execution of the TSF self tests and the results of the tests.	In case of violation of integrity, Modified TSF data or executable code
FTA_SSL.1	Locking of an interactive session by the session locking mechanism, Successful unlocking of an interactive session.	-
FTA_SSL.3	Termination of an interactive session by the session locking mechanism.	-

FAU_SAA.1 Potential violation analysis

Hierarchical to : No other components.

Dependencies : FAU_GEN.1 Audit data generation

94 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 SFR.

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

a) Accumulation or combination of [Authentication unsuccessful audit events in auditable events of FIA_UAU.1, Audit events of violation of control rule in auditable events of FDP_IFF, Audit events of violation of integrity in auditable events of FPT_TST.1] known to indicate a potential security violation;

b) [{ determined by the Security target author } any other rules].

FAU_SAR.1 Audit review

Hierarchical to : No other components.

Dependencies : FAU_GEN.1 Audit data generation

96 FAU_SAR.1.1 The TSF shall provide [the authorized administrator] with the capability to read [all audit data] from the audit records.

97 FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Application Notes: In case where this security functional requirement cannot be completely implemented as the TOE security functional requirements, the TOE operational environment can support the review function of audit data.

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

98 FAU_SAR.3.1 The TSF shall provide the ability to apply [assignment : *methods of selection and/or ordering*] of audit data based on [assignment : *criteria with logical relations*].

Application Notes: In case where this security functional requirement cannot be completely implemented as the TOE security functional requirements, the TOE operational environment can support the review function of audit data.

FAU_SEL.1 Selective audit

Hierarchical to : No other components.

Dependencies : FAU_GEN.1 Audit data generation

FMT_MTD.1 Management of TSF data

99 FAU_SEL.1.1 The TSF shall be able to select the set of audited events from the set of all auditable events based on the following attributes:

a) [selection: *object identity, user identity, subject identity, host identity, event type*]

b) [assignment: *list of additional attributes that audit selectivity is based upon*]

FAU_STG.1 Protected audit trail storage

Hierarchical to : No other components.

Dependencies : FAU_GEN.1 Audit data generation

100 FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

101 FAU_STG.1.2 The TSF shall be able to *prevent* unauthorized modifications to the stored audit records in the audit trail.

Application Note : In case where this security functional requirement cannot be completely implemented as the TOE security functional requirements, the TOE operational environment can support to protect the audit trail storage.

FAU_STG.3 Action in case of possible audit data loss

Hierarchical to : No other components.

Dependencies : FAU_STG.1 Protected audit trail storage

102 FAU_STG.3.1 The TSF shall [notify to the authorized administrator, { determined by the Security target author } actions to be taken in case of possible audit storage failure] if the audit trail exceeds [assignment: *pre-defined limit*].

Application Notes : In case where this security functional requirement cannot be completely implemented as the TOE security functional requirements, the TOE operational environment can support actions to be taken in case of possible audit data loss.

FAU_STG.4 Prevention of audit data loss

Hierarchical to : FAU_STG.3 Action in case of possible audit data loss

Dependencies : FAU_STG.1 Protected audit trail storage

103 FAU_STG.4.1 The TSF shall *prevent audited events, except those taken by the authorized user with special rights* and [{ determined by the Security target author } other actions to be taken in case of audit storage failure] if the audit trail is full.

Application Notes : If audit storage is full, only the authorized administrator shall be allowed to perform operations. Only after the authorized administrator restores storage can audit records be generated. Also, in case where this security functional requirement cannot be completely implemented as the TOE security functional requirements, the TOE operational environment can support prevention of the audit data loss.

5.1.2 User data protection

FDP_IFC.2 Complete information flow control

Hierarchical to : FDP_IFC.1 Subset information flow control

Dependencies : FDP_IFF.1 Simple security attributes

104 FDP_IFC.2.1 The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment : *list of subjects and information*] and all operations that cause that information to flow to and from subjects covered by the SFP.

105 FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

FDP_IFF.1 Simple security attributes

Hierarchical to : No other components.

Dependencies : FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

106 FDP_IFF.1.1 The TSF shall enforce the [assignment : *information flow control SFP*] based on the following types of subject and information security attributes: [assignment : *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*].

107 FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment : for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

108 FDP_IFF.1.3 The TSF shall enforce the [assignment : *additional information flow control SFP rules*].

109 FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [assignment : *rules, based on security attributes, that explicitly authorize information flows*].

110 FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment : *rules, based on security attributes, that explicitly deny information flows*].

5.1.3 Identification and authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to : No other components.

Dependencies : FIA_UAU.1 Timing of authentication

111 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*].

112 FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [prevent users from being authenticated till the authorized administrator takes proper action, { determined by the Security target author } list of actions].

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FIA_SOS.1 Verification of secrets

Hierarchical to : No other components.

Dependencies : No dependencies.

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

Application Notes : The "defined quality metric" includes, in case of password authentication mechanism, a minimum length, a combination rule, or a modification frequency, and so on.

FIA_UAU.1 Timing of authentication

Hierarchical to : No other components.

Dependencies : FIA_UID.1 Timing of identification

115 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.

116 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.

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to : No other components.

Dependencies : No dependencies.

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

Application Notes : The single-use authentication mechanism can be applied to both authorized administrators and user and single-use authentication mechanism may not be used as long as the provided services conform to the security policy. Examples of single-use authentication mechanisms are single-use password and encrypted time stamp, etc.

FIA_UAU.7 Protected authentication feedback

Hierarchical to : No other components.

Dependencies : FIA_UAU.1 Timing of authentication

118 FIA_UAU.7.1 The TSF shall provide only [assignment : *list of feedback*] to the user while the authentication is in progress.

FIA_UID.2 User identification before any action

Hierarchical to : FIA_UID.1 Timing of identification

Dependencies : No dependencies.

119 FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.4 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

120 FMT_MOF.1.1 The TSF shall restrict the ability to [selection : *determine the behavior of, disable, enable, modify the behavior of*] the functions [assignment : *list of functions*] to [the authorized administrator].

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_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

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

FMT_MSA.3 Static attribute initialization

Hierarchical to : No other components.

Dependencies : FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

122 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.

123 FMT_MSA.3.2 The TSF shall allow the [the authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1(1) Management of TSF data

Hierarchical to : No other components.

Dependencies : FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

124 FMT_MTD.1.1 The TSF shall restrict the ability to *modify, delete* the [identification and authentication data] to [the authorized administrator].

FMT_MTD.1(2) Management of TSF data

Hierarchical to : No other components.

Dependencies : FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

125 FMT_MTD.1.1 The TSF shall restrict the ability to [selection : *change_default, query, modify, delete*, clear, [assignment : *other operations*]] the [audit data, { determined by the Security target author } list of the TSF data] to [the authorized administrator].

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

126 FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [audit storage capacity, some number of unsuccessful authentication attempts, time interval which self test occurs] to [the authorized administrator].

127 FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits : [specified actions in FAU_STG.3, FIA_AFL.1, specified self tests in FPT_TST.1].

FMT_SMF.1 Specification of Management Functions

Hierarchical to : No other components.

Dependencies : No dependencies.

128 FMT_SMF.1.1 The TSF shall be capable of performing the following management functions : [assignment : *list of 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

129 FMT_SMR.1.1 The TSF shall maintain the roles [the authorized administrator].

130 FMT_SMR.1.2 The TSF shall be able to associate users with **the authorized administrator** roles.

5.1.5 Protection of the TSF

FPT_TST.1 TSF testing

Hierarchical to : No other components.

Dependencies : No other components.

131 FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation, at the request of the authorized user, [at the conditions { determined by the*

Security target author } conditions under which self test should occur] to demonstrate the correct operation of [selection : *[assignment : parts of TSF]*, *the TSF*].

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

133 FPT_TST.1.3 The TSF shall provide **the authorized administrator** with the capability to verify the integrity of stored TSF executable code.

5.1.6 TOE access

FTA_SSL.1 TSF-initiated session locking

Hierarchical to : No other components.

Dependencies : FIA_UAU.1 Timing of authentication

134 FTA_SSL.1.1 The TSF shall lock an interactive **the authorized administrator** session after [assignment : *time interval of **the authorized administrator** inactivity*] by :

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of **the authorized administrator** data access/display devices other than unlocking the session.

135 FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session : [assignment : *events to occur*].

FTA_SSL.3 TSF-initiated termination

Hierarchical to : No other components.

Dependencies : No dependencies.

136 FTA_SSL.3.1 The TSF shall terminate an interactive user session after a [assignment *: time interval of user inactivity*].

5.2 Security Assurance Requirements

137 The security assurance requirements for this PP consist of the following components from Part 3 of the CC, summarized in the following [Table 5] and evaluation assurance level is EAL4.

[Table 5] Security Assurance Requirements

Assurance Class	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	Production 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.3	Focused vulnerability analysis

5.2.1 Security Target evaluation

ASE_INT.1 ST introduction

Dependencies :

No dependencies.

Developer action elements :

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

Content and presentation elements :

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

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

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

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

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

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

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

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

Evaluator action elements :

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

148 ASE_INT.1.2E The evaluator shall confirm that the TOE 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 :

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

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

Content and presentation elements :

151 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.

152 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.

153 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.

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

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

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

157 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.

158 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.

159 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.

160 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 :

161 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 :

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

Content and presentation elements :

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

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

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

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

Evaluator action elements :

167 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 :

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

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

Content and presentation elements :

170 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.

171 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.

172 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.

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

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

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

Evaluator action elements :

176 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 :

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

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

Content and presentation elements :

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

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

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

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

183 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 :

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

185 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 :

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

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

Content and presentation elements :

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

189 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.

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

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

192 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.

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

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

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

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

Evaluator action elements :

197 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 :

198 ASE_TSS.1.1D The developer shall provide a TOE summary specification.

Content and presentation elements :

199 ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements :

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

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

5.2.2 Development

ADV_ARC.1 Security architecture description

Dependencies :

ADV_FSP.1 Basic functional specification

ADV_TDS.1 Basic design

Developer action elements :

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

203 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.

204 ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements :

205 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.

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

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

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

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

Evaluator action elements :

210 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 :

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

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

Content and presentation elements :

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

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

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

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

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

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

Evaluator action elements:

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

220 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 :

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

222 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 :

223 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.

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

225 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 :

226 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 :

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

228 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 :

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

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

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

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

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

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

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

236 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 and called interfaces to other modules.

237 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.

238 ADV_TDS.3.10C The mapping shall demonstrate that all behavior described in the TOE design is mapped to the TSFIs that invoke it.

Evaluator action elements :

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

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

5.2.3 Guidance Documents

AGD_OPE.1 Operational user guidance

Dependencies :

ADV_FSP.1 Basic functional specification

Developer action elements :

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

Content and presentation elements :

242 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.

243 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.

244 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.

245 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.

246 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.

247 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.

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

Evaluator action elements :

249 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 :

250 AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements :

251 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.

252 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 :

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

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

5.2.4 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 Objectives

Developer action elements :

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

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

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

Content and presentation elements :

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

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

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

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

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

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

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

265 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.

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

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

Evaluator action elements :

268 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 :

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

Content and presentation elements :

270 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.

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

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

Evaluator action elements :

273 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 :

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

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

Content and presentation elements :

276 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 :

277 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 :

278 ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation elements :

279 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 :

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

281 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 :

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

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

Content and presentation elements :

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

285 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 :

286 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 :

287 ALC_TAT.1.1D The developer shall identify each development tool being used for the TOE.

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

Content and presentation elements :

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

290 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.

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

Evaluator action elements :

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

5.2.5 Tests

ATE_COV.2 Analysis of coverage

Dependencies :

ADV_FSP.2 Security-enforcing functional specification

ATE_FUN.1 Functional testing

Developer action elements :

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

Content and presentation elements :

294 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.

295 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 :

296 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 :

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

Content and presentation elements :

298 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.

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

300 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 :

301 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 :

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

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

Content and presentation elements :

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

305 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.

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

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

Evaluator action elements :

308 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 :

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

Content and presentation elements :

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

311 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 :

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

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

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

5.2.6 Vulnerability assessment

AVA_VAN.3 Focused vulnerability analysis

Dependencies :

ADV_ARC.1 Security architecture description

ADV_FSP.2 Security-enforcing 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

Developer action elements :

315 AVA_VAN.3.1D The developer shall provide the TOE for testing.

Content and presentation elements :

316 AVA_VAN.3.1C The TOE shall be suitable for testing.

Evaluator action elements :

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

318 AVA_VAN.3.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

319 AVA_VAN.3.3E The evaluator shall perform an independent 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.

320 AVA_VAN.3.4E 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 Enhanced-Basic attack potential.

5.3 Security Requirements Rationale

321 Security Requirements Rationale demonstrate that the described security requirements are suitable to satisfy security objectives and, as a result, appropriate to address security problems.

5.3.1 Security Functional Requirements Rationale

322 Rationale of security functional requirements demonstrates the followings.

- Each TOE security objective has at least one security functional requirement tracing to it.
- Each TOE security functional requirement traces back to at least one TOE security objectives.

[Table 6] Summary of Mappings Between Security Objectives and Security Functional Requirements

Security Objectives / Security Functional Requirements	O. Audit	O. Data Protection	O. Identification and Authentication	O. Information Flow Control	O. Management
FAU_ARP.1	X				
FAU_GEN.1	X				
FAU_SAA.1	X				
FAU_SAR.1	X				
FAU_SAR.3	X				
FAU_SEL.1	X				
FAU_STG.1	X				
FAU_STG.3	X				
FAU_STG.4	X				
FDP_IFC.2				X	
FDP_IFF.1				X	
FIA_AFL.1			X		
FIA_ATD.1			X		
FIA_SOS.1			X		
FIA_UAU.1		X	X		X
FIA_UAU.4			X		
FIA_UAU.7			X		
FIA_UID.2		X	X		X
FMT_MOF.1					X
FMT_MSA.1					X
FMT_MSA.3					X
FMT_MTD.1(1)					X
FMT_MTD.1(2)					X
FMT_MTD.2					X
FMT_SMF.1					X
FMT_SMR.1					X
FPT_TST.1		X			
FTA_SSL.1		X			X
FTA_SSL.3		X			X

FAU_ARP.1 Security alarms

323 This component ensures handling ability in the event of detecting security violation, therefore satisfies The TOE security objective of O. Audit.

FAU_GEN.1 Audit data generation

324 This component ensures the ability to define events for audit and to generate audit record, therefore satisfies the TOE security objective of O. Audit.

FAU_SAA.1 Potential violation analysis

325 This component ensures the ability to point out security violation by inspecting the audited events, therefore satisfies the TOE security objective of O. Audit.

FAU_SAR.1 Audit review

326 This component ensures the ability of the authorized administrator to review audit record, therefore satisfies the TOE security objective of O. Audit.

FAU_SAR.3 Selectable audit review

327 This component ensures the ability to search and sorting audit data by bases to hold logical relations, therefore satisfies the TOE security objective of O. Audit.

FAU_SEL.1 Selective audit

328 This component ensures the ability to include or exclude events for audit on the basis of attributes, therefore satisfies the TOE security objective of O. Audit.

FAU_STG.1 Protected audit trail storage

329 This component ensures the ability to protect audit record from unauthorized modification and deletion, therefore satisfies the TOE security objective of O. Audit.

FAU_STG.3 Action in case of possible audit data loss

330 This component ensures handling ability in the audit trail exceeds the pre-defined limit, therefore satisfies the TOE security objective of O. Audit.

FAU_STG.4 Prevention of audit data loss

331 This component ensures handling ability in the audit storage is full, therefore satisfies the TOE security objective of O. Audit.

FDP_IFC.2 Complete information flow control

332 This component ensures that security policy for the TOE information flow control is defined and that scope of security policy is defined, therefore satisfies the TOE security objective of O. Information Flow Control.

FDP_IFF.1 Simple security attributes

333 This component provides the rules to control information flow on the basis of security attributes, therefore satisfies the TOE security objective of O. Information Flow Control.

FIA_AFL.1 Authentication failure handling

334 This component ensures the ability to define the count of authentication failure attempt by user and to take handling actions when the defined count is reached or exceeded, therefore satisfies the TOE security objective of O. Identification and Authentication.

FIA_ATD.1 User attribute definition

335 This component defines security attribute list for each user, therefore satisfies the TOE security objective of O. Identification and Authentication.

FIA_SOS.1 Verification of Secrets

336 This component provides mechanism to verify whether password satisfies the defined quality metric, therefore satisfies the TOE security objective of O. Identification and Authentication.

FIA_UAU.1 Timing of authentication

337 This component ensures the ability to successfully authenticate the authorized administrator, therefore satisfies the TOE security objectives of O. Management, O. Data Protection and O. Identification and Authentication.

FIA_UAU.4 Single-use authentication mechanisms

338 This component ensures the ability to prevent reusing of authentication data, therefore satisfies the TOE security objective of O. Identification and Authentication.

FIA_UAU.7 Protected authentication feedback

339 This component ensures that only the designated authentication feedback is provided to user while authentication is in progress, therefore satisfies the TOE security objective of O. Identification and Authentication.

FIA_UID.2 User identification before any action

340 This component ensures the ability to successfully identify user, therefore satisfies the TOE security objectives of O. Management, O. Data Protection and O. Identification and Authentication.

FMT_MOF.1 Management of security functions behavior

341 This component ensures the ability for the authorized administrator to manage security function, therefore satisfies the TOE security objective of O. Management.

FMT_MSA.1 Management of security attributes

342 This component ensures that the authorized administrator manages security attributes applied to access control and information flow control policies, therefore satisfies the TOE security objective of O. Management.

FMT_MSA.3 Static attribute initialization

343 This component provides default values of security attributes applied to access control and information flow control policies, therefore satisfies the TOE security objective of O. Management.

FMT_MTD.1(1) Management of TSF data

344 This component provides the ability for the authorized administrator to handle statistical processing of audit data, therefore satisfies the TOE security objectives O. Management.

FMT_MTD.1(2) Management of TSF data

345 This component provides the ability for the authorized administrator to backup and recovery major files composing the TOE, therefore satisfies the TOE security objective of O. Management.

FMT_MTD.2 Management of limits on TSF data

346 This component ensures that the authorized administrator manages limits of TSF data and takes handling actions when the indicated limits are reached or exceeded, therefore satisfies the TOE security objective of O. Management.

FMT_SMF.1 Specification of management functions

347 This component requires to specify management functions, such as security attributes, TSF data and security functions, etc., to be executed by TSF, therefore satisfies the TOE security objective of O. Management.

FMT_SMR.1 Security roles

348 This component ensures the ability to associate user with the authorized administrator role, therefore satisfies the TOE security objective of O. Management

FPT_TST.1 TSF testing

349 This component ensures to run a suite of self tests to demonstrate the correct operation of the TSF and provides the authorized user with the capability to verify the integrity of the TSF data

and the TSF executable code, therefore satisfies the TOE security objectives of O. Data Protection.

FTA_SSL.1 TSF-initiated session locking

350 This component requires to lock an interactive session after time interval of user inactivity and events to occur prior to unlocking the session, therefore satisfies the TOE security objectives of O. Management and O. Data Protection.

FTA_SSL.3 TSF-initiated termination

351 This component requires to terminate an interactive session after time interval of the authorized general user inactivity, therefore satisfies the TOE security objective of O. Management and O. Data Protection

5.3.2 Security Assurance Requirements Rationale

352 Evaluation assurance level of this firewall protection profile is EAL4.

353 EAL4, as an assurance package to require methodically designed, tested and reviewed, 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.

354 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.

355 EAL4 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, a description of the basic modular design of the TOE, and a subset of the implementation, to understand the security behavior. The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, implementation representation, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with an Enhanced-Basic attack potential.

5.4 Rationale of Dependency

5.4.1 Dependency of Security Functional Requirements

356 [Table 7] shows dependency of security functional requirements

357 FDP_IFF.1 depends on FDP_IFC.1 and this is satisfied by FDP_IFC.2 that is in hierarchical relationship with FDP_IFC.1.

358 FIA_UAU.1 and FMT_SMR.1 depends on FIA_UID.1 and this is satisfied by FIA_UID.2 that is in hierarchical relationship with FIA_UID.1.

359 FMT_MSA.1 depends on FDP_ACC.1 or FDP_IFC.1 and this is satisfied by FDP_IFC.2 that is in hierarchical relationship with FDP_IFC.1.

360 FAU_GEN.1 depends on FPT_STM.1. However, the TOE accurately records the security-related events by using reliable time stamps provided in the TOE operational environment. Therefore, dependency of FAU_GEN.1 is satisfied by OE.Time Stamp security objectives for the operational environment, in place of FPT_STM.1.

[Table 7] Dependencies of Functional Components for the TOE

No.	Functional Components	Dependencies	Ref. No.
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT_STM.1	OE.Time Stamp
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4
6	FAU_SEL.1	FAU_GEN.1, FMT_MTD.1	2, 22
7	FAU_STG.1	FAU_GEN.1	2
8	FAU_STG.3	FAU_STG.1	7
9	FAU_STG.4	FAU_STG.1	7
10	FDP_IFC.2	FDP_IFF.1	11
11	FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	10, 21
12	FIA_AFL.1	FIA_UAU.1	15
13	FIA_ATD.1	-	-
14	FIA_SOS.1	-	-
15	FIA_UAU.1	FIA_UID.1	18
16	FIA_UAU.4	-	-
17	FIA_UAU.7	FIA_UAU.1	15
18	FIA_UID.2	-	-
19	FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	24, 25

20	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1, FMT_SMR.1	10 24, 25
21	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	20, 25
22	FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	24, 25
23	FMT_MTD.2	FMT_MTD.1, FMT_SMR.1	22, 25
24	FMT_SMF.1	-	-
25	FMT_SMR.1	FIA_UID.1	18
26	FPT_TST.1	-	-
27	FTA_SSL.1	FIA_UAU.1	15
28	FTA_SSL.3	-	-

5.4.2 Dependency of Security Assurance Requirements

361 The dependency of each EAL provided in the CC has already been satisfied.

6. PP Application Notes

362 This PP can be utilized as of the following. Product developer or marketer can draw up the Security Target by conforming all contents defined in this protection profile and user can utilize them for selection, operation and management of the product intended for use.

363 This PP 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, developer shall define additional security problems, security objectives and security requirements. If the TOE is implemented by being physically distributed in the network, developer shall define additional security problems, security objectives and security requirements in the Security Target in order to protect data being transferred among each component from external threats.

364 In case where external entities that interact with the TOE (Ex.: DBMS to store audit data, etc.) are included in the ST, the ST author shall ensure that the TOE runs the test on the external entity and takes the actions(in the event of test failure), by adding FPT_TEE.1 (testing of external entities) requirements.

REFERENCES

[1] Common Criteria for Information Technology Security Evaluation (Ministry of Information & Communication Public Notice No. 2005-25).

[2] Common Criteria for Information Technology Security Evaluation, Version 3.1r2, CCMB, 2007. 9.

[3] Common Methodology for Information Technology Security Evaluation, Version 3.1r2, CCMB, 2007. 9.

[4] U.S. Department of Defense Firewall Protection Profile for Basic Robustness Environments Version 0.6a, September 2001

[5] U.S. Department of Defense Application-level Firewall Protection Profile for Medium Robustness Environments Version 1.0, June 28, 2000

[6] U.S. Department of Defense Application-level Firewall Protection Profile for Basic Robustness Environments Version 1.0, June 22, 2000

[7] U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments Version 1.4, May 1, 2000

[8] U.S. Government Application-level Firewall Protection Profile for Low-Risk Robustness Environments Version 1.d, July 20, 1999

[9] U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Robustness Environments Version 1.1, April 1999

[10] Information Assurance Technical Framework Release 3.0, National Security Agency, September 1999

ACRONYMS

CC	Common Criteria
EAL	Evaluation Assurance Level
IT	Information Technology
OSP	Organizational Security Policy
PP	Protection Profile
SFR	Security Functional Requirement
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface