Label_Based
Access Control System
By TSonNet

REDOWL SecuOS V4.0 for MS Windows 2003

Security Target

Version 1.7

May 2007

Trust System On The Net(TSonNet) Co., Ltd
Seoul Branch Office : 12 Floors West Build. IT venture tower, 78 Garak-Dong Songpa-Gu Seoul Republic of Korea
TEL : 02-2142-1380, FAX : 02-2142-1387
DaeJeon Head Office : 5 Floor IT Plex, 59-2 Jang-Dong Yuseong-Gu DaeJeon Republic of Korea
TEL : 042-360-5000, FAX : 042-360-5050
URL : www.tsonnet.co.kr E-mail : tsonnet@tsonnet.co.kr

Version History

Ver. No.	Ver. Date	Description	Revised by
1.0	2006.02.01	First Release	Kim, Eui Tak
1.1	2006.02.21	First Update	Kim, Eui Tak
1.2	2006.03.23	Second Update	Kim, Eui Tak
1.3	2006.03.24	Third Update	Kim, Eui Tak
1.4	2006.12.13	Forth Update	Kim, Eui Tak
1.5	2007.04.05	Fifth Update	Kim, Eui Tak
1.6	2007.05.04	Sixth Update	Kim, Eui Tak
1.7	2007.05.11	Seventh Update	Kim, Eui Tak

Proprietary Notice

Contents

Reference

References

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.3 August 2006

[LACSPP] Label-based Access Control System Protection Profile for Government V1.1

1. Introduction

1.1. Security Target Identification

This section contains the document management and identification of TOE. The developer and the evaluator can identify and verify this document with the follows.

- Evaluation standard : Common Criteria V2.3
- Evaluation level : EAL 3+
- Evaluation Body : Korea Information Security Agency
- PP Claim : Label-based Access Control System Protection Profile for Government V1.1
- TOE : REDOWL SecuOS V4.0 for MS Windows 2003
- Document title : Security Target V1.7
- Document identification : D-ST-1.7
- Document writer : TSonNet Co.Ltd.

1.2. Security Target Overview

The ST is for REDOWL SecuOS V4.0 for MS Windows 2003 that has followed closely the specification contained in LACSPP(Label-based Access Control System Protection Profile for Government V1.1, Republic of Korea). REDOWL SecuOS V4.0 for MS Windows 2003 is OS based secure OS solution, prevents unlawful behaviors and events from attackers and handles them well.

This ST identifies threats, assumptions and organization's security policies in Label-based Access Control System and includes the system's security goals and requirements.

The PP is intended to provide a moderate level of protection. The assurance requirements(EAL3+) and the minimum strength of function were chosen to be consistent with that level of risk.

1.3. CC Conformance Claims

This ST has followed the bellows.

- LACSPP, Label-based Access Control System Protection Profile for Government V1.1

- Common Criteria for Information Technology security system (Ministry of Information Communication Notification No.2005-25) V2.3 Part 2 Conformant

- Common Criteria for Information Technology security system (Ministry of Information Communication Notification No.2005-25) V2.3 Part 3 conformant

  ✓ This ST is the CC Part3' EAL3 assurance requirements conformant and additional assurance requirement-ADV_IMP.2, ADV_LLD.1, ALC_TAT.1, ATE_DPT.2, AVA_VLA.2- for government conformant. Consequently, assurance requirement is following the EAL3+.

This ST has followed the function strength of PP.

1.4. Organization of the Security Target

This document is organized by the follow.

Chapter 1, Introduction – Introduces TOE document identify, overview, PP claims and glossary

Chapter 2, TOE Description – Provides and overview of the TOE security functions and boundary

Chapter 3, TOE Security Environment – Describes the threats, organizational security policies and assumptions that pertain to the TOE

Chapter 4, Security Objectives – Identifies the security objectives that are satisfied by the TOE and the TOE environment

Chapter 5, IT Security Requirements – Presents the security functional and assurance requirements met by the TOE

Chapter 6, TOE Summary Specification – Describes the security functions provided by the TOE to satisfy the security requirements and objectives

Chapter 7, Protection Profile Claims – Presets the rationale concerning compliance of the ST with the LACSPP

Chapter 8, Rationale – Presents the rationale for the security objectives, requirements, and TOE summary specifications as to their consistency, completeness and suitability.

1.5. Glossary

- Mandatory Access Control(MAC)

  A kind of access control as a means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity."

- Object

  An entity within the TSC that contains or receives information and upon which subjects perform operation

- Attack potential

  The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker’s expertise , resources and motivation.

- Strength-of Function(SOF)

  A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its its underlying security mechanisms.

- SOF-basic

  A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

- SOF-medium

  A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing moderate attack potential

- Iteration

  The use of a component more than once with varying operations

- Security Target(ST)

  A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE

- Protection Profile(PP)

An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs

- Security level

  The combination of a hierarchical classification and a set of non-hierarchical categories that represents the sensitivity of information

- Human User

  Any person who interacts with the TOE

- Selection

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

- 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

- Element

  An indivisible security requirement

- External IT Entity

  Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE

- Authentication Data

  Information used to verity the claimed identity of a user

- Discretionary Access Control(Discretionary Access Control)

  A kind of access control as "a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control

- Assets

  Information or resources to be protected by the countermeasures of a TOE

- Refinement

  The addition of details to a component

- Organizational Security Policies

  Security rules, processes, habitual, guidance and etc. by enforcement in an organization

- Dependency

  A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives

- Subject

  An entity within the TSC that causes operations to be performed

- Sensitivity Label

  Security attributes represents a subject or an object

- Augmentation

  The addition of one or more assurance component(s) from Part3 to an EAL or assurance package

- Component

  The smallest selectable set of elements that may be included in a PP, an ST, or a package

- Class

  A grouping of families that share common focus

- Target of Evaluation(TOE)

  An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation

- Evaluation Assurance Level(EAL)

  A package consisting of assurance components form Part 3 that represents a point on the CC predefined assurance scale

- Family

  A grouping of components that share security objectives but may differ in emphasis

- Assignment

  The specification of an identified parameter in a component

- Extension

The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC

- TOE Security Function(TSF)

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

- TOE Security Policy(TSP)

  A set of rules that regulate how assets are managed, protected and distributed within a TOE

- TSF Data

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

- TSF Scope of Control(TSC)

  The interactions that can occur with or within a TOE and are subject to the rules of the TSP

- Multi Level Security(MLS)

  The application of a computer system to process information with different sensitivities (i.e. classified information at different security levels), permit simultaneous access by users with different security clearances and needs-to-know, and prevent users from obtaining access to information for which they lack authorization.

- Bell & Lapadula Model(BLP Model)

  This model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive, e.g. "Top Secret", down to the least sensitive, e.g. "Unclassified" or "Public. The Bell-LaPadula model focuses on data confidentiality and access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity

- Audit Trail

  An audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function. Audit records typically result from activities such as transactions or communications by individual people, systems, accounts or other entities. The Webopedia defines an audit trail as "a record showing who has accessed a computer system and what operations he or she has performed during a given period of time."

2. TOE Description

2.1. TOE Overview

This TOE is a secure OS solution. Without any loss of response time, performance and compatibility, it provides information security at OS platform level which are usually presented by security applications. This TOE is a security product which performs Mandatory Access Control, Multi Level Security by labeling policy, Access Control, audit tracing, detections of hacking and integrated security managements.

2.2. TOE Introduction

This TOE is a secure OS, which was developed by integrating security functions to the existing OS kernel, to protect system from various hacking attacks due to the OS' vulnerabilities. For the efficient usage of this TOE, it is able to install many agent TOE to many systems and manage those agent servers by one integrated (enterprise) server. For more convenient use of TOEs installed in MS Windows 2003 Server system, the security administrator can install GUI (Graphic User Interface) in other MS Windows system to control TOEs on remote access.

TOE security kernel provides following security functions. Firstly, it allows security labels to subjects and objects of the system to prevent violation attempts on the resources. By this labeling, it provides MAC (Mandatory Access Control) and Multi-label based access control functions. Secondly, TOE provides also Discretional Access Control (DAC) which provided by common operating systems. Thirdly, TOE performs firm access-controls by providing access-control lists toward system resources of an organization. This TOE can serve as an integrated server and an agent server as well. So, it is possible to install this TOE to a server to manage from an integrated server, and collect log or valuable data to the integrated server and control them. The integrated server can distribute security policies to connected agent servers, and also can collect main information of agent servers.

This TOE has integrated management function to provide more easy-to-use interface to the security administrators. The integrated management function has all the options used in integrated server system to control the connected servers to it, and shows graphical statistics data collected from the integrated servers.

2.3. TOE Environment and Boundary

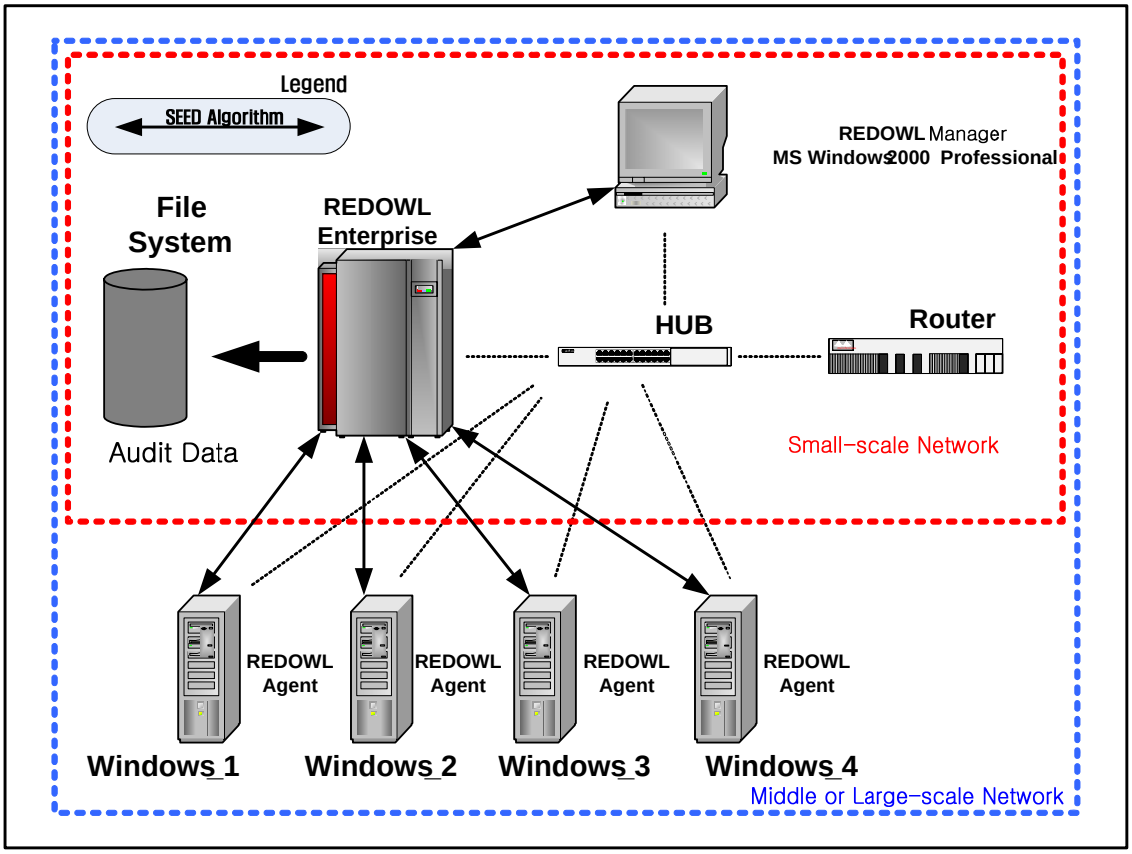
The operational environments of TOE are small sized network systems or medium sized

network systems, and also includes logical and physical limits.

2.3.1 TOE Environment

This TOE can be used two different way when operated. Firstly, it can be installed to only one specific server and operate in case of small network system. And secondly, in case of a large-scale network system which includes many servers, it can be installed to many agent servers, then integrated to a enterprise server and managed through it.

As this TOE comprises both of enterprise and agent functions, there is no agent-alone module. When this TOE is installed to a system, you should select whether this machine must be operated as an enterprise server or an agent server. By setting up a REDOWL manager to the third Windows 2000 Professional system, we can search for audit data collected from enterprise servers or confirm statistics information.



[Figure 2-1] Installation and operational environment of TOE

TOE is divided to REDOWL Enterprise (“Enterprise” in the following) server, REDOWL Agent (“Agent” in the following) server, and REDOWL Manager (“Manager” in the following). Each system needs different systematic environments. Enterprise servers integrate Agent servers and presents console-based user interface. Manager presents Windows-based graphical user interface (GUI) which enables to manage Enterprise servers remotely.

Enterprise servers are running on MS Windows 2003 loadable platforms, and need at least 1Gbytes of RAM and 36Gbytes of hard disk space for the operation. The specific patches of OS kernel does not need to be installed to the system before the installation of secure os.

Agent servers are also running on MS Windows 2003 loadable platforms, and need at least 1Gbytes of RAM and 18Gbytes of hard disk space. The specific patches of OS kernel does not need to be installed to the system before the installation of secure OS.

Manager server is running on MS Windows 2000 Professional loadable platforms, and need at least 256Mbytes of RAM and 10Gbytes of hard disk space. MS patch of Windows should be the one which is SP(Service Pack)4 or released later than SP4.

[Table 2-1] System Installation Environment

Division	REDOWL Enterprise	REDOWL Agent	REDOWL Manager
Operation System	Windows 2003	Windows 2003	MS Windows 2000 Professional(SP4)
CPU	Intel Pentium 4 (More than 1GHz)	Intel Pentium 4 (More than 1GHz)	Intel Pentium 3 (More than 500MHz)
Memory	More than 1Gbyte	More than 1Gbyte	More than 256Mbyte
Hard Disk	More than 36Gbyte	More than 18Gbyte	More than 10Gbyte
NIC	10/100base Ethernet card	10/100base Ethernet card	10/100base Ethernet card

2.3.2 TOE Physical Boundary

TOE is physically divided to Enterprise, Agent and Manager systems. Enterprise and Agent systems are installed to MS Windows 2003 operating systems. When a TOE is installed, we can select whether the TOE will be used as an Enterprise server or an Agent server. After the installation, a TOE will be running as an Enterprise or Agent server. TOE's system requirements are shown in [Figure 2-1]. Followings are hardware devices which could be added to Enterprise or Agent servers systems.

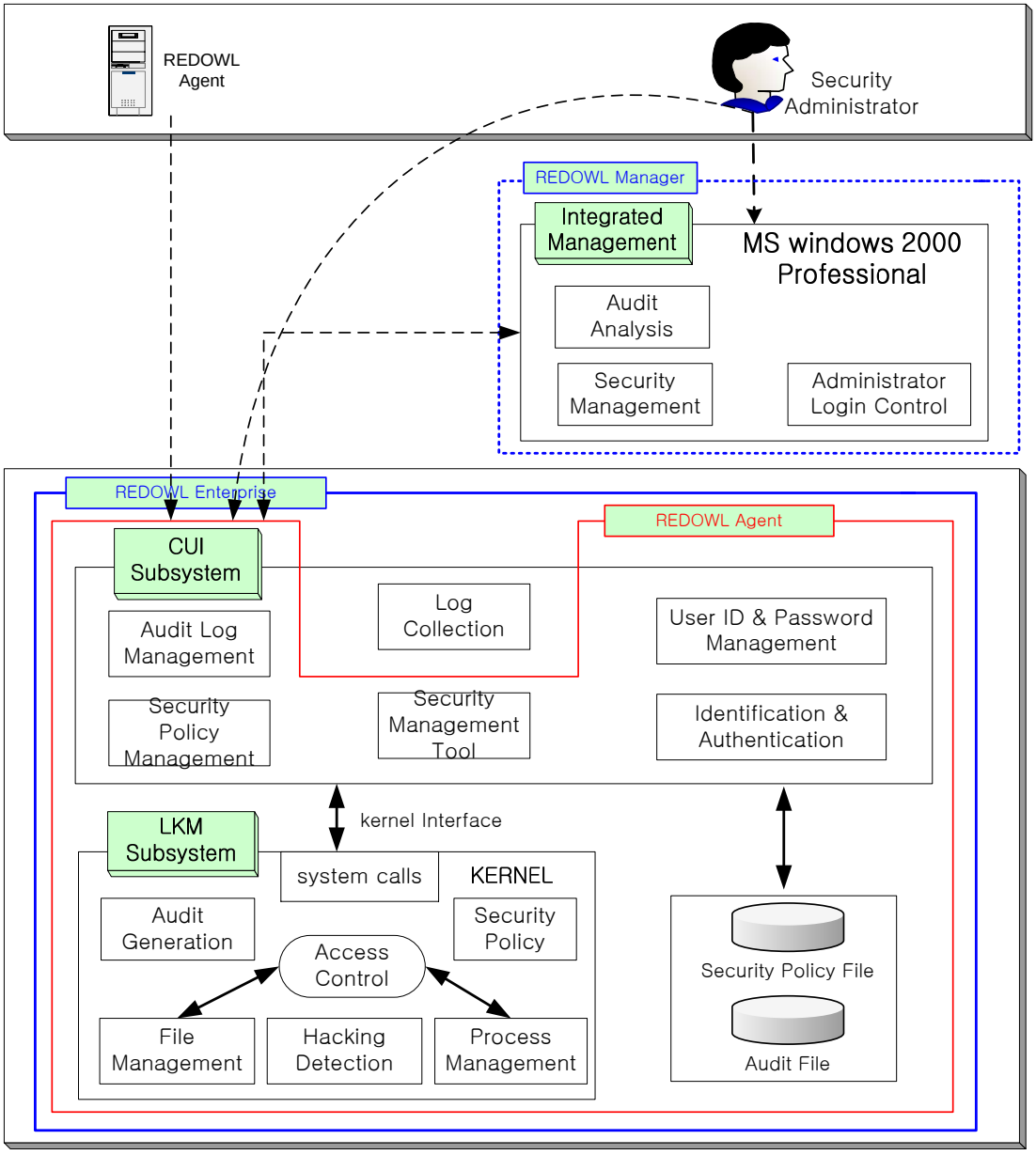
- Monitors : VGA or LCD monitors compatible to IBM PCs
- Hard disk : SCSI hard disks compatible to IBM PC
- SCSI adaptor : SCSI adaptors compatible to IBM PCs
- CD-ROM drive : CD-ROM drives compatible to IBM PCs

2.3.3 TOE Logical Boundary and Functions

The evaluation extent of this TOE limits to 3 main components. The encryption algorithm used between main components is SHA-1, and the security protocol of socket communication between internal and external interface is SEED algorithm. The encryption algorithm and security protocol

used in this TOE is not included for this evaluation. [Figure 2-2] shows the range of TOE.

The main components of TOE include LKM, CUI and GUI. As the core component, LKM performs MAC (Mandatory Access Control), detecting hacking attacks by tracing 'root' privileged daemon processes, prevention mechanism of resource reuse and controls executions of system commands by users or IP addresses by managing extra access control lists. And LKM also collects and generates audit data for every security events.



[Figure 2-2] Scale of TOE

CUI(Character User Interface) is the interface between security administrator, GUI(Graphic User Interface) and LKM. By using CUI, it is able to operate the activation and termination of REDOWL

system, setting up and inquiry of security information or audit data.

GUI(Graphic User Interface) provides graphical interface to REDOWL administrator. GUI performs the same functions as CUI component, and those commands called by GUI are conducted through CUI subsystem. And separately from CUI, GUI presents statistics and analysis for audit data.

For the secure channel, TOE uses SEED algorithm and transforts encryption/decryption key using session key.

TOE classfies logically the 7 security functions , ‘Security Audit, ‘Protection of user data’, ‘Identification and authentication’, ‘Security management’, ‘Protections of TSF’, ‘Separated TOE security functions’ and ‘Offer of secure paths and channels for TOE’. The followings are main security functions of TOE.

A. Security Audit

Successes and failures of security events on TOE are recorded to the strictly separated storing space sequentially with time-stamps on them. Stored audit records are only classified or searched by authorized administrators.

B. Protection of user data

TOE performs strong security policies and confront intrusions by providing multi-label based kernel level access control to the subjects and objects of the system.

C. Identification and authentication

TOE controls connections by identification and authentication algorithm of itself, other than that of OS. Additionally, TOE limits system accessing effectively by regulating accesses to specific IP addresses or ports.

D. Security management

TOE permits only authorized administrators to manage and operate security policies over informational flow. When authorized administrators access to TOE, it forms secure communicative sessions by using OpenSSL. Only authorized administrators can setup and manage or inquire for TOE related data, security attributes and identification or authentication data.

E. Protections of TSF

TOE confirms periodically if its security functions are regularly operated, and if there is an irregular performance, informs the results to authorized administrators. It performs

protections over TOE data and functions through perfection verification test to its principal data or executive files periodically or when it is demanded by authorized administrators. And also, it is possible to set-up, modify, back-up or restore security policies of secure OS.

F. Separated TOE Security Functions

The internal/external user can not access the TOE Security area because of being separated between TOE security function area and ordinary operating system area. The user does not recognize the security area and also can not try to access the security area.

G. Offer of secure paths and channels for TOE

TOE activates its own screen saver when authorized administrators don't perform any function for the set-up time, and the password is needed on resume. By using SEED algorithm, it is possible to control unauthorized users' illegal accesses.

3. TOE Security Environment

Security environment of TOE consists of supposed cases to which describes security of TOE environment, possible threats to TOE resources of environment, and an organization's security policies, such as regulations, procedures, customs or guidelines which TOE should consider for the security reasons.

3.1. Assumptions

Supposed cases are descriptions about the security environment that TOE is implemented or should be implemented in the future. Supposed cases are classified into cases identical to LACSPP and additional cases.

3.1.1 Same assumptions which are identical to LACSPP

Definition	Contents
A. Physical security	TOE is placed in a physically secured environment, and protected from unauthorized physical modification.
A. Trusted administrator	Authorized administrators of TOE are not ill-willed users, and educated with TOE management functions, and perform their duties appropriately according to administrator's guidelines.
A. Hardened OS	By removing OS' services or tools(Telnet, FTP) not need by TOE, it is possible to reinforce vulnerabilities of OS, and reliability / stability of OS is guaranteed.

3.1.2 Additional assumptions

Definitions	Contents
AA. TIME	IT environment provides reliable time-stamps from OS or NTP servers following RFC1305.

3.2. Threats

Threat sources are those IT substances or users, who are trying to access illegally or commit violence to the resources to be protected by TOE. Threat sources toward TOE have low level of professional knowledge, resources and motivations.

3.2.1 Threats to TOE

Definitions	Contents
T. Deficient codes	Threat source can effect TOE's security functions by making use of deficient codes included in development process.
T. Recording failure	Possibility of not being able to record security events due to the vanishment of storage space.
T. Data violation	Threat sources can effect TOE's security functions by violating TOE composition data and trusted data.
T. Authentication attempts by unauthorized	Threat sources can attempt to unauthorized authentications toward TOE.
T. Disguise and bypassing	Threat sources can access to TOE by gaining unauthorized access control of reliable accounts, or bypassing security functions.
T. Rest information	In case of TOE reusing resources, threat sources can access to essential information illegally due to the incomplete removal of object data.

3.2.2 Threats to TOE Environment

Definitions	Contents
TE. Infirmity of management	TOE can be organized, managed and used by authorized administrators in insecure ways.
TE. Distribution/ Installation	TOE's security can be damaged during distributions and installations.

3.3. Security policy of the organization

The regulations, procedures, customs and guidelines, forced by an organization that TOE should fulfill, are distinguished into security policies of an organization, same as LACSPP, and additional organization's security policies.

Definitions	Contents
P. Audit Record	Security events should be recorded and maintained, and recorded data should be investigated for clearing up the responsibilities of security activities.
P. Mandatory Access Control	TOE should have capability of controlling accesses toward objects by the basis of subject's security labeling.
P. Allowance of security labels	TOE should have capability of allowing or canceling of security labels in accordance with the organization's access control policies and procedures.
P. Identification and authentication	Identification and authentication process should be executed before information access is authorized.
P. Secure management	Authorized administrators should manage TOE in secure way.
P. Cryptographic	Encryption algorithm and modules to be used in TOE should be approved by the head of National Intelligence Service.
P. Discretionary Access Control	TOE should have capability of controlling accesses toward information by identities of users or user-belonged groups.

4. Security Objectives

4.1. Security objectives of TOE

Security information of a user is generated, added, modified and removed by security administrator, and security information contains security attributes as follows.

Definitions	Contents
O. Audit Record	TOE should record and maintain security events and provide measures to investigate recorded data for clearing up the responsibilities of security activities.
O. Mandatory Access Control	TOE should have capability of controlling accesses toward objects by the basis of subject's security labeling.
O. Inspection of deficient codes	Investigations on developed codes should be operated to confirm if there is a fault on it. Inspections on deficient codes should be executed to figure out the possibility of influences on TOE's compositions.
O. Management	TOE should present management measures in a secure way for authorized administrators to manage TOE efficiently.
O. Data protection	TOE should protect TSF data or secured data, which is stored in TOE, from unauthorized exposure, modification and removal.
O. Allowance of security labels	TOE should have capability of allowing or canceling of security labels in accordance with the organization's access control policies and procedures.
O. Identification and authentication	Users should be identified only by TOE, and only authenticated users should be able to access to TOE by authentications of user identities.
O. Discretionary Access Control	TOE should have capability of controlling accesses toward resources by identities of users or user-belonged groups.
O. Self protection of functions	When TOE starts, it should protect TOE itself from modification, inactivation and by-passing attempts of security functions.
O. Removal of the rest information	To prevent the reuse of object's resources, TOE should remove information in case of resource reuse.

4.2. Security objectives to TOE environment

System's security administrator should guarantee the efficient usage and management of auditing function. Security purpose for the environment is divided into the security purpose for the identical environment to LACSPP, and security purpose for the additional environment.

4.2.1 Same security objectives to TOE environment with LACSPP

Definitions	Contents
OE. Physical security	TOE should be placed in a physically secured environment which only authorized administrators can access into.
OE. Trusted administrator	Authorized administrators of TOE should not have ill-wills, and have been educated with TOE management functions, and perform their duties appropriately according to administrator's guidelines.
OE. Secure management	TOE should be distributed and installed in secure way, and also organized, managed and used by authorized administrators securely.
OE. Hardened OS	By removing OS' services or tools not needed by TOE, Hardened OS vulnerabilities and reliability / stability OS should be guaranteed.

4.2.2 Security objectives to environment

Definitions	Contents
OEA.TIME	IT environment should provide reliable time-stamps from OS or NTP servers following RFC1305.

5. IT Security Requirements

5.1. TOE Security Function Requirements

This section specifies the security functional requirements(SFRs) for the TOE. This section organizes the SFRs by CC class.

[Table 5-1] Security Function Requirements

Class	Component	
Security Audit	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted 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_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_IFC.1	Subset information flow control
	FDP_IFF.2	Hierarchical security attributes
	FDP_ITC.1	Import of user data without security attributes
	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.7	Protection authentication feedback
	FIA_UID.2	User identification before any action
	FIA_USB.1	User-subject binding
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_REV.1	Revocation
	FMT_SMR.1	Security roles
	FMT_SMF.1	Specification of management functions

Class	Component	
Protection of the TSF	FPT_AMT.1	Abstract machine testing
	FPT_RVM.1	Non-bypassability of the TSP
	FPT_SEP.1	TSF domain separation
	FPT_STM.1	Reliable time stamps
	FPT_TST.1	TSF testing
TOE Access	FTA_SSL.1	TSF-initiated session locking
Trusted Path/Channels	FTP_ITC.1	Inter TSF trusted channel

5.1.1. Security Audit

FAU_ARP.1 Security alarms

Hierarchical to : No other components

FAU_ARP.1.1 The TSF shall take[the list of follows] upon detection of a potential security violation immediately.

a) Generating and writing the events about disruptive actions]

Dependencies : FAU_SAA.1 Potential violation analysis

FAU_GEN.1 Audit data generation

Hierarchical to : No other components

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

a) Start-up and shut-down of the audit functions;

b) All auditable events for the minimum level of audit and;

c) [Auditable events in [Table 5-2], and events bypassing access control policy { events when the security functions detect intrusions, events when the security handles security functions and logs about users commands history}]

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [referring [Table 5-2] Auditable events, relevant information on { events when the security functions detect intrusions, events when the security handles security functions and logs about users commands history}]

Dependencies : FPT_STM.1 Reliable time stamps

[Table 5-2] Auditable events

Component	Auditable Events	Additional Audit Contents
FAU_ARP.1	Reactions to emergency disruptive actions	-
FAU_SAA.1	Start-up and shout-down analysis audit functions, and reactions automatically	-
FAU_SEL.1	Audit environment configurations changed during activating audit collection functions	-
FDP_ACF.1	Successful requirements of operations About objects controlled by SFP	Object identification information
FDP_IFF.2	Decisions about permitting information flow	Subjects labels, Objects names and labels
FDP_ITC.1	Successful inputs to user' data Including security attributes	-
FIA_AFL.1	TSF detects when meets maximum unsuccessful authentication attempts number and recovers normal state	-
FIA_SOS.1	Denial secrets information testing by TSF	-
FIA_UAU.1	The failure of authentication mechanism	-
FIA_UAU.4	Attempts reusing authentication data	-
FIA_UID.2	The failure of user identification mechanism including user identity	Users identifications provided to TOE
FIA_USB.1	Linking between user security attributes and subject	-
FMT_MOF.1	All changes for TSF function	-
FMT_MSA.1	All changes for security attributes	Changed Security attributed
FMT_MTD.1	All changes for TSF data values	Changed TSF data value
FMT_REV.1	Revocation attempts about security attributes	-
FMT_SMF.1	Using management function	-
FPT_STM.1	Change for time	-
FPT_TST.1	Execution of TSF self test and test results	TSF data or execution code changed during infracting integrity
FTA_SSL.1	Locks session by session locking mechanism, and releases the lock	-
FTP_ITC.1	The troubles of secure channel, and the identification of subject or user to the secure channel	-

FAU_GEN.2 User identity association

Hierarchical to : No other components

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identify of the user that caused the event.

Dependencies : FAU_GEN.1 Audit data generation

FAU_SAA.1 Potential violation analysis

Hierarchical to : No other components

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.

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

a) the accumulations or combinations [events for the failure of authentication in the auditable events of FIA_UAU.1, events for access control violations in the auditable events of FDP_ACF.1 and FDP_IEF, events for integrity violations in the auditable events of FPT_TST.1] known by potential violation

b) [the violations of identification and authentication security rules, the accumulation or combination for the violations of access control rules]

Dependencies : FAU_GEN.1 Audit data generation

FAU_SAR.1 Audit review

Hierarchical to : No other components

FAU_SAR.1.1 The TSF shall provide [security administrator] with the capability to read [all of audit information] from the audit records.

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

Dependencies : FAU_GEN.1 Audit data generation

FAU_SAR.2 Restricted audit review

Hierarchical to : No other components

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except security administrator that have been granted explicit read-access.

Dependencies : FAU_SAR.1 Audit review

FAU_SAR.3 Selectable audit review

Hierarchical to : No other components

FAU_SAR.3.1 The TSF shall provide the ability to perform *searches, sorting* of audit data based on [the followings].

a) user identification

b) object identification

c) subject's label

d) Object's label

Dependencies : FAU_SAR.1 Audit review

FAU_SEL.1 Selective audit

Hierarchical to : No other components

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the followings attributes ;

a) user identification

b) object identification

c) subject's label

d) Object's label

Dependencies : FAU_GEN.1 Audit data generation

FMT_MTD.1 Management of TSF data

FAU_STG.1 Protected audit trail storage

Hierarchical to : No other components

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

FAU_STG.1.2 The TSF shall be able to *prevent* modifications to the audit records.

Dependencies : FAU_GEN.1 Audit data generation

FAU_STG.3 Action in Case of Possible audit data loss

Hierarchical to : No other components

FAU_STG.3.1 The TSF shall take [writing the information as records, stopping whole of TOE functions] if audit trail exceeds [the limitation of storage(the storate of server installed TOE))].

Dependencies : FAU_STG.1 Protected audit trail storage

FAU_STG.4 Prevention of audit data loss

Hierarchical to : FAU_STG.3

FAU_STG.4.1 The TSF shall ignore auditable events except those taken by the authorized user with special rights and [secure space and backup auditable events by hands] if audit trail is full.

Dependencies : FAU_STG.1 Protected audit trail storage

5.1.2. User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to : No other components

FDP_ACC.1.1 The TSF shall enforce the [Discretionary Access Control] on [all subjects], [*subjects and objects's operation list(read, write, execute, create, delete, rename) handling by* ***Discretionary Access Control polic***].

Dependencies : FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to : No other components

FDP_ACF.1.1 The TSF shall enforce [Discretionary Access Control policy] to objects based on [the followings].

a) [the user's identification of subject]

b) [the user group's identification of subject]

b) [*the list of Discretionary Access Control security attributes connected with the followings,*

i) *if the user's identification is higher than or same the object's security level, the operation is permitted*

ii) *if the user group's identification is higher than or same the object's level, the operation is permitted*

iii) *the operation permit value is decided by the subject' identification*]

FDP_ACF.1.2 The TSF shall enforce the followings rules to determine if an operation among controlled subjects and controlled objects is allowed :

[*the list of Discretionary Access Control security attributes connected with the followings,*

i) *the operation is permitted if the user's identification of subject is same with the user's identification of object access control attributes to each operation.*

ii) *the operation is permitted if the user group's identification of subject is same with the user group's identification of object access control attributes to each operation.*

iii) *if the user's identification of subject is not same with the user's identification of object access control attributes to each operation and if the subject identification is higher than or same, the operation is permitted but if lower than, the operation is not permitted.*

iv) *if the user group's identification of subject is not same with the user group's identification of object access control attributes to each operation and if the user group's identification of subject is higher than or same, the operation is permitted but if lower than, the operation is not permitted.*]

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules : [if subject is a security administrator, TSF explicitly authorizes access of subjects to objects]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [rules being supported by DAC].

Dependencies : FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_IFC.1 Subset information flow control

Hierarchical to : No other components

FDP_IFC.1.1 The TSF shall enforce the [Mandatory Access Control] on [subjects], [the operation list of object(processes, files, directories) and the operation list of subjects to subjects, the operation list of subjects to objects(read, write, execute, delete, create) handling by MAC].

Dependencies : FDP_IFF.1 Simple security attributes

FDP_IFF.2 Hierarchical security attributes

Hierarchical to : FDP_IFF.1

FDP_IFF.2.1 The TSF shall enforce [Mandatory Access Control policy] based on the types of subjects security attributes and objects security attributes like [the followings].

[a) subject's security label

b) object's security label

c) the coverage of clearance and category label mixed { the clearance is consisted from 0 to 15, the category is consisted of the 6 of numeric(from 1 to 9) and English alphabet(from A to F) }]

FDP_IFF.2.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules, based on the ordering relationships between security attributes hold :

[a) if the subject's label is higher than or same the object's, the subject can read the object.

b) if the object's label is *same with the subject's label*, the subject can get written permission to the object.

c) if the label of a subject A is higher than or same with the label of subject B, information can flow from subject A to subject B.]

FDP_IFF.2.3 The TSF shall enforce [the following list of additional information flow control :

a) If directories or files,

- P privilege : represents the status of an execute file(the clearance is '0') authorized by security administrator
- Y privilege : represents that the read permission of the present file is granted

b) If processes

- P privilege : the super privilege of TOE. If an user get the privilege, he can do everything in the system and the privilege can be inherited to subjects
- I privilege : the install privilege of TOE. It can not apply security policy that security administrator makes. The privilege is for 'package install', 'authorized execute file generation' and 'kill' process privilege.

- A privilege : the authorized privilege of TOE. The process inherited A privilege can make execute files and execute them without the security administrator authorization.]

FDP_IFF.2.4 The TSF shall provide the following [P privilege, Y privilege for 'files information flow control', P privilege, I privilege, and A privilege for 'processes information flow control'].

FDP_IFF.2.5 The TSF shall explicitly authorize an information flow based on [the following rules] permitted explicitly an information flow based on security attributes .

[a) All subject and object has rules permitted information flow according to security attributes.

b) The security administrator permits explicitly information flow to all subject and object.

c) The ordinary subject allows explicitly information flow by permitting operation to same object with each security attributes.

d) When the subject creates the object, the security attributes of object is inherited from the security attributes of subject. So, TOE allows explicitly information flow between subject and object.

e) When the subject with security attributes accesses the object without security attributes, TOE allows explicitly access.

FDP_IFF.2.6 the TSF shall explicitly deny an information flow based on [the following rules] denied explicitly an information flow based on security attributes.

[a) All subject and object has rules denied information flow according to security attributes.

b) The ordinary subject denies explicitly information flow to the subject or object with security administrator security attributes.

c) The ordinary subject denies explicitly using security administrator's operation.

FDP_IFF.2.7 The TSF shall enforce the following relationships for any two valid security labels.

a) There exists an ordering function that, given two valid security labels, determines the following ;

- security labels are equal
- one security label is greater than the other
- security labels are incomparable ; and

b) There exists a "LUB(least upper bound)" in the set of security label, such that, given any two valid security labels, there is a valid security label that is greater than or equal to the two valid security labels ; and

c) There exists a "GLB(greatest upper bound)" in the set of security labels, such that, given any two valid security labels, there is a valid security label that is not greater than the two valid security labels.

Dependencies : FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_ITC.1 Import of user data without security attributes

Hierarchical to : No other components

FDP_ITC.1.1 The TSF shall enforce [Mandatory Access Control policy] when importing user data, controlled under Mandatory Access Control policy, from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the **Mandatory Access Control policy** from outside the TSC.

[a) when an authorized user imports an user data from outside the TSC, he must give the security label to the data.

b) control by Mandatory Access Control policy]

Dependencies : [FDP_ACC.1 Subset access control,
FDP_IFC.1 Subset information flow control],
FMT_MSA.3 Static attribute initialization

FDP_RIP.1 Subset residual information protection

Hierarchical to : No other components

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon de-allocation of the resource from the following objects [files labeled].

Dependencies : No dependencies

5.1.3. Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to : No other components

FIA_AFL.1.1 The TSF shall detect when [3] unsuccessful authentication attempts occur related to [every authentication].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [display warning message, stop the function of user authentication for 3minutes, and generate audit data to the event].

Dependencies : FIA_UAU.1 Timing of authentication

FIA_ATD.1 User attribute definition

Hierarchical to : No other components

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

[a) user identification

b) group identification belonging the user

c) security label

d) authentication data]

Dependencies : No dependencies

FIA_SOS.1 Verification of secrets

Hierarchical to : No other components

FIA_SOS.1.1 The TSF shall provide mechanism to verify that secret meet [the 6 ~ 8 of combined numeric, English alphabet, and wild key(such as, '!','@','#','$'), and the changing secrets by period].

Dependencies : No dependencies

Attention when apply : The minimum password length, the rule of combining, and the changing period can be changed in password authentication mechanism.

FIA_UAU.1 Timing of authentication

Hierarchical to : No other components

FIA_UAU.1.1 The TSF shall allow [asking to the process of authentication, all actions permitted by os exeption with the action denied by the additional MAC from TSF]on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user doing actions Except explicit actions in FIA_UAU.1.1.

Dependencies : FIA_UID.1 Identification

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to : No other components

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [authentication mechanism by providing SEED alghorithm].

Dependencies : No dependencies

FIA_UAU.7 Protection authentication feedback

Hierarchical to : No other components

FIA_UAU.7.1 The TSF shall provide only [password input screen represented with '*' key] to the user while the authentication is in progress.

Dependencies : FIA_UAU.1 Timing of authentication

FIA_UID.2 User identification before any action

Hierarchical to : FIA_UID.1 Identification

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing **any other TSF-mediated actions** on behalf of that user.

Dependencies : No dependencies

FIA_USB.1 User-subject binding

Hierarchical to : No other components

FIA_USB.1.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user : [the user identification, the group identification belonging user, security label]

Dependencies : FIA_ATD.1 User attribute definition

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users : [the user identification, the group identification belonging user, security label, access coverage limited as user's security label]

Dependencies : FIA_ATD.1 User attribute definition

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users : [changing order by the user identification, the group identification belonging user, user's security label]

Dependencies : FIA_ATD.1 User attribute definition

5.1.4. Security Management

FMT_MOF.1 Management of security functions behavior

Hierarchical to : No other components

FMT_MOF.1.1 The TSF shall restrict the ability to *determine the behavior of, disable, enable, enable, modify the behavior of* [all security function] to [the security administrator].

Dependencies : FMT_SMR.1 Security roles,

FMT_SMF.1 Specification of management functions

FMT_MSA.1(1) Management of security attributes (DAC : Discretionary Access Control)

Hierarchical to : No other components

FMT_MSA.1.1 The TSF shall enforce the [DAC Policy] to restrict the ability to c*hange_default , query, modify* the security attributes of [DAC associated with objects] to [the security administrator, the owner of object].

Dependencies : [FDP_ACC.1 Subset access control,
FDP_IFC.1 Subset information flow control],
FMT_SMF.1 Specification of management functions,
FMT_SMR.1 Security roles

FMT_MSA.1(2) Management of security attributes (MAC : Mandatory Access Control)

Hierarchical to : No other components

FMT_MSA.1.1 The TSF shall enforce the [MAC Policy] to restrict the ability to *change* **the security label** of [MAC associated with objects or subjects] to [the security administrator].

Dependencies : [FDP_ACC.1 Subset access control,
FDP_IFC.1 Subset information flow control],
FMT_SMF.1 Specification of management functions,
FMT_SMR.1 Security roles

FMT_MSA.3(1) Static attribute initialization (DAC : Discretionary Access Control)

Hierarchical to : No other components

FMT_MSA.3.1 The TSF shall enforce the [DAC Policy] to provide *restrictive* default value for security attributes that are used to enforce **DAC Policy**.

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

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

FMT_MSA.3(2) Static attribute initialization (MAC : Mandatory Access Control)

Hierarchical to : No other components

FMT_MSA.3.1 The TSF shall enforce the [MAC Policy] to provide *restrictive* default value for security attributes that are used to enforce **MAC Policy**.

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

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

FMT_MTD.1(1) Management of TSF data

Hierarchical to : No other components

FMT_MTD.1.1 The TSF shall restrict the ability to *change defualt, query, delete, clear* the [audit data] to [the security administrator].

Dependencies : FMT_SMR.1 Security roles,
FMT_SMF.1 Specification of management functions

FMT_MTD.1(2) Management of TSF data

Hierarchical to : No other components

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

Dependencies : FMT_SMR.1 Security roles,
FMT_SMF.1 Specification of management functions

FMT_MTD.1(3) Management of TSF data

Hierarchical to : No other components

FMT_MTD.1.1 The TSF shall restrict the ability to *change* [authentication data] to [the security administrator].

Dependencies : FMT_SMR.1 Security roles,
FMT_SMF.1 Specification of management functions

FMT_MTD.1(4) Management of TSF data

Hierarchical to : No other components

FMT_MTD.1.1 The TSF shall restrict the ability to *change_defualt, query, modify, delete, clear, [create]* [TSF data associated with security, except the TSF data mentioned above] to [the security administrator].

Dependencies : FMT_SMR.1 Security roles,
FMT_SMF.1 Specification of management functions

FMT_REV.1(1) Revocation (User)

Hierarchical to : No other components

FMT_REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the *subjects* within the TSC to [the security administrator].

FMT_REV.1.2 The TSF shall enforce [the following] rules.

[a) The TSF shall revoke immediately the authentication associated with security .

b) The security administrator can revoke the processes created by subjects.]

Dependencies : FMT_SMR.1 Security roles

FMT_REV.1(2) Revocation (Object)

Hierarchical to : No other components

FMT_REV.1.1 The TSF shall restrict the ability to revoke the security attributes associated with the *objects* within the TSC to [the security administrator].

FMT_REV.1.2 The TSF shall enforce [the following] rules.

[a) To revoke access control associated with objects, the TSF shall do when checks the access permission of objects.

b) The security administrator can revoke by force of the files created by subjects]

Dependencies : FMT_SMR.1 Security roles

FMT_SMR.1 Security roles

Hierarchical to : No other components

FMT_SMR.1.1 The TSF shall maintain [the following] roles.

[a) the security administrator]

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

Dependencies : FIA_UID.1 Identification

FMT_SMF.1 Specification of management functions

Hierarchical to : No other components

FMT_SMF.1.1 The TSF shall be capable of performing the following security management function : [security policy configuration and broadcasting, integrity inspection, user management, backup & recovery]

Dependencies : No dependencies

5.1.5. Protection of the TSF

FPT_AMT.1 Abstract machine testing

Hierarchical to : No other components

FPT_AMT.1.1 The TSF shall run a suite of tests *during initial start-up, during normal operation by period, at the request of a security administrator* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Dependencies : No dependencies

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to : No other components

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies : No dependencies

FPT_SEP.1 TSF domain separation

Hierarchical to : No other components

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

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

Dependencies : No dependencies

FPT_STM.1 Reliable time stamps

Hierarchical to : No other components

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

Dependencies : No dependencies

Attention to apply : The TOE can maintain the reliable time stamps by 2 methods. The firstly, it can use the NTP server, and the secondly, it can use the Operating System installed the TOE. Now, the TOE gets the reliable time from the Operating System. The administrator can decide which one selects.

FPT_TST.1 TSF testing

Hierarchical to : No other components

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up, during normal operation by period, at the request of a security administrator* to demonstrate the correct operation of the TSF.

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

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

Dependencies : FPT_AMT.1 Abstract machine testing

5.1.6. TOE Access

FTA_SSL.1 TSF-initiated session locking

Hierarchical to : No other components

FTA_SSL.1.1 The TSF shall lock an interactive session after [time interval of **authorized users** inactivity-minimum 30 seconds, maximum 3,600 seconds] by ;

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

b) disabling any activity of the user' data access/display devices other than unlocking the session

c) if the time interval of authorized users is occurred,

- locking display devices for GUI

FTA_SSL.1.2 The TSF shall require [the authentication of the security administrator for GUI, re-login for CUI] to occur prior to unlocking the session.

Dependencies : FIA_UAU.1 Timing of authentication

5.1.7. Trusted Path/Channels

FTP_ITC.1 Inter TSF trusted channel

Hierarchical to : No other components

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit *TSF* to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [the remote management function].

Dependencies : No dependencies

Attention when apply : The TOE provides a trusted channel using SEED algorithm provided by the IT environment .

5.2. TOE Assurance Requirements

This section is consisted of the security assurance requirements of CC Part3, the assurance level is EAL3+. [Table 5-3] shows the assurance components to the security assurance requirements.

The additional assurance components in the Security Target are the following.

- ADV_IMP.2 Implementation of the TSF
- ADV_LLD.1 Descriptive low-level design
- ALC_TAT.1 Well-defined development tools
- ATE_DPT.2 Testing : low-level design
- AVA_VLA.2 Independent vulnerability analysis

[Table 5-3] TOE assurance requirements

Assurance Class	Assurance Component	
Configuration Management	ACM_CAP.3	Authorization controls
	ACM_SCP.1	TOE CM coverage
Delivery and Operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.2	Implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support	ALC_DVS.1	Identification of security measures
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing : low-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Dependent testing – sample
Vulnerability Assessment	AVA_MSU.1	Examination of guidance
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent vulnerability analysis

5.2.1. Configuration management

ACM_CAP.3 Authorization controls

Dependencies

ALC_DVS.1 Identification of security measures

Developer action elements

ACM_CAP.3.1D The developer shall provide a reference for the TOE.

ACM_CAP.3.2D The developer shall use a CM system.

ACM_CAP.3.3D The developer shall provide CM documentation.

Evidence elements

ACM_CAP.3.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.3.2C The TOE shall be labeled with its reference.

ACM_CAP.3.3C The CM documentation shall include a configuration list and a CM plan.

ACM_CAP.3.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.3.5C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.3.6C The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.

ACM_CAP.3.7C The CM system shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.3.8C The CM plan shall describe how the CM system is used.

ACM_CAP.3.9C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.3.10C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.3.11C The CM system shall provide measures such that only authorized changes are made to the configuration items..

ACM_SCP.1 TOE CM coverage

Dependencies

ACM_CAP.3 Authorization controls

Developer action elements

ACM_SCP.1.1D The developer shall provide a list of configuration items for the TOE.

Evidence elements

ACM_SCP.1.1C The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.

5.2.2. Delivery and operation

ADO_DEL.1 Delivery procedures

Dependencies

No dependencies

Developer action elements

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Evidence elements

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

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

Dependencies

AGD_ADM.1 Administrator guidance

Developer action elements

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Evidence elements

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

5.2.3. Development

ADV_FSP.1 Informal functional specification

Dependencies

ADV_RCR.1 Informal correspondence demonstration

Developer action elements

ADV_FSP.1.1D The developer shall provide a functional specification.

Evidence elements

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

ADV_HLD.2 Security enforcing high-level design

Dependencies

ADV_FSP.1 Informal functional specification

ADV_RCR.1 Informal correspondence demonstration

Developer action elements

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

Evidence elements

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

ADV_IMP.2 Implementation of the TSF

Dependencies

ADV_LLD.1 Descriptive low-level design

ADV_RCR.1 Informal correspondence demonstration

ALC_TAT.1 Well-defined development tools

Developer action elements

ADV_IMP.2.1D The developer shall provide the implementation representation for the entire TSF.

Evidence elements

ADV_IMP.2.1C The implementation representation shall unambiguously define the TSF to a level

of detail such that the TSF can be generated without further design decisions.

ADV_IMP.2.2C The implementation representation shall be internally consistent.

ADV_IMP.2.3C The implementation representation shall describe the relationships between all portions of the implementation

ADV_LLD.1 Descriptive low-level design

Dependencies

ADV_LLD.1 Descriptive low-level design

ADV_RCR.1 Informal correspondence demonstration

Developer action elements

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

Evidence elements

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.2C The low-level design shall be internally consistent.

ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

ADV_RCR.1 Informal correspondence demonstration

Dependencies

No dependencies

Developer action elements

ADV_RCR1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Evidence elements

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

5.2.4. Guidance documents

AGD_ADM.1 Administrator guidance

Dependencies

ADV_FSP.1 Informal functional specification

Developer action elements

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Evidence elements

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_USR.1 User guidance

Dependencies

ADV_FSP.1 Informal functional specification

Developer action elements

AGD_USR.1.1D The developer shall provide user guidance.

Evidence elements

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

5.2.5. Life cycle support

ALC_DVS.1 Identification of security measures

Dependencies

No dependencies

Developer action elements

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

Evidence elements

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.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

ALC_TAT.1 Well-defined development tools

Dependencies

ADV_IMP.1 Subset of the implementation of the TSF

Developer action elements

ALC_TAT.1.1D The developer shall identify the development tools being used for the TOE.

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

Evidence elements

ALC_TAT.1.1C All development tools used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

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

5.2.6. Tests

ATE_COV.2 Analysis of coverage

Dependencies

ADV_FSP.1 Informal functional specification

ATE_FUN.1 Functional testing

Developer action elements

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

Evidence elements

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

ATE_DPT.2 Testing : low-level design

Dependencies

ADV_HLD.2 Security enforcing high-level design

ADV_LLD.1 Descriptive low-level design

ATE_FUN.1 Functional testing

Developer action elements

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

Evidence elements

ATE_DPT.2.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design and low-level design.

ATE_FUN.1 Functional testing

Dependencies

No dependencies

Developer action elements

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

ATE_FUN.1.2D The developer shall provide test documentation.

Evidence elements

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

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified

ATE_IND.2 Dependent testing - sample

Dependencies

ADV_FSP.1 Informal functional specification

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

ATE_FUN.1 Functional testing

Developer action elements

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

Evidence elements

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

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.

5.2.7. Vulnerability assessment

AVA_MSU.1 Examination of guidance

Dependencies

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

ADV_FSP.1 Informal functional specification

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

Developer action elements

AVA_MSU.1.1D The developer shall provide guidance documentation..

Evidence elements

AVA_MSU.1.1C The guidance documentation 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.

AVA_MSU.1.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.1.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.1.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_SOF.1 Strength of TOE security function evaluation

Dependencies

ADV_FSP.1 Informal functional specification

ADV_HLD.1 Descriptive high-level design

Developer action elements

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Evidence elements

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST

AVA_VLA.2 Independent vulnerability analysis

Dependencies

ADV_FSP.1 Informal functional specification

ADV_HLD.2 Security enforcing high-level design

ADV_IMP.1 Subset of the implementation of the TSF

ADV_LLD.1 Descriptive low-level design

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

Developer action elements

AVA_VLA.2.1D The developer shall perform a vulnerability analysis.

AVA_VLA.2.2D The developer shall provide vulnerability analysis documentation.

Evidence elements

AVA_VLA.2.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.

AVA_VLA.2.2C The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.

AVA_VLA.2.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.2.4C The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

5.3. Security requirements to IT environment

The IT security requirements to environment in the TOE is the following.

FPT_STM.1 Reliable time stamp

Hierarchical to : No other components

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

Dependencies : No dependencies

6. TOE Summary Specification

6.1. IT Security Functions

TOE's security functions are consisted of 23 functions. [Table 6-1] shows requirements of security functions.

[Table 6-1] TOE security functions and requirements for security functions

Class of security function	Security functions	Requirements for security functions
Security Audit	AU_1(Audit record generating)	FAU_GEN.1,FAU_GEN.2
	AU_2(Audit record inquiry)	FAU_SAA.1,FAU_SAR.1,FAU_SAR.2 FAU_SAR.3,FAU_SEL.1
	AU_3(Audit record protection)	FAU_ARP.1,FAU_STG.1,FAU_STG.3 FAU_STG.4
	AU_4(Limitation of audit investigation privilege)	FAU_SAR.2
	AU-5(Analysis of potential violations)	FAU_ARP.1, FAU_SAA.1
Protection of user data	MAC(Mandatory Access Control)	FAU_SAR.2,FAU_STG.1,FDP_IFC.1 FDP_IFF.2,FDP_ITC.1,FIA_USB.1, FMT_MSA.1(2),FMT_MSA.3(2), FMT_REV.1(1), FMT_REV.1(2)
	DAC(Discretionary Access Control)	FAU_SAR.2,FAU_STG.1,FDP_ACC.1 FDP_ACF.1,FIA_USB.1,FMT_MSA.1(1),FMT_MSA.3(1),FMT_REV.1(1), FMT_REV.1(2)
	ACL(Access Control List)	FAU_SAR.2,FAU_STG.1,FDP_ACC.1 FDP_ACF.1,FIA_USB.1,FMT_MSA.1(1),FMT_MSA.3(1),FMT_REV.1(1), FMT_REV.1(2)
	RDP(Residual Data Protection)	FDP_RIP.1
Identification and authentication	IA_1(Authentication failure disposal)	FIA_AFL.1
	IA_2(Definition of user identity)	FIA_ATD.1, FIA_USB.1
	IA_3(Verification of confidential information)	FIA_SOS.1
	IA_4(Identification and authentication)	FIA_UAU.1, FIA_UID.2, FMT_SMR.1, FIA_UAU.4
	IA_5(Authentication feedback protection)	FIA_UAU.7

Class of security function	Security functions	Requirements for security functions
Security management	SM_1(Security function management)	FMT_MOF.1, MFT_SMR.1, FMT_SMF.1
	SM_2(Security attributes management)	FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.3(1), FMT_MSA.3(2), FMT_REV.1(1), FMT_REV.1(2), FMT_SMF.1
	SM_3(TSF data management)	FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FPT_STM.1, FMT_SMF.1
TSF protection	PT_1(Abstract machine testing)	FPT_AMT.1
	PT_2(Impossibility of TSP bypassing)	FPT_RVM.1
	PT_3(TSF testing)	FPT_TST.1
	PT_4(TSF protection)	FPT_SEP.1
TOE access	AT(Session lock by TSF)	FTA_SSL.1
Trusted paths / channels	TR(Trusted channels between TSFs)	FTP_ITC.1

6.1.1. Security Adudit

Security Audit is classified into 5 security functions. 5 security functions are AU_1(Audit record generating), AU_2(Audit record inquiry), AU_3(Audit record protection), AU_4(Limitation of audit investigation privilege) and AU_5(Analysis of potential violations).

■ AU_1(Audit record generating)

Various security events occurring in security module are recorded to audit data. Audit information related to security policy violating events, such as calling out of security system-calls, Mandatory Access Control and Discretionary Access Control, are generated and collected. To generate and manage security kernel originated audit date, TOE operates as follows:

- Each module of security kernel requests audit data collecting module for the generation of audit data
- Audit data generating module stores audit data requested by each module after filtering phase
- Audit data is copied to audit data structure after filtering phase, and examination of comparison is operated to find identical data from the prior audit record
- If there is identical data in it, TOE counts the number of identical data in audit data

structure and terminates the process.

- If there is no identical data in it, TOE inspects if the number of data is more than 1024 stored in a linked list.
- If the number of data is more than 1024, TOE allocates a new kernel memory and store audit data.
- If the memory allocation is denied, TOE terminates the process without storing audit data.
- If the number of data is less than 1024, TOE stores audit data in a linked list.

Audit data stored in a linked list is copied to user memory area in periodical calling order of console management, and delivered to console management. In console management, periodically collected audit data are stored to files.

■ AU_2(Audit record inquiry)

Security audit data management function is to inquiry each Agent server's security audit data, existing as ASCII text file format, through integrated management GUI interface. It presents the function of observing security audit data, generated on multiple Agent servers, in real time.

The inquiry function of each Agent server operates as follows:

- Security administrator performs the inquiry function using the integrated management.
- The integrated management delivers commands to the console management to inquire contents of security audit log, then read in ASCII text files of security audit data from the console management, then transmits them to the integrated management.

It can trail real time audit log data from every Agent servers, which are registered to the integrated management server, and operates as follows:

- Security administrator can trail real time security audit by executing real time tracing function of the integrated management.
- It can performs real time auditing on a single Agent server of a number of servers using security management.

Audit data analysis function is to investigate the existence of hacking attacks, internally or externally, by process, by user, and conditional search is also practicable. Security administrator can modify the field information of audit data to print out.

Statistics of audit data function is to print out statistics data of audit records collected from the whole Agent server, by server, by process, by user or by message.

■ AU_3(Audit record protection)

TSF generates the audit data and stores it when the storage scale of audit data exceeds the limit. Atter TOE system halding, the security administrator logins the server and backups the audit data than recovers the server.

■ AU_4(Limitation of audit investigation privilege)

TSF should protect audit data from modifications and removals by unauthorized users. TOE doesn't allow any user to access audit data except authorized users by setting up access privileges or security labels on audit data. The privilege of audit investigation is limited to security administrator when audit log analysis and audit log statistics functions are operated.

Audit log analysis can only be performed by security administrator. This function is to investigate the existence of hacking attacks, internally or externally, by process, by user, and conditional search is also practicable. Security administrator can modify the field information of audit data to print out.

Statistics of audit data function can be only operated by security administrator. Statistics of audit data function is to print out statistics data of audit records, collected from the whole Agent server, by server, by process, by user or by message. Security administrator can choose the output cycle of statistics data from once a day, a week or a month. Statistics output graph is can be stored as a figurative file.

■ AU_5(Analysis of potential violations)

Analysis of potential violations is related to analysis of audit log, audit log statistics and intrusion alarm function. Audit data analysis function is to investigate the existence of hacking attacks, internally or externally, by process, by user, and conditional search is also practicable. Security administrator can modify the field information of audit data to print out.

Statistics of audit data function is to print out statistics data of audit records collected from the whole Agent server, by server, by process, by user or by message. Security administrator can choose the output cycle of statistics data from once a day, a week or a month. Statistics output graph is can be stored as a figurative file.

Intrusion alarm function is to alert when audit data related to an intrusion generates. Security administrator can enable or disable the alarm function using integrated management.

6.1.2. User Data Protection

There are 3 security functions for user data protection. 3 of them are MAC(Mandatory Access Control), DAC(Discretionary Access Control) and RDP(Residual Data Protection).

■ MAC(Mandatory Access Control)

Mandatory Access Control provides mandatory controls over accesses in accordance with security labels configured to subjects and objects. Mandatory access control provides a multi level access control using mathematically verified BLP model.

It operates as follows to perform Mandatory Access Control functions:

- When the security administrator accesses to the system from local console or remote hosts, he/she is authorized by his/her ID & Password and security password.
- The security kernel hooks every system calls, if a process accesses a file, the security kernel checks the policy of DAC at first.
- For checking Discretionary Access Controls, identities of subjects and objects are investigated, and access-denied in case of no access privilege.
- When an access permitted through DAC, investigate if the process has a privilege. In case of a privilege assigned by security administrator, the access to file is approved.
- If not a privileged process, investigate if the files security clearance is “0”..
- If clearance is “0”, permits the access to the file.
- If clearance is not “0”, compares the category of file with the subject.
- To compare the security level of process with file, compare the security level(clearance, category) information set in information table of user process with the security level(clearance, category) information set in file.
  - If the security levels of both subject and object are equal, the subject can read/write to the object.
  - If the security level of subject is higher than the object’s, the object can read the object.
  - If the security level of subject is lower than the object’s, the access of subject to the

object is denied.

- All security events related to the operations of Mandatory Access Control are recorded to audit data and stored as a file at REDOWL Enterprise.

Security administrator can assign a clearance from 1 to 15. Clearance 1 is higher than clearance 15. The security administrator can assign a category from 1 to 15. Category 1 is higher than category 15. Category can be assigned in compliance with the hierarchical structure of quarters. Higher quarters are supposed to have higher clearance than lower quarters, higher category involves lower category. Namely, access availability is decided by the hierarchical relations of clearances and the inclusive relations of categories.

And, TOE controls the additional information flow like the follows to the subject and the object.

- An additional information flow if directories or files
  - ‘P’ privilege : represents the status of an execute file(clearance is ‘0’) authorized by security administrator. If the file is not authorized, denies execution it.
  - ‘Y’ privilege : represents that the read permission of the present file is granted.
- An additional information flow if processes
  - ‘P’ privilege : the super privilege of TOE. If a subject gets the privilege, one can do everything in the system and the privilege can be inherited to subjects.
  - ‘I’ privilege : the install privilege of TOE. It can not apply security policy that security administrator makes. The privilege is for ‘package install’, ‘authorized execute file generation’ and ‘kill’ process privilege.
  - ‘A’ privilege : the authorized privilege of TOE. The process inherited a privilege can make execute files and execute them without the security administrator authorization.

■ DAC(Discretionary Access Control)

Discretionary Access Control is performed using access control regulations provided from MS Windows OS to which this TOE is installed. This TOE supports Mandatory Access Control,

and Discretionary Access Control. DAC is operated or used based on the follows:

- Perform access control based on identities of subjects and objects which OS manages.

■ RDP(Residual Data Protection)

This TOE should provide functions of not allowing the reuse of information allocated to subjects or objects. TSF of TOE hooks “unlink” system call of OS to make resource information unusable when withdrawing security level setup files from memory. It calls out “original” system call if there is access privilege for the object directory. And also, it operates the functions of object reuse prevention by initializing unlinked file fields.

6.1.3. Identification and Authentication

Identification and authentication is divided into 5 security functions. 5 security functions are IA_1(Authentication failure adjustment), IA_2(User property definition), IA_3(Verification of confidential information), IA_4(Identification and authentication) and IA_5(Protection of authentication feedback). Authentication data used in identification and authentication is provided in form which is suitable to EAL 3+, and assured in the vulnerability analysis note through the analysis method of probability and permutation. The security administrator authentication uses probability and permutation mechanism.

■ IA_1(Authentication failure adjustment)

Authentication failures are adjusted through the security administrator authentication functions. The security administrator authentication function is to distinguish that he/she is a security administrator or not, and identification and authentication is the major roles. When the security administrator attempts to log in, the authentication module should perform as follows:

- Checks whether the valid account or not by getting input ID and password for security administrator authentication.
- Certify whether the right user or not by comparing the input password with the OS password file's content.
- Lock out the user account for 3 minutes after the number of failed attempts which security administrator configured in advance.

■ IA_2(Definition of user identity)

User control function is to inquire general information and security attributes assigned to users or to configure them. The information managed in this function are user ID, username and password information.

■ IA_3(Verification of confidential information)

For the verification of confidential information, password management function is provided. With password management function, security administrators of REDOWL SecuOS system can change his/her password, and the rules applied to password modifications are as follows:

- New password which input to change should be different from the old one.
- Length of password (e.g. the minimum is 6 characters, and the maximum is 8 characters) confirmation
- Rule of combination (e.g. a password should contain letters from more than 2 characters of the below)

- Alphabets : 26 letters of each capitals and lowercase letters(A~Z, a~z)
- Wild characters : 32 letters(! " # $ % & ' ( ) * + , - / . : ; < = > ? @ [\ ] ^ _ ` { | } ~)
- Numerals : 0 ~ 9

- New password, containing more than 3 identical characters to the previous one, is not acceptable.
- New password with the sequence of more than 3 same characters or continuous character are not acceptable.

User can create or modify a password when above rules are satisfied.

■ IA_4(Identification and authentication)

Identification and authentication is divided to 2 functions. 2 functions are the security administrator authentication and the authentication success function. The security administrator authentication is to identify a security administrator, to perform authentication and to prevent the reuse of password information. Authentication success function is to handle the success of identification and authentication.

User authentication function is to check whether an user is a security administrator or not. The main function of user authentication is identification and authentication, and to prevent the reuse of user password information. When a user attempts to login to the system, user authentication module operates as follows:

- Investigate whether the valid account or not by getting input of user ID and password for user authentication.
  - Lock out the user account for 3 minutes after 3 times of failed attempts of user authentication

Authentication success function is to handle the success process lastly after a login session satisfies authentication, account management and session management. This function operates as follows:

- Record audit log of login success

- Record audit log of user login time

■ IA_5(Authentication feedback protection)

This TOE provides password input window and clearance input window when authentication performs for protecting authentication feedback. When a user input password, print out an error message automatically and record the event if the specified number of failures occur. User management and password management function ard used to protect authentication feedback.

User management function is to inquire or configure general information assigned to the account and security attributes.

With password management function, the security administrators of REDOWL SecuOS system can change or modify their password.

- When the security administrator intends to change the security password:
  - The security administrator only changes his/her security password
  - At client module of TOE, checks that he/she has the execution privilege or not, and than if he/she does not have, denies the execution
  - Whenever changes the security password, gets old password and new password, and than converts them by SHA-1 algorithm, stores the result values to TOE' security password file by ASCII.

6.1.4. Security Management

Security management is divided to 3 security functions. 3 security functions are SM_1 (security functions management), SM_2 (security attributes management) and SM_3 (TSF data management).

■ SM_1(Security functions management)

Security functions management is divided into agent server management, system user inquiry, remote command execution and text file inquiry. Agent server management function is to register or inquire agent server information which is controlled by the integrated management server. This functions is to manage information such as, IP address of agent server, DNS name, OS version, whether or not REDOWL SecuOS is being performed. Agent server management can be implemented by authorized security administrators and through integrated management, and following three management commands are provided for the implementation:

- Inquire server information of itself
- Inquire server information of a remote server
- Add/Modify/Delete server information of agent server from integrated management

server

System user inquiry function is to inquire the information of users who are using the OS system. By this function, information, such as user ID who connected to the system, IP address and access time, can be inquired.

Remote command execution function is to execute discretionary OS commands from the designated agent server remotely, and to bring in the result of execution. Remote command execution function can be operated by security administrator and the integrated management.

Text file inquiry function is to read in contents of text files placed in designated agent servers. By this function, reading in the whole text file, parts of the text file or the lines of specific pattern is available. This function can be only operated by security administrator and integrated management, and provides six CUI-based commands as follows:

- Reading in the whole text file placed in a designated agent server
- Reading in only specific lines of a text file placed in a agent server
- Reading in lines of a text file, which is consistent with the pattern suggested by parameter, placed in a agent server
- Reading in the whole text file by connecting to the agent servers which are registered to the integrated management server.
- Reading in only specific lines of a text file by connecting to the agent servers which are registered to the integrated management server.
- Reading in lines of a text file, which are consistent with the pattern suggested by parameter, by connecting to the agent servers which are registered to the integrated management server.

■ SM_2(Security attributes management)

Security attributes management is divided into user privilege management, security password management, file security information management, process security attributes management, security policy management, OS user account management and password management.

User management function is to inquire or configure the information assigned to users. Information managed through this function is user ID, username and password information.

- Inquire user information registered to the remote server or the local server
- Inquire all user's information registered to each agent server by connecting to the agent server which are registered to the integrated management servers.

- Add/Modify/Delete user's information from the agent server through the integrated management server

Security password management function is to add/modify security password by REDOWL SecuOS system's security administrator.

- Security administrator modifies the password of oneself

File security information management function is to inquire/configure the information or security attribute of a file or directory. This function can be used by security administrator. Also, inquiry/configuring of a remote agent server's files or directories, in accordance with parameter inputs, is possible.

- The command that inquire general information and security information of a file which is belonged to a specific directory of a designated agent server.
- Managing command that add/modify/delete clearance and category of a specific file or directory of a designated agent server.

Process security attribute management function is to inquire general information and security attribute of a process, and to configure the security privilege to a specific process. This function can be operated by security administrator.

- Command that inquire the general information and security information of all processes in a agent server.
- Command used when a security administrator or a user modify clearance and category of a process of oneself.
- Command used when a security administrator inquire or configure the information of clearance and category of all processes executed in an agent server.

Security policy management function is used to transmit security policy data of the integrated management server to a remote agent server, or to configure security policy to the security kernel. Security policy management can be operated by a security administrator.

- Transmit security policy files from the integrated management server to agent server registered to the management server selectively.
- Configure the security policy file to security kernel.

User account (of the OS) management function is to manage the minimum usage period, the maximum usage period, the inactivated period, the expiration date and the warning date of an user account. This function can be used by the security administrator.

- OS user account management

Password management (for OS accounts) is to lock-out/release and modify/delete passwords. This function can only be operated by the authorized security administrator.

- OS user password management

■ SM_3(TSF Data management)

TSF data management is divided into backup/restoration of security attributes, user management, and integrity data information management. Backup and restoration of security attributes is to store security information of certain directories of an agent server, and to restore security information to the agent server.

- Store a certain directory's security information of an agent server to the integrated management server.
- Restore the back-up file of security attributes.

User management function controls that prevents users in OS to access the file being stored users information without security administrator privilege. In TOE, it provides separated access area for sensitive data, and nobody cannot access that area without security privilege. If somebody without any privilege accesses that area, TOE generates audit data and denies the access.

- Separation TSF Data area and ordinary OS area.
- Access Control to important files and directories by configuring security attributes
- Automatically privilege inheritance to the object with security attributes

Integrity data management manages the hash values generated by TOE. TOE usually stores important files to hash values using SHA-1 algorithm. During starting TOE, during operating TOE periodily, and when security administrator asking, TOE compares original important files and hash values.

- Query, delete and search to audit data

- Various static and analysis report based on audit data

6.1.5. Protection of the TSF

TSF protection is divided into 4 security functions. 4 security functions are PT_1(Abstract machine testing), PT_2(Impossibility of TSP bypassing), PT_3(TSF testing) and PT_4(TSF protection).

■ PT_1(Abstract machine testing)

Abstract machine testing is to confirm the performance of Abstract machine which is supposed to perform Mandatory Access Control of REDOWL SecuOS, and executed aperiodically as follows by the security administrator's requests to:

- File system supported by OS
- Processes related network
- Some nessesary processes during OS operating

■ PT_2(Impossibility of TSP bypassing)

Impossibility of TSP bypassing is divided into three functions. Three functions are Agent server Management, User management and Security Policy Management. The security policies can be configured compulsorily to users by these three functions.

Agent server management is to register or inquire the information of agent servers which are managed by the integrated management server. The information includes the IP address of agent server, DNS name, the OS version, the performance status of TOE. This function can be operated by the authorized security administrator.

- Searches information of a server of oneself
- Searches information of a remote server
- Add/modify/delete information of a new agent server to the integrated management server

User management is to inquire or configure the general information and security attributes assigned to users. Information managed through this function are user ID, username and the password information.

- Command that inquire the user information registered to a local server of oneself or a remote server.
- Command that inquire every users' information registered to agent servers which are managed by the integrated management server.
- Command that add/modify/delete users' security attributes to agent servers through the

integrated management server.

Security policy management is to transmit the security policy data of the integrated management server to remote agent servers, or to configure agent servers' security policies to the security kernel. Security policy management is operated by the security administrator or the integrated management.

- Commands which are used to transmit security policy files from the integrated management server to the registered agent servers selectively.
- Commands configuring security policy files to the security kernel

■ PT_3(TSF testing)

TSF should implement a series of tests comparing hash values of the whole files, the file size and the time value for showing the accurate performance of supposed cases of security concern during TOE starting, periodically operating TOE, when asking security administrator . Before TSC functions being approved to operate, TSF executes each security function after comparing setting points of MAC for forcing TSP. In case of detecting errors in data integrity, TSF generates audit data for the corresponding event.

■ PT_4(TSF protection)

TSF operates the most important part of TOE. This TOE controls accesses of unauthorized users by installing to separated domains, as general user system domain and TOE's domain. No user can access to the directory where TOE installed, except the system administrator and the security administrator, and followings are contents which protected area is separated:

- The directory and file territory where TOE is installed.
- ID and password of the security administrator cannot be found in the general password management file, and are managed as the specific file of TOE security territory.
- TOE security configuration files are existing in the directories of TOE territory.

6.1.6. TOE Access

AT(Session lock by TSF) security function inside TOE access

■ AT(Session lock by TSF)

TSF should provide the corresponding function when a user intends to close a log-on session,

and control accesses of unauthorized users by locking out log-on session when the user doesn't use the system for minimum 30 seconds, maximum 3,600 seconds. To unlock the locking status the security administrator must inputs the security administrator password and system administrator password.

6.1.7. Trusted Path/Channels

TR(Trusted channels between TSFs) security function guarantees secure courses/channels.

- TR(Trusted channels between TSFs)

  TSF should offer a communication channel which is distinguished logically from other communicative channels and provide assured identification of a terminal and protect channel data from modifications or exposures. This TOE provides secure channel using SEED algorithm.

6.2. TOE Security Assurance Measures

This TOE fulfills assurance requirements of EAL3+ evaluation assurance grade. [Table 6-2] shows the fulfillments of assurance requirements and assurance measures.

[Table 6-2] Fulfillments of assurance requirements and assurance measures

Assurance class	Assurance components	Assurance measures and its theoretical basis	Document names
Configuration management	ACM_CAP.3	Configuration management is to identify and manage configuration items automatically using CVS.	Configuration management documents
	ACM_SCP.1	Configuration trail is possible by controlling development, user documents and source codes.	
Dilevery and operation	ADO_DEL.1	Providing users with procedures for secure TOE distribution.	Dilevery and operation
	ADO_IGS.1	Providing secure procedures for installation, generation, and initiation of TOE	Administrator guidance
Development	ADV_FSP.1	By describing every TSF and TSF's external interfaces in an atypical way, substantialize the security function requirements of TOE clearly and entirely.	Functional specifications documents
	ADV_HLD.2	Describe TSF structure, as a subsystem, and security functionality which each subsystem provides.	High-level design documents
	ADV_IMP.2	Represent that concrete descriptions for TSF satisfy security functions requirement.	Implementation representation document
	ADV_LLD.1	Provide detailed specifications of TSF	Low-level design document
	ADV_RCR.1	Provide conformity of statement of functions, primary specifications and detailed specifications for the conformity analysis.	Representaion correspondence document
Guidance documents	AGD_ADM.1	Provide administrator's manual for the system administrator.	Administrator guidance
	AGD_USR.1	Provide user manual of security functions for general users' TOE utilizations.	

Assurance class	Assurance components	Assurance methods	Assurance measures
Life cycle support	ALC_DVS.1	Describe physical, procedural, human and security concerning counterplans needed for protecting the confidentiality and the integrity of TOE designing and implementing processes.	Life cycle support document
	ALC_TAT.1	Document identifications for developing tools of TOE, implementations of developing tools and selection specifics of accessory options.	
Tests	ATE_COV.2	Offer of test scope analysis	Test documents
	ATE_DPT.2	Offer of test detailed analysis	
	ATE_FUN.1	Documentation of TSF test results	
	ATE_IND.2	Offer of security function specifics	TOE
Vulnerability assessment	AVA_MSU.1	The manuals should be well-defined, consistent, complete and reasonable about every operations of TOE.	Administrator guidance
	AVA_SOF.1	Perform analysis of security function intensity over authentication mechanisms identified in ST/LACSPP in which TOE's security function intensity is declared.	Vulnerability assessments documenet
	AVA_VLA.2	Analyze TOE presentation and make documents of identified specifics of vulnerabilities to find methods of user violating TSP.	

6.3. Strength of Security Functions (SOF)

Among IT security functions realized in this TOE, password section, which is related to the mechanism of GUI, is the only section which can be strength analyzed using permutation. The SOF of the relevant mechanism satisfies security function requirements of FIA_UAU.1(Authentication) and FIA_UAU.4(reuse prevention mechanism), and defined as ‘Strength of security function - medium’.

7. Protection Profile Claims

This section provides the PP conformance claim statements and supporting justification and refers, refines, adds TOE security environments, security objectives and IT security requirements.

7.1. Protection Profile Reference

The TOE conforms to the following PP which made by Korea Information Security Agency. The PP has made out using “Common Criteria for Information Technology Security system (the Ministry of Information and Communication Notice No.2005-25)”. [Table 7-1] shows PP requirement in this ST.

- Label-based Access Control System Protection Profile for Government V1.1, (17/ May/ 2006)

7.2. Protection Profile Refinements

This ST refers and updates the part of LACSPP V1.1 by Security Target writers. [Table 7-1] shows PP requirement in this ST.

[Table 7-1] PP requirements in ST

Classification			Security environment, objectives, policies	Status
TOE Security Environment	**Assumption**		A. Physical security	Reference
			A. Trusted administrator	Reference
			A. Hardened OS	Reference
			AA.TIME	Add
	Threats	**Threats to TOE**	T. Deficient codes	Reference
			T. Recording failure	Reference
			T. Data violation	Reference
			T. Authentication attempts By unauthorized	Reference
			T. Disguise and bypassing	Reference
			T. Rest information	Reference
		Threats to TOE environment	TE. Infirmity of management	Reference
			TE. Distribution/installation	Reference
	Security policy of the organization		P. Audit Record	Reference
			P.MAC	Reference
			P. Allowance of Security labels	Reference
			P. Identification and Authentication	Reference
			P. Secure management	Reference
			P. Cryptographic	Reference
			P.DAC	Reference
Security Objectives	**TOE Security objectives**		O. Audit Record	Reference
			O.MAC	Reference
			O. Inspection of Deficient codes	Reference
			O. Management	Reference
			O. Data protection	Reference
			O. Allowance of Security labels	Reference
			O Identification and Authentication	Reference
			O. DAC	Reference
			O. Self protection of Functions	Reference
			O. Removal of the rest Information	Reference
	Security objectives to TOE environment		OE. Physical security	Reference
			OE. Trusted administrator	Reference
			OE. Secure management	Reference
			OE .Hardened OS	Reference
			OEA. TIME	Add

Classification		Components	Status
IT Security Functional Requirements	**Security audit**	FAU_ARP.1	Refinement
		FAU_GEN.1	Refinement
		FAU_GEN.2	Reference
		FAU_SAA.1	Refinement
		FAU_SAR.1	Reference
		FAU_SAR.2	Reference
		FAU_SAR.3	Refinement
		FAU_SEL.1	Refinement
		FAU_STG.1	Reference
		FAU_STG.3	Refinement
		FAU_STG.4	Refinement
	User data protection	FDP_ACC.1	Refinement
		FDP_ACF.1	Refinement
		FDP_IFC.1	Refinement
		FDP_IFF.2	Refinement
		FDP_ITC.1	Refinement
		FDP_RIP.1	Refinement
	Identification and Authentication	FIA_AFL.1	Refinement
		FIA_ATD.1	Refinement
		FIA_SOS.1	Refinement
		FIA_UAU.1	Refinement
		FIA_UAU.4	Refinement
		FIA_UAU.7	Refinement
		FIA_DID.2	Reference
		FIA_USB.1	Reference
	Security management	FMT_MOF.1	Refinement
		FMT_MSA.1(1)	Refinement
		FMT_MSA.1(2)	Refinement
		FMT_MSA.3(1)	Reference
		FMT_MSA.3(2)	Reference
		FMT_MTD.1(1)	Reference
		FMT_MTD.1(2)	Reference
		FMT_MTD.1(3)	Reference
		FMT_MTD.1(4)	Reference
		FMT_REV.1	Refinement
		FMT_REV.1(2)	Refinement
		FMT_SMR.1	Refinement
		FMT_SMR.1	Refinement
	Protection of the TSF	FPT_AMT.1	Refinement
		FPT_RVM.1	Reference
		FPT_SEP.1	Reference
		FPT_STM.1	Reference
		FPT_TST.1	Refinement
	TOE access	FTA_SSL.1	Refinement
	Trusted path/channels	FTP_ITC.1	Refinement

7.3. Protection Profile Additions

In this ST, assumptions, organization' policies, security objectives and security objectives to TOE environment are added to LACSPP V1.1.

[Table 7-2] The assumptions, security policies, security objectives and security requirement for TOE environment added in LACSPP

Identification	Contents
AA. TIME	The IT environment provides trusted Time Stamp from "OS" or NTP server that follows RFC1305.
OEA.TIME	The IT environment provides trusted time stamps from "OS" or NTP server that follows RFC1305.
FPT_STM.1	The TOE gets trusted time stamps from OS based on time information established by the security administrator.

8. Rationale

This section describes the security requirements rationale satisfied with security objectives based on security environment(threats, assumptions, organization policies). The rationale shows TOE provides efficient IT security response in TOE security environment.

8.1. Security Objectives Rationale

Security objectives rationale shows that meets the specific security objectives, does not excess them.

Security objectives rationale proofs the followings.

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

[Table 8-1] depicts security environment to security objective mappings, [Table 8-2] depicts the rationale of security objectives for threats.

[Table 8-1] Security objectives to security environment mappings

Security Objectives / Security Environment	TOE security objectives										Security objectives to TOE environment				
	O. Audit Record	O. MAC	O. Inspection of deficient code	O. Management	O. Data protection	O. Allowance of security labels	O. Identification &	O. DAC	O. Self protection of functions	O. Removal of the rest information	OE. Physical security	OE. Trusted administrator	OE. Secure management	OE. Hardened OS	OEA. Time
A. Physical security											×				
A. Trusted administrator												×			
A. Hardened OS														×	
AA. SSL certificate of TOE															
AA. TIME															×
T. Deficient coded			×												
T. Recording failure	×														
T. Data violation					×		×		×						
T. Authentication attempts by unauthorized							×								
T. Disguise& bypassing							×		×						
T. Rest information										×					
TE. Infirmity of management												×	×		
TE. Distribution & installation												×	×		
P. Audit Record	×														
P. MAC		×				×									
P. Allowance of Security labels		×				×									
P. Identification & Authentication							×								
P. Secure management				×									×		
P. Cryptographic				×											
P. DAC								×							

8.1.1. The rationale of security objectives for threats

The rationale of security objectives for threats is same with [Table 8-2].

[Table 8-2] The rationale of security objectives for threats

Threats	Security Objectives	Rationale
T. Deficient coded	O. Inspection of Deficient coded	This security objectives inspects that the TOE has been some deficient codes and those codes reflexes to the each subsystems of TOE.
T. Recording failure	O. Audit Record	The TOE provides the functions of storing and searching security events, and alternative actions when the function is failed.
T. Data violation	O. Data protection O. Identification and authentication O. Self protection of functions	The TOE shall protect the TSF data being stored in TOE from the unauthorized accesses or users and provide the self protection against to threats.
T. Authentication attempts by unauthorized	O. Identification and authentication	The TOE shall control the unauthorized accesses and use the process of identification and authentication to block the unauthorized user to access the TSF data.
T. Disguise and Bypassing	O. Identification and authentication O. Self protection of function	The security objectives for the identification & authentication, and the self protection can remove the threats that unauthorized users disguise themselves as authorized users, and the attack the TOE by bypassing.
T. Rest information	O. Removal of the rest information	The security objective removes properly some data from the TOE objects, so it protects some from unauthorized accesses.
TE. Infirmity of Management	OE. Trusted administrator OE. Secure management	The authorized user of TOE is reliable and assures maintaining the TOE securely. The TOE shall ensure that he or she distributes, installs and uses TOE securely.
TE. Distribution and Installation	OE. Trusted administrator OE. Secure management	The authorized user of TOE is reliable and assures maintaining the TOE securely. The TOE shall ensure that he or she distributes, installs and uses TOE securely.

8.1.2. The rationale of security objectives for assumptions

The rationale of security objectives for assumptions is same with [Table 8-3].

[Table 8-3] The rationale of security objectives for assumptions

Assumptions	Security Objectives	Rationale
A. Physical security	OE. Physical security	The TOE assures that the only authorized user can access the TOE and the TOE is located in secure place being separated physically.
A. Trusted administrator	OE. Trusted administrator	The authorized user of TOE is reliable and assures maintaining the TOE securely.
A. Hardened OS	OE. Hardened OS	The TOE assures the security and reliability by that the security objectives removes the unnecessary services or functions of the OS, and reinforces the vulnerabilities of the OS.
AA. TIME	OEA. TIME	The TOE assures the accurate time stamp from OS providing.

8.1.3. The rationale of security objectives for security policies

The rationale of security objectives for security policies is same with [Table 8-4].

[Table 8-4] The rationale of security objectives for security policies

Security Policy	Security Objectives	Rationale
P. Audit Record	O. Audit Record	To support the security policy, the TOE provides the measures that writes and investigates security events.
P. MAC	O. MAC O. Allowance of Security labels	The TOE assures the access control to the information flow based on the user's security label, and assures that information or users get proper security labels or remove them according to the security policy and process of organization.
P. Allowance of Security labels	O. MAC O. Allowance of Security labels	The TOE assures the access control to the information flow based on the user's security label, and assures that information or users get proper security labels or remove them according to the security policy and process of organization.
P. Identification and authentication	O. Identification and authentication	The TOE shall control the unauthorized accesses and use the process of identification and authentication to block the unauthorized user to access the TSF data.
P. Secure management	O. Management OE. Secure management	The authorized user of TOE is reliable and assures maintaining the TOE securely. The TOE shall ensure that he or she distributes, installs and uses TOE securely.
P. Cryptographic	O. Management	The security objective provides the measure that the administrator accesses the TOE from the remote system.
P.DAC	O. DAC	To support the security policy, the TOE controls the resources of accesses based on the user's identification

8.2. Security Requirements Rationale

Security requirements rationale shows that IT security requirements are satisfied with specific security objectives.

8.2.1. TOE Security function requirements rationale

TOE security function requirements rationale shows the followings.

- Each security objectives is handled by at least one TOE security function requirement. Exceptionally, O. Inspection of deficient codes is handled by assurance requirements.
- Each TOE security requirements is handled by at least one TOE security objective.

[Table 8-5] Security objectives to the security requirements mappings

Security Objectives / Security Requirements	O. Audit Record	O. MAC	O. Management	O. Data protection	O. Allowance of security labels	O. Identification and Authentication	O. DAC	O. Self protection of function	O. Rest information
FAU_ARP.1	×								
FAU_GEN.1	×								
FAU_GEN.2	×								
FAU_SAA.1	×								
FAU_SAR.1	×								
FAU_SAR.2	×								
FAU_SAR.3	×								
FAU_SEL.1	×								
FAU_STG.1	×								
FAU_STG.3	×								
FAU_STG.4	×								
FDP_ACC.1							×		
FDP_ACF.1							×		
FDP_IFC.1		×							
FDP_IFF.2		×							

Security Objectives / Security Requirements	O. Audit Record	O. MAC	O. Management	O. Data protection	O. Allowance of security labels	O. Identification and Authentication	O. DAC	O. Self protection of function	O. Rest information
FDP_ITC.1		×							
FDP_RIP.1									×
FIA_AFL.1						×			
FIA_ATD.1						×			
FIA_SOS.1						×			
FIA_UAU.1			×	×		×			
FIA_UAU.4						×			
FIA_UAU.7						×			
FIA_UID.2			×	×		×			
FIA_USB.1						×			
FMT_MOF.1			×						
FMT_MSA.1(1)			×				×		
FMT_MSA.1(2)		×	×		×				
FMT_MSA.3(1)			×				×		
FMT_MSA.3(2)		×	×		×				
FMT_MTD.1(1)			×						
FMT_MTD.1(2)			×						
FMT_MTD.1(3)			×						
FMT_MTD.1(4)			×						
FMT_REV.1(1)			×		×				
FMT_REV.1(2)			×		×				
FMT_SMR.1			×						
FMT_SMF.1			×						
FPT_AMT.1				×				×	
FPT_RVM.1								×	
FPT_SEP.1								×	
FPT_STM.1	×								
FPT_TST.1				×				×	
FTA_SSL.1				×				×	
FTP_ITC.1			×						

[Table 8-6] Security objectives to TOE security function requirements mappings

Security objectives	Security requirements	Rationale
O. Audit Record	FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_SEL.1, FAU_STG.1, FAU_STG.3, FAU_STG.4, FPT_STM.1	This security objective satisfies the security requirements with the detection for the disclosure or loss of whole audit data. At the moment, FTP_STM.1 provides the reliable time stamps to audit information. Also, the security objective assures the integrity and confidentiality to the important audit data by TSF through the prevention function and access control function of audit information. If some problems occurs in the audit information, the alarm is sounded by FAU_ARP.1
O. MAC	FDP_IFC.1, FDP_IFF.2, FMT_MSA.1(2),FMT_MSA.3(2)	FDP_IFC.1, FDP_IFF.2 provide the policy of Mandatory Access Control and assure that the authorized user controls MAC policy through the FMT_MSA.1(1), FMT_MSA.3(1)
O. Management	FIA_UAU.1, FIA_UID.2, FMT_MOF.1, FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.3(1), FMT_MSA.3(2), FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_REV.1(1), FMT_REV.1(2), FMT_SMR.1, FMT_SMF.1, FPT_ITC.1	FPT_ITC.1 supports the trusted channels to TOE. The user who is identified by FIA_UAU.1, FIA_UID.2 manages the security functions thorough the FMT_MOF.1 and FMT_SMF.1 components . The authorized user or the owner of objects use FMT_MSA.1 to manage DAC and MAC polices. FMT_MTD is used for managing the audit data, the identification and authentication, TSF data. FMT_REV.1,2 is used for the security attributes of revocation.
O. Data protection	FIA_UAU.1, FIA_UID.2, FPT_AMT.1, FPT_TST.1, FTA_SSL.1	The user who is identified by FIA_UAU.1, FIA_UID.2 executes the abstract machine testing using FPT_AMT.1, takes actions to the errors for the TSF testing and the TSF data integrity.
O. Allowance of Security labels	FMT_MSA.1(2), FMT_MSA.3(2), FMT_REV.1(1), FMT_REV.1(2)	The authorized user manages MAC policies through FMT_MSA.1(2) and FMT_MSA.3(2), and removes the security attributes through the FMT_REV.1.
O. Identification and Authentication	FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.7, FIA_UID.2, FIA_USB.1	The TOE shall identify whole users and objects through FIA_UID.2, FIA_USB.1, and assures the trusted identification and authentication through FIA_UAU.1, FIA_UAU.4 and FIA_UAU.7 not to reuse authentication data.

Security objectives	Security requirements	Rationale
O. DAC	FDP_ACC.1, FAP_ACF.1	FDP_ACC.1 configures the coverage of DAC security policy. The DAC security policy identified by FDP_ACF.1 is performed.
O. Self protection Of functions	FPT_AMT.1, FPT_RVM.1, FPT_SEP.1, FPT_TST.1, FTA_SSL.1	The TOE can check the accuracy operation of abstract machine through FPT_AMT.1 to protect Oneself. FPT_RVM.1 prevents the bypassing attack and FPT_SEP.1 prevents the fundamental attack through the FPT_SEP.1 which separates the security domain and non security domain. FPT_TST.1,2 provides the integrity to the security information and TSF function. FTA_SSL.1 provides the TOE self protection function through the locking user's non activity period.
O. Rest information	FDP_RIP.1	When the object is allocated to resources, the TOE assures that the objects does not use prior information.

8.2.2. TOE Assurance requirements rationale

The assurance level of ST is for EAL3+ based on considering the assets, threat level and SOF level to TOE. The following components are added to EAL3 assurance requirements.

- ADV_IMP.2 Implementation of the TSF
- ADV_LLD.1 Descriptive low-level design
- ALC_TAT.1 Well-defined development tools
- ATE_DPT.2 Testing : low-level design
- AVA_VLA.2 Independent vulnerability analysis

The ‘O. Inspection of deficient codes’ in security objectives checks program codes made by developers, whether them have deficient codes or not. ADV_IMP.2 and ATE_DPT.2 components are added because of inspecting that the deficient codes are effected to the TOE internal subsystems

By The dependency of ADV_IMP.2, ADV_LLD.1 and ALC_TAT.1 are added. AVA_VLA.2 is added because the TOE needs vulnerability testing by developer and evaluator.

8.2.3. IT Environment requirements rationale

The ST has two security objectives(Time Stamp, SSL Protocol) for IT environment. [Table 8-6-1] depicts the rationale of security requirements for IT environment.

[Table 8-6-1] The rationale of security requirements for IT environment

Security objectives	Security requirements	Rationale
OEA.TIME	FPT_STM.1	This component assures that the IT environment provides reliable time stamp that TSF is able to use. Therefore, this component is satisfied with “OEA.TIME” which shall provide the reliable NTP server or OS.

8.3. Dependency Rationale

This section provides the dependency of TOE security requirements and assurance requirements.

8.3.1. The dependency of TOE security requirements

[Table 8-7] depicts the satisfaction of all functional requirement dependencies. For each functional requirement included in the ST. FMT_SMR.1 is dependent on FIA_UID.1. That means it is satisfied with FIA_UID.1 and FIA_UID.2. FDP_IFC.1 is dependent on FDP_IFF.1. So, it is satisfied with FDP_IFF.1 and FDP_IFF.2.

[Table 8-7] The dependencies of the function components

No.	Function components	Dependencies	Reference No.
1	FAU_ARP.1	FAU_SAA.1	4
2	FAU_GEN.1	FPT_STM.1	42
3	FAU_GEN.2	FAU_GEN.1, FIA_UID.1	2, 24
4	FAU_SAA.1	FAU_GEN.1	2
5	FAU_SAR.1	FAU_GEN.1	2
6	FAU_SAR.2	FAU_SAR.1	5
7	FAU_SAR.3	FAU_SAR.1	5
8	FAU_SEL.1	FAU_GEN.1, FMT_MTD.1	2,31,32,33,34
9	FAU_STG.1	FAU_GEN.1	2
10	FAU_STG.3	FAU_STG.1	9
11	FAU_STG.4	FAU_STG.1	9
12	FDP_ACC.1	FDP_ACF.1	13
13	FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	12, 29
14	FDP_IFC.1	FDP_IFF.1	15
15	FDP_IFF.2	FDP_IFC.1, FMT_MSA.3	14, 30
16	FDP_ITC.1	FDP_ACC.1, FDP_IFC.1, FMT_MSA.3	12, 14, 30
17	FDP_RIP.1	-	-
18	FIA_AFL.1	FIA_UAU.1	21
19	FIA_ATD.1	-	-
20	FIA_SOS.1	-	-
21	FIA_UAU.1	FIA_UID.1	24
22	FIA_UAU.4	-	-
23	FIA_UAU.7	FIA_UAU.1	21
24	FIA_UID.2	-	-
25	FIA_USB.1	FIA_ATD.1	19
26	FMT_MOF.1(1)	FMT_SMR.1, FMT_SMF.1	37, 38
27	FMT_MSA.1(1)	FDP_ACC.1, FDP_IFC.1, FMT_SMR.1, FMT_SMF.1	12, 14, 37, 38
28	FMT_MSA.1(2)	FDP_ACC.1, FDP_IFC.1, FMT_SMR.1	12, 14, 37,38
29	FMT_MSA.3(1)	FMT_MSA.1, FMT_SMR.1	28, 37
30	FMT_MSA.3(2)	FMT_MSA.1, FMT_SMR.1	29, 37

No.	Function components	Dependencies	Reference No.
31	FMT_MTD.1(1)	FMT_SMR.1, FMT_SMF.1	37, 38
32	FMT_MTD.1(2)	FMT_SMR.1, FMT_SMF.1	37, 38
33	FMT_MTD.1(3)	FMT_SMR.1, FMT_SMF.1	37, 38
34	FMT_MTD.1(4)	FMT_SMR.1, FMT_SMF.1	37, 38
35	FMT_REV.1(1)	FMT_SMR.1	37
36	FMT_REV.1(2)	FMT_SMR.1	37
37	FMT_SMR.1	FMT_UID.1	24
38	FMT_SMF.1	-	-
39	FPT_AMT.1	-	-
40	FPT_RVM.1	-	-
41	FPT_SEP.1	-	-
42	FPT_STM.1	-	-
43	FPT_TST.1	FPT_AMT.1	38
44	FTA_SSL.1	FIA_UAU.1	21
45	FTP_ITC.1	-	-

8.3.2. The dependency of TOE assurance requirements

The dependency of TOE assurance requirements is satisfied with the CC, therefore in this section that was omitted. [Table 8-8] depicts the dependency of assurance requirements to EAL 3 added. The ST is satisfied with the dependency of all assurance requirements.

[Table 8-8] The dependencies of the additional assurance components

No.	Assurance components	Dependencies	Reference No.
1	ADV_IMP.2	ADV_LLD.1 ADV_RCR.1 ALC_TAT.1	2 EAL 3 3
2	ADV_LLD.1	ADV_HLD.2 ADV_RCR.1	EAL3 EAL3
3	ALC_TAT.1	ADV_IMP.1	1
4	ATE_DPT.2	ADV_HLD.2 ADV_LLD.1 ATE_FUN.1	EAL3 2 EAL3
5	AVA_VLA.2	ADV_FSP.1 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1 AGD_ADM.1 AGD_USR.1	EAL3 EAL3 1 2 EAL3 EAL3

8.4. TOE Summary Specification Rationale

This section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements and the assurance measures, address the assurance measures.

The collection of assurance measures work together to address all of the security assurance requirements as indicated in [Table 8-9]. The collection of security functions work together to provide all of the security requirements as indicated in [Table 8-10]. [Table 8-11] depicts the rationale of TSS. The strength of security requirements is described in the vulnerability assessment report.

[Table 8-9] TOE Assurance requirements to the assurances mappings

Assurance Components	Configuration management	Delivery and operation	Information Functional specification	Security enforcing High-level design	Descriptive low-level design	Subset of the implementation of	Administrator Guidance	User guidance	Life cycle support	Tests	Vulnerability Assessment
ACM_CAP.3	×										
ACM_SCP.1	×										
ADO_DEL.1		×									
ADO_IGS.1		×									
ADV_FSP.1			×								
ADV_HLD.2				×							
ADV_IMP.2						×					
ADV_LLD.1					×						
ADV_RCR.1			×	×	×	×					
AGD_ADM.1							×				
AGD_USR.1								×			
ALC_DVS.1									×		
ALC_TAT.1									×		
ATE_COV.2										×	
ATE_DPT.2										×	
ATE_FUN.1										×	
ATE_IND.2										×	
AVA_MSU.1											×
AVA_SOF.1											×
AVA_VLA.2											×

[Table 8-10] TOE Security requirements to the security functions mappings

Security function	Security Components	AU1	AU2	AU3	AU4	AU5	MAC	DAC	RDP	IA1	IA2	IA3	IA4	IA5	SM1	SM2	SM3	PT1	PT2	PT3	PT4	AT	TR
Security Audit	FAU_ARP.1			×		×																	
	FAU_GEN.1	×																					
	FAU_GEN.2	×																					
	FAU_SAA.1		×			×																	
	FAU_SAR.1		×																				
	FAU_SAR.2		×		×		×	×															
	FAU_SAR.3		×																				
	FAU_SEL.1		×																				
	FAU_STG.1			×			×	×															
	FAU_STG.3			×																			
	FAU_STG.4			×																			
User Data Protection	FDP_ACC.1							×															
	FDP_ACF.1							×															
	FDP_IFC.1						×																
	FDP_IFF.2						×																
	FDP_ITC.1						×																
	FDP_RIP.1								×														
Identification and Authentication	FIA_AFL.1									×													
	FIA_ATD.1										×												
	FIA_SOS.1											×											
	FIA_UAU.1												×										
	FIA_UAU.4												×										
	FIA_UAU.7													×									
	FIA_UID.2												×										
	FIA_USB.1						×	×			×												
Security Management	FMT_MOF.1														×								
	FMT_MSA.1(1)							×								×							
	FMT_MSA.1(2)						×									×							
	FMT_MSA.3(1)							×								×							
	FMT_MSA.3(2)						×									×							
	FMT_MTD.1(1)																×						
	FMT_MTD.1(2)																×						
	FMT_MTD.1(3)																×						
	FMT_MTD.1(4)																×						
	FMT_REV.1(1)						×	×								×							
	FMT_REV.1(2)						×	×								×							
	FMT_SMR.1												×		×								
	FMT_SMF.1														×	×	×						
TSF Protection	FPT_AMT.1																	×					
	FPT_RVM.1																		×				
	FPT_SEP.1																				×		
	FPT_STM.1																×						
	FPT_TST.1																			×			

Security Function	Security Component	AU1	AU2	AU3	AU4	AU5	MAC	DAC	RDP	IA1	IA2	IA3	IA4	IA5	SM1	SM2	SM3	PT1	PT2	PT3	PT4	AT	TR
TOE Access	FDP_ACC.1																					×	
Secure Path/Channel	FIA_AFL.1																						×

[Table 8-11] The rationale of TSS

Security functions	Security requirements	Rationale
AU_1 (Audit record generating)	FAU_GEN.1, FAU_GEN.2	AU_1 identifies the various audit events from TOE and performs the important work that associated the user making audit events with the audit events.
AU_2 (Audit record inquiry)	FAU_SAA.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_SEL.1	AU_2 provides the security function that the authorized user only searches and sorts the audit data collected.
AU_3 (Audit record protection)	FAU_ARP.1, FAU_STG.1, FAU_STG.3, FAU_STG.4	The audit data generated and collected shall be protected from unauthorized removal and the TOE shall protect the audit data before the storage is full and sends email to the authorized user.
AU_4 (Limitation of audit investigation privilege)	FAU_SAR.2	The audit data shall be permitted to the authorized user.
AU-5 (Analysis of potential violations)	FAU_ARP.1, FAU_SAA.1	The TSF shall analysis the potential violations through mixing various rules when inspects violations and then, report the violations to the authorized user
MAC (Mandatory Access Control)	FAU_SAR.2, FAU_STG.1, FDP_IFC.1, FDP_IFF.2, FDP_ITC.1, FIA_USB.1, FMT_MSA.1(2),FMT_MSA.3(2),FMT_REV.1(1), FMT_REV.1(2)	The MAC provides Mandatory Access Control between the subjects to subjects, the subjects to objects and controls the information flow through providing the security label to the subjects and objects. Because the MAC controls all of subjects and objects, the security administrator only changes or removes the specific subjects and objects.
DAC (Discretionary Access Control)	FAU_SAR.2, FAU_STG.1, FDP_ACC.1, FDP_ACF.1, FIA_USB.1,FMT_MSA.1(1),FMT_MSA.3(1),FMT_REV.1(1), FMT_REV.1(2)	The TSF controls the accesses that All users are classified by the user identification of subjects and the group identification of user and then, the TSF controls the access coverage and the information flow at discretion. The TSF applies the operation of between controlled subjects and controlled objects to OS access control list.
RDP (Residual data protection)	FDP_RIP.1	When the TSF gets back the resource from the file with security labels, it protects the residual data of resource from the unauthorized subjects.

Security functions	Security requirements	Rationale
IA_1 (Authentication failure adjustment)	FIA_AFL.1	When users authentication are failed, the TSF shall detect them, and create the audit data and then send e-mails to the security administrator.
IA_2 (Definition of user identity)	FIA_ATD.1, FIA_USB.1	The security function shall associate activated subjects with users, since it maintains the lists of user's identification, user's group, security label, authentication data to users.
IA_3 (Verification of confidential information)	FIA_SOS.1	The security function provides the verification mechanism to the secrets that the changing cycle and setting rule of authentication data.
IA_4 (Identification and authentication)	FIA_UAU.1, FIA_UID.2, FMT_SMR.1, FIA_UAU.4	All user who accesses to TOE gets permission throughout the process of authentication and identification.
IA_5 (Authentication feedback protection)	FIA_UAU.7	The security function limits and encrypts the feedback of authentication to the input window with display view for the security label to prevent using authentication data by stealth during user authentication.
SM_1 (Security functions management)	FMT_MOF.1, FMT_SMR.1, FMT_SMF.1	The authorized user has abilities that he decides, stops, initiates, changes various functions for security management.
SM_2 (Security attributes management)	FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.3(1), FMT_MSA.3(2), FMT_REV.1(1), FMT_REV.1(2) FMT_SMF.1	The security function can restrict owner or authorized user not to change and query the security attributes of DAC related with object. And also it can restrict the authorized user not to remove the MAC related with subjects or objects, so can restrict removal ability from the specific subject can not remove the security attributes.
SM_3 (TSF Data management)	FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FPT_STM.1 FMT_SMF.1	The authorized user manages the TSF data management function like the audit information, identification and authentication data, the operation of security data including time stamp(delete, change, initiate).
PT_1 (Abstract machine testing)	FPT_AMT.1	The abstract machine test performs a series on testing the status of security options, the status of access control lists and daemon process with super privileges whenever the authorized user asks.
PT_2 (Impossibility of TSP bypassing)	FPT_RVM.1	The TSF provides the mandatory function to control the TSP in TSC, so it can provide the impossibility of TSP bypassing.
PT_3 (TFS testing)	FPT_TST.1	The TSF compares the modify time with the creative time, hash value of the whole files, and file size to proof correct operation of TSF. If the error is happen, it creates the audit data.

Security functions	Security requirements	Rationale
PT_4 (TSF protection)	FPT_SEP.1	The TSF daemon and security data storage shall be separate physically to protect TSF oneself from the unauthorized intrusion.
AT (Session lock by TSF)	FTA_SSL.1	The TOE shall provide function that locks the session during the authorized user being non-activity.
TR (Secure channels between TSFs)	FTP_ITC.1	The TSF shall separate logically other communication channels, provide secure channel between TSFs to prevent them from unauthorized changes or exposures.

8.5. Protection Profile Claims Rationale

The ST refers to the following PP made by the Korea Information Security Agency(KISA). Also the PP is based on the CC. The ST is same with the PP in the security objectives and security requirements.

- Label-based Access Control System Protection Profile for Government V1.1, (17/May/2006)

8.6. Strength of Function Rationale

The TOE minimum strength of function of SOF-medium was chosen to be consistent with the LACSPP(The assets of TOE are middle level and the threat agent has low level of professional knowledge, resources and motivations.). The SOF-medium strength level is sufficient to meet the objectives of the TOE given the security environment described in the ST.