NEC GROUP INFORMATION LEAKAGE PREVENTION SYSTEM V1.0 (Japanese Version) SECURITY TARGET

Version 1.12

December 12, 2007

NEC Corporation

This document is a translation of the evaluated and certified security target written in Japanese.

Revision History

Version	Date	Revision Details	Publisher
1.00	Apr 23, 2007	First edition.	NEC Corporation
1.01	May 18, 2007	Added a description of I/O port controls and implemented overall review and modification in relevant to this addition.	NEC Corporation
1.02	Jun 8, 2007	Modifications on instructions from the evaluation body	NEC Corporation
1.03	Jul 13, 2007	Modifications on instructions from the evaluation body	NEC Corporation
1.04	Aug 3, 2007	Modifications on instructions from the evaluation body	NEC Corporation
1.05	Aug 15, 2007	Modifications on instructions from the evaluation body	NEC Corporation
1.06	Aug 22, 2007	Modifications on instructions from the evaluation body	NEC Corporation
1.07	Aug 31, 2007	Modifications on instructions from the evaluation body	NEC Corporation
1.08	Oct 10, 2007	Modifications on instructions from the evaluation body	NEC Corporation
1.09	Oct 15, 2007	Modifications on instructions from the evaluation body	NEC Corporation
1.10	Oct 19, 2007	Modifications on instructions from the evaluation body	NEC Corporation
1.11	Nov 14, 2007	Modifications on instructions from the evaluation body	NEC Corporation
1.12	Dec 12, 2007	Modifications on instructions from the evaluation body	NEC Corporation

■ Trademarks and Registered Trademarks

All brand names and product names described in this document are trademarks or registered trademarks of their respective companies.

Table of Contents

Reference

This document uses the following reference materials.

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model September 2006 Version 3.1 Revision 1 CCMB-2006-09-001
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2006 Version 3.1 Revision 1 CCMB-2006-09-002
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components September 2006 Version 3.1 Revision 1 CCMB-2006-09-003
- Common Methodology for Information Technology Security Evaluation Evaluation Methodology September 2006 Version 3.1 Revision 1 CCMB-2006-09-004

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model September 2006 Version 3.1 Revision 1 CCMB-2006-09-001 Japanese Version 1.2, March 2007 Information Security Certification Office, IT Security Center, Information-technology Promotion Agency, Japan
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2006 Version 3.1 Revision 1 CCMB-2006-09-002 Japanese Version 1.2, March 2007 Information Security Certification Office,IT Security Center, Information-technology Promotion Agency, Japan
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components September 2006 Version 3.1 Revision 1 CCMB-2006-09-003 Japanese Version 1.2, March 2007 Information Security Certification Office,IT Security Center, Information-technology Promotion Agency, Japan
- Common Methodology for Information Technology Security Evaluation Evaluation Methodology September 2006 Version 3.1 Revision 1 CCMB-2006-09-004 Japanese Version 1.2, March 2007 Information Security Certification Office, IT Security Center, Information-technology Promotion Agency, Japan

Symbols and Abbreviated Terms

<CC related abbreviations>

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

<TOE related abbreviations>

AP	Application Program
CPU	Central Processing Unit
DB	Database
DBMS	Database Management System
GB	Giga Byte
GHz	Gigahertz
HDD	Hard Disk Drive
ID	Identification
IEEE	The Institute of Electrical and Electronics Engineers, Inc.
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
MB	Mega Byte
OS	Operating System
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
SSL	Secure Socket Layer
USB	Universal Serial Bus

<Terms and definitions related to TOE>

Terminology	Definitions
Administrator privilege	One of user privileges used in Microsoft operating systems. It permits a user to change the operating system settings.
NEC	NEC Corporation
NEC group	NEC and its subsidiaries
I/O port	A port used for data transfer between a PC and its peripherals (e.g. USB ports, IEEE1394 ports, serial ports, parallel ports, infrared ports, PCMCIA ports and printer ports).
Java	An object-oriented programming language. Java runtime environment.
JDBC	An AP interface for connection between Java and database.
LogViewer	An administrative tool to view/search logs that run on the log server application software.
LogViewer startup control information	Control information for using the LogViewer.
USB device	A generic name of peripherals that are connected to the USB port on a PC.
Web	A synonym of World Wide Web. A hypertext system available on Internet.
Winny	A file sharing software.
Windows network workgroup	One of the network IDs used in Microsoft operating systems. It is a logical group of computers on a network that allows sharing of resources such as files and printers.
Cryptographic key input control information	Information for reading a common key to encrypt/decrypt a file
Generic AP file	A generic name of application programs that run on client's operating systems such as Microsoft Office Word/Excel/PowerPoint. User data in executable format that does not contain source codes.
Administrator	A generic name of a person who performs the TOE management operations on administrator and client terminals.
External Media	Media connected to a client and recognized as a removal media by the operating system (e.g. External HDD, USB memory, PCMCIA memory, etc.).
Administrative Terminal	A PC used by an administrator to read/search client control information.
Authorised USB Device	A USB device authorised by the Administrator.
Authorised External Media	Any media (external HDD, USB memory, PCMCIA memory and others) connected to a client terminal and identified as a removal media by the operating system. It stores authorised external media input /output control information written by the Administrator.

Terminology	Definitions
Group Name	An arbitrary name assigned to each department.
Client	A PC used within the NEC group.
Client Control Information	A PC control policy created by the Administrator and defined to each client PC or the definition information used to control the behavior of each client PC.
Client Setup Image	A file to be created by the Administrator that contains information necessary to predefine the client's operational environment. It also contains client control information.
User Inactivity Period Before Reauthentication is Required	Time from when a logged-on user attempts his or her last access to the TOE till when the TOE requests a reauthentication to that user
Asset Management System	A system to manage company-owned assets, which is used independently by the TOE.
Printer Port	A port used to output client's print data to a printer.
Maintenance Mode	A mode to be specified when starting Windows to maintain the Microsoft Windows operating system.
User	A generic name of Administrators, client administrators and general users.
Registry	An area storing configuration settings necessary to control client's operating system.
Log	Audit information stored in the audit trail.

1. ST Introduction

This chapter covers ST Reference, TOE Reference, TOE Overview and TOE Description.

1.1. ST Reference

ST Title:	NEC Group Information Leakage Prevention System V1.0 (Japanese Version) Security Target
Version:	1.12
ST Publisher:	NEC Corporation
ST Publishing Date:	December 12, 2007

1.2. TOE Reference

TOE Title:	NEC Group Information Leakage Prevention System (Japanese Version)
TOE Version:	V1.0

1.3. TOE Overview

1.3.1. Usage and Major Security Features of the TOE

This TOE is an information leakage prevention system that is deployed throughout the NEC group companies. The TOE is designed to restrict the user's PC operations relevant to taking information out of a PC. This is implemented by defining the PC control policy in accordance with the privilege assigned to each user by the Administrator and enforcing that policy to each user PC.

The main security features of the TOE include identification and authentication, access control, cryptography and auditing.

- Identification and Authentication
  - A function to identify and authenticate a user
- Access Control
  - A function to control the input / output PC operations from or to its I/O port or a printer
  - A function to control the execution of a user program
  - A function to control the output of a file to the authorised external media
  - A function to control the output of a file to the authorised USB device
  - A function to control the creation and modification of the client control information
- Cryptography
  - A function to encrypt and decrypt a file

- A function to create an encryption/decryption key
- A function to encrypt/decrypt a file when inputting/outtputing it from or to the authorised external media or the authorised USB device

- Auditing
  - A function to create and transfer logs to the log server
  - A function to view and search logs stored in the log server

1.3.2. TOE Type

This TOE is the information leakage prevention software intended for use by all NEC group employees.

1.3.3. Required Non-TOE Hardware/Software/Firmware

All hardware/software necessary to run the TOE is shown in Tables 1-1 and 1-2.

Table 1-1 Hardware Configuration

Hardware		Description
Log Server	CPU	Pentium 4 3.0GHz or above
	Memory	2GB or above
	HDD	100GB or above
	Graphic	1024x768 or higher resolution 256 or higher color display
Common to admin/client terminals	CPU	Pentium 3 1.0GHz or above
	Memory	512MB or above
	HDD	40GB or above
	Graphic	1024x768 or higher resolution 256 or higher color display

Table1-2 Software Configuration

Hardware	Software	
	Type	Product Name
Log Server	Antivirus	Networks Associates Technology VirusScan Enterprise 8.0i
Admin. Terminal	Antivirus	Networks Associates Technology VirusScan Enterprise 8.0i
Client	Antivirus	Networks Associates Technology VirusScan Enterprise 8.0i
	AP	Generic AP file *

* The generic AP file is not required to run the TOE. It is simply listed since it is subject to the TOE access control)

1.4. TOE Description

1.4.1. System operations

The Administrator is allowed to setup log servers and administrator terminals, create general user's client control information, client setup image, common key to encrypt/decrypt a file and cryptographic key input control information, view and search log information stored in the log server to update client control information as needed, forcibly change client's passwords, and uninstall the NEC Group Information Leakage Prevention System V1.0's client application software Ver1.0 (Japanese Version).

The client control information is created by setting secure values in accordance with the TOE guidance documentation shown in Table 1-5, considering the system usage by each department and user.

Before setting up client terminals, each general user is required to delete all the software specified in the prohibited software list on the NEC Group Standard. The setup itself can be accomplished using the client setup image distributed by the Administrator and importing a common key to encrypt/decrypt a file with the distributed encryption key input control information. Once the setup is completed, each general user can log into the client terminal using the general user ID and password that is assigned by the Administrator, and use any I/O ports, user programs, printers and authorised external media based on the client control information.

Each general user is allowed to obtain the client control information only and apply it according to the individual instructions from the Administrator. It should be noted that the general user is not allowed to change any client control information. For details about the client control information, refer to Table 1-3.

Table 1-3 Client Control Information Details

Item	Description
General user ID	An ID used to identify a general user of the TOE
General user password	A password used to authenticate a general user of theTOE
Password minimum length	Minimum number of password characters used for authentication
Password validity period	Defined validity period of a password in days
Warning size of audit trail storage	When the recorded log data exeedes this predetermined threshold, a warning message is generated to each user.
Maximum permissible number of consecutive authentication failures	Number of consecutive logon failures before a PC is locked.
Authorised external media input / output control information	Information necessary to determine whether to permit the use of an authorised external media

Item	Description
Authorised USB device input / output control information	Information necessary to determine whether to permit the use of an authorised USB device
User inactivity period before authentication is required	Time from when a logged-on user attempts his or her last access to the TOE till when the TOE requests a reauthentication to that user
I/O port control information	Information necessary to determine whether to permit the use of an I/O port
Printer control information	Information necessary to determine whether to permit the full use or partial use of a printer
Authorised printer information	Detailed information on partial use of a printer
External media output control information	Information necessary to determine whether to permit the file output to the external media
Prohibited user program information	Name of a prohibited user program

This TOE shall be used in Windows network workgroup in each department.
It runs on the log servers and the administrator terminals with Administrator privilege, and on normal client terminals with a given operating system's user privilege other than administrator privilege.
Since the TOE cannot protect personal equipments from loss and theft, only-company-provided log servers, administrator/client terminals, external media and other devices that are managed under the company rules and the asset management system are authorised for use. Client terminals are provided to each general user through the Administrator.

1.4.2. Roles of TOE-related users

The TOE-related users include Administrators, client administrators, general users, System Managers and corporate network managers. Users directly using the TOE can be categorized into Administrators, client administrators or general users and perform operations within a given privilege. All TOE-related users must comply with working rules and regulations.

(1) Administrator (a person who operates an administrator terminal)
The Administrator shall be informed of his or her roles and designated by the System Manager at each department and shall be responsible for managing all clients and log servers at each department. The roles include, but not limited to:

- Assigning a user ID and a password
- Creating and distributing the client setup image
- Creating and distributing the client control information

- Creating and distributing the common key to encrypt/decrypt a file
- Creating and distributing the control information for encryption key input
- Registering and distributing the authorised external media
- Viewing and searching log information

(2) Client administrator

The Administrator doubles as the client administrator responsible for managing clients at each department. The roles include, but not limited to:

- Forcibly changing a client password
- Uninstalling the NEC Group Information Leakage Prevention System V1.0 client application software Ver1.0 (Japanese Version) installed on the client.

(3) General user

The general user can use a client terminal based on the client control information created by the Administrator. The roles include, but not limited to:

- Using a client
- Retrieving the client control information that is distributed from the Administrator
- Retrieving a common key to encrypt/decrypt files that is distributed from the Administrator.

(4) System Manager

The System Manager shall be a trusty person, designated in each department and informed of his or her roles prior to designation.

(5) Corporate network manager

The corporate network manager is responsible for operating and maintaining the NEC Group's Intranet.

1.4.3. Physical Scope of the TOE

The following subsections describe the operational environment of the TOE and all the hardware and software and guidance parts that consititute the TOE.

1.4.3.1. Operational Environment of the TOE

The Figure 1-1 shows the network configuration consisting of log servers, administrator/client terminals and other related IT equipments on which the TOE operates.

(1) Physical Layout and Network

The log servers, administrator terminals and clients on which the TOE operates shall be all connected to the company LAN and installed within the company's premises with physical entry controls where entering these premises is only permitted to NEC Group employees and those authorised by them. The log servers storing log information shall be installed on a rack within the facilities which are physically segmented and equipped with doors with a locking mechanism (hereafter called as "secure rooms").

Entering those secure rooms is only permitted to the Administrator and those authorised by the Administrator. The Administrator must accompany those authorised third parties and watch their movements.

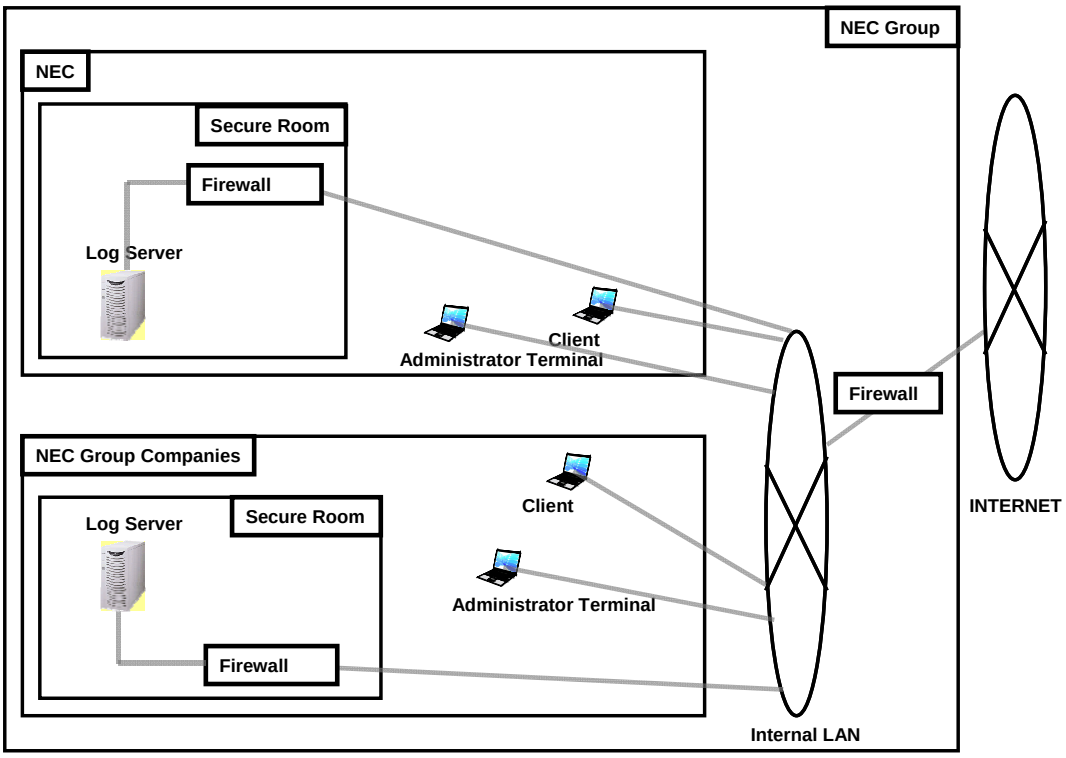

Figure 1-1 Operational Environment of the NEC Group Information Leakage Prevention System (Japanese Version)

(2) Company LAN

The Company LAN is connected to external networks via an appropriately configured firewall. The secure room is also interconnected to the Company LAN via an appropriately configured firewall to allow communications among log servers, administrator terminals and clients.

(3) Clients

All the clients connected to the Company LAN are used by general users or client administrators. Log information created by clients is transferred to the log server via the Company LAN.

(4) Administrator terminals

The administrator terminals connected to the Company LAN are used by the Administrator. Log information created by the administrator terminal is transferred to the log server. The administrator terminal allows the Administrator to view or search log information on the log server via the Company LAN.

(5) Log servers

The log servers are installed within the NEC Group's secure rooms and connected to the Company LAN via a firewall. They will retain log information transferred from the administrator/client terminals.

1.4.3.2. TOE Components

The software portion of the area surrounded by the dashed line in Figure 1-2 represents the physical scope of the TOE.

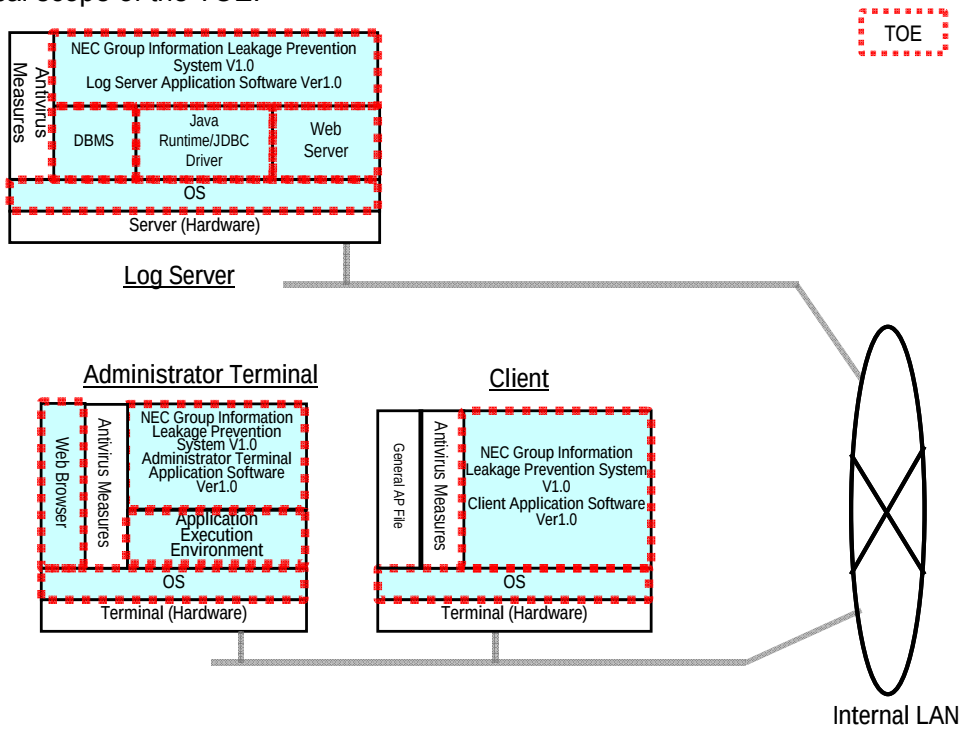

Figure 1-2 NEC Group Information Leakage Prevention System Components (Japanese Version)

The TOE software component names and their verions are shown in Table 1-4.

Table 1-4 TOE Software Components

Equipment	Type	Software Component Name
Log server	AP	NEC Group Information Leakage Prevention System V1.0 (Japanese Version) Log Server Application Software Ver1.0
	OS	Microsoft Windows Server 2003 Standard Edition（SP1）
	DBMS	Microsoft SQL Server 2005 Standard Edition（SP1）
	JDBCdDriver	Microsoft SQL Server 2005 JDBC Driver Ver1.0
	Web Server	Apache Tomcat 5.5.17 Apache Axis 1.4
	Java runtime	Sun Java Runtime Environment (JRE) 5.0 Update 11
Administrator terminal	AP	NEC Group Information Leakage Prevetion System V1.0 (Japanese Version) Administrator Application Software Ver1.0
	OS	Microsoft Windows XP Professional（SP2）
	Web Browser	Microsoft Internet Explorer 6.0（SP2）
	Application Execution Environment	Microsoft .NET Framework 2.0 Microsoft .NET Framework 2.0 Japanese Language Pack
Client	AP	NEC Group Information Leakage Prevetion System V1.0 (Japanese Version) Client Application Software Ver1.0
	OS	Microsoft Windows XP Professional（SP2）

In Figure 1-2, the hardware and software components other than those TOE software components listed in Table 1-4 are outside the scope of the TOE. For information about those hardware and software components outside the scope of the TOE, refer to Tables 1-1 and 1-2.

1.4.3.3. TOE Guidance Documents

The guidance documents for installation and operation of the TOE are shown in Table 1-5.

Table 1-5 TOE Guidance Document

Type	Guidance Document Name
Installation Guidance	NEC Group Information Leakage Prevention System V1.0 Install Guide (Japanese Version)
Operational User Guidance	NEC Group Information Leakage Prevention System V1.0 Administrator Guide (Japanese Version)
	NEC Group Information Leakage Prevention System V1.0 User Guide (Japanese Version)

1.4.4. Logical Scope of the TOE

The area surrounded by the dashed line in Figure 1-3 represents the logical scope of the TOE.

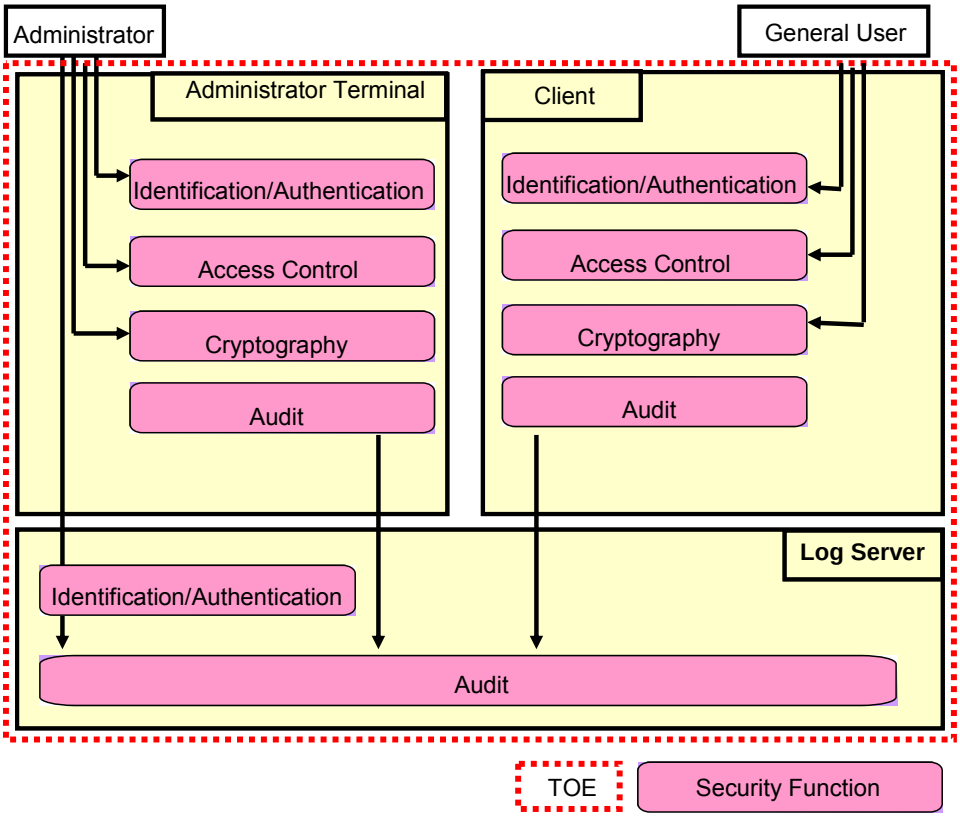

Figure 1-3 Logical Configuration of the NEC Group Information Leakage Prevention System (Japanese Version)

The following subsections describe the TOE security functions shown in Figure 1-3.

1.4.4.1. Security functions provided by the TOE

(1) Audit

(Administrator/Client Terminal)

- Generation and transfer of log data to the log server
- Protection of log data during the transfer

(Log server)

- Viewing and searching log data stored in the log server database

(2) Identification/authentication

Note that the identification/authentication function described in this section refers to that provided by the application programs on the administrator/client terminals and log servers

such as Administrator Terminal Application Software Ver1.0 for NEC Group Information Leakage Prevention System V1.0 (Japanese Version), Client Application Software Ver1.0 for NEC Group Information Leakage Prevention System V1.0 (Japanese Version)and Log Server Application Software Ver1.0 for NEC Group Information Leakage Prevention System V1.0 (Japanese Version). It is not the identification/authentication function provided by the operating system.

(Administrator Terminal)

- Identification/authentication required for the Administrator to log on to the administrator terminal
- Identification/authentication required to unlock a PC in the locked-out state due to the “user inactivity period” setting
- Changing an administrator password

(Client)

- Identification/authentication required for the general user or the client administrator to log on to the client terminal
- Identification/authentication required to unlock a PC in the locked-out state due to the “user inactivity period” setting
- Changing a general user password

(Log Server)

- Identification/authentication required for the Administrator to view or search the log data stored in the log server

(3) Access Control

(Administrator terminal)

- Creation and change of the client control information

(Client)

- Reference of the client control information
- Implementation of the following functions based on the client control information:
  - Whether to enable or disable I/O ports and a printer
  - Execution of a general AP file and change of a file name
  - File output to the authorised external media
  - File input /output to the authorised USB device

(4) Encryption

(Administrator terminal)

- Creation of a key file to encrypt/decrypt a data file that is obtained or created by a general user who uses a client

(Client)

- Read or delete of a key to encrypt/decrypt a data file that is obtained or created by general users who use a client
- Encryption/decryption of a data file that is obtained or created by a general user who uses a client
- Encryption/decryption of a file to be output/input to or from an authorised external media

1.4.5. TOE assets

The TOE assets are the following TSF data and user data.

<TSF Data>

TSF data on administrator/client terminals include:

- Administrator ID
- Administrator password
- LogViewer startup control information
- Client control information (see Table 1-3)
- Log data

<User Data>

User data on client terminals include the following:

- General AP files
- Data created by the general AP file and managed on the client terminal

2. Conformance Claims

This chapter describes CC conformance claim, PP claim, Package claim and conformance rationale.

2.1. CC Conformance claim

The CC conformance claims of this ST are listed below:

Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and general model, September 2006, Ver.3.1, Japanese Version 1.2
Part 2: Security components, September 2006, Ver3.1, Japanese Version 1.2
Part 3: Security assurance components, September 2006, Ver.3.1, Japanese Version 1.2
CC Part 2 Conformance
CC Part 3 Conformance

2.2. PP claim

This ST conforms to no PPs.

2.3. Package claim

The Package conformance claims of this ST are listed below:

Package	EAL1 Augmented
Augmented Components	ASE_OBJ.2, ASE_REQ.2 and ASE_SPD.1

2.4. Conformance rationale

This ST has no PP conformance rationale since it does not claim any PP conformance.

3. Security Problem Definition

This chapter describes threats, organisational security policies and assumptions.

3.1. Threats

The consideration of threat agents associated with this TOE is as follows:
Of those personnel identified in Section 1.4.2, System Managers, corporate network managers and the Administrators are considered trusty persons, thus they will not attempt illegal use of the TOE. On the other hand, it seems unlikely that general users will maliciously attack the TOE in contrary to the Company rules and regulations, however, they might use the client terminals of other persons or attempt unauthorised client operations driven by way of experiment.
The administrator terminals are connected to the company LAN and used only in the Company premises. On the other hand, the client terminals and the external media may be used outside the Company premises. Those client terminals and external media taken out of the Company premises may be illegally used by those other than the NEC Group Company employees (hereafter called as “third parties”).

T.INJUSTICE_LOGON (injustice logon)
General users or third parties may masquerade as an authorised user of the TOE to modify or disclose user data or TSF data.

T.UNAUTHORISED_ACCESS (unauthorised operations)
General users may attempt unauthorised operations including, but not limited to, output to unauthorised printers, execution of unauthorised programs and use of unauthorised I/O ports to disclose the user data that is stored in the client terminals.

T.INJUSTICE_CONNECT (injustice equipment connections)
A third party may connect the external media or the client’s HDD to the unauthorised equipment to disclose the user data that is stored in the external media or the client’s HDD.

3.2. Organisational security policies

Organisational security policies are shown below:

P.LOG_COLLECT (log collection)
Log data collected by each administrator/ client terminal is stored on the central log server.

P.RESTRICTED_MEDIA (only authorised external media is allowed)

Only authorised external media can be used to write the data from the client terminal.

P.SECURITY_PARAMETER (appropriately configured security parameter settings)

The Administrator shall set the client control information to appropriate values based on the TOE guidance document.

3.3. Assumptions

Assumptions are shown below:

A.MANAGE_SAFE_PLACE (safe installation of administrator terminals)

The administrator terminals will be installed inside the Company building where only NEC Group employees and those who are authorised by them are granted entrance to the building.

A.FACILITIES_IN_SECURE_ROOM (equipment installation at a secure room)

The log servers and the associated log backup media will be installed or placed in rooms with physical entry controls.

A.UNJUST_SOFTWARE (countermeasures against unjust software)

Antivius software will be installed on all log servers (running the TOE) and administrator/client terminals. The pattern files of antivirus software and the security patches of the operating system that is part of the TOE components will be also applied appropriately.

A.PASSWORD_MANAGEMENT (password management)

The TOE users will keep their passwords for accessing the TOE confidential. They also will set non-guessable passwords and change them at appropriate intervals.

A.NETWORK (network environments)

The company LAN will be connected to external networks via a security equipment that prevents unauthorised communications from the external networks. The secure room network will be connected via security equipment that permits only the protocols necessary for communication with log servers and administrator/client terminals.

A.OPERATOR_MANAGEMENT (management of administrator)

The Administrator will be a trusty person who never attempts unauthorised operations.

A.LOG_BACKUP (log backup)

Countermeasures for prevention from loss of log data on the log servers will be taken.

A.PC_STARTUP_SET (PC startup control setting)

All PCs provided to general users will be configured not to start up in the maintenance mode.

4. Security Objectives

This chapter describes security objectives for the TOE, security objecives for the operational environment and security objectives rationale.

4.1. Security objectives for the TOE

The security objectives for the TOE are as follows:

O.I&A (user identification and authentication)

The TOE shall uniquely identify all users and will authenticate the claimed identify before granting access to the TOE. The TOE shall also grant the use of the TOE only to those users who succeeded in identification and authentication process within the defined number of login attempts.

O.RE_AUTH (reauthentication)

The TOE shall issue a reauthentication request when it is not accessed from the logged-on user for a given period of time. The TOE shall restrict the use of its functions other than an authentication function during the reauthentication.

O.ACCESS_CONTROL (access control)

The TOE shall control the operations to be executed by the process acting on behalf of a user in accordance with the configuration settings and the privileges assigned to those users.

O.AUDIT (audit)

The TOE shall provide the means of recording and protecting any TOE related security events as log information. The TOE shall also grant log reference only to the Administrator.

O.ACCESS_CONTROL_MEDIA (access control to the external media)

The TOE shall restrict general user’s writing to the external media.

O.CRYPTOGRAPHY (cryptography)

The TOE shall provide the means of encrypting user data when storing it on the external media or on the client terminal.

O.LOG_COLLECT (log collection)

The TOE shall ensure a secure transfer of the log information created by administrator/client terminals to the log server.

4.2. Security objectives for the operational environment

Security objectives for the operational environment are listed below:

OE.SECURITY_PARAMETER (appropriate security parameter setting)

The administrator shall set the client control information to appropriate values in accordance with the guidance document in order to ensure a secure TOE operation.

OE.MANAGE_PC_PLACE (safe installation of administrator terminals)

The administrator terminals shall be installed, managed and maintained in the facility with physical entry controls where only NEC Group employees and those granted by them can be accessed.

OE.FACILITIES_IN_SECURE_ROOM (equipment installation at a secure room)

The log servers shall be installed in a secure room with appropriate entry controls and placed in a rack with a locking mechanism to ensure that only the Administrator is allowed access.

The backup media containing log information shall be stored in a cabinet that is placed in a secure room with appropriate physical entry controls to ensure that only the Administrator is allowed access.

It is the Administrator’s responsibility that he or she closely supervises all behaviors of persons who have been granted access to these secure rooms.

OE.UNJUST_SOFTWARE (countermeasures against unjust software)

Users shall install antivirus software on all log servers and administrator/client terminals and keep all virus pattern files updated. They also shall appropriately apply the security patches of the operating system that is part of the TOE components.

OE.PASSWORD_MANAGEMENT (password management)

The TOE users shall memorize their passwords for accessing the TOE, and they shall not leak passwords to others.

The TOE users shall set hard-to-guess/analyze passwords and change their passwords at appropriate time intervals.

OE.NETWORK (network environments)

The Company-LAN shall be connected to external networks via an appropriately configured firewall. The local area network of a secure room shall also be connected to the Company-LAN via an appropriately configured firewall so that a log server can communicate with administrator/client terminals through the firewall.

OE.OPERATOR_MANAGEMENT (management of administrators)

The System Manager shall designate a trusty Administrator who is assumed not to commit injustices. The System Manager shall supervise the activities of these Administrators so that they will not commit injustices and lead them to operate the TOE appropriately.

OE.LOG_BACKUP (log backup)

Backup copies of log data stored on the log servers shall be taken regularly to avoid loss of log data.

OE.LOG_COLLECT (log collection)

All administrator and client log data shall be transferred to the corresponding log server regularly for central management.

OE.USERDATA_CRYPTOGRAPHY (user data cryptography)

When storing user data on the administrator/client terminals or the external media, each user shall keep it in a cryptographic folder or encrypt a folder.

OE.PC_STARTUP_SET (PC startup control setting)

The Administrator shall configure all PCs provided to general users not to start up in the maintenance mode.

4.3. Security objectives rationale

The security objectives are to counter the threats defined in the previous chapter or they are to realize the assumptions and the organisational security objectives of the TOE. The relation between the security objective and the threat to be countered, the corresponding organisational security policy and the assumption is shown in Table 4-1.

Table 4-1Relation between security objectives and the security problem definition

Threat / Organisational Security Policy / Assumption — Security Objectives of the TOE / Security Objectives of the Operational Environment	T.INJUSTICE_LOGON	T.UNAUTHORISED_ACCESS	T.INJUSTICE_CONNECT	P.LOG_COLLECT	P.RESTRICTED_MEDIA	P.SECURITY_PARAMETER	A.MANAGE_SAFE_PLACE	A.FACILITIES_IN_SECURE_ROOM	A.UNJUST_SOFTWARE	A.PASSWORD_MANAGEMENT	A.NETWORK	A.OPERATOR_MANAGEMENT	A.LOG_BACKUP	A.PC_STARTUP_SET
O.I&A	x													
O.RE_AUTH	x													
O.ACCESS_CONTROL		x												
O.AUDIT		x												
O.ACCESS_CONTROL_MEDIA					x									
O.CRYPTOGRAPHY			x											
O.LOG_COLLECT				x										
OE.SECURITY_PARAMETER						x								
OE.MANAGE_PC_PLACE							x							
OE.FACILITIES_IN_SECURE_ROOM								x						
OE.UNJUST_SOFTWARE									x					
OE.PASSWORD_MANAGEMENT										x				
OE.NETWORK											x			
OE.OPERATOR_MANAGEMENT												x		
OE.LOG_BACKUP													x	
OE.LOG_COLLECT				x										
OE.USERDATA_CRYPTOGRAPHY			x											
OE.PC_STARTUP_SET														x

As shown in Table 4-1, each security objective corresponds to one or more threats, organisational security policies and assumptions.

The following describes how each threat can be countered by the security objective and how each organisational security policy and assumption can be realized by the security objective.

[Threats]

This section provides a justification for the reasons why the security objective can counter all possible attacks pertaining to the following threats.

T.INJUSTICE_LOGON (injustice logon)

This threat refers to a situation where a general user or a third party masquerades as an authorised user to illegitimately use his or her administrator or client terminal. The effective

countermeasures to this threat are as follows:

(a) An unauthorised user masquerades as an authorised user.

For this type of attack, threat can be diminished by implementing user identification/authentication, and restricting the use of the TOE to authorised users only.

The security objective to counter this attack is O.I&A.

(b) A general user masquerades as an authorised user when an authorised user left his or her desk.

For this type of attack, the corresponding threat can be diminished by requesting a reauthentication when the TOE is not accessed for a given period of time and restricting the use of its functions other than an authentication function during the reauthentication.

The security objective to counter this attack is O.RE_AUTH.

To counter the T.INJUSTICE_LOGON, it is necessary to counter all the attacks (a) and (b). Thus, it is possible to counter the threat T.INJUSTICE_LOGON by implementing O.I&A and O.RE_AUTH that corresponds to the respective attack.

T.UNAUTHORISED_ACCESS (unauthorised operations)

This threat refers to a situation where unauthorised access is intentionally or accidentally attempted by a general user. The effective countermeasures to this threat are as follows:

(a) A general user attempts unauthorised access.

For this type of attack, the corresponding threat can be removed by defining user previleges for individual TOE operations including printer output, user program execution and I/O port input / output and by clarifying both permissible and prohibited operations.

The effective countermeasures to this attack are O.ACCESS_CONTROL.

In addition, recording all log data relating to user program execution with exact date and time will plant in user's subconscious mind the idea that all user operations are monitored thereby enabling the restraining unauthorised access (unauthorised user program execution) and diminishing a threat as a result. The security objective to counter this attack is O.AUDIT.

To counter T.UNAUTHORISED_ACCESS, it is necessary to counter the above attack (a). Thus, it is possible to counter T.UNAUTHORISED_ACCESS by implementing O.ACCESS _CONTROL and O.AUDIT that corresponds to the attack.

T.INJUSTICE_CONNECT (injustice equipment connection)

This threat refers to a situation where user data is disclosed by a third party due to theft or

loss of the external media or client terminals. The effective countermeasures to this attack are as follows:

(a) A third party obtains the external media and may disclose the user data stored in that media.

For this type of attack, the corresponding threat can be diminished by encypting the user data stored in the external media and allowing only authorised users to decrypt that user data. The security objective to counter this attack is O.CRYPTOGRAPHY.

(b) A third party obtains a client terminal and discloses the user data stored in that terminal.

For this type of attack, the corresponding threat can be diminished by encrypting the user data stored in the client terminal and allowing only authorised users to decrypt that user data. The security objective to counter this attack is O.CRYPTOGRAPHY and OE.USERDATA_CRYPTOGRAPHY.

To counter T.INJUSTICE_CONNECT, it is necessary to counter the attacks (a) and (b). Thus, it is possible to counter T.INJUSTICE_CONNECT by implementing O.CRYPTO GRAPHY and OE.USERDATA_CRYPTOGRAPHY that corresponds to the respective attack.

[Organizational security policies (OSPs)]

P.LOG_COLLECT (log collection)

This organisational security policy addresses the log servers that store log information. The effective security objectives include:

a. Secure log collection by log server

Log data created by administrator/client terminals is encrypted and collected at the associated log server’s log database. The TOE security objective that meets this policy is O.LOG_COLLECT.

b. Regular log collection by log server

Log data created by administrator/client terminals is collected at the associated log server’s log database for centralized management by the Administrator. The TOE security objective that meets this policy is OE.LOG_COLLECT.

To meet P.LOG_COLLECT, it is necessary to meet O.LOG_COLLECT and OE.LOG_COLLECT. Thus, the P.LOG_COLLECT can be realized by achieving O.LOG_COLLECT and OE.LOG_ COLLECT as security countermeasures that meet the respective requirements.

P.RESTRICTED_MEDIA (only authorised external media is allowed)
This organisational security policy permits the use of only authorised external media. The effective security objectives include:
a. Write restriction to the authorised external media
Restricting write access by a general user only to authorised external media can restrict available external media only to authorised external media. The TOE security objective that meets this policy is O.ACCESS_CONTROL_MEDIA.

To meet P.RESTRICTED_MEDIA, it is necessary to meet O.ACCESS_CONTROL_MEDIA. Thus, P.RESTRICTED_MEDIA can be realized by achieving O.ACCESS_CONTROL_ MEDIA as security countermeasures that meet the requirement.

P.SECURITY_PARAMETER (appropriate security parameter setting)
This organisational security policy addresses security parameters configured by the Administrator. Effective security objectives include:
a. Secure variable setting
To ensure secure TOE operation, the Administrator shall set each client control information parameter to an appropriate value as described in the guidance document. The security objective for the operational environment that meest this policy is OE.SECURITY_PARAMETER.

To meet P.SECURITY_PARAMETER, it is necessary to meet OE.SECURITY_PARAMETER. Thus, P.SECURITY_PARAMETER can be realized by achieving the OE.SECURITY_ PARAMETER as security countermeasures that meet the requirement.

[Assumptions]

A.MANAGE_SAFE_PLACE (safe installation of administrator terminals)
This assumption addresses the TOE related hardware (Administrator terminals) installation. Effective security objectives include:
a. Restricting places where Administrator terminals are installed
The administrator terminals that provide the functionality to create, distribute and manage the key to encrypt/decrypt a user data file and also create the client control information shall be installed inside the building where only NEC Group employees and persons authorised by them are allowed access. The security objective for the operational envrionment that

meet this policy is OE.MANAGE_PC_PLACE.

To meet A. MANAGE_SAFE_PLACE, it is necessary to meet OE.MANAGE_PC_PLACE. Thus, A. MANAGE_SAFE_PLACE can be realized by achieving OE.MANAGE_PC_PLACE as security countermeasures that meet the requirement.

A.FACILITIES_IN_SECURE_ROOM (equipment installation at a secure room)

This assumption addresses the TOE related hardware (log servers) installation. Effective security objectives include:

a. Restricting rooms where equipments storing log data are installed

All the hardware storing log data (log servers) shall be installed at rooms where only the Administrator and persons authorised by the Administrator are allowed access. The log server and the log backup media shall be placed on a rack or cabinet in a secure room to which only the Administrator is allowed access. The security objective for the operational environment that meets this policy is OE.FACILITIES_IN_SECURE_ROOM.

b. Restricting persons allowed to access secure rooms

Persons allowed to access secure rooms shall be restricted only to the Administrator and persons authorised by the Administrator. The security objective for the operational environment that meets this policy is OE.FACILITIES_IN_SECURE_ROOM.

To meet A.FACILITIES_IN_SECURE_ROOM, it is necessary to meet both requirements (a) and (b). Thus, A.FACILITIES_IN_SECURE_ROOM can be realized by achieving OE. FACILITIES _IN_SECURE_ROOM as security countermeasures that meet respective requirements.

A.UNJUST_SOFTWARE (countermeasures against unjust software)

This assumption addresses antivirus and security patch software. Effective security objectives include:

a. Introducing antivirus software to the TOE related hardware

Antivirus software shall be introduced to the TOE related hardware (log servers and administrator/client terminals). The security objective for the operational environment that meets this policy is OE.UNJUST_SOFTWARE.

b. Applying pattern files and security patch software appropriately

The most recent pattern files of antivirus software and security patch software shall be applied. The security objective for the operational environment that meets this policy is

OE.UNJUST_SOFTWARE.

To meet A.UNJUST_SOFTWARE, it is necessary to meet both requirements (a) and (b). Thus, A.UNJUST_SOFTWARE can be realized by achieving the corresponding OE.UNJUST_SOFTWARE as security countermeasures that meet respective requirements.

A.PASSWORD_MANAGEMENT (password management)

This assumption addresses passwords managed by the Administrator, the client administrator and the general users. Effective security objectives include:

a. Managing passwords appropriately

All Administrators, client administrators and general users shall guard their passwords for accessing the TOE. The security objective for the operational environment that meets this policy is OE.PASSWORD_MANAGEMENT.

b. Changing passwords regularly

All Administrators, client administrators and general users shall change their passwords for accessing the TOE at regular time intervals. The security objective for the operational environment that meets this policy is OE.PASSWORD_MANAGEMENT.

To meet A.PASSWORD_MANAGEMENT, it is necessary to meet both requirements (a) and (b). Thus, A.PASSWORD_MANAGEMENT can be realized by achieving the corresponding OE.PASSWORD_MANAGEMENT to meet respective requirements.

A.NETWORK (network environments)

This assumption addresses establishing the network environments. Effective security objectives include:

a. Restricting a connection between the Company LAN and external networks

The Company LAN shall be connected to external networks via a firewall to prevent unjust communications from external networks. The security objective for the operational environment to meet this policy is OE.NETWORK.

b. Restricting the connection to a secure room network

The network of a secure room where the TOE (log server) is installed shall be connected to the Company LAN via an appropriately configured firewall to allow the connection between a log server and administrator/client terminals. The security objective for the operational environment that meets this policy is OE.NETWORK.

To meet A.NETWORK, it is necessary to meet both requirements (a) and (b). Thus, A.NETWORK can be realized by achieving the corresponding OE.NETWORK as security countermeasures that meet respective requirements.

A.OPERATOR_MANAGEMENT (management of administrators)

This assumption addresses the designation of the Administrator. Effective security objectives include:

a. Designating a trusty person

The Administrator shall be designated from the Company employees by the System Manager. The Administrator shall be those who well understand his or her roles and responsibilities, faithful to his or her mission, and never attempt malicious actions. The security objective for the operational environment that meets this policy is OE.OPERATOR_MANAGEMENT.

b. System Manager's supervision

The System Manager shall have the Administrator report the daily activities to prevent fraud and receive training in TOE operation skills. The security objective for the operational environment that meets this policy is OE.OPERATOR_MANAGEMENT.

To meet A.OPERATOR_MANAGEMENT, it is necessary to meet both requirements (a) and (b). Thus, A.OPERATOR_MANAGEMENT can be realized by achieving the corresponding OE.OPERATOR_MANAGEMENT as security countermeasures to counter the respective requirements.

A.LOG_BACKUP (log backup)

This assumption addresses the management of a log server that stores log data. Effective security objectives include:

a. Protecting log data stored in the database

Log data on the log server shall be backed up regularly to prevent against data loss. The security objective for the operational environment to counter this policy is OE.LOG_BACKUP.

To counter A.LOG_BACKUP, it is necessary to meet the requirement (a). Thus, A.LOG_BACKUP can be realized by achieving the corresponding OE.LOG_BACKUP as security measures to counter the requirement.

A.PC_STARTUP_SET (PC startup control setting)

This assumption addresses the PC startup setting. Effective security objectives include:

a. PC startup control setting

Before providing a PC to each general user, the Administrator shall configure it not to startup in the maintenance mode. The security objective for the operational environment to counter this policy is OE.PC_STARTUP_SET.

To counter A.PC_STARTUP_SET, it is necessary to counter the above requirement. Thus, A.PC_STARTUP_SET can be realized by achieving the corresponding OE.PC_STARTUP _SET as security meansures to counter the requirement.

5. Extended Components Definition

5.1. Extended components Definition

This ST does not define extended components as it complies with CC Part 2 and CC Part 3.

6. Security Requirements

This chapter describes security functional requirements, security assurance requirements and security requirement rationale.

Terms and definitions used in this chapter are as follows:

<Subject>

Subject	Definition
Administrator process	A process acting on behalf of the Administrator
General user process	A process acting on behalf of the general user

<Object>	Definition
I/O port	Client's I/O port used for data input / output based on client control information
Cryptographic key file to be exported	A file containing a common key (to encrypt/decrypt files) to be exported from the administrator terminal
Cyptographic key file to be imported	A file containing a common key (to encrypt/decrypt files) to be imported to a client
Encryption key file	A file for storing the common key data to encrypt / decrypt a file on a client machine
General AP file	A program file whose execution is controlled on a client machine based on the client control information

<Operation>

Operation	Definition
Input / output	File output to an I/O port or file input from the I/O port
Execution/chane file names	Execution of a general AP file on a client machine and change of file name
Read/write	Writing data to an exported encryption file, reading an imported encryption key file and writing a encryption key file

<Security Attributes>

Security Attribute Name	Attributes	Parameters
I/O control information	Information to determine whether to permit the use of USB ports, IEEE1394 ports, serial/parallel ports, infrared ports and PCMCIA ports	Enable and disable
Printer control information	Information to specify usage range of a printer	Partial allow, all allow and all deny
Authorised printer information	Information to uniquely specify a printer	Driver name, port name, server name, printer name, URL and IP address
Authorised USB device input / output control information	Information to determine whether to permit the use of an authorised USB device	Maker ID, product ID and serial number

Security Attribute Name	Attributes	Parameters
External media output control information	Information to specify usage range of an external media	Only authorised external media is allowed, all external media is denied and all external media is allowed
Authorised external media input / output control information	Information to determine whether to permit the use of authorised external media	Group name and keyword
Port name	Name of a port that controls data input / output based on client control information	USB port, IEEE1394 port, serial/parallel port, infrared port, PCMCIA port and printer port
Prohibited user program information	Information to specify the name of a program that is prohibited from startup	Any character strings that represent a program name
File name	Name of a program file	A character string consisting of 255 or less characters
Administrator ID	ID assigned to the Administrator	A character string consisting of 1 to 127 characters
General user ID	ID assigned to the general user	A character string consisting of 1 to 127 characters
User ID	Generic name of Administrator ID and general user ID	A character string consisting of 1 to 127 characters
Cryptographic key input control information	Information to read a common key for file cryptography	Alpha-numeric characters consisting of 8 to 32 characters

<Other terms>

Terms	Attributes
Event ID	The number to identify audit records
Type of event	A classification of audit records: Error, Warning and Information
Category	A classification of audit records, which the Administrator can use as a keyword when searching audit records.
Common key for authorised external media	A cryptographic key data used to encrypt a file when writing it to the authorised external media or to decrypt a file when reading it from the authorised external media.
Common key to crypt/decrypt a file	A cryptographic key data used to encrypt/ decrypt user data
Maximum permissible number of consecutive authentication failures	Maximum number of consecutive authentication failures without causing a PC lockout in the process of authenticating administrator/client terminals. When this threshold is exceeded, the associated PC is locked out for a predetermined periof of time.
Consecutive failed authentication attemps counter	A counter that retains the information on number of consecutive authentication failures during the authentication of administrator/client terminals.
User inactivity period before reauthentication is required	Time from when a logged-on user attempts his or her last access to the TOE till when the TOE requests a reauthentication to that user
Message	Details of events stored in the audit record

6.1. Security functional requirements

All security functional requirement components given in CC Part 2 are used directly.

Security Audit (FAU)

FAU_GEN.1 Audit data generation
Hierarchical to: No other components
Dependencies: FPT_STM.1 Reliable time stamps

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

- Startup and shutdown of the audit functions;
- All auditable events for the [selection, choose one of: minimum, basic, detailed, not specified] level of audit; and
- [assignment: other specifically defined auditable events].

[Selection, choose one of: minimum, basic, detailed, not specified]: not specified
[Assignment: other specifically defined auditable events]: see Table 6-1.

Table 6-1 other specifically defined auditable events

Functional Requirements	Auditable Events
FDP_ACF.1a	• Success or failure in writing to the external media
FDP_ACF.1b	• Success or failure in starting a program file • Failure in changing program file name
FIA_AFL.1	• Attainment of a threshold value of the consecutive failed authentication attempts counter and a subsequent action to be taken (PC lockout for a certain defined period)
FIA_UAU.2	• Success or failure in user identification and authentication
FIA_UAU.6	• Success or failure in user identification and authentication
FIA_UID.2	• Success or failure in user identification and authentication
FMT_MTD.1	• Success or failure in user ID registration, update or delete • Success or failure in user password registration or update

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

- Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST,
- [Assignment: other audit relevant information].

[Assignment: other audit relevant information]:

- Event ID
- Category (that shows the classification of log category)

- PC name
- IP address
- MAC address

FAU_GEN.2 User Identity Association
Hierarchical to: No other components
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

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

FAU_SAR.1 Audit review
Hierarchical to: No other components
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [assignment: authorised users] with the capability to read [assignment: list of audit information] from the audit records.

[Assignment: authorised users]: the Administrator who entered LogViewer start-up control information

[Assignment: list of audit information]:
{date and time of the event, type of event, subject identity, the outcome of the event, event ID,Category, PC name, IP address and MAC address}

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

FAU_SAR.2 Restricted audit review
Hieararchical to: No other components
Dependencies: FAU_SAR.1 Audit review

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

[Refinement]:Users that have been granted access → Administrators that have been granted access

FAU_SAR.3 Selectable audit review
Hieararchical to: No other components
Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform [selection: searches, sorting, ordering] of audit data based on [assignment: criteria with logical relations].

[Assignment: criteria with logical relations]: the following criteria can be specified for searching.

- Period / time of day
- User ID

- PC name
- IP address
- MAC address
- Type of event
- Category
- Event ID

[Selection: searching, sorting, ordering]: searching

FAU_STG.1 Protected audit trail storage
Hiearchical to: No other components
Dependencies: FAU_GEN.1 Audit data generation

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

FAU_STG.1.2 The TSF shall be able to [selection: choose one of: prevent, detect] unauthorised modifications to the stored audit records in the audit trail.

[Selection: choose one of: prevent, detect]: prevent

FAU_STG.3 Action in case of possible audit data loss
Hiearchical to: No other components
Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [assignment: actions to be taken in case of possible audit storage failure] if the audit trail exceeds [assignment: pre-defined limit].

[Assignment: pre-defined limit]: an alarming size of audit trail that is configured in the client control information by the Administrator.

[Assignment: action in case of possible audit storage failure]: the TOE shall issue a notification to the associated Administrator and the general user.

FAU_STG.4 Prevention of audit data loss
Hiearchical to: FAU_STG.3 Action in case of possible audit data loss
Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [selection, choose one of: “ignore auditable events”, “prevent auditable events, except those taken by the authorised user with special rights”, “overwrite the oldest stored audit reports”] and [assignment: other actions to be taken in case of audit storage failure] if the audit trail is full.

[selection, choose one of: “ignore auditable events”, “prevent auditable events, except those taken by the authorised user with special rights”, “overwrite the oldest stored audit records”] : overwrite the oldest stored audit records

[assignment: other actions to be taken in case of audit storage failure] : None

Cryptographic support (FCS)

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components

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

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

[assignment: list of standards] : See “Standard” in Table 6-2.

[assignment: cryptographic key generation algorithm] : See “Cryptographic key generation algorithm” in Table 6-1.

[assignment: cryptographic key sizes] : See “Cryptographic key sizes” in Table 6-2.

Table 6-2 List of standards for cryptographic key generation, cryptographic key generation algorithm and cryptographiz key sizes

Type of Key	Standard	Cryptographic key generation algorithm	Cryptographic key sizes
Common key for authorised external media	FIPS PUB 197	AES	128bit
Common key for file cryptography	FIPS PUB 46-3	3DES	168bit
	FIPS PUB 197	AES	128/192/256bit

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components

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

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

[assignment: list of standards] : None

[assignment: cryptographic key destruction method] : Manual destruction

FCS_COP.1 Cryptographic operation
Hierarchical to: No other components
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

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

The above assignments are shown in Table 6-3.

[assignment: list of standards] : See “Standards” in Table 6-3.

[assignment: cryptographic algorithm] : See “Cryptographic algorithm” in Table 6-3.

[assignment: cryptographic key sizes] : See “Cryptographic key sizes” in Table 6-3.

[assignment: list of cryptographic operations] : See “Cryptographic operations” in Table 6-3.

Table 6-3 List of standards for cryptographic operations, cryptographic algorithm, cryptographic key sizes and cryptographic operations

Type of key	Standards	Cryptographic algorithm	Cryptographic key sizes	Cryptographic operations
Common key for authorised external media	FIPS PUB 197	AES	128bit	Encryption for writing or decryp -tion for reading files to or from the authorised external media
Common key for file cryptography	FIPS PUB 46-3	3DES	168bit	Encryption/decryption of user data
	FIPS PUB 197	AES	128/192/256bit	

User Data Protection (FDP)

FDP_ACC.1a Subset access control (Input / output control of I/O ports)
Hierarchical to: No other components
Dependencies: FDP_ACF.1 Security attribute based access control

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

[assignment: access control SFP]: External input / output access control policy

[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP] : See below.

<Subject>
- General user process

<Object>
- I/O ports

<operations among subjects and objects covered by the SFP>

See Table 6-4.

Table 6-4 Operations among subjects and objects coverd by the SFP

Subjects	Objects	Operations
general user process	I/O ports	Input / output

FDP_ACC.1b Subset access control (Operation control of program files)

Hierarchical to: No other components
Dependencies: FDP_ACF.1 Security attribute based access control

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

[assignment: access control SFP]: Program file access control policy

[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP] : See below .

<Subject>
- General user process

<Object>
- General AP files

<operations among subjects and objects covered by the SFP>

See Table 6-5.

Table 6-5 Operations among subjects and objects covered by the SFP

Subject	Object	Operations
general user process	general AP files	execution and change of file names

FDP_ACC.1c Subset access control (Input / output control of cryptographic key files)

Hierarchical to: No other components
Dependencies: FDP_ACF.1 Security attribute based access control

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

[assignment: access control SFP] : Cryptographic key file input / output control policy

[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]: See below.

<Subjects>
- Administrator process
- General user process

<Objects>
- Cryptographic key file to be exported
- Cryptographic key file to be imported
- Cryptographic key file

<operations among subjects and objects covered by the SFP>

See Table 6-6.

Table 6-6 Operations among subjects and objects covered by the SFP

Subject	Object	Operations
Administrator process	Export cryptographic key files	Write
General user process	Import cryptographic key files	Read
General user process	Cryptographic key files	Write

FDP_ACF.1a Security attributes based access control (input / output control of I/O ports)

Hierarchical to: No other components
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

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

[assignment: access control SFP] : External input / output access control policy

[assignment: list of subjects and objects controlled under the indicatel SFP, and for each, the SFP-relavant security attributes, or named groups of SFP-relevant security attributes] : See the following tables.

<subjects controlled under the indicatel SFP, and for each, the SFP-relavant security attributes>: See Table 6-7.

Table 6-7 Subjects and SFP-relevant security attributes corresponding to each subject

Controlled subjects	SFP-relevant security attributes corresponding to each subject
General user process	• I/O port control information • Printer control information • Authorised printer information • Authorised USB device input / output control information • External media output control information • Authorised external media input / output control information

<objects controlled under the indicatel SFP, and for each, the SFP-relavant security attributes>

See Table 6-8.

Table 6-8 Objects and SFP-relevant security attributes corresponding to each subject

Controlled objects	SFP-relevant security attributes corresponding to each object
I/O port	Port name

FDP_ACF.1.2a The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects] : See Table 6-9.

Table 6-9 Rules governing access

Subject	Object	Operations	Rules
General user process	I/O port	Input / output	• The general user process executes input / output operation on the I/O port when the I/O port control information is set to “enable”. • The general user process does not execute input / output operation on the I/O when the I/O port control information is set to “disable”. • The general user process excutes input / output operation on the I/O supporting a USB interface when the authorised USB device input / output control information matches the connected USB device information. • The general user process does not excute input / output operation on the I/O port supporting a USB interface when the authorised USB device input / output control information does not match the connected USB device information. • The general user process executes input / output operation on the specified I/O port supporting an external media when the external media output control information is set to “available only for authorised external media”. • The general user process executes input / output operation on the I/O port available for all external media when the external media output control information is set to “all external media are allowed”. • The general user process does not execute input / output operation on the I/O port supporting an external media when the external media output control information is set to “use of all external media are prohibited”. • The general user process executes input / output operation on the I/O port supporting an external media when the authorised external media input / output control information matches the connected external media information. • The general user process does not execute input / output operation on the I/O port supporting an external media when the authorised external media

Subject	Object	Operations	Rules
			input / output control information does not match the connected external media information.
		Output	• The general user process executes input / output operation on the I/O port specified in the authorised printer information when the printer control information is set to “partially allowed”. • The general user process executes output operation on the I/O port when the printer control information is set to “all allowed”. • The general user process does not execute output operation on the I/O port when the printer control information is set to “all prohibited”.

The controlled subjects shown in Table 6-9 are allowed to execute only controlled operations on the controlled objects.

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

[assignment: rules, based on security attributes, that explicitly authorise access of subject to objects] : None

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

[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]: None

FDP_ACF.1b Security attribute based access control (program file operation control)
Hierarchical to: No other components
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

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

[assignment: access control SFP]: Program file access control policy

[assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]:

See the following tables.

<subjects controlled under the indicated SFP, and for each, the SFP-relevant security attributes>

See Table 6-10.

Table 6-10 Subjects, and for each, the SFP-relevant security attributes

Controlled subjects	SFP-relevant security attributes
General user process	Prohibited user program information

<objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes>

See Table 6-11.

Table 6-11 Objects, and for each, the SFP-relevant security attributes

Controlled objects	SFP-relevant security attributes
General AP files	File name

FDP_ACF.1.2b The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects] : See Table 6-12.

Table 6-12 Rules governing access

Subjects	Objects	Operations	Rules
General user process	General AP file	Execution, change file names	The general user process does not execute a general AP file with a file name specified in the prohibited user program or change that file name.

The controlled subjects shown in Table 6-12 are allowed to perform only controlled operations to controlled objects.

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

[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects] : None

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

[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects] : None

FDP_ACF.1c Security attribute based access control (input / output control of cryptographic key files)
Hierarchical to: No other components
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

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

[assignment: access control SFP] : Cryptographic key file input / output control policy

[assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]: See the following tables.

<subjects controlled under the indicated SFP, and for each, the SFP-relevant security attributes>

See Table 6-13

Table 6-13 Subjects, and for each, the SFP-relevant security attributes

Controlled subjects	SFP-relevant security attributes
Administrator process	None
General User process	None

<objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes>

See Table 6-14.

Table 6-14 Objects, and for each, the SFP-relevant security attributes

Controlled objects	SFP-relevant security attributes
Cryptographic key file to be exported	None
Cryptographic key file to be imported	None
Cryptographic key file	Cryptographic key input control information

Access control to those objects shown in Table 6-14 shall be enforced only based on the security attribute “Cryptographic key input control information”.

FDP_ACF.1.2c The TSF shall enfoce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects] : See Table Table 6-15.

Table 6-15 Rules governing access

Subjects	Objects	Operations	Rules
administrator Process	Exported cryptographic key files	Write	The administrator process writes the common key data to encrypt files and the cryptographic key input control information.
General User Process	Imported cryptographic key files	Read	The general user process reads the cryptographic key input control information.
	Cryptographic key files	Write	The general user process writes the common key data to encrypt a file when it accepts the input of cryptographic key input control information contained in the common key data to encrypt a file.

The controlled subject shown in Table 6-15 is allowed to execute only controlled operations to the controlled objects.

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

[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects] : None

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

[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects] : None

FDP_ETC.2 Export of user data with security attributes (export of a common key to encrypt files)

Hierarchical to: No other components
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ETC.2.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] when exporting user data, controlled under the SFP(s), outside of the TOE.

[assignment: *access control SFP(s) and/or information flow control SFP(s)*] : Cryptographic key file input / output control policy

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the

TOE, are unambigously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE: [assignment: *additional exportation control rules*].

[assignment: *additional exportation control rules*] : Add the cryptographic key input control information to the common key to encrypt a file.

FDP_ITC.2 l Import of user data with security attributes (import of a common key to encrypt files)

Hierarchical to: No other components
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1Trusted path]
FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_ITC.2.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] when importing user data, controlled under the SFP, from outside of the TOE.

[assignment: *access control SFP(s) and/or information flow control SFP(s)*] : Cryptographic key file input / output control policy

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: additional importation control rules].

[assignment: *additional importation control rules*] : Add the cryptographic key input control information to the common key to encrypt files

Identification and Authentication (FIA)

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

[selection: *[assignment: positive integer number], an administrator configurable positive*

integer within [assignment: range of acceptable values]] : positive integer value in the range of 1 through 99 that can be defined by the Administrator

[refinement]: unsuccessful authentication attemps → consecutive unsuccessful authentication attempts after the last successful authentication

[assignment: *list of authentication events*] :
- Authentication of the Administrator after the last successful authentication
- Authentication of the general user after the last successful authentication

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

[assignment: *list of actions*] : See Table 6-16.

Table 6-16 List of actions at authentication failure

Authentication Events	Actions
Authentication of the Administrator	The TOE will lockout a PC for a random period of 180 to 210 seconds and then set a value of the consecutive unsuccessful authentication attemps counter to 0.
Authentication of a general user	The TOE will lockout a PC for a random period of 180 to 210 seconds and then set a value of the consecutive unsuccessful authentication attemps counter to 0.

FIA_ATD.1 User attribute definition
Hierarchical to: No other components
Dependencies: No dependencies

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

[assignment: *list of security attributes*] : I/O port control information, printer control information, authorised printer information, authorised USB device input / output control information, external media output control information, prohibited user program information, authorised external media input / output control information and user ID

FIA_SOS.1 Verification of secrets
Hiearchical to: No other components
Dependencies: No dependencies

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

[assignment: *a defined quality metric*] : See Table 6-17.

Table 6-172 List of defined quality metric

Secret Information	Quality Metric
Administrator / general user password	• ASCII characters including: - 26 alphabetical uppercase characters [A through Z] and 26 lowercase characters (a through g), total 52 characters. - 10 numeric characters [0 through 9] - 32 symbols [!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~] • Maximum password length defined by the Administrator • Maximum password age defined by the Administrator
Cryptographic key input control information	• ASCII characters including: - 26 alphabetical uppercase characters [A through Z] and 26 lowercase characters (a through g), total 52 characters. - 10 numeric characters [0 through 9] - 32 symbols [!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~] • Number of digits must be within 8 through 32
LogViewer startup control information	• ASCII characters including: - 26 alphabetical uppercase characters [A through Z] and 26 lowercase characters (a through g), total 52 characters. - 10 numeric characters [0 through 9] - 32 symbols [!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~] • Number of digits must be within 8 through 127

FIA_UAU.2 User authentication before any action (Administrators, client administrators and general users)
Hiearchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1a The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user user.

[Refinement]: User → Administrator, client administrator and general user

FIA_UAU.6 Re-authenticating
Hierarchical to: No other components
Dependencies: No dependencies

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

[Refiment]: User → Administrator and general user

[assignment: *list of conditions under which re-authentication is required*] :
• A threshold value of user inactivity period before reauthentication is required defined by the Administrator is exceeded.

FIA_UAU.7 Protected authentication feedback
Hierarchical to: No other components
Dependencies: FIA_UAU.1 Timing of authentication

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

the authentication is in progress.

[assignment: *list of feedback*] :
・Dummy characters (* or ●) equivalewt to the number of input characters are displayed.

FIA_UID.2 User identification before any action (Administrators, Client Administrators and General Users)
Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies

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

[Refiment]: User → Administrator, client administrator and general user

FIA_USB.1 User-subject binding
Hieararchical to: No other components
Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user user: [assignment: list of user security attributes].

[assignment: list of user security attributes] : I/O port control information, printer control information, authorised printer information, authorised USB device input / output control information, external media output control information, authorised external media input / output control information, prohibited user program information and user ID

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: [assignment: *rules for the initial association of attributes*].

[assignment: *rules for the initial association of attributes*] : None

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: [assignment: *rules for the changing of attributes*].

[assignment: *rules for the changing of attributes*] : None

Security Management (FMT)

FMT_MSA.1a Management of security attributes (input / output control of I/O ports)
Hierarchical to: No other components
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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

identified roles].

[Assignment: *access control SFP, information flow control SFP*]: External input / output access control policies

[Selection: *change_default, query, modify, delete, [assignment: other operations]*]: See the “Operations” column on Table 6-18.

[Assignment: *list of security attributes*]: See the “Security Attributes” column on Table 6-18.

[Assignment: *the authorised identified roles*]: See the “Roles” column on Table 6-18.

Table 6-18 Management of Security Attributes (Input / output control of I/O ports)

Security Attributes	Operations	Roles
I/O port control information	Modify	Administrator
Printer control information	Modify	Administrator
	Query	Client administrator
	Query	General user
Authorised USB device input / outputcontrol information	Modify	Administrator
Authorised printer information	Modify	Administrator
	Query	Client administrator
	Query	General user
External media output control information	Modify	Administrator
	Query	Client administrator
	Query	General user
Authorised external media input / output control information	Modify	Administrator

FMT_MSA.1b Management of Security Attributes (Operational Control of Program Files)

Hierarchical to: No other components

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

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

[Assignment: *access control SFP, information flow control SFP*]: Program file access control policy

[Selection: *change_default, query, modify, delete, [assignment: other operations]*]: See the “Operations” column on Table 6-19.

[Assignment: *list of security attributes*]: See the “Security Attributes” column on Table

6-19.

[Assignment: *the authorised identified roles*]: See the “Roles” column on Table 6-19.

Table 6-19 Management Security Attributes (Operational Control of Program Files)

Security Attribute	Operation	Role
Prohibited user program information	Modify	Administrator
	Query	Client administrator
	Query	General user

FMT_MSA.1c Management of Security Attributes (Input / output cryptographical key files)

Hierarchical to: No other components
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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

[Assignment: *access control SFP, information flow control SFP*]: Cryptographic key file input / output control policy

[Selection: *change_default, query, modify, delete, [assignment: other operations]*]: See the “Operations” column on Table 6-20.

[Assignment: *list of security attributes*]: See the “Security Attributes” column on Table 6-20.

[Assignment: *the authorised identified roles*]: See the “Roles” column on Table 6-20.

Table 6-20 Management of Security Attributes (Input / output control of cryptographical key files)

Security Attributes	Operations	Roles
Cryptographical key input control information	Generation	Administrator

FMT_MSA.3a Static Attribute Initialisation (input / output control of I/O ports)

Hierarchical to: No other components
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

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

[Assignment: *access control SFP, information flow control SFP*]: External input / output access control policy

[Selection, *choose one of: restrictive, permissive, [assignment: other property]*]: restrictive

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

[Assignment: *the authorised identified roles*]: Administrator

FMT_MSA.3b Static Attribute Initialisation (operational control of program files)
Hierarchical to: No other components
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

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

[Assignment: *access control SFP, information flow control SFP*]: Program file access control policy

[Selection, choose one of: *restrictive, permissive, [assignment: other property]*]: restrictive

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

[Assignment: *the authorised identified roles*]: Administrator

FMT_MSA.3c Static Attribute Initialisation (Input / output control of cryptographic key files)
Hierarchical to: No other components
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

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

[Assignment: *access control SFP, information flow control SFP*]: Cryptographic key file input / output control policies

[Selection, choose one of: *restrictive, permissive, [assignment: other property]*]: restrictive

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

[Assignment: *the authorised identified roles*]: Administrator

FMT_MTD.1 Management of TSF Data
Hierarchical to: No other components
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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

[Selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]: See the “Operations” column in Table 6-21.

[Assignment: *list of TSF data*]: See the “TSF Data” column in Table 6-21.

[Assignment: *the quthorised identified roles*]: See the “Roles” column in Table 6-21.

Table 6-21 Management of TSF Data

TSF Data	Operations	Roles
Administrator ID	Registration, Query	Administrator
General user ID	Registration, Query	Administrator
	Query	Client administrator
	Query	General user
Administrator password	Registration, Modify	Administrator
Client administrator password	Registration	Administrator
	Modify	Client administrator
General user password	Registration	Administrator
	Modify	client administrator
	Modify	general user
Maximum password length	Modify	Administrator
Maximum password age	Modify	Administrator
Warning size of audit trail storage	Modify	Administrator
Maximum permissible numberof consecutive authentication failures	Modify	Administrator
User inactivity period before reauthentication is required	Modify	Administrator
LogViewer startup control information	Modify	Administrator

FMT_SMF.1 Specification of Management functions
Hierarchical to: No other components
Dependencies: None

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

[Assignment: *list of management functions to be provided by the TSF*]: See Table 6-22.

Table 6-22 List of management functions to be provided by the TSF

Functional Requirements	Management Requirements Stipulated in CC Part 2	Management Item
FAU_GEN.1	• None	• None
FAU_GEN.2	• None	• None
FAU_SAR.1	• Maintenance of user groups with read privileges to the audit record (delete, modify and add)	• LogViewer startup control information
FAU_SAR.2	• None	• None
FAU_SAR.3	• None	• None
FAU_STG.1	• None	• None
FAU_STG.3	• Maintenance of thresholds • Maintenance of actions to be taken when failure of audit storage is imminent (delete, modify and add)	• Warning size of audit trail storage • None (actions are fixed. They are excluded from the targets of management)
FAU_STG.4	• Maintenance of actions to be taken when failure of audit storage is imminent (delete, modify and add)	• None
FCS_CKM.1	• Change management of cryptographic key attributes. Examples of key attributes include type of key (public, private and common), validity and application (digital signature, key cryptography, key exchange and data cryptography)	• None (fixed)
FCS_CKM.4	• Change management of cryptographic key attributes. Examples of key attributes include type of key (public, private and common), validity and application (digital signature, key cryptography, key exchange and data cryptography)	• None (fixed)
FCS_COP.1	• None	• None
FDP_ACC.1a	• None	• None
FDP_ACC.1b	• None	• None
FDP_ACC.1c	• None	• None
FDP_ACF.1a	• Management of attributes used to explicit access or deny control	• Security attributes including: - I/O port control information - Printer control information - Authorised printer information - Authorised USB device input / output control information - External media output control information - Authorised external media input / output control information - Port name
FDP_ACF.1b	• Management of attributes used to explicit access or deny control	• Security attributes including: - Prohibited user program - File name
FDP_ACF.1c	• Management of attributes used to explicit access or deny control	• Security attributes including: - Cryptographic key input control information

Functional Requirements	Management Requirements Stipulated in CC Part 2	Management Item
FDP_ETC.2	• Additional export control rules can be defined by a user with defined roles.	• Cryptographic key input control information
FDP_ITC.2	• Modification of additional control rules applied for import	• None (fixed)
FIA_AFL.1	• Management of a threshold value of unsuccessful authentication attempts • Management of actions to be taken in the event of an authentication failure	• Maximum permissible number of authentication failures • None (actions are fixed)
FIA_ATD.1	• If included in the assignment, an authorised administrator can define additional security attributes to users.	• None
FIA_SOS.1	• Management of metric used in verification of secrets	• Maximum user password length • Maximum user password age
FIA_UAU.2	• Management of authentication data by the Administrator • Management of authentication data by a user associated with this data	• User password
FIA_UAU.6	• If an authorised administrator can request a reauthentication, reauthentication request should be included in the management.	• User inactivity period before reauthentication is required
FIA_UAU.7	• None	• None
FIA_UID.2	• Management of user identification information	• User ID
FIA_USB.1	• An authorised manager can define the security attributes of a default subject • An authorised manager can change the security attributes of a subject	• None • None
FMT_MSA.1a	• Managing the group of roles that can interact security attributes	• None (fixed)
FMT_MSA.1b	• Managing the group of roles that can interact security attributes	• None (fixed)
FMT_MSA.1c	• Managing the group of roles that can interact security attributes	• None (fixed)
FMT_MSA.3a	• Managing the group of roles that can specify initial values. • Managing permissive or restrictive default values for the predefined access control SFP.	• None (fixed) • None (fixed)
FMT_MSA.3b	• Managing the group of roles that can specify initial values. • Managing permissive or restrictive default values for the predefined access control SFP.	• None (fixed) • None (fixed)
FMT_MSA.3c	• Managing the group of roles that can specify initial values. • Managing permissive or restrictive default values for the predefined access control SFP.	• None (fixed) • None (fixed)
FMT_MTD.1	• Managing the group of roles that can interact with the TSF data.	• None (fixed)
FMT_SMF.1	• None	• None
FMT_SMR.1	• Managing the group of users that are part of a role.	• None (fixed)

Functional Requirements	Management Requirements Stipulated in CC Part 2	Management Item
FPT_ITT.1	• Management of the types of modification against which the TSF should protect; • Managing the mechanism used to provide the protection of the data in transit between different parts of the TSF.	• None (fixed) • None (fixed)
FPT_STM.1	• Managing time stamps	• None

FMT_SMR.1 Security Roles
Hierarchical to: No other components
Dependencies: FIA_UID.1 Timing of identification

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

[Assignment: *authorised identified roles*]:
- Administrator
- Client Administrator
- General User

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

Protection of the TSF (FPT)

FPT_ITT.1 Basic Internal TSF Data Transfer Protection
Hierarchical to: No other components
Dependencies: None

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

[Selection: disclosure, modification]: Disclosure, Modification

FPT_STM.1 Reliable Time Stamps
Hierarchical to: No other components
Dependencies: None

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.2. Security assurance requirements

The evaluation assurance level of this TOE is EAL1+ASE_OBJ.2, ASE_REQ.2 and ASE_SPD.1. All security assurance requirement components given in EAL 1 components and ASE_OBJ.2, ASE_REQ.2 and ASE_SPD.1 stipulated in CC Part 3 are used directly.

Stipulated EAL1+ASE_OBJ.2, ASE_REQ.2 and ASE_SPD.1 components:

(1) ADV: Development
ADV_FSP.1: Basic functional specification

(2) AGD: Guidance documents

AGD_OPE.1: Operational user guidance
AGD_PRE.1: Preparative procedures

(3) ALC: Life-cycle support
ALC_CMC.1: Labelling of the TOE
ALC_CMS.1: TOE CM coverage

(4) ASE: Security Target evaluation
ASE_CCL.1: Conformance claims
ASE_ECD.1: Extended components definition
ASE_INT.1: ST introduction
ASE_OBJ.2: Security objectives
ASE_REQ.2: Derived security requirements
ASE_SPD.1: Security problem definition
ASE_TSS.1: TOE summary specification

(5) ATE: Tests
ATE_IND.1: Independent testing - comformance

(6) AVA: Vulnerability assessment
AVA_VAN.1: Vulnerability survey

6.3. Security requirements rationale

6.3.1. Security Functional Requirements Rationale

Table 6-23 shows the correspondence between security functional requirements and TOE security objectives.

Table 6-23 Correspondence between Security Functional Requirements and TOE Security Objectives

	O.I&A	O.ACCESS_CONTROL	O.ACCESS_CONTROL_MEDIA	O.RE_AUTH	O.AUDIT	O.CRYPTOGRAPHY	O.LOG_COLLECT
FAU_GEN.1					**x**		
FAU_GEN.2					**x**		
FAU_SAR.1					**x**		
FAU_SAR.2					**x**		
FAU_SAR.3					**x**		
FAU_STG.1					**x**		

	O.I&A	O.ACCESS_CONTROL	O.ACCESS_CONTROL_MEDIA	O.RE_AUTH	O.AUDIT	O.CRYPTOGRAPHY	O.LOG_COLLECT
FAU_STG.3					x		
FAU_STG.4					x		
FCS_CKM.1						x	
FCS_CKM.4						x	
FCS_COP.1						x	
FDP_ACC.1a		x	x				
FDP_ACC.1b		x					
FDP_ACC.1c						x	
FDP_ACF.1a		x	x				
FDP_ACF.1b		x					
FDP_ACF.1c						x	
FDP_ETC.2						x	
FDP_ITC.2						x	
FIA_AFL.1	x						
FIA_ATD.1	x	x	x				
FIA_SOS.1	x						
FIA_UAU.2	x						
FIA_UAU.6				x			
FIA_UAU.7	x			x			
FIA_UID.2	x						
FIA_USB.1	x	x	x				
FMT_MSA.1a		x	x				
FMT_MSA.1b		x					
FMT_MSA.1c						x	
FMT_MSA.3a		x	x				
FMT_MSA.3b		x					
FMT_MSA.3c						x	

	O.I&A	O.ACCESS_CONTROL	O.ACCESS_CONTROL_MEDIA	O.RE_AUTH	O.AUDIT	O.CRYPTOGRAPHY	O.LOG_COLLECT
FMT_MTD.1		x	x				
FMT_SMF.1	x	x	x			x	
FMT_SMR.1	x	x	x			x	
FPT_ITT.1							x
FPT_STM.1					x		

Table 6-23 shows how each security functional requirement corresponds to at least one TOE security objectives. The following provides a description of how each TOE security objective can be realized by security funational requirements.

Firstly, we will refine and analyze necessary countermeasures for each TOE security objective. Secondly, we will determine all required functions for each countermeasure. Lastly, we will verify that all these required functions can be satisfied; thereby we can demonstrate the realization of each security objective. For those required functions, we will demonstrate that at least one security functional requirement can satisfy each necessary countermeasure.

O.I&A (user identification and authentication)

This TOE security objective requires user restriction so that only authorised users can be granted access to the TOE. Details of this security objective and the associated functional requirements are as follows:

a. User identification before granting access to the TOE

Before each user is granted access to the TOE, the TSF shall require each user to identify itself as an authorised user. That is to say, the TSF that is executable before user identification is one to identify each user. The security functional requirement corresponding to this requirement is FIA_UID.2.

b. User authentication before granting access to the TOE

Before each user is granted access to the TOE, the TSF shall require each user to authenticate itself as an authorised user. That is to say, the TSF that is only executable before user authentication is one to authenticate each user. The security functional requirement corresponding to this requirement is FIA_UAU.2.

c. Hard-to-guess authentication information

In reliable authentication practice, user authentication information must be hard for most people to guess except the user. To make it hard to guess, it is required to clearly define a necessary level of quality to the user authentication information and verify that such a level of quality is satisfied. The security functional requirement corresponding to this requirement is FIA_SOS.1.

d. Granting the use of the TOE when user identification and authentication is succedded

A user who succeeded in identification and authentication can access the TOE from the client terminal that succeeded in identification and authentication. At this time, the TOE generates a subject acting on behalf of a user, and maintains and associates the security attributes required for the user to use the TSF. The security functional requirement corresponding to this requirement is FIA_ATD.1 and FIA_USB.1.

e. Disabling the use of the TOE if a user does not succeed in the authentication within a defined number of attemps.

Users who failed in the authentication shall be regarded as a non-authorised TOE user. The TOE implements a predefined action (disabling the TOE for a certain period of time) when the number of user authentication failures exceeds the maximum permissible number of consecutive authentication failures defined by the Administrator. The security functional requirement corresponding to this requirement is FIA_AFL.1.

f. Displaying user authentication entries in dummy characters

User authentication entries shall be displayed in dummy characters to protect the information from stealing during the authentication. The security functional requirement corresponding to this requirement is FIA_UAU.7.

g. Provision of the management functions corresponding to the result of authentication

When user authentication is successful, the TOE shall provide the management functions dependent on the result of authentication. The security functional requirements

corresponding to this requirement are FMT_SMF.1.

h. Associating security roles depending on authentication results

If a user succeeds in the authentication, the TOE shall associate and maintain the security roles dependent on authentication results. The security functional requirement corresponding to this requirement is FMT_SMR.1.

To satisfy the O.I&A security objective, it is necessary to satisfy all requirements, (a), (b), (c), (d), (e), (f) (g) and (h) above. Thus, this security objective can be realized by satisfying the FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.7, FIA_UID.2, FIA_USB.1, FMT_SMF.1 and FMT_SMR.1 functional requirements.

O.ACCESS_CONTROL (access control)

This TOE security objective requires that a general user or the process acting on behalf of the user is granted access to I/O ports, user program files or printer ports in accordance with the predetermined access privilege. Details of this security objective and the associated functional requirements are as follows:

a. Enforcing access control to program files

It is required to determine unauthorised operations and subjects for each program file and enforce a set of these rules. Thus, the TSF shall associate a general user process with the list of program file operations, and based on it, enforce the access control when a program file is executed or its file name is changed. The security functional requirement corresponding to this requirement is FDP_ACC.1b and FDP_ACF.1b.

b. Enforcing access control to I/O ports

It is required to determine authorised operations and subjects for each I/O port and enforce a set of these rules. Thus, the TSF shall associate a general user process with the list of I/O port operations, and based on it, enfoce the input and output control. The security functional requirement corresponding to this requirement is FDP_ACC.1a and FDP_ACF.1a.

c. Combining a user with the process

The TOE shall combine general user related security attributes including I/O port control information, printer control information, authorised printer information, authorised USB

device input / output control information, external media output control information, prohibited user program information and user ID with subjects acting on befalf of users. The security functional requirement corresponding to this requirement is FIA_ATD.1 and FIA_USB.1.

d. To enforce intended access control, critical TOE operations are granted only to the Administrator and general users are granted to access to the security attributes such as I/O port control information, printer control information, authorised printer information, authorised USB device input / output control information, external media output control information, prohibited user program information and user ID in accordance with the predetermined user roles. The security functional requirement corresponding to this requirement is FMT_MSA.1a and FMT_MSA.1b. Only the Administrator is allowed to modify these security attributes (a general user is not allowed to do that). The security functional requirement corresponding to this requirement is FMT_MSA.3a and FMT_MSA.3b.

   In addition, general users are granted access to both the critical TOE operational settings and the operating system's various control settings in accordance with the predetermined user roles. The security functional requirement corresponding to this requirement is FMT_MTD.1.

   The TOE shall provide management functions corresponding to the security functions. The security functional requirement corresponding to this requirement is FMT_SMF.1.

   The TOE shall associate the Administrator and the general user with their rules and maintain them. The security functional requirement corresponding to this requirement is FMT_SMR.1.

To satisfy the O.ACCESS_CONTROL security objective, it is necessary to satisfy all requirements, (a), (b), (c) and (d) above. Thus, this security objective can be realized by satisfying the FIA_ATD.1, FIA_USB.1, FDP_ACC.1a, FDP_ACF.1a, FDP_ACC.1b, FDP_ACF.1b, FMT_MSA.1a, FMT_MSA.1b, FMT_MSA.3a, FMT_MSA.3b, FMT_MTD.1, FMT_SMF.1 and FMT_SMR.1 functional requirements.

O. ACCESS_CONTROL_MEDIA (access control to the external media)

This TOE security objective requires that a general user or the process acting on behalf of the user is granted access to the authorised external media in accordance with the predetermined access privilege. Details of this security objective and the associated functional requirements are as follows:

a. Enforcing access control to the authorised external media
   It is required to control access of general users to the authorised external media by determing authorised operations and rules on it. The security functional requirement corresponding to this requirement is FDP_ACC.1a and FDP_ACF.1a.

b. Combining a user with the process
   The TOE shall combine general user related security attributes including external media output control information, authorised external media input / output control information and user ID with the subject acting on behalf of a general user. The security functional requirement corresponding to this requirement is FIA_ATD.1 and FIA_USB.1.

c. To enforce intended access control, all critical TOE operations are granted only to the Administrator and general users are granted access to the security attributes such as external media output control information, authorised external media input / output control information and user ID in accordance with the predetermined user roles. The security functional requirement corresponding to this requirement is FMT_MSA.1a.

   Only the Administrator is allowed to modify these security attributes (general users are not allowed to do that). The security functional requirement corresponding to this requirement is FMT_MSA.3a.

   In addition, general users are granted access to the critical TOE operational settings in accordance with the predetermined user roles. The security functional requirement corresponding to this requirement is FMT_MTD.1.

   The TOE shall provide management functions corresponding to the security functions. The security functional requirement corresponding to this requirement is FMT_SMF.1.

   The TOE shall associate the Administrator and the general users with their roles and

maintain this. The security functional requirement corresponding to this requirement is FMT_SMR.1.

To satisfy the O.ACCESS_CONTROL_MEDIA security objective, it is necessary to satisfy the requirements (a), (b) and (c) above. Thus, this security objective can be realized by satisfying the FIA_ATD.1, FIA_USB.1, FDP_ACC.1a, FDP_ACF.1a, FMT_MSA.1a, FMT_MSA.3a, FMT_MTD.1, FMT_SMF.1 and FMT_SMR.1 functional requirements.

O. RE_AUTH (reauthentication)

This TOE security objective requires a reauthentication operation when the TOE is not accessed from a logged-on Administrator or general user for a certain period of time. Details of this security objective and the associated functional requirements are as follows:

a. Reauthentication

The TOE shall reauthenticate the Administrator or general user when the TOE is not accessed for a certain defined period of time. The security functional requirement corresponding to this requirement is FIA_UAU.6.

b. Secreting authentication information

The TOE shall protect a password in the password entry field with dummy characters. The security functional requirement corresponding to this requirement is FIA_UAU.7.

To satisfy the O.RE_AUTH security objective, it is necessary to satisfy the requirements (a) and (b) above. Thus, this security objective can be realized by satisfying the FIA_UAU.6 and FIA_UAU.7 security functional requirements.

O.AUDIT (audit)

This TOE security objective requires log collection and protection. Log is the information that provides evidence for reviewing the TOE operational state at a later date. It must be available any time when required. Hence, log protection requires the consideration of secure log collection, view and search. Details of this security objective and the associated functional requirements are as follows:

a. Collecting necessary logs

In regards to those audit requirements shown in Table 6-1, the TOE shall collect log

information as well as reliable time stamps with user identity association. The security functional requirement corresponding to this requirement is FAU_GEN.1 for log collection, FPT_STM.1 for reliable time stamps and FAU_GEN.2 for user identify association.

b. Collecting all logs

The TOE shall prevent the stored log in the audit trail from unauthorised deletion and modification. If the log exeeeds the predefined warning size of audit trail storage, the TOE shall inform the Administrator or general user of the possibility of log data loss. In addition, if the audit trail storage becomes full, the TOE shall implement necessary actions to prevent log data loss. The security functional requirement corresponding to this requirement is FAU_STG.1, FAU_STG.3 and FAU_STG.4.

c. Restricting users accessislbe to logs

The TOE shall allow only the Administrator to read the audit trail log stored in the log server. However, the Administrator shall not be allowed to read logs collected by administrator and client terminals.

In addition, the TOE shall provide the functionality to sort and search logs under the predetermined conditions. The security functional requirement to this requirement is FAU_SAR.1, FAU_SAR.2 and FAU_SAR.3.

To satisfy the O.AUDIT security objective, it is necessary to satisfy the requirements (a), (b) and (c) above. Thus, this security objective can be realized by satisfying the FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1, FAU_STG.3, FAU_STG.4 and FPT_STM.1 functional requirements corresponding to each requirement.

O.CRYPTOGRAPHY (cryptography)

This TOE security objective requires the enforcement of cryptographically secured storage of user data files in the client terminal or writing to the authorised external media. Details of this security objective and the associated functional requirements are as follows:

a. Generating cryptographic keys

The TOE shall generate cryptographic keys according to the internationally-standardized cryptographic key generation mechanism. The security functional requirement corresponding to this requirement is FCS_CKM.1.

b. Cryptographical operations

The TOE shall encrypt or decrypt a given data file using the cryptographic key generated by the FCS_CKM.1 function when writing it to the authorised external media. The security functional requirement corresponding to this requirement is FCS_COP.1.

c. Writing cryptographic keys

The TOE shall allow only the Administrator to write the key to encrypt or decrypt a file. The security functional requirement corresponding to this requirement is FDP_ETC.2.

d. Deleting a cryptographic key

The TOE shall allow only the authorised general user who owns the encryption/decryption key to delete it. The security functional requirement corresponding to this requirement is FCS_CKM.4.

e. Controlling cryptographic key input

The TOE shall allow only the Administrator to manage the security attributes (cryptographic key input control information) that are used in cryptographic key input control. The security functional requirements corresponding to this requirement is FMT_MSA.1c and FMT_MSA.3c.

In addition, it is required to determine the authorised operations and rules for reading the key to encrypt/decrypt a file, and enforce access control based on these operations and rules. The security functional requirements corresponding to this requirement is FDP_ ACC.1c, FDP_ACF.1c and FDP_ITC.2.

f. Associating cryptographic key management functions with roles

The TOE shall provide management functions associated with the cryptographic security functions. The security functional requirements corresponding to this requirement is FMT_SMF.1.

In addition, the TOE shall associate the roles between the Administrator and the general user, and maintain it. The security functional requirements corresponding to this requirement is FMT_SMR.1.

To satisfy the O.CRYPTOGRAPHY security objective, it is necessary to satisfy the requirements (a), (b), (c), (d), (e) and (f) above. Thus, this security objective can be realized by satisfying the FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FDP_ACC.1a,

FDP_ACF.1a, FDP_ETC.2, FDP_ITC.2, FMT_MSA.1c, FMT_MSA.3c, FMT_SMF.1 and FMT_SMR.1 functional requirements corresponding to each requirement.

O.LOG_COLLECT (log collection)

This TOE security objective requires secure log collection from the administrator/client terminals to the log server. Details of this security objective and the associated functional requirements are as follows:

a. Secure log transfer

The TOE shall provide secure transfer of logs generated by the administrator/client terminals and protect these logs from disclosure and modification that could occur during the transfer. The security functional requirements corresponding to this requirement is FPT_ITT.1.

To satisfy the O.LOG_COLLECT security objective, it is necessary to satisfy the requirement (a) above. Therefore, this security objective can be realized by satisfying the FPT_ITT.1 functional requirement.

6.3.2. Dependency of security functional requirements

Table 6-24 shows the dependency of security requirement components.

Table 6-24 Dependency of security requirement components

Item	Components used by the TOE	Dependency components specified in CC Part 2	Dependency components of the TOE	Components not satisfying any dependencies	Validity
1	FAU_GEN.1	FPT_STM.1	FPT_STM.1	None	
2	FAU_GEN.2	FAU_GEN.1	FAU_GEN.1	None	
		FIA_UID.1	FIA_UID.2	None	
3	FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	None	
4	FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	None	
5	FAU_SAR.3	FAU_SAR.1	FAU_SAR.1	None	
6	FAU_STG.1	FAU_GEN.1	FAU_GEN.1	None	
7	FAU_STG.3	FAU_STG.1	FAU_STG.1	None	
8	FAU_STG.4	FAU_STG.1	FAU_STG.1	None	
9	FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1]	FCS_COP.1	None	
		FCS_CKM.4	FCS_CKM.4		
		FMT_MSA.2	None	FMT_MSA.2	*1
10	FCS_CKM.4	[FCS_CKM.2 or FCS_COP.1]	FCS_COP.1	None	

Item	Components used by the TOE	Dependency components specified in CC Part 2	Dependency components of the TOE	Components not satisfying any dependencies	Validity
		FCS_CKM.1	FCS_CKM.1		
		FMT_MSA.2	None	FMT_MSA.2	*1
11	FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1	None	
		FCS_CKM.4	None	FCS_CKM.4	
		FMT_MSA.2	None	FMT_MSA.2	*1
12	FDP_ACC.1a	FDP_ACF.1	FDP_ACF.1a	None	
13	FDP_ACC.1b	FDP_ACF.1	FDP_ACF.1b	None	
14	FDP_ACC.1c	FDP_ACF.1	FDP_ACF.1c	None	
15	FDP_ACF.1a	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1a FMT_MSA.3a	None	
16	FDP_ACF.1b	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1b FMT_MSA.3b	None	
17	FDP_ACF.1c	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1c FMT_MSA.3c	None	
18	FDP_ETC.2	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1c	None	
19	FDP_ITC.2	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1c	None	
		[FTP_ITC.1 or FTP_TRP.1]	None	[FTP_ITC.1 or FTP_TRP.1]	*2
		FPT_TDC.1	None	FPT_TDC.1	*3
20	FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	None	
21	FIA_ATD.1	None	None	None	
22	FIA_SOS.1	None	None	None	
23	FIA_UAU.2	FIA_UID.1	FIA_UID.2	None	
24	FIA_UAU.6	None	None	None	
25	FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	None	
26	FIA_UID.2	None	None	None	
27	FIA_USB.1	FIA_ATD.1	FIA_ATD.1	None	
28	FMT_MSA.1a	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1a	None	
		FMT_SMR.1	FMT_SMR.1	None	
		FMT_SMF.1	FMT_SMF.1	None	
29	FMT_MSA.1b	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1b	None	
		FMT_SMR.1	FMT_SMR.1	None	
		FMT_SMF.1	FMT_SMF.1	None	
30	FMT_MSA.1c	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1c	None	
		FMT_SMR.1	FMT_SMR.1	None	
		FMT_SMF.1	FMT_SMF.1	None	
31	FMT_MSA.3a	FMT_MSA.1	FMT_MSA.1a	None	
		FMT_SMR.1	FMT_SMR.1	None	
32	FMT_MSA.3b	FMT_MSA.1	FMT_MSA.1b	None	
		FMT_SMR.1	FMT_SMR.1	None	

Item	Components used by the TOE	Dependency components specified in CC Part 2	Dependency components of the TOE	Components not satisfying any dependencies	Validity
33	FMT_MSA.3c	FMT_MSA.1	FMT_MSA.1c	None	
		FMT_SMR.1	FMT_SMR.1	None	
34	FMT_MTD.1	FMT_SMR.1	FMT_SMR.1	None	
		FMT_SMF.1	FMT_SMF.1	None	
35	FMT_SMF.1	None	None	None	
36	FMT_SMR.1	FID_UID.1	FID_UID.2	None	
37	FPT_ITT.1	None	None	None	
38	FPT_STM.1	None	None	None	

As shown in Table 6-24, all necessary dependencies are satisfied except for those denoted by an asterisk in the Validity field. The following provides the rationale why dependency is not required for these exceptions.

*1) FCS_CKM.1, FCS_COP.1 → FMT_MSA.2

The security attributes handled by FCS_CKM.1 and FCS_COP.1 are those relating to the cryptographic key and each attribute value is determined based on the standardized algorithm, thus there is no possibility of these attribute values being defined or modified by the user. Therefore, these dpendencies are not required.

*2) FDP_ITC.2 → FTP_ITC1 or FTP_TRP.1

When exporting a key to the media, the Administrator will set the cryptographic key input control information to the key to ensure a secure key transfer to the target authorised general user, thus there is no need to use a secure communication channel. Therefore, these dpendencies are not required.

*3) FDP_ITC.2 → FPT_TDC.1

The security attribute of the cryptographic key input control information is generated inside the TOE for importing, thus there is no need to maintain the consistency of the security attribute with that of other different IT products. Therefore, this dependency is not required.

6.3.3. Security assurance requirements rationale

This TOE envisions private usage, not intended for use in a customer environment. Thus, since it does not require a high level of assurance, EAL1 is adequate for this requirement. However, on the ground that the TOE is an information leakage prevention system, it requires a complete security target evaluation that includes the implementation of threat analysis, thus ASE_OBJ.2, ASE_REQ.2 and ASE_SPD.1 are augmented.

7. TOE Summary Specification

This chapter describes the TOE summary specification.

7.1. TOE summary specification

This section describes the TOE security functions.

7.1.1. Audit Function

[FAU_GEN.1]

In order to manage the log generation and generated information required to audit the secure TOE operations, the TOE generates logs when predefined security relevant events or unexpected events occur.

The log is generated when the following auditable events occur:
- Success or failure in writing to the external media
- Success or failure in starting a program file
- Failure in changing a program file name
- Attainment of a threshold value of the consecutive failed authentication attempts counter and a subsequent action to be taken (PC lockout for a certain defined period)Success or failure in user identification and authentication
- Success or failure in user identification and authentication
- Success or failure in user ID registration, update or delete
- Success or failure in user password registration or update

Note that auditable events can occur only between the user login completion after the TOE startup and the shutdown of the TOE. Thus, the audit function starts and ends between them.

The log consists of the following items:
- Date and Time (date and time of events): Date and time of log generation
- Event type (type of event): indicates an event type classification such as Error, alarm and Information
- User ID (subject identification information)
- Message (event result): indicates a detailed event content
- Event ID (other audit relevant information)
- Category (other audit relevant information): indicates a log category classification
- PC name (other audit relevant information)
- IP address (other audit relevant information)
- MAC address (other audit relevant information)

[FAU_GEN.2]

In order to manage the log generation and generated information required to audit the secure TOE operations, the TOE associates these events with user IDs that caused the events and generate these logs.

[FAU_SAR.1]

The TOE provides the Administrator who entered LogViewer startup control information with logs stored on the log server based on the list of the following audit information.

<List of audit information>
- Date and time of the event
- Event type→Type of event
- User ID(subject identity)
- Message(the outcome of the event)
- Event ID
- Category
- PC name
- IP address
- MAC address

For those logs that can be read by the Administrator, the TOE also displays an audit item for each auditable event.

[FAU_SAR.2]

The TOE compares the input LogViewer startup control information with that retained inside the TOE and prohibits access to the logs stored on the log server by those other than the Administrator who input the matched LogViewer startup control information.

[FAU_SAR.3]

The TOE supports the search request by the following search item:

<Supported log search conditions>
- Period / time of day
- User ID
- PC name
- IP address
- MAC address
- Type of event
  - Category
  - Event ID

[FAU_STG.3]

When logs stored in the audit trail exceeds the alarm size that is predefined in the client control information by the Administrator, the TOE displays on the client or administrator terminal screen a message indicating the occurrence of a possibility of causing the log loss.

[FAU_STG.４]

When logs stored in the audit trail reach the predefined storage capacity limit, the TOE

overwrites logs beginning with the chronologically oldest logs stored on the administrator/client terminals.

[FPT_ITT.1]
The TOE supports a SSL-based secure log transfer from the administrator/client terminal to the log server for log collection.

[FPT_STM.1]
The TOE provides reliable time stamps for generation of logs to be stored in the audit trail.

7.1.2. Access control function

[FAU_STG.1]
The TOE protects the logs in the audit trail from unauthorised modification by not providing any interfaces other than those used for registration of logs and log transfer to the log server.
Besides, the TOE protects logs in the audit trail from unauthorised modification by not providing any interface that allows direct editing of the logs in the audit trail whatever OS privileges a user is assigned to.

[FDP_ACC.1a] [FDP_ACF.1a]
The TOE executes input / output control operations on the I/O port for the general user process based on the external input / output control policy. Whether to allow access to that I/O port is determined based on the client control information defined by the Administrator and imported to the client. The operations between the subject and the object controlled by the external input / output access control policy are shown in Table 7-1, the subject controlled by the external input / output access control policy and the corresponding SFP relevant security attributes in Table 7-2, and the object and the corresponding SFP relevant security attributes in Table 7-3.

Table 7-1 The operations between the subject and the object controlled by the external input / output access control policy

Subject	Object	Operations
General user process	I/O port	Input / output

Table 7-2 The subject and the corresponding SFP relevant security attribute

Controlled subject	Corresponding SFP relevant security attribute
General user process	I/O port control information Printer control information Authorised printer information Authorised USB device input / output control information External media output control information Authorised external media input / output control information

Table 7-3 The subject and the corresponding SFP relevant security attribute

Controlled object	Corresponding SFP relevant security attribute
I/O port	Port name

[Assignment: access control SFP]: External input / output access control policy

The TOE executes the operations between any subject and any object controlled by the client control information based on the rules shown in Table 7-4.

Table 7-4 Rules of access management

Subject	Object	Operation	Rule
General user process	I/O port	Input / output	• The general user process executes input / output operation on the I/O port when the I/O port control information is set to “enable”. • The general user process does not execute input / output operation on the I/O when the I/O port control information is set to “disable”. • The general user process excutes input / output operation on the I/O supporting a USB interface when the authorised USB device input / output control information matches the connected USB device information. • The general user process does not excute input / output operation on the I/O port supporting a USB interface when the authorised USB device input / output control information does not match the connected USB device information. • The general user process executes input / output operation on the specified I/O port supporting an external media when the external media output control information is set to “available only for authorised external media”. • The general user process executes input / output operation on the I/O port available for all external media when the

Subject	Object	Operation	Rule
			external media output control information is set to “all external media are allowed”. • The general user process does not execute input / output operation on the I/O port supporting an external media when the external media output control information is set to “use of all external media are prohibited”. • The general user process executes input / output operation on the I/O port supporting an external media when the authorised external media input / output control information matches the connected external media information. • The general user process does not execute input / output operation on the I/O port supporting an external media when the authorised external media input / output control information does not match the connected external media information.
		Output	• The general user process executes input / output operation on the I/O port specified in the authorised printer information when the printer control information is set to “partially allowed”. • The general user process executes output operation on the I/O port when the printer control information is set to “all allowed”. • The general user process does not execute output operation on the I/O port when the printer control information is set to “all prohibited”.

[FDP_ACC.1b] [FDP_ACF.1b]

The TOE associates a general user authorised by the identification and authentication function (client) with the general user process that executes program operations on behalf of that general user. The general user process executes a program file based on the client control information parameter settings configured and imported onto the client by the Administrator or changes a file name based on the program file access control policy.

The operations between any subject and any object controlled under the program file access control policy are shown in Table 7-5, the controlled subject and the corresponding SFP relevant security attributes in Table 7-6, and the controlled object and the corresponding SFP relevant security attributes in Table 7-7.

Table 7-5 The operations between any subject and any object controlled under the program file access control policies

Subject	Object	Operation
General user process	General AP file	Execute, change file names

Table 7-6 The controlled subject and the corresponding security attribute

Controlled subject	Corresponding SFP relevant security attribute
General user process	Prohibited user program information

Table 7-7 The object and the corresponding security attribute

Controlled object	Corresponding SFP relevant security attribute
General AP file	File name

The TOE executes the operations between any subject and any object controlled by the imported client control information based on the rules shown in Table 7-8.

Table 7-8 Rules of access management

Subject	Object	Operation	Rule
General user process	General AP file	Execute, change file names	The general user process shall not execute a general AP file with a file name specified in the prohibited user program information nor change the file name.

[FDP_ACC.1c] [FDP_ACF.1c]

The TOE associates the Administrator or the general user authorised by the identification and authentication function (client) with the Administrator process or the general user process executing any operations on behalf of the Administrator or the general user inside the TOE. The administrator process writes the common key to encrypt/decrypt files used for assigning the cryptographic key input control information to the cryptographic key file to be exported without any security attribute based on the cryptographic key file input / output control policy. The general user process reads the cryptographic key file to be imported without any security attribute, compares the input character string from the general user to that defined in the cryptographic key input control information, and if they match, writes the file cryptography common key to the cryptographic key file based on the cryptographic key file input / output control policy.

The operations between any subject and any object controlled based on the cryptographic key file input / output control policy for the common key to encrypt/decrypt files are shown in Table 7-9, the subject and the corresponding SFP relevant security attribute in Table 7-10, and the object and the corresponding SFP relevant security attribute in Table 7-11.

Table 7-9 The operations between any subject and any object controlled based on the cryptographic key file input / output control policies

Subject	Object	Operation
Administrator process	Cryptograhic key file to be exported	Write
General user process	Cryptograhic key file to be imported	Read
General user process	Cryptographic key file	Write

Table 7-10 The subject and the corresponding security attribute

Controlled subject	Corresponding SFP relevant security attribute
Administrator process	None
General user process	None

Table 7-11 The object and the corresponding SFP relevant security attribute

Controlled object	Corresponding SFP relevant security attribute
Cryptographic key file to be exported	None
Cryptographic key file to be imported	None
Cryptographic key file	Cryptographic key input control information

The TOE executes the operations between any subject and any object controlled by the cryptographic key input control information based on the rules shown in Table 7-12.

Table 7-12 Rules of access management

Subject	Object	Operation	Rule
Administrator process	Cryptographic key file to be imported	Write	The Administrator process writes the common key data for file cryptography and cryptographic key input control information data.
General user process	Cryptographic key file to be imported	Read	The general user process reads the common key file to be imported.
	Cryptographic key file	Write	The general user process writes the common key data to encrypt / decrypt files when the cryptographic key input control information contained in the common key data is input.

[FDP_ETC.2]

Using the cryptographic function (client), the TOE adds the cryptographic key input control information to the cryptographic key and write that information based on the cryptographic key file input / output control policy defined in [FDP_ACC.1c]. This write operation can be executed only by the Administrator.

[FDP_ITC.2]

When reading the key used to encrypt a file, the TOE compares the cryptographic key input control information added to the key with the input character string. If they match, the TOE permits the reading based on the cryptographic key file input / output control policy defined in [FDP_ACC.1c].

[FIA_ATD.1]

The TOE associates and retains the following security attributes dependent on each user.

<List of security attributes to be retained>

- I/O port control information
- Printer control information
- Authorised printer information
- Authorised USB device input / output control information
- External media output control information
- Authorised external media input / output control information
- Prohibited user program information
- User ID

[FIA_USB.1]

The TOE associates the list of the following user security attributes with the subject acting on behalf of the Administrator or the general user inside the TOE dependent on each logged-on user.

<List of user security attributes>

- I/O port control information
- Printer control information
- Authorised printer information
- Authorised USB device input / output control information
- External media output control information
- Authorised external media input / output control information
- Prohibited user program information
- User ID

[FMT_MSA.1a]

In accordance with the external input / output access control policy, the TOE allows the roles (Administrator or general user) to manage the security attributes as shown in Table 7-13.

The TOE restricts those security attributes by providing only necessary interfaces dependent on different roles.

Table 7-13 Management of security attributes (input / output control of I/O ports)

Security Attribute	Operations	Roles
I/O port control information	Modify	Administrator
Printer control information	Modify	Administrator
	Qeury	Client administrator
	Qeury	Ggeneral user
Authorised USB device input / output control information	Modify	Administrator
Authorised printer information	Modify	Administrator
	Qeury	Client administrator
	Qeury	General user
External media output control information	Modify	Administrator
	Qeury	Client administrator
	Qeury	General user
Authorised external media input / output control information	Modify	Administrator

[FMT_MSA.1b]

In accordance with the program file access control policy, the TOE allows the roles (Administrator or general user) to manage the security attributes as shown in Table 7-14. The TOE restricts those security attributes by providing only necessary interfaces dependent on different roles.

Table 7-14 Management of security attributes (program startup control)

Security Attribute	Operation	Role
Prohibited user program information	Modify	Administrator
	Query	Client administrator
	Query	General user

[FMT_MSA.1c]

In accordance with the cryptographic key file input / output control policy, the TOE allows the roles (Administrator or general user) to manage the security attributes as shown in Table 7-15. The TOE restricts those security attributes by providing only necessary interfaces dependent on different roles.

Table 7-15 Management of security attributes (cryptographic key file input / output control)

Security Attribute	Operation	Role
Cryptographic key input control information	Creation	Administrator

[FMT_MSA.3a]

The TOE defines a restrictive default value to the security attributes used to enforce the external input / output access control policy (Table 7-13). Note that only the Administrator is allowed to define the default value of these security attributes.

[FMT_MSA.3b]

The TOE defines a restrictive default value to the security attributes used to enforce the program file access control policy (Table 7-14). Note that only the Administrator is allowed to define the default value of these security attributes.

[FMT_MSA.3c]

The TOE defines a restrictive default value to the security attributes used to enforce the cryptographic key file input / output control policy (Table 7-15). Note that only the Administrator is allowed to define the default value of these security attributes.

[FMT_MTD.1]

The TOE controls the TSF data operations by not providing any interfaces other than those for operations associated with the roles shown in Table 7-16.

Table 7-16 List of operations and roles to the TSF data

TSF Data	Operation	Role
Administrator ID	Entry, Query	Administrator
General user ID	Entry, Query	Administrator
	Query	Client administrator
	Query	General user
Administrator password	Entry, Modify	Administrator
Client Administrator password	Entry	Administrator
	Modify	Client administrator
General user password	Entry	Administrator
	Modify	Client administrator
	Modify	General user
Minimum password length	Modify	Administrator
Maximum password age	Modify	Administrator
Maximum size of audit trail storage	Modify	Administrator
Maximum permissible number of	Modify	Administrator

TSF Data	Operation	Role
consecutive authentication failures		
User inactivity period before reauthentication is required	Modify	Administrator
LogViewer startup control information	Modify	Administrator

[FMT_SMF.1]

To maintain the security functions appropriately, the TOE allows only the authenticated Administrator to manage the following items.

- LogViewer startup control information
- Maximum size of audit trail storage
- The following security attributes:
  - I/O port control information
  - Printer control information
  - Authorised printer information
  - Authorised USB device input / output control information
  - External media output control information
  - Authorised external media input / output control information
  - Port name
  - Prohibited user program information
  - File name
- Cryptographic key input control information
- Maximum number of consecutive authentication failures
- Maximum user password length
- Maximum user password age
- User password
- Authorised external media identification/authentication information
- User inactivity period before reauthentication is required
- User ID

[FMT_SMR.1]

As a result of identification and authentication, the TOE associates the role of the Administrator, the client administrator and general user.

7.1.3. Identification/Authentication Function

[FIA_AFL.1]

The TOE compares the password corresponding to a user ID that is entered by the Administrator or the general user with those user IDs and passwords retained inside the TOE. If they do not match, the TOE increments the consecutive failed authentication attempts counter assigned for each user ID. Meanwhile, if a value of the consecutive failed authentication attempts counter reaches the maximum permissible number of consecutive authentication failures, the TOE locks out the PC.
The maximum permissible number of consecutive authentication failures is defined for each general user and Administrator. It shall be defined in the range of 1 to 99 by the Administrator.

[FIA_SOS.1]
When an Administrator password, a general user password or the cryptographic key input control information is entered, the TOE guarantees that the quality metric shown in Table 7-17 is satisfied.

Table 7-17 List of defined quality metric

Secrets	Quality Metrics
Administrator / general user password	• ASCII characters including: - 26 alphabetical uppercase characters [A through Z] and 26 lowercase characters (a through g), total 52 characters. - 10 numeric characters [0 through 9] - 32 symbols [!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~] • Maximum password length defined by the Administrator • Maximum password age defined by the Administrator
Cryptographic key input control information	• ASCII characters including: - 26 alphabetical uppercase characters [A through Z] and 26 lowercase characters (a through g), total 52 characters. - 10 numeric characters [0 through 9] - 32 symbols [!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~] • Number of digits must be within 8 through 32
LogViewer startup control information	• ASCII characters including: - 26 alphabetical uppercase characters [A through Z] and 26 lowercase characters (a through g), total 52 characters. - 10 numeric characters [0 through 9] - 32 symbols [!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~] • Number of digits must be within 8 through 127

[FIA_UAU.2] [FIA_UID.2]
Before general users, client administrators or Administrators use the client/administrator terminal, the TOE compares the user ID and password entered by these users with that retained inside the TOE. If these users are identified and authenticated as authorised users, the TOE permits the use of each terminal.

As for the use of a log server, the TOE identifies and authenticates each user by comparing the LogViewer startup control information entered by the Administrator.

Note that the identification/authentication function provided by the TOE is the one that is realized by a set of the administrator terminals, the client terminals, and those APs on the log servers including the NEC Group Information Leakage Prevention System V1.0, Administrator Terminal Application SoftwareVer V1.0, NEC Group Information Leakage Prevention System V1.0 Client Application Software Ver1.0 and NEC Group Information Leakage Prevention System V1.0 Log Server Application Software Ver1.0, not the one realized by the operating system.

[FIA_UAU.6]

If the logged-on Administrator or the general user's inactivity period exceeds "the user inactivity period before reauthentication is required" defined by the Administrator, the TOE requires reauthentication based on the user-ID and password before permitting the use of the TOE.

[FIA_UAU.7]

During the authentication the TOE displays the predefined dummy characters (* or ●) instead of the password characters entered, so as not to display the actual input data directly.

7.1.4. Cryptographic Function

[FCS_CKM.1]

The TOE generates a cryptographic key based on the specific standard, cryptographic key generation algorithm and key length shown in Table 7-18.

Table 7-18 Cryptographic Key and Key Generation Algorithm

Type of Key	Standard	Cryptographic Key Generation Algorithm	Key Length
Common key for authorised external media	FIPS PUB 197	AES	128bit
Common key for file cryptography	FIPS PUB 46-3	3DES	168bit
	FIPS PUB 197	AES	128/192/256bit

The TOE generates a common key for authorised external media when registering an

authorised external media. As for the common key to encrypt/decrypt files, the general user reads a common key created by the Administrator to encrypt/decrypt user data files.

[FCS_CKM.4]
The TOE allows only those general users who are the key owner and authorised by the identification/authentication function (client) to use the TOE to delete cryptographic key files associated with unneeded cryptographic keys.

[FCS_COP.1]
The TOE performs cryptographic operations using those keys shown in Table 7-19.

Table 7-19 Cryptographic standard, algorithm, key length and operations

Type of Key	Standard	Cryptographic Algorithm	Key Length	Cryptographic Operations
Common key for authorised external media	FIPS PUB 197	AES	128bit	Excryption for writing or decription for reading a file to or from the authorised external media
Common key for file cryptography	FIPS PUB 46-3	3DES	168bit	Encryption/description of user data
	FIPS PUB 197	AES	128/192 /256bit	

Cryptographic operations using these keys are as follows:
The TOE uses the common key for authorised external media when registering an authorised external media. The TOE performs file cryptography using the common key for authorised external media when writing a file to the authorised external media. As for the common key for file cryptography, the general user reads a common key created by the Administrator to encrypt/decrypt user data files.