NEC Group Secure Information Exchange Site

Version 1.0

SECURITY TARGET

Version 1.14

April 3, 2008

NEC Corporation

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

Revision History

Version	Summary	Revision Details		Date	Publisher
		Chapter	Changes Made		
1.00	Initial version	-	-	2007/9/19	NEC Corporation
1.01	Reflected the internal review	1	Modified the TOE description	2007/10/12	NEC Corporation
		3	Modified the threats and the assumptions	2007/10/12	
		4	Modified the security objectives rationale	2007/10/12	
		6	Modified the security requirements	2007/10/12	
		7	Modified the TOE summary specification	2007/10/12	
1.02	Reflected the evaluation result and the ST correspondence analysis	1 3 ~ 4 6 ~ 7	Entire modification based on correspondence relation	2007/11/14	NEC Corporation
		2 and 5	Modified the extended components definition	2007/11/14	
1.03	Reflected the evaluation result	1	Modified the TOE overview Modified the TOE description	2007/12/7	NEC Corporation
		3	Modified the representation of threats	2007/12/7	
		4	Modified the security objectives	2007/12/7	
		5	Modified the extended components definition	2007/12/7	
		6	Modified the security requirements	2007/12/7	
		7	Modified the TOE summary specification	2007/12/7	
1.04	Reflected the evaluation result	1	Modified the TOE description	2007/12/21	NEC Corporation
		4	Deleted unnecessary security objectives	2007/12/21	
		6	Deleted unnecessary security functional requirements	2007/12/21	
		7	Modified the TOE summary specification	2007/12/21	
1.05	Reflected the evaluation result	3	Modified the representation of threats	2008/1/15	NEC Corporation
		4	Modified the security objectives	2008/1/15	
		6	Modified the definition of security functional requirements	2008/1/15	
1.06	Reflected the evaluation result	1	Modified the software configuration description	2008/1/18	NEC Corporation
		3	Modified the representation of threats	2008/1/18	
		4	Deleted unnecessary security objectives	2008/1/18	
		5	Modified the extended functional components description	2008/1/18	
		6	Modified the security functional requirements	2008/1/18	
		7	Modified the TOE summary specification	2008/1/18	
1.07	Reflected the evaluation result	6	Modified the security functional requirements	2008/1/25	NEC Corporation

Version	Summary	Revision Details		Date	Publisher
		Chapter	Changes Made		
		7	Modified the TOE summary specification	2008/1/25	
1.08	Reflected the evaluation result	6	Modified the TOE summary specification	2008/1/30	NEC Corporation
1.09	Reflected the evaluation result	6	Modified the TOE summary specification	2008/1/31	NEC Corporation
1.10	Reflected the evaluation result	4	Added additional objectives Added additional objectives description Modified the security objectives rationale	2008/2/14	NEC Corporation
		5	Corrected typographical errors	2008/2/14	
		6	Modified the security functional requirements Modified the security requirements rationale	2008/2/14	
		7	Added additional summary specification description	2008/2/14	
1.11	Reflected the evaluation result	1	Added additional description of the TOE software configuration	2008/2/22	NEC Corporation
		6	Deleted unnecessary security functional requirements description	2008/2/22	
		7	Modified the summary specification description	2008/2/22	
1.12	Reflected the evaluation result	1	Corrected typographical errors on the TOE guidance	2008/3/7	NEC Corporation
		6	Deleted unnecessary security functional requirements description	2008/3/7	
			Modified the security requirements rationale	2008/3/7	
		7	Modified the TOE summary specification	2008/3/7	
1.13		4 6~7	Modified the user description	2008/3/31	NEC Corporation
		6	Modified the assurance requirements	2008/3/31	
		7	Modified the one-time URL description	2008/3/31	
1.14		1	Modified the security function description	2008/4/3	NEC Corporation

■ Trademarks and registered trademarks

All product and company 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 Part1:
  Introduction and general model September 2006 Version 3.1 Revision 1 CCMB-2006-09-001

- Common Criteria for Information Technology Security Evaluation Part2:
  Security functional components September 2006 Version 3.1 Revision 1 CCMB-2006-09-002

- Common Criteria for Information Technology Security Evaluation Part3:
  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
  March 2007, Translation Version 1.2
  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
  March 2007, Translation Version 1.2
  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
  March 2007, Translation Version 1.2
  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
  March 2007, Translation Version 1.2
  Information Security Certification Office, IT Security Center
  Information-technology Promotion Agency, Japan

Terminology

<CC related abbreviations>

CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

Definitions of terms and abbreviations used in this ST are shown in Table 1.

Table 1 Definitions of Terms and Abbreviations

Term / Abbreviation	Definition
.NET Framework	Microsoft’s application development and execution environments
ActiveX Control	Software for Microsoft’s Internet Explorer extension
DBMS	Database Management System, software for database management
DMZ	DeMilitarized Zone, an area that is isolated from external networks (e.g. Internet) and Intranet
GB	Giga Byte, a unit of information
Internet Explorer	Microsoft’s application software used to browse Web pages
Internet Information Server	Microsoft’s Internet server software
NEC	NEC Corporation
NEC Group	A term used to refer to NEC and all its subsidiaries collectively
OS	OS, the basic software, that manages the sharing of the resources of a computer such as input/output function and memory management
PIN	Personal Identification Number, a unique number used to identify individuals
RAID1	Redundant Arrays of Inexpensive Disks 1, a technique used to write the same information to multiple hard disks simultaneously
SSL	Secure Socket Layer, a communication protocol developed by Netscape Communications to enable secure encrypted communications over the Internet
Internet	Internationally interconnected networks
Intranet	A private network that is contained within an enterprise
Area	The basic unit of business data management. Multiple Areas can be created.
Area-user	A user such as NEC Group employee, on-premise worker and customer, who is authorised to access folders in the specific area
Storage Server	An external storage unit for storing data and program
Storage System	Software to manage the Storage Server
Security Patch	A piece of software designed and distributed to fix security vulnerabilities which were found in the OS.

Term / Abbreviation	Definition
Database Server	A server running DBMS
Firewall	A system to prevent unauthorised intrusion and access via networks
Folder	The basic business data unit to be stored in the area. Multiple folders can be created.
User ID	User identification code
One-Time URL	A URL that is available for a specified period of time. It shows the destination folder. One-time URL contains identification information.
Expiration date of one-time URL	A period of time during which a given one-time URL is available.
Business Data	Any business document data to be exchanged between internal users and between internal users and customers.
Customer	An employee of business partners who are not authorised to use the NEC Intranet.
On-premise Worker	An employee of contractors who are authorised to use the NEC Intranet.
External Web Server	An external Web server used for the NEC Group Secure Information Exchange Site
External User Client	A client terminal for the customers who use the TOE via Internet
Internal Authentication Server	A server running the internal authentication service
Internal Authentication Service	A service to centrally manage internal user IDs and passwords and provide authentication information to the various systems used by NEC Group
Internal Web Server	An internal Web server used for the NEC Group Secure Information Exchange Site
Internal User	An employee of NEC Group or contractors working at NEC
Internal User Client	A client terminal for the internal users who use the TOE on the NEC Intranet

1. ST Introduction

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

1.1. ST Reference

This section describes ST identification information.

ST Title:	NEC Group Secure Information Exchange Site Version 1.0 Security Target
ST Version:	1.14
ST Publishing Date:	April 3, 2008
ST Publisher:	NEC Corporation

1.2. TOE Reference

This section describes TOE identification information.

TOE Title:	NEC Group Secure Information Exchange Site
TOE Version:	1.0

1.3. TOE Overview

This section describes TOE type, usage and major security features of the TOE and required non-TOE hardware/software/firmware.

1.3.1. TOE Type

This TOE is a business software system that enables secure exchange of business data.

1.3.2. Usage and Major Security Features of the TOE

This TOE is the business data exchange system that provides services for preventing the miss-delivery of business data and the information leakage in communications between internal users and customers. The basic operation of the TOE is that an employee of NEC Group first creates an Area that is an administered data storage area, and then creates a folder in that Area. An internal user or a customer uploads business data to that folder. The uploaded data is then downloaded by internal users or customers for their business use.

As service functions, the TOE provides the Upload function, the Download function, Area Maintenance function, the User Maintenance function, the Set Personal Information function and the Administration function.

As security functions, the TOE protects the business data to be exchanged by the TOE from unauthorized access, miss-delivery and information leakage. It also collects audit logs. The overview of major security functions provided by the TOE is as follows:

[Security functions provided by the TOE]

Identification and Authentication

A function to identify and authenticate the users of the TOE

Access Control

A function to control access to the business data based on the user roles of the TOE

Auditing

A function to generate and view the audit trail of the TOE

Cryptography

A function to encrypt and decrypt the communication data between the TOE and a user

1.3.3. Required Non-TOE Hardware/Software/Firmware

This section describes the operational environments of the TOE.

1.3.3.1. Required Hardware

Table 2 shows the required hardware configuration in the operational environments of the TOE. The TOE operates correctly and reliably in the operational environments as shown in Table 2.

Table 2 Hardware Configuration

Equipment Name		Type	Description
Storage Server			
	Main Unit	Vendor Name	NEC
		Product Name	iStorage NS460
		Model Name	NF8100-145A
		CPU	Dual Core Intel Xeon Processor 3GHz
		Memory	3GB(2GB+1GB)
		HDD	73GB×2(15000rpm, RAID1)
		LAN	1000BASE-T×2(standard)
		Expansion Disk	Physical capacity: 2100GB(300GB×7)RAID5
Internal Web Server			
	Main Unit	Vendor Name	NEC
		Product Name	Express5800/120Ri-2 (XD2/3G(4))
		Model Name	N8100-1318
		CPU	Dual Core Intel Xeon Processor 3GHz × 2CPU
		Memory	4GB(2GB×2)
		HDD	73GB×2(15000rpm, RAID1)
		LAN	1000BASE-T×2(standard)
External Web Server			
	Main Unit	Vendor Name	NEC
		Product Name	Express5800/120Ri-2 (XD2/3G(4))
		Model Name	N8100-1318
		CPU	Dual Core Intel Xeon Processor 3GHz × 2CPU
		Memory	4GB(2GB×2)
		HDD	73GB×2(15000rpm, RAID1)
		LAN	1000BASE-T×2(standard)
Database Server			
	Main Unit	Vendor Name	NEC
		Product Name	Express5800/140Re-4(XMPD/3.40G(16))
		Model Name	N8100-1276

Equipment Name		Type	Description
		CPU	Dual Core Intel Xeon Processor 3.40GHz×4
		Memory	4GB(2GB×2)
		LAN	1000BASE-T×2(standard)
		External Storage	1148GB
Internal User Client			
	Main Unit	The client that is capable of running the OS defined in the Internal User Client column in Table 3 “Software Configuration”	
External User Client			
	Main Unit	The client that is capable of running the OS defined in the External User Client column in Table 3 “Software Configuration”	

1.3.3.2. Required Software

Table 3 shows the required software configuration in the operational environments of the TOE. The TOE operates correctly in the software configuration identified in Table 3.

Table 3 Software Configuration

Equipment Name			
	Vendor Name	Product Name	Type
Storage Server			
	Microsoft	Windows Storage Server 2003 R2	OS
Internal Web Server			
	Microsoft	Windows Server 2003 R2 _Standard Edition	OS
External Web Server			
	Microsoft	Windows Server 2003 R2 _Standard Edition	OS
Database Server			
	Microsoft	Windows Server 2003 R2_Standard Edition	OS
	Oracle	Oracle Database 10g Standard Edition 1 Processor	DBMS
Internal User Client			
	Microsoft	Windows 2000 Professional SP4, Windows XP Professional SP2, Windows Vista Business, Windows Vista Enterprise	OS
External User Client			
	Microsoft	Windows 2000 Professional SP4, Windows XP Professional SP2, Windows Vista Business, Windows Vista Enterprise	OS

1.4. TOE Description

This section describes System Overview, Roles of TOE-Related Users, Physical Scope of the TOE and Logical Scope of the TOE.

1.4.1. System Overview

Traditionally, e-mail services have been used as a means of exchanging business data. However, it is at increased risk for misdelivery or information leakage. The TOE is the information leakage prevention system that restricts those internal users allowed to exchange business data with the customers, prevents misdelivery by providing a PIN to the customers separately, and protects data from information leakage by cryptographic means.

In the TOE operation it is first required to create “areas” and “folders” for storing the business data to be exchanged. Each area can contain multiple folders. The area is a top level management structure for business data. Multiple areas can be created.

The folder is the smallest unit of storing business data. Multiple folders can be created in each area. For each folder, the person who has created an associated area will register the internal users and the customers who can access to that folder.

These internal users and customers are permitted to upload their business data to the predefined folder. At this time, it is required to specify the internal users and the customers who are allowed to download that data.

The TOE provides these specified internal users and customers with one-time URL via e-mail. To use a one-time URL each internal user must be authenticated by the internal authentication system outside the TOE, and each customer by PIN authentication. The PIN must be sent to the customers in a secure manner to ensure that only authorised internal users or customers can download the business data stored in a specific folder.

1.4.2. Roles of TOE-Related Users

Roles of TOE-related users are as follows.

TOE-related users are categorised into Operations Manager, Database Administrator and Storage Administrator. They perform their roles within the assigned privileges.

Users of the TOE-provided services are System Administrator, Auditor, NEC Group employee, On-premise Worker and Customer.

User roles of the NEC Group employee are categorised into NEC Group employees, area-users with administrator privileges and area-users with NEC Group employee/on-premise worker privileges. User roles of the on-premise worker are categorised into on-premise workers and area-users with NEC Group employee/on-premise worker privileges. User roles of the customer are area-user with customer privileges only.

All these users perform their roles within the assigned privileges. Table 4 shows the relation between the roles of TOE users and their assigned privileges.

Table 4 Relation between roles of TOE users and assigned privileges

		NEC Group employee	On-premise worker	Area-user with administrator privileges	Area-user with NEC Group employee/on-premise worker privileges	Area-user with customer privileges
Pre-Operation Phase	Create areas	×	-	▨	▨	▨
	View, update or delete areas	×	-	▨	▨	▨
Operation Phase	Create, update or delete folders	▨	▨	×	-	-
	Register, update or delete internal users and customers accessible to folders	▨	▨	×	-	-
	Delete files stored in a folder	▨	▨	×	-	-
	Determine area-users with administrator privileges	▨	▨	×	-	-
Utilisation Phase	View a list of accessible areas	×	×	▨	▨	▨
	View a list of folders registered in the folder-user	▨	▨	×	×	-
	View folders registered in the folder-user	▨	▨	×	×	×
	Upload	▨	▨	×	×	×
	Delete files which one uploaded	▨	▨	×	×	×
	Upload request	▨	▨	×	×	-
	Download	▨	▨	×	×	×
	Set personal mail addresses	▨	▨	×	×	-

TOE-related users perform the following roles and operations:

□ **Operations Manager**

A person who is responsible for managing the overall TOE operations

- Designate System Administrator, Database Administrator, Storage Administrator and Auditor
- Obligate System Administrator, Database Administrator, Storage Administrator and Auditor to comply with system operation-related rules and procedures and implement information security training
- Train the TOE users to improve and maintain the security awareness

□ **Database Administrator**

A person who is responsible for managing the DBMS outside the TOE

- Set the DBMS appropriately before the TOE’s initial settings are made

□ **Storage Administrator**

A person who is responsible for managing the storage system other than the TOE

- Set the storage system appropriately before the TOE’s initial settings are made

TOE users perform the following TOE related operations:

□ **NEC Group employee**

A person who is authorised to create, update and delete areas using an internal user client.

- Create, update and delete areas
- View accessible areas and folders

□ **On-premise worker**

A person who is authorised to view areas or folders using an internal user client

- View accessible areas and folders

□ **Area-user with administrator privileges**

A person who is responsible for business data-related operations and controls using an internal user client

- Any NEC Group employee who has created areas is referred to as an area-user with administrator privileges
- Create, update and delete a particular folder
- Register, update and delete the internal workers and the customers who are authorised to use folders
- Assign operational privileges to area-users with NEC Group employee/on-premise worker privileges
- Assign administrator privileges to any NEC Group employees registered as a folder-user

□ **Area-user with NEC Group employee/on-premise worker privileges**

A person who performs business data related operations using an internal user client

- All NEC Group employees and on-premise workers registered as folder-users by the area-user with administrator privileges are defined as area-users with NEC Group employee/on-premise worker privileges in the associated folder.
- Any on-premise workers cannot be defined as area-users with administrator privileges.

□ **Area-user with customer privileges**

A person who performs business data related operations using an external user client

- Any customers registered as folder-users by the area-user with administrator privileges are defined as area-users with customer privileges in the associated folder.
- Any customers cannot be defined as area-users with administrator privileges.

□ **System Administrator**

A person who is responsible for managing the TOE operations using the Internal Web server or the External Web server

- Perform the initial settings of the TOE
- Start and stop the TOE operation

□ **Auditor**

A person who is authorised to view the TOE audit trail data using the Internal Web server

- Implement the TOE auditing

1.4.3. Physical Scope of the TOE

The following subsections describe the operational environment of the TOE and the hardware/software structures.

1.4.3.1. Operational Environment of the TOE

The operational environment of the TOE is shown in Figure 1.

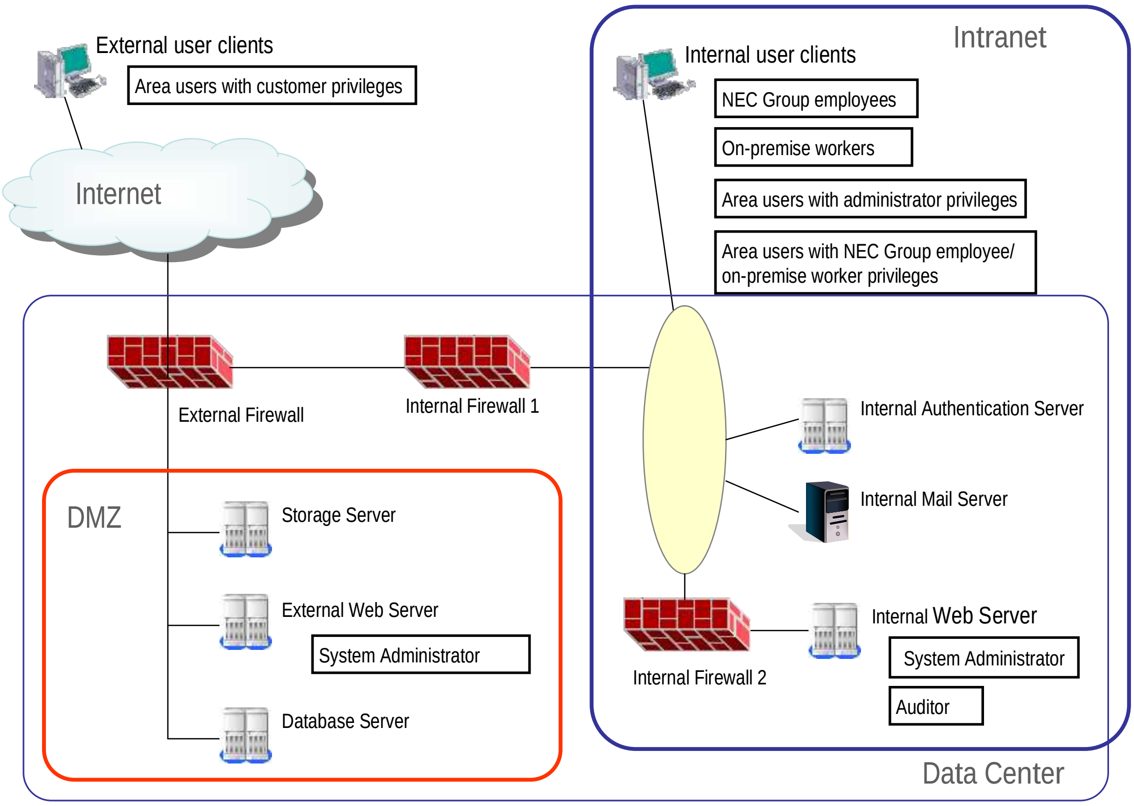


Figure 1 Operational Environment of the TOE

(1) Physical Layout and Network

All TOE-related internal clients connecting to the company's intranet are referred to as internal user clients, and all TOE-related external clients connecting to the Internet are referred to as external user clients.

These internal user clients are installed within the company's premises with physical entry controls where entering these premises is permitted only to NEC Group employees and those on-premise workers specifically authorised by the NEC Group employees.

The data center houses the TOE-related Internal Web Server, Internal Authentication Server, Internal Mail Server, Internal Firewall 1, Internal Firewall 2 and External Firewall. External Web Server, Storage Server and Database Server are particularly placed in the DMZ within the data center. The data center is protected by appropriate physical entry controls to ensure that only authorised personnel are allowed access to the facility and their actions are watched closely.

The DMZ is protected by External Firewall. It uses SSL for maintaining secure communications.

Internal Web Server, Internal Authentication Server and Internal Mail Server are protected by Internal Firewall 1. The Internal Web server is further protected by Internal Firewall 2 to ensure that only authorised personnel are allowed access. It uses SSL to maintain secure communications.

(2) External Web Server

The External Web server accepts business data related access requests from external user clients via Internet and External Firewall, and accesses Database Server or Storage Server in the DMZ. The System Administrator gain access to the External Web server directly.

(3) Internal Web Server

The Internal Web server accepts authentication requests from the internal user clients via Internet and Internal Firewall 2, and accesses the Internal Authentication server.

It also accepts business data related access requests from the internal user clients via Intranet and Internal Firewall 2, and accesses Database Server or Storage Server in the DMZ. The System Administrator and the Auditor gain access to the Internal Web server directly.

(4) Storage Server

Storage Server stores the business data uploaded by the internal users or the customers. Access to the server is performed via External Web Server or Internal Web Server.

(5) Database Server

Database Server stores the information about the business data that has been uploaded by internal users or customers. Access to the server is performed via External Web server or Internal Web Server.

(6) External User Client

External user clients are used by customers. They can have access to the External Web server via Internet and External Firewall.

(7) Internal User Client

Internal user clients are used by internal users. They can have access to the Internal Web server via Internet and Internal Firewall 2.

(8) External Firewall

External Firewall controls communications between Internet and the DMZ. It monitors packet flow to Storage Server, Database Server and External Web Server, and performs access control based on the predefined rules.

(9) Internal Firewall 1

Internal Firewall 1 controls communications between the Intranet and the DMZ or Internal Web Server.

(10) Internal Firewall 2

Internal Firewall 2 monitors packet flow to Internal Web Server, and performs access control based on the predefined rules.

(11) Internal Authentication Server

Internal Authentication Server is connected to the data center network and provides internal authentication services. The server can be accessed from the Internal Web server.

(12) Internal Mail Server

Internal Mail Server is connected to the data center network and provides the function to distribute e-mails. The server can be accessed from the Internal Web server.

1.4.3.2. Physical Scope of the TOE (Components)

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

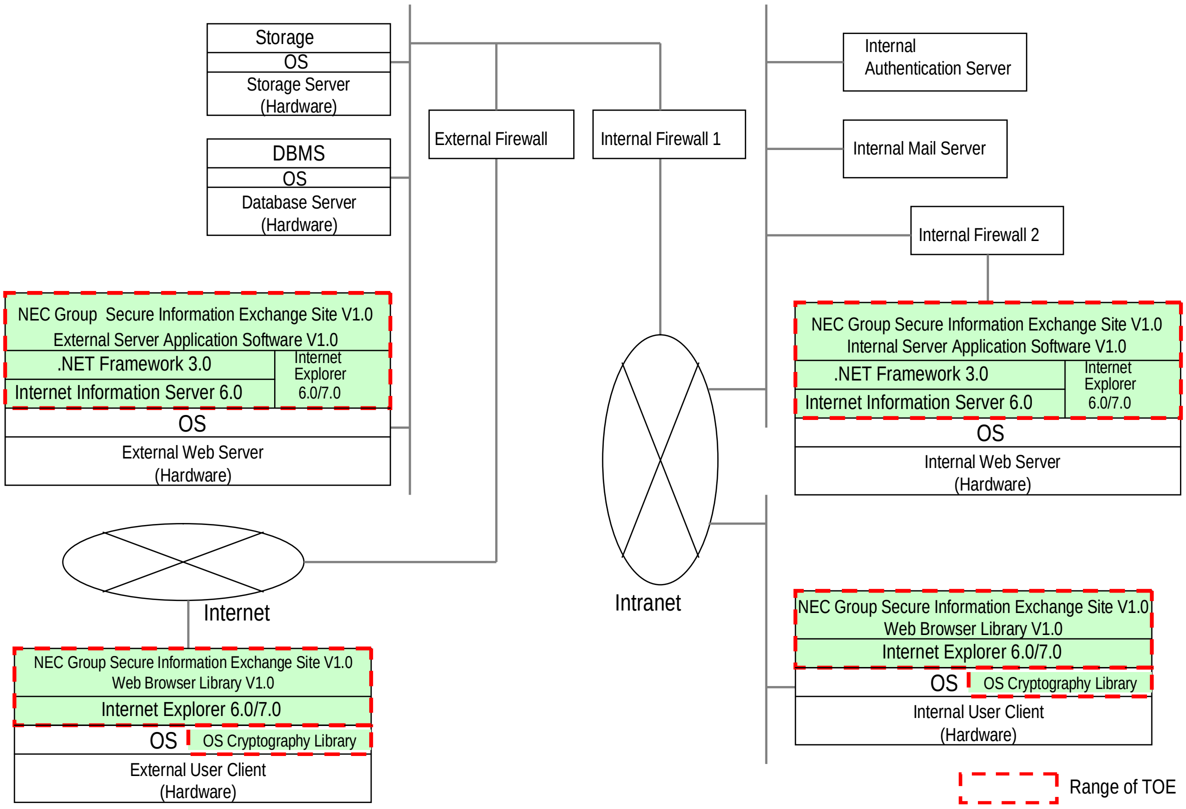

Storage
OS
Storage Server (Hardware)
DBMS
OS
Database Server (Hardware)
NEC Group Secure Information Exchange Site V1.0 External Server Application Software V1.0
.NET Framework 3.0
Internet Explorer 6.0/7.0
Internet Information Server 6.0
OS
External Web Server (Hardware)
Internet
NEC Group Secure Information Exchange Site V1.0 Web Browser Library V1.0
Internet Explorer 6.0/7.0
OS
OS Cryptography Library
External User Client (Hardware)
External Firewall
Internal Firewall 1
Intranet
Internal Authentication Server
Internal Mail Server
Internal Firewall 2
NEC Group Secure Information Exchange Site V1.0 Internal Server Application Software V1.0
.NET Framework 3.0
Internet Explorer 6.0/7.0
Internet Information Server 6.0
OS
Internal Web Server (Hardware)
NEC Group Secure Information Exchange Site V1.0 Web Browser Library V1.0
Internet Explorer 6.0/7.0
OS
OS Cryptography Library
Internal User Client (Hardware)
Range of TOE

Figure 2 Physical Scope of the TOE (Components)

The software configuration of the TOE is shown in Table 5. The TOE will operate correctly and reliably in the software configuration identified in the table.

Table 5 Software Configuration of the TOE

Equipment Name			
	Vendor Name	Product Name	Type
Internal Web Server			
	NEC	NEC Group Secure Information Exchange Site V1.0 Internal Server Application Software V1.0	Application software
	Microsoft	Internet Explorer 6.0/Internet Explorer 7.0	Web browser
	Microsoft	.NET Framework 3.0	Application execution environment

Equipment Name			
	Vendor Name	Product Name	Type
	Microsoft	Internet Information Server 6.0	Web server
External Web Server			
	NEC	NEC Group Secure Information Exchange Site V1.0 External Server Application Software V1.0	Application software
	Microsoft	Internet Explorer 6.0/Internet Explorer 7.0	Web browser
	Microsoft	.NET Framework 3.0	Application execution environment
	Microsoft	Internet Information Server 6.0	Web server
Internal User Client			
	NEC	NEC Group Secure Information Exchange Site V1.0 Web Browser Library V1.0	ActiveX Control
	Microsoft	Internet Explorer 6.0/Internet Explorer 7.0	Web browser
	Microsoft	OS Cryptographic Processing Library	OS library
External User Client			
	NEC	NEC Group Secure Information Exchange Site V1.0 Web Browser Library V1.0	ActiveX Control
	Microsoft	Internet Explorer 6.0/Internet Explorer 7.0	Web browser
	Microsoft	OS Cryptographic Processing Library	OS library

1.4.3.3. Physical Scope of the TOE (Guidance)

The following TOE guidance manuals are provided:

- NEC Group Secure Information Exchange Site Version 1.0 Operation Manual V1.04, January 8, 2008 (Japanese version)
- NEC Group Secure Information Exchange Site Version 1.0 User Manual V1.03, February 28, 2008 (Japanese version)
- NEC Group Secure Information Exchange Site Version 1.0 User Manual (for NEC Group users) V1.03, February 28, 2008 (Japanese version)

1.4.4. Logical Scope of the TOE

The logical configuration of the TOE is shown in Figure 3.

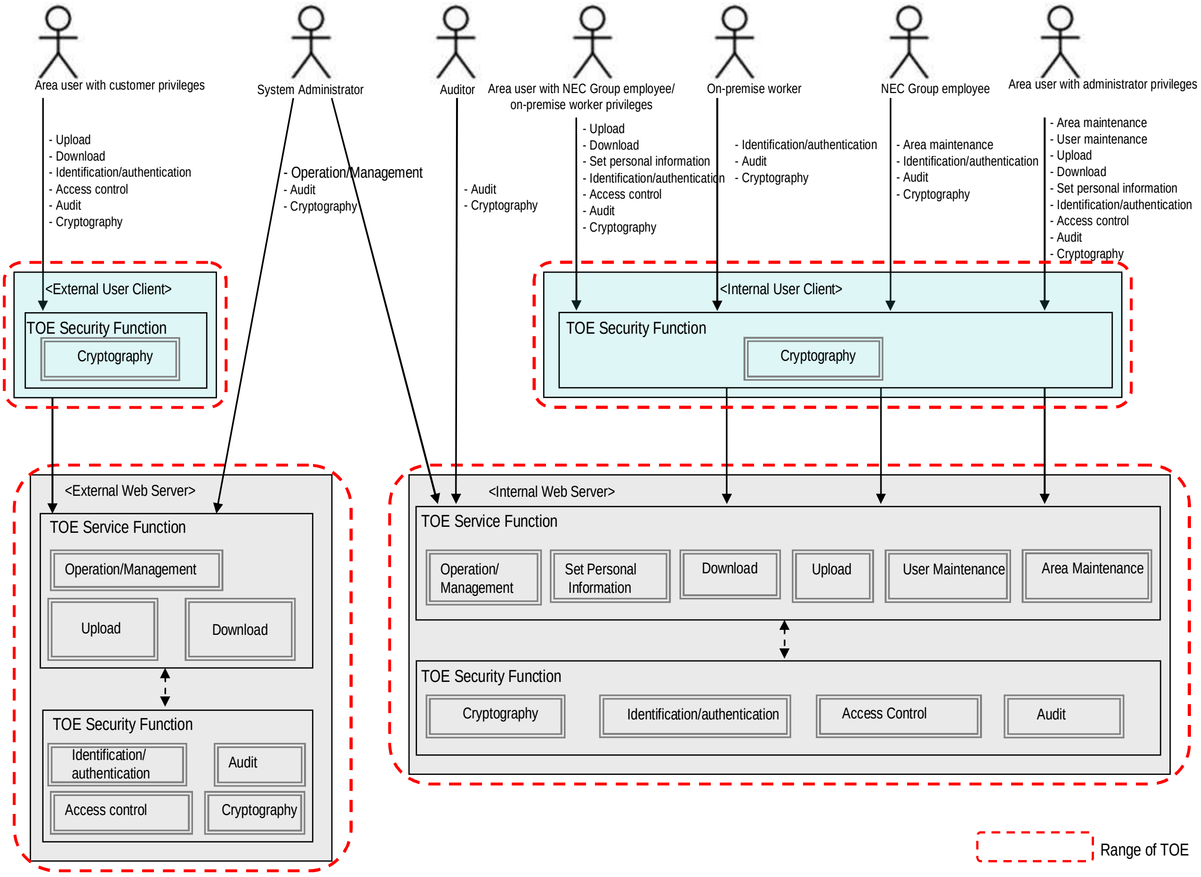


Figure 3 Logical Configuration of the TOE

The following subsections describe the logical configuration of the TOE, where the TOE-provided functions are classified into “Service” and “Security”.

1.4.4.1. TOE-Provided Service Function

TOE Service Function:
The following describes the TOE-provided service functions in details.

[Area Maintenance]
The Area Maintenance function is illustrated in Figure 4.

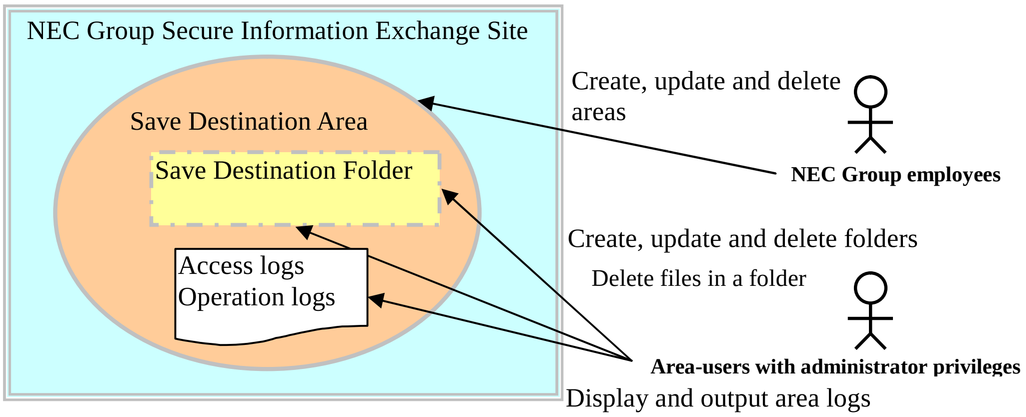

NEC Group Secure Information Exchange Site
Save Destination Area
Save Destination Folder
Access logs
Operation logs
Create, update and delete areas
NEC Group employees
Create, update and delete folders
Delete files in a folder
Area-users with administrator privileges
Display and output area logs

Figure 4 Area Maintenance

The Area Maintenance function is used to create, update and delete areas and folders, delete files in a folder, and display and output area logs.

The update area operation changes area names and the update folder operation changes folder names.

[User Maintenance]

The User Maintenance function is illustrated in Figure 5.

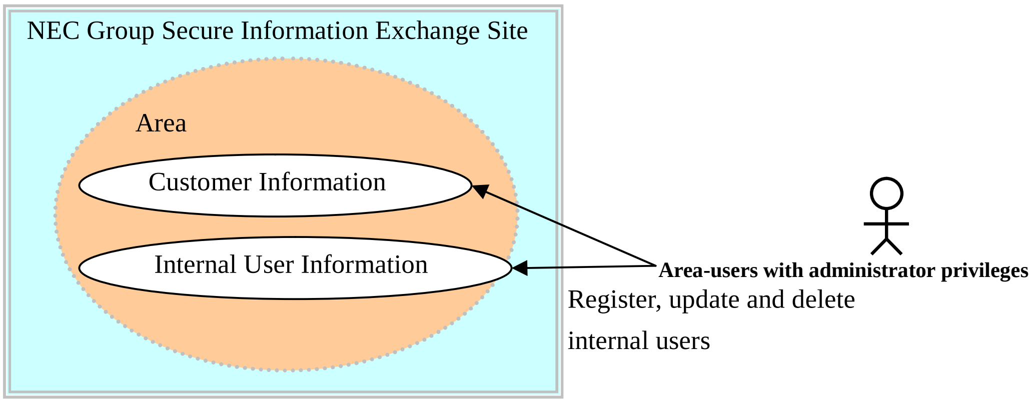

NEC Group Secure Information Exchange Site
Area
Customer Information
Internal User Information
Area-users with administrator privileges
Register, update and delete
internal users

Figure 5 User Maintenance

The User Maintenance function is used to register, update and delete the internal users and the customers. The update internal user/customer operation updates internal user/customer information.

[Upload Request]

The Upload Request function is illustrated in Figure 6.

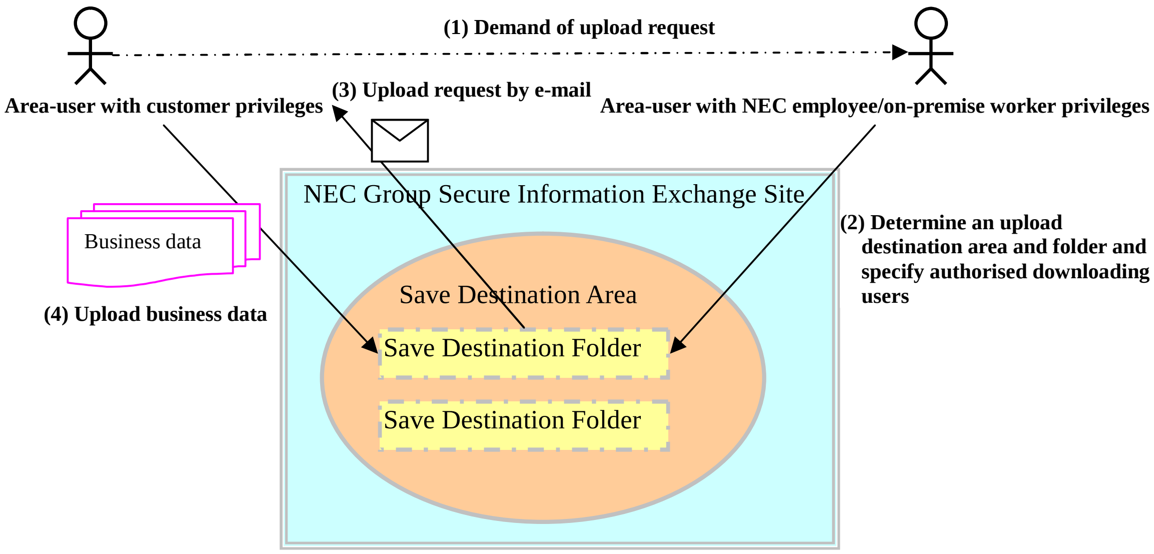

(1) Demand of upload request
Area-user with customer privileges
(3) Upload request by e-mail
Area-user with NEC employee/on-premise worker privileges
NEC Group Secure Information Exchange Site
Business data
(2) Determine an upload destination area and folder and specify authorised downloading users
Save Destination Area
(4) Upload business data
Save Destination Folder
Save Destination Folder

Figure 6 Upload Request

The Upload Request function enables area-users with customer privileges to upload their business data.

[Upload]

The Upload function is illustrated in Figure 7.

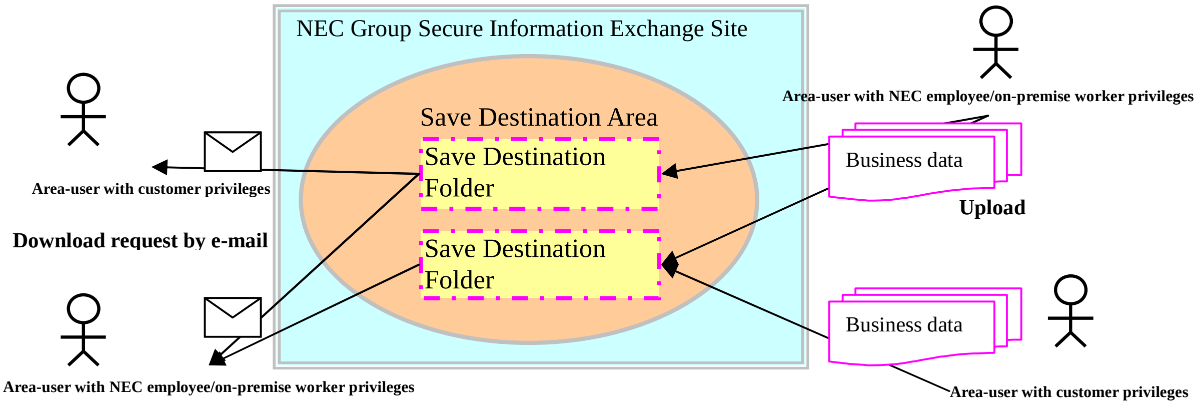

NEC Group Secure Information Exchange Site
Area-user with NEC employee/on-premise worker privileges
Save Destination Area
Save Destination Folder
Business data
Area-user with customer privileges
Upload
Download request by e-mail
Save Destination Folder
Business data
Area-user with NEC employee/on-premise worker privileges
Area-user with customer privileges

Figure 7 Upload

The Upload function enables uploading of business data.

[Download]

The Download function is illustrated in Figure 8.

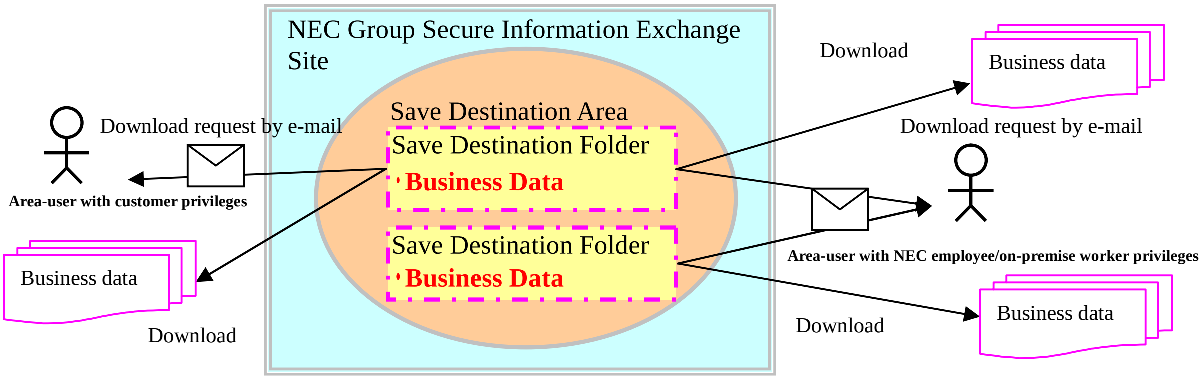

NEC Group Secure Information Exchange Site
Save Destination Area
Save Destination Folder
Business Data
Save Destination Folder
Business Data
Download request by e-mail
Area-user with customer privileges
Business data
Download
Download
Business data
Download request by e-mail
Area-user with NEC employee/on-premise worker privileges
Business data
Download

Figure 8 Download

The Download function enables downloading of business data. The downloading is allowed only one time. When all associated authorised users complete the downloading, the business data stored in the folder is automatically deleted.

[Set Personal Information]

The Set Personal Information is illustrated in Figure 9.

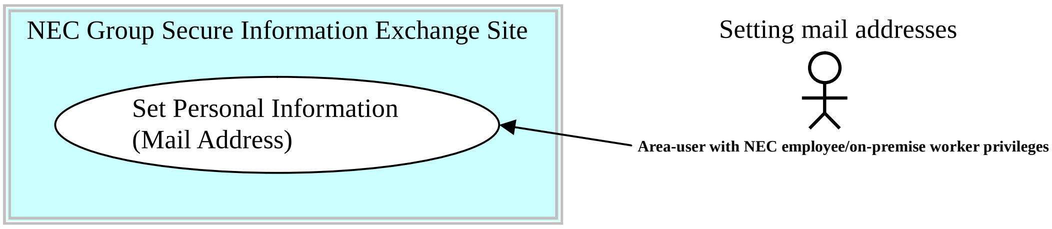

NEC Group Secure Information Exchange Site
Set Personal Information
(Mail Address)
Setting mail addresses
Area-user with NEC employee/on-premise worker privileges

Figure 9 Set Personal Information

The set personal information function is used to change mail addresses.

[Administration]

The Administration function is illustrated in Figure 10.

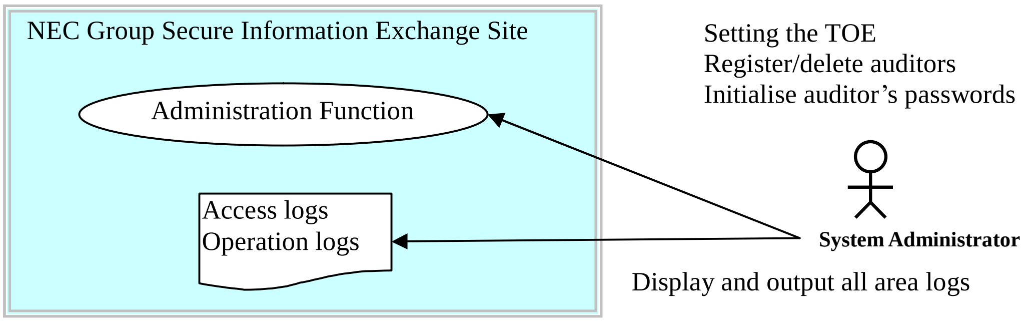


Figure 10 Operation

The Administration function is used to start and stop the TOE operation, register and delete Auditors, initialise Auditor's password, and display and output all area logs.

1.4.4.2. TOE-Provided Security Functions

The TOE-provided security functions are described below.

TOE Security Function

[Identification and Authentication]

The TOE provides the identification and authentication function to permit each user to access the TOE.

□ Area-user with customer privileges
- Identification by one-time URL and authentication by PIN must be succeeded.
- When the user enters an invalid PIN for the same one-time URL, the TOE counts the number of such failed PIN attempts. When the failed PIN attempts exceed the predetermined threshold, the TOE disables the issued one-time URL.

□ Area-user with NEC Group employee/on-premise worker privileges
- Identification by one-time URL must be succeeded.
- The user attempts access to the TOE via one-time URL and needs to be authenticated by the internal authentication system. When the user fails in the authentication, the TOE counts the number of such failed authentication attempts. When the number of failed authentication attempts exceeds the predetermined threshold, the TOE disables the issued one-time URL.

□ NEC Group employee and on-premise worker
- Identification by user ID must be succeeded.

□ System Administrator
- Identification by URL must be succeeded.

□ Auditor
- Identification by URL must be succeeded.

[Auditing]

The TOE generates an audit record when an auditable event occurs. The Auditor uses this function to view and search audit records.

[Access Control]

Based on the defined user privileges the TOE determines whether to permit each TOE user to access the business data and the associated area and folder storing that data.

[Encryption]

The TOE provides all TOE users with the function to protect communications data between Web servers and Web browsers by means of SSL encryption and decryption.

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 are listed below.

Common Criteria for Information Technology Security Evaluation

Part 1:	Introduction and general model, September 2006, version 3.1, Japanese version 1.2
Part 2:	Security components, September 2006, version 3.1, Japanese version 1.2
Part 3:	Security assurance components, September 2006, version 3.1, Japanese version 1.2

CC Part 2 Conformance:	CC Part 2 Extensions
CC Part 3 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 conformance rationale since it does not claim any PP conformance.

3. Security Problem Definition

This chapter describes threats, organizational security policies and assumptions.

3.1. Threats

This section describes the assets protected by the TOE and the threats.

3.1.1. Assets protected by the TOE

Types of user data, assets to be protected by the TOE, are shown in Table 6.

Table 6 User Data

Data Name	Description
Business data	Data uploaded by area-users with administrator privileges, those with NEC Group employee/on-premise worker privileges and those with customer privileges
Upload area information	Information about folders stored in the area to which business data is uploaded, the customers who made upload request, the users who performed the upload, and who permitted the download.
Area-user information	Information about area-users with NEC Group employee privileges, those with on-premise worker privileges and those with customer privileges who are registered by area-users with administrator privileges.

3.1.2. Threats

This section describes threats against the TOE.

T.SPOOFING (spoofing)

A third party not having any specialised knowledge may maliciously access the TOE via Internet or a TOE user may masquerade as an authorised user and access the TOE via NEC Intranet to destroy or disclose the business data.

T.ILLEGAL_ACCESS (illegal access)

An authorised TOE user, who is an NEC group employee, on-premise worker, area-user with administrator privileges, area-user with NEC employee/on-premise worker privileges and area-user with customer privileges may destroy or disclose the business data, upload area information or area-user information by performing the following operations that are not authorised for each user role.

- Creating, updating or deleting areas by TOE users other than the NEC Group employees.
- Creating, updating or deleting folders by TOE users other than area-users with administrator privileges.
- Registering, updating or deleting folder-users (NEC Group employees, on-premise workers and customers) by TOE users other than area-users with administrator privileges.
- Downloading, uploading or deleting business data by TOE users other than area-users with NEC Group employee/on-premise worker privileges or those with customer privileges.

T.LISTEN-IN_NW_DATA (listen-in network data)

A third party not having any specialised knowledge may maliciously listen in or tamper business data that are exchanged between Web servers and networks to disclose, destroy or tamper the data.

T.MISDELIVERY (misdelivery)
An authorised TOE user may accidentally send a URL to an unintended customer, resulting in the disclosure of business data.

3.2. Organisational security policies

This section describes organizational security policies that are applied to the TOE and its operational environment.

P.ADMIN_IDENTIFY (identification of an administrator)
The System Administrator and the Auditor who use the TOE are subject to the TOE identification to keep a record of TOE access logs.

P.AUDIT_LOG (audit logs)
To track unauthorised operations on the TOE assets to be protected, the ability to access the TOE audit logs must be restricted to the Auditor only.

3.3. Assumptions

This section describes the assumptions on the environments for physical security, personnel security and TOE usage.

3.3.1. Assumptions on the environment for physical security

The assumptions on the environment for physical security are as follows:

A.DATACENTER (data center)
It is assumed that Internal Web Server, External Web Server, Database Server, Storage Server, Internal Authentication Server and Internal Mail Server are all placed in the data center which is protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

A.NETWORK (network)
It is assumed that access to the Internal Web server from the Intranet is restricted by Internal Firewall 2 that is appropriately configured.
It is assumed that access to the External Web server from the Internet is restricted by External Firewall that is appropriately configured.

A.SYSTEM_ADMIN (restrictions on TOE access by System Administrator)
It is assumed that the System Administrator accesses the Internal Web server or External Web server directly.

A.AUDIT_ADMIN (restrictions on TOE access by System Administrator)
It is assumed that the Auditor accesses the Internal Web server directly.

3.3.2. Assumptions on the environment for personnel security

The assumptions on the environment for personnel security are as follows:

A.ADMINISTRATOR (trusty administrator)
It is assumed that Operations Manager, System Administrator, Auditor, Storage Administrator and Database Administrator perform actions that are assigned to their roles, and never perform malicious actions.

3.3.3. Assumptions on the environment for TOE usage

No assumptions on the environment for TOE usage.

4. Security Objectives

This chapter describes security objectives for the TOE, security objectives 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 (customer identification and authentication)
The TOE shall generate a one-time URL and an associated PIN for area-users with customer privileges when they use the TOE. The TOE shall execute identification by one-time URL and authentication by PIN, and permit only those who succeeded within the specified number of identification and authentication attempts to use the TOE.

O.IDENTIFY (internal user identification)
The TOE shall identify NEC Group employees and on-premise workers when they use the TOE.

O.ADMIN_IDENTIFY (administrator identification)
The TOE shall identify the System Administrator and the Auditor when they use the TOE.

O.ACCESS_CONTROL (access control)
The TOE shall protect user data against unauthorised access by providing the TOE users with only necessary functions from among the following functions dependent on types of their roles.

- Only NEC Group employees are allowed to create, update and delete areas.
  (The NEC Group employees who created areas are defined as area-users with administrator privileges for that area).
- Only area-users with administrator privileges are allowed to create, update and delete the folders stored in the area.
- Only area-users with administrator privileges are allowed to register, update and delete users (NEC Group employees, on-premise workers and customers) on the folders.
  (The users who have been registered on each folder are defined as area-users with NEC employee/on-premise worker or customer privileges).
- Area-users with NEC Group employee/on-premise worker or customer privileges are allowed to download/upload or delete the business data stored in the folders specified by area-users with administrator privileges.

O.AUDIT (audit)
The TOE shall manage the security related events concerning access control and identification/authentication functions as audit logs. Since attacks against SSL communication are not assumed, the events concerning encryption are excluded from auditing. In addition, persons accessible to the audit logs must be restricted to Auditors only. The audit logs must include date and time of events, place of events and the result.

O.ENCRYPT (encryption)
The TOE shall use SSL for communication between a TOE user and the TOE, and keep the user data confidential to protect against improper tampering or disclosure.

4.2. Security objectives for the operational environment

Security objectives for the operational environment are listed below.

OE.TRUSTED_ROLE (trusted role)

The Operations Manager shall designate System Administrator, Storage Administrator, Database Administrator and Auditor. The Operations Manager shall also have them understand their roles and manage them to prevent from their taking malicious actions.

OE.NETWORK (network environment)

All the Company networks to which Internal/External Web servers are connected shall be isolated from the external environment using an appropriately configured firewall.

OE.ADMIN_TRAINING (administrator education and training)

All Database Manager, Storage Manager, System Manager and Auditor shall be educated and trained on the safety management of the TOE assets and the TOE. In addition, the Auditor must understand methods to check and handle the audit logs generated by the TOE.

OE.DATACENTER (data center environment)

The data center shall be protected by appropriate entry controls to ensure that only authorised Operations Manager, Auditor, System Administrator, Storage Administrator and Database Administrator are allowed access, and their actions in the data center must be monitored.

OE.AUTHENTICATION (internal authentication server)

All NEC Group employees and on-premise workers using the TOE shall use the internal authentication service.

OE.SEND_PIN (transmission of PIN)

The PIN shall be sent to area-users with customer privileges, who are legitimate TOE users, in ways different from one-time URL used by the TOE, for example, telephone or e-mail using another address.

OE.SYSTEM_ADMIN (restriction of use by System Administrator)

The System Administrator shall access the Internal Web server or External Web server directly.

OE.AUDIT_ADMIN (restriction of use by Auditor)

The Auditor shall access the Internal Web server directly.

OE.OS_TIMESTAMP (OS timestamp)

The OS running the TOE shall provide a high reliable timestamp.

4.3. Security objectives rationale

This section describes the relation between security objectives and the security problem definition, and the validity of security objectives.

4.3.1. Relation between security objectives and the security problem definition

The relation between security objectives and the security problem definition (threats, organizational security policies and assumptions) is shown in Table 7.

The “×” on the table represents correspondences.

Table 7 Relation between security objectives and the security problem definition

	T.SPOOFING	T.ILLEGAL_ACCESS	T.LISTEN-IN_NW_DATA	T.MISDELIVERY	P.ADMIN_IDENTIFY	P.AUDIT_LOG	A.DATACENTER	A.NETWORK	A.ADMINISTRATOR	A.SYSTEM_ADMIN	A.AUDIT_ADMIN
O.I&A	×			×							
O.IDENTIFY	×										
O.ADMIN_IDENTIFY					×						
O.AUDIT	×	×				×					
O.ACCESS_CONTROL		×									
O.ENCRYPT			×								
OE.TRUSTED_ROLE									×		
OE.NETWORK								×			
OE.ADMIN_TRAINING	×	×							×		
OE.DATACENTER							×				
OE.AUTHENTICATION	×										
OE.SEND_PIN	×			×							
OE.SYSTEM_ADMIN										×	
OE.AUDIT_ADMIN											×
OE.OS_TIMESTAMP	×	×									

As shown, each security objective corresponds to one or more threats, organisational security policies and assumptions.

4.3.2. Validity of security objectives

This section describes the security objectives rationale for each security problem.

4.3.2.1. Security objectives rationale for threats

This section describes how the following threats are countered by the security objectives:

T.SPOOFING (spoofing)

This threat may be posed by a malicious third party with no specialised knowledge attempting to access the TOE via Internet, or by a TOE user attempting to access the TOE via NEC’s Intranet. Specific spoofing methods that may be employed by these persons and the effective security objectives associated with these methods are as follows:

a. Accessing the TOE by a malicious third party with no specialised knowledge

This attack may be posed by a malicious third party with no specialised knowledge attempting to access the TOE to manipulate the business data. This threat can be diminished by limiting the time duration for which a user can gain one-time URL based access to the identification information or by limiting the number of incorrect consecutive PIN authentication attempts (O.I&A). In addition, since the PIN is sent separately from one-time URL, the possibility of the PIN information being captured over the Internet by sniffers is minimized thus the threat can be diminished (OE.SEND_PIN). Furthermore, the threat can be mitigated by collecting audit logs including reliable time (O.AUDIT and OE.OS_TIMESTAMP), and by implementing Auditor's checking the collected logs and taking appropriate actions when the possibility of attacks has been increased (OE.ADMIN_TRAINING).

b. Usage of the TOE not in compliance with TOE user's roles

This attack is the unauthorised use of the TOE not in compliance with the predefined TOE user's roles. This threat can be diminished by authenticating all NEC Group employees and on-premise workers who attempt to use internal authentication services (OE.AUTHENTICATION) and by identifying their user roles (O.IDENTIFY). Furthermore, the threat can be mitigated by collecting audit logs including reliable time (O.AUDIT and OE.OS_TIMESTAMP), and by implementing Auditor's checking the collected logs and taking appropriate actions when the possibility of attacks has been increased (OE.ADMIN_TRAINING).

Hence, the security objectives to counter the threat are O.I&A, O.IDENTIFY, O.AUDIT, OE.ADMIN_TRAINING, OE.AUTHENTICATION and OE.OS_TIMESTAMP.

T.ILLEGAL_ACCESS (illegal access)

This threat may be performed by legitimate TOE users. The following describes the methods of illegal accesses that may be employed by them and the effective countermeasures corresponding to each method.

a. Unauthorised operations

This threat can be removed by assigning appropriate access privileges for each TOE operation to restrict permissible user operations (O.ACCESS_CONTROL).

Furthermore, the threat can be mitigated by collecting audit logs including reliable time (O.AUDIT and OE.OS_TIMESTAMP), and by implementing Auditor's checking the collected logs and taking appropriate actions when the possibility of attacks has been increased (OE.ADMIN_TRAINING).

Hence, the security objectives to counter the threat are O.AUDIT, O.ACCESS_CONTROL, OE.ADMIN_TRAINING and OE.OS_TIMESTAMP.

T.LISTEN-IN_NW_DATA (listening in network data)

This threat may be posed by malicious third parties with no specialised knowledge. The following describes methods of illegal accesses to the network data that may be employed by them and the effective security objectives corresponding to each method.

a. Interception, destruction or manipulation of communications data between the External Web server and an external user client or between the Internal Web server and an internal user client.

This attack may include, but not limited to, illicit acquisition of data transmitted between the External Web server and an external user client or between the Internal Web server and an internal Web client, and transmission of destructed/manipulated communications data. This threat can be diminished by keeping such data confidential using SSL (O.ENCRYPT).

Hence, the security objective to counter the threat is O.ENCRYPT.

T.MISDELIVERY (misdelivery)

This threat may be posed by authorised TOE users. The following describes the possibility of causing the misdelivery of business data by them and the effective security objectives corresponding to it.

a. Delivery to incorrect customers

This threat may be caused by registering an incorrect mail address on the TOE and sending a URL referencing a specific business data source to that mail address.

The threat can be diminished by requiring not only URL but also PIN authentication before permitting access to the business data (O.I&A). It can also be diminished by sending a PIN by means of telephone or e-mail with a different mail address to area-users with customer privileges in advance (OE.SEND_PIN).

Hence, the security objectives to counter the threat are OE.SEND_PIN and O.I&A.

4.3.2.2. Security objectives rationale for organisational security policies

This section describes the effectiveness of the security objectives to counter the organisational security policies.

P.ADMIN_IDENTIFY (identification of administrators)

This organisational security policy addresses the identification of System Administrator and Auditor who use the TOE. Effective security objectives for this requirement are as follows:

a. Identification of System Administrators and Auditors

The TOE provides the function to identify System Administrator and Auditor.

The security objectives corresponding to this policy are O.ADMIN_IDENTIFY.

Hence, P.ADMIN_IDENTIFY can be achieved by satisfying O.ADMIN_IDENTIFY.

P.AUDIT_LOG (audit logs)

This organisation security policy addresses the access to audit logs. Effective security objectives for this requirement are as follows:

a. Restricting access to audit logs to only Auditor

The TOE provides the function to permit only Auditor to view audit logs.

The security objectives corresponding to this policy are O.AUDIT.

Hence, P.AUDIT_LOG can be achieved by satisfying O.AUDIT.

4.3.2.3. Security objectives rationale for assumptions

This section describes the effectiveness of the security objectives to counter the assumptions.

A.DATACENTER (data center)

This assumption addresses a place where TOE-related hardware is installed. Effective security objectives for this requirement are as follows:

a. Restricting buildings where TOE-related hardware is installed

The TOE and the TOE-related hardware shall be installed inside the building such as data center where physical entry controls are implemented to ensure that only authorised personnel are allowed access, and all visitors are supervised.

The environmental security objective corresponding to this assumption is OE.DATACENTER.

Hence, A.DATACENTER can be achieved by satisfying OE.DATACENTER.

A.NETWORK (network)

This assumption addresses the creation of the network environment. Effective security objectives are:

a. Restricting access to networks to only necessary communications

Access to the Internal Web server running the TOE via Intranet shall be restricted to only necessary communications using the Internal Firewall 2 that is appropriately configured.

Access to the Internal Web server via Internet shall be restricted to only necessary communications using the External Firewall that is appropriately configured.

The environmental security objectives corresponding to this assumption are OE.NETWORK.

Hence, A.NETWORK can be achieved by satisfying OE.NETWORK.

A.ADMINISTRATOR (trusted administrator)

This assumption addresses trusted administrators. Effective security objectives are:

a. Participation in education and training opportunities

All Database Administrator, Storage Administrator, System Administrator and Auditor shall participate in education and training opportunities relating to the TOE assets and safety management.

The environmental security objectives corresponding to this assumption are OE.ADMIN_TRAINING.

b. Stringent personal selection and appropriate management

The Operations Manager shall make stringent personal selection in accordance with roles of System Administrator, Storage Administrator, Database Administrator and Auditor, have them understand their assigned roles and manage them to prevent their malicious actions.

The environmental security objectives corresponding to this assumption are OE.TRUSTED_ROLE.

To satisfy the above requirements (a) and (b) is to satisfy the security objectives of A.ADMINISTRATOR. Hence, A.ADMINISTRATOR can be achieved by satisfying OE.ADMIN_TRAINING and OE.TRUSTED_ROLE.

A.SYSTEM_ADMIN (restrictions on System Administrator's use of the TOE)
This assumption addresses restrictions on System Administrator's use of the TOE. Effective security objectives are:

a. Restrictions on System Administrator's use of the TOE
The System Administrator shall be permitted access to the TOE using the Internal or External Web server. The environmental security objectives corresponding to this assumption are OE.SYSTEM_ADMIN.

Hence, A.SYSTEM_ADNIN can be achieved by satisfying OE.SYSTEM_ADMIN.

A.AUDIT_ADMIN (restrictions on Auditor's use of the TOE)
This assumption addresses restrictions on Auditor's use of the TOE. Effective security objectives are:

a. Restrictions on Auditor's use of the TOE
The Auditor shall be permitted access to the TOE using the Internal Web server. The environmental security objectives corresponding to this assumption are OE.AUDIT_ADMIN.

Hence, A.AUDIT_ADMIN can be achieved by satisfying OE.AUDIT_ADMIN.

5. Extended Components Definition

This chapter describes Extended Components Definition.

5.1. Extended Functional Components

FTP_ITC_EX "Trusted channel inside the TOE" is defined as an extended component in the security functional components defined in CC Part 2. The reason for defining this extended component is as follows:

[Necessity of an extended component]

- It is needed to define a requirement of protecting data to be transmitted between two different TOEs (trusted channel) but a precisely defined requirement does not exist in CC Part 2 Security Functional Requirements.

[Reason for applying the class to the extended functional component]

- The existing FTP class has been applied because the requirement addresses a trusted communication.

[Reason for applying the family to the extended functional component]

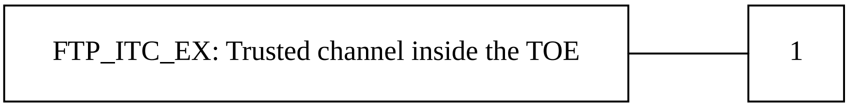
- This newly defined requirement addresses a trusted channel between two different TOEs but it does not apply to the existing families in the FTP class, FTP_ITC (the TSF and a trusted IT product) and FTP_TRP (the TSF and a user). Hence, ITC_EX has been identified and defined as a new family.

5.1.1. Trusted channel inside the TOE (FTP_ITC_EX)

Family Behaviour

This family defines requirements for the creation of a trusted channel between two different TOE components for the performance of security critical operations. This family should be included whenever there are requirements for the secure communication of user or TSF data between two different TOE components.

Component levelling



FTP_ITC_EX.1 Trusted channel inside the TOE, requires that the TSF provide a trusted communication channel between two different TOE components.

Management: FTP_ITC_EX.1

The following actions could be considered for the management functions in FMT:

- Configuring the actions that require trusted path, if supported.

Audit: FTP_ITC_EX.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Failure of the trusted channel functions.
- Basic: All attempted uses of the trusted channel functions.

FTP_ITC_EX.1 Trusted channel inside the TOE

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC_EX.1.1

The TSF shall provide a communication channel between two different TOE components that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC_EX.1.2

The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].

6. Security Requirements

This chapter describes security requirements.

6.1. Definition of subjects and objects in the TOE

Tables 8, 9, 10 and 11 below describe the subjects, objects, operations and security attributes relevant to the TOE security functions.

Table 8 List of subjects

SFR	Subject	Definition
FDP_ACC.1 FDP_ACF.1	NEC Group employee process	A process to run on behalf of NEC Group employees. It has security attributes such as type of user, user identity and user-URL.
	On-premise worker process	A process to run on behalf of on-premise workers. It has security attributes such as type of user, user identity and user-URL.
	Customer process	A process to run on behalf of customers. It has security attributes such as type of user, user identity and user-URL.

Table 9 List of objects

SFR	Object	Definition
FDP_ACC.1 FDP_ACF.1	Area	The area stores the information relevant to a specific area to which business data files are uploaded. It has a security attribute of authorised area-user information.
	Folder	The folder stores the information relevant to a specific folder to which business data files are uploaded. It has security attributes of authorised folder-user information and authorised user-URL.
	Business data file	The business data file stores the information relevant to the uploaded business data files. It has security attributes of uploader information, downloader information and authorised user-URL.

Table 10 List of operations

SFR	Operation	Description
FDP_ACC.1 FDP_ACF.1	Create areas	This operation is used to create areas
	View/update area names	This operation is used to view/update area names
	Delete areas	This operation is used to delete areas
	Create folders	This operation is used to create folders
	View folder names	This operation is used to view folder names
	Update folder names	This operation to update folder names
	View/update mail addresses (within a specific area)	This operation is used to view/update mail addresses of users registered within a specific area
	View/update an mail address (user itself)	This operation is used to view/update an mail address of a user itself
	Delete folders	This operation is used to delete folders
	Upload request	This operation is used to register an upload request
	Upload	This operation is used to upload business data files

SFR	Operation	Description
	Upload (one-time URL)	This operation is used to upload business data files using one-time URL
	Delete uploaded files (one-time URL)	This operation is used to delete uploaded business data files
	Delete uploaded files	This operation is used to delete uploaded business data files
	Download/confirmation of uploaded files	This operation is used to download or confirm uploaded files
	Download/confirmation of uploaded files using one-time URL	This operation is used to download or confirm uploaded files using one-time URL

Table 11 List of security attributes

SFR	Security attributes	Description	Value
FDP_ACC.1 FDP_ACF.1	Type of user	The attribute specifying type of each area-user	- NEC Group employee - On-premise worker - Customer
	User identity	The attribute specifying each area-user	The value of user identifier
	User-URL	The attribute specifying each one-time URL user	The value of one-time URL
	Authorised area-user information	The attribute specifying each authorised area-user	A list of values of user identifiers
	Authorised folder-user information	The attribute specifying each authorised folder-user	A list of values of user identifiers
	Uploader information	The attribute specifying the user who uploaded a business data file	The value of user identifier or one-time URL
	Downloader information	The attribute specifying the user who are permitted to download a business data file	A list of values of user identifiers
	Authorised user-URL	The attribute specifying the user who are permitted to use a specific folder and a business data file using one-time URL	A list of values of one-time URLs

6.2. Security functional requirements

This section describes the security functional requirements for each class.

6.2.1. FAU: Security audit

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:

- Start-up 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

The following shows auditable minimum level of actions (definitions in CC) for each selected functional requirement, associated auditable events during TOE operation (see Table 12), and individually defined auditable events.

Table 12 Auditable actions below the basic level (definitions in CC) and associated auditable events

Functional requirements	Auditable actions	Auditable events
FAU_GEN.1	None	None
FAU_GEN.2	None	None
FAU_SAR.1	- Basic: Reading of information from the audit records.	- Viewing audit records
FAU_SAR.2	- Basic: Unsuccessful attempts to read information from the audit records.	- Failure in viewing audit records
FAU_SAR.3	- Detailed: the parameters used for the viewing.	None
FDP_ACC.1	None	None
FDP_ACF.1	- Minimum: Successful requests to perform an operation on an object covered by the SFP. - Basic: All requests to perform an operation on an object covered by the SFP. - Detailed: The specific security attributes used in making an access check.	- Successful/unsuccessful attempts to create an area by NEC group employees. - Successful/unsuccessful attempts to update or delete an area by NEC group employees. - Successful/unsuccessful attempts to create, update or delete folders by area-users with administrator privileges. - Successful/unsuccessful attempts to register upload requests by area-users with NEC Group employee/on-premise worker privileges. - Successful/unsuccessful attempts to register upload requests by area-users with administrator privileges. - Successful/unsuccessful attempts to upload business data by area-users with NEC Group employee/on-premise worker privileges. - Successful/unsuccessful attempts to upload business data by area-users with customer privileges. - Successful/unsuccessful attempts to upload

Functional requirements	Auditable actions	Auditable events
		business data by area-users with administrator privileges. - Successful/unsuccessful attempts to delete uploaded files by area-users with NEC Group employee/on-premise worker privileges. - Successful/unsuccessful attempts to delete uploaded files by area-users with customer privileges. - Successful/unsuccessful attempts to delete files from the folder by area-users with administrator privileges. - Successful/unsuccessful attempts to download business data by area-users with NEC Group employee/on-premise worker privileges. - Successful/unsuccessful attempts to download business data by area-users with customer privileges. - Successful/unsuccessful attempts to download business data by area-users with administrator privileges.
FIA_AFL.1a	- Minimum: The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).	- Invalidation of a one-time URL in case that the cumulative number of unsuccessful authentication attempts reached a specific threshold.
FIA_AFL.1b	- Minimum: The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).	- Invalidation of a one-time URL in case that the cumulative number of unsuccessful authentication attempts reached a specific threshold.
FIA_ATD.1	None	None
FIA_SOS.2a	- Minimum: Rejection by the TSF of any tested secrets; - Basic: Rejection or acceptance by the TSF of any tested secret; - Detailed: Identification of any changes to the defined quality metrics.	- Verification of the defined quality metrics of one-time URL (successful/unsuccessful)

Functional requirements	Auditable actions	Auditable events
FIA_SOS.2b	- Minimum: Rejection by the TSF of any tested secrets; - Basic: Rejection or acceptance by the TSF of any tested secret; - Detailed: Identification of any changes to the defined quality metrics.	- Verification of the PIN quality metrics (successful/unsuccessful)
FIA_UAU.2	- Minimum: Unsuccessful use of the authentication mechanism; - Basic: All use of authentication mechanisms - Detailed: All TSF mediated actions performed before authentication of the user.	- Successful/unsuccessful authentication of area-users with customer privileges.
FIA_UID.2a	- Minimum: Unsuccessful use of the user identification mechanism, including the user identify provided; - Basic: All use of the user identification mechanism, including the user identify provided.	- Successful/unsuccessful identification of area-users with customer privileges. - Successful/unsuccessful identification of area-users with NEC Group employee/on-premise worker privileges using one-time URL.
FIA_UID.2b	- Minimum: Unsuccessful use of the user identification mechanism, including the user identify provided; - Basic: All use of the user identification mechanism, including the user identify provided.	None
FIA_UID.2c	- Minimum: Unsuccessful use of the user identification mechanism, including the user identify provided; - Basic: All use of the user identification mechanism, including the user identify provided.	None
FIA_USB.1	- Minimal: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject). - Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).	None
FMT_MSA.1	- All modifications of the initial values of security attributes.	- Modification of authorised area-user information - Modification of authorised folder-user information
FMT_MSA.3a	- Basic: Modifications of the default setting of permissive or restrictive rules. - Basic: All modifications of the initial values	None

Functional requirements	Auditable actions	Auditable events
	of security attributes.	
FMT_MSA.3b	- Basic: Modifications of the default setting of permissive or restrictive rules. - Basic: All modifications of the initial values of security attributes.	None
FMT_SAE.1	- Basic: Specification of the expiration time for an attribute; - Basic: Action taken due to attribute expiration.	None
FMT_SMF.1	- Minimal: Use of the management functions.	None
FMT_SMR.1	- Minimal: Modifications to the group of users that are part of a role; - Detailed: Every use of the rights of a role.	None
FTP_ITC_EX.1	- Minimal: Failure of the initiator and target of failed trusted channel functions. - Basic: All attempted uses of the trusted channel functions.	None

[assignment: other specifically defined auditable events]
None

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]

- Company code
- Department code

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]
Auditor
[assignment: list of audit information]
{date and time of event, type of event, user code, event result (success or fail), company code and department code}

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
Hierarchical 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.

FAU_SAR.3 Selectable audit review
Hierarchical 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*].
[selection: searches, sorting, ordering]
Searches
[assignment: criteria with logical relations]
Searchable range of dates

6.2.2. FDP: User data protection

FDP_ACC.1 Subset access control
Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1
The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].
[assignment: access control SFP]
<Business operation access control policy>
[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].
<Subjects>

- NEC Group employee process
- On-premise worker process
- Customer process

<Objects>

- Area
- Folder
- Business data file

<List of operations among subjects and objects covered by the SFP>

- Creation of areas by NEC Group employees
- View and update of area names by NEC Group employees
- Delete of areas by NEC Group employees
- Creation of folders by NEC Group employees
- View of folder names by NEC Group employees
- Update of folder names by NEC Group employees
- View and update of email addresses (within an area) by NEC Group employees
- View and update of an email address (one's own mail address) by NEC Group employees
- Delete of folders by NEC Group employees
- Registration of an upload request by NEC Group employees
- Upload of business data files by NEC Group employees
- Delete of upload files by the NEC Group employees
- Download or confirmation of uploaded files by NEC Group employees
- Download or confirmation of uploaded files by NEC Group employees using one-time URL
- View of folder names by on-premise workers
- View and update of a mail address (one's own mail address) by on-premise workers
- Registration of an upload request by on-premise workers
- Upload of business data files by on-premise workers
- Delete of uploaded files by on-premise workers
- Download or confirmation of uploaded files by on-premise workers
- Download or confirmation of uploaded files by on-premise workers using one-time URL
  View of folders by customers
- Upload of business data files by customers using one-time URL
- Delete of uploaded files by customers using one-time URL
- Downloading of business data by customers using one-time URL

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF1.1

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

[assignment: access control SFP]

<Business operation 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]

Table 13 lists the subjects controlled under the SFP, and for each, the SFP-relevant security attributes.

Table 13 Subjects and the corresponding security attributes

Controlled subjects	Corresponding SFP-relevant security attributes
NEC Group employee process On-premise worker process Customer process	Type of user
	User identity
	User-URL

Table 14 lists the objects controlled under the SFP, and for each, the SFP-relevant security attributes.

Table 14 Objects and the corresponding security attributes

Controlled objects	Corresponding SFP-relevant security attributes
Area Folder Business data file	Authorised area-user information
	Authorised folder-user information
	Uploader information
	Downloader information
	Authorised user-URLs

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

For details, see Table 15 below.

Table 15 Rules governing access to the TOE

Controlled subjects	Security attributes of subjects	Controlled operations	Controlled objects	Security attributes of objects
NEC group employee process	- Type of user: NEC Group employee	Create areas	Areas	None
	- Type of user: NEC Group employee - User identity: same with authorised area-user information	View and update area names	Areas	- Authorised area-user information: same with user identity
		Delete areas	Areas	- Authorised area-user information: same with user identity
		Create folders	Areas	- Authorised area-user information: same with user identity
		View folder names	Folders	- Authorised area-user information: same with user identity
		Update folder names	Folders	- Authorised area-user information: same with user identity
		View/update mail addresses within the area	Folders	- Authorised area-user information: same with user identity
		Delete folders	Folders	- Authorised area-user

Controlled subjects	Security attributes of subjects	Controlled operations	Controlled objects	Security attributes of objects
				information: same with user identity
		Request uploads	Folders	- Authorised area-user information: same with user identity
		Upload business data	Folders	- Authorised area-user information: same with user identity
		Delete uploaded files	Business data files	- Authorised area-user information: same with user identity
		Download/ confirmation of uploaded files	Business data files	- Authorised area-user information: same with user identity
	- Type of user: NEC Group employee - User identify: same with authorised folder-user	View folder names	Folders	- Authorised folder-user information: same with user identity
		View/update own mail address	Folders	- Authorised folder-user information: same with user identity
		Upload request	Folders	- Authorised folder-user information: same with user identity
		Upload	Folders	- Authorised folder-user information: same with user identity
	- Type of user: NEC group employee - User identify: same with uploaded user information	Delete uploaded files	Business data files	- Uploader information: same with user identify
	- Type of user: NEC group employee - User identify: same with downloaded user information	Download/ confirmation of uploaded files	Business data files	- Downloader information: same with user identity
	- Type of user: NEC group employee - User-URL: same with assigned URL	Download/ confirmation of uploaded using one-time URL	Business data files	- Authorised user-URL: same with user-URL
On-premise worker process	- Type of user: On-premise worker - User identity: same with authorised folder-user	View folder names	Folders	- Authorised folder-user information: same with user identity
		View/update own mail address	Folders	- Authorised folder-user information:

Controlled subjects	Security attributes of subjects	Controlled operations	Controlled objects	Security attributes of objects
	information			same with user identity
		Upload request	Folders	- Authorised folder-user information: same with user identity
		Upload business data	Folders	- Authorised area-user information: same with user identity
	- Type of user: On-premise worker - User identity: same with uploader information	Delete uploaded files	Business data files	- Uploader information: same with user identity
	- Type of user: On-premise worker - User identity: same with downloader information	Download/confirmation of uploaded files	Business data files	- Downloader information: same with user identity
	- Type of user: On-premise worker - User-URL: same with user-URL	Download/confirmation of uploaded files using one-time URL	Business data files	- Authorised user-URL: same with user-URL
Customer process	- Type of user: Customer - User-URL: same with authorised user-URL	Upload business data (one-time URL)	Folders	- Authorised user-URL: same with user-URL
	- Type of user: Customer - User-URL: same with uploader information	Delete uploaded files (one-time URL)	Business data files	- Uploader information: same with user-URL
	- Type of user: Customer - User-URL: same with authorised user-URL	Download/confirmation of uploaded files using one-time URL	Business data files	- Authorised user-URL: same with user-URL

Only if the subject’s security attribute matches the object’s security attribute, the use of the TOE services is permitted.

FDP_ACF.1.3
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].
[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
None

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].
[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
None

6.2.3. FIA: Authentication failures

FIA_AFL.1a Authentication failure handling {area-users with customer privileges}
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1a
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]]
[assignment: positive integer number]
3
[assignment: list of authentication events]
PIN authentication of area-users with customer privileges

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

FIA_AFL.1b Authentication failure handling {area-users with NEC Group employee/on-premise worker privileges}
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication
FIA_AFL.1.1b
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]]
[assignment: positive integer number]
3
[assignment: list of authentication events]

- Authentication of area-users with NEC Group employee/on-premise worker privileges using the internal authentication service via one-time URL

FIA_AFL.1.2b

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

[assignment: list of actions]

Invalidation of one-time URL

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]

- Type of user (NEC Group employee, on-premise user and customer)
- User identity
- User-URL

FIA_SOS.2a TSF Generation of secrets {one-time URL}

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.2.1a

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

[assignment: a defined quality metric]: the following quality metrics.

<quality metric>

- The one-time URL is a fixed 27-digit character string that is generated randomly for each access attempt by users.
- The one-time URL uses the following ASCII characters.

Upper-alpha characters:	[A-Z] (26 characters)
Lower-alpha characters:	[a-z] (26 characters)
Numerical characters:	[0-9] (10 characters)
Symbol characters:	[+/] (2 characters)

FIA_SOS.2.2a

The TSF shall be able to enforce the use of TSF generated secrets for [assignment: list of TSF functions].

[assignment: list of TSF functions]

One-time URL in the identification and authentication function

FIA_SOS.2b TSF Generation of secrets { PIN }

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.2.1b

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

[assignment: a defined quality metric]: the following quality metrics.

<quality metric>

- The PIN is a fixed 16-digit character string that is generated randomly.
- The PIN uses the following ASCII characters.

Upper-alpha characters:	[A-Z] (26 characters)
Lower-alpha characters:	[a-z] (26 characters)
Numerical characters:	[0-9] (10 characters)
Symbol characters:	[+/] (2 characters)

FIA_SOS.2.2b
The TSF shall be able to enforce the use of TSF generated secrets for [assignment: list of TSF functions].
[assignment: list of TSF functions]
PIN in the identification and authentication function

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1Timing of authentication
Dependencies: FIA_UID.1 Timing of authentication
FIA_UAU.2.1
The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Refinement: user → Area-user with customer privileges
authenticated → authenticated by PIN authentication

FIA_UID.2a User identification before any action {identification by one-time URL}
Hierarchical to: No other components.
Dependencies: No dependencies.
FIA_UID.2.1a
The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Refinement: user → Area-user with customer privileges and NEC Group employee/on-premise worker privileges
identified → identified by one-time URL

FIA_UID.2b User identification be any action {identification using user ID used in the internal authentication service}
Hierarchical to: No other components.
Dependencies: No dependencies.
FIA_UID.2.1b
The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Refinement: user → NEC Group employee and on-premise worker
identified → identified by User ID used in the internal authentication service

FIA_UID.2c User identification before any action {identification using URL}
Hierarchical to: No other components.
Dependencies: No dependencies.
FIA_UID.2.1c
The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Refinement: user → System Administrator and Auditor
identified → identified by URL

FIA_USB.1 User-subject binding

Hierarchical 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: [assignment: *list of user security attributes*].

[assignment: list of user security attributes]

- Type of user
- User identity
- User-URL

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]

See Table 16.

Table 16 Rules for the initial association of attributes

User	Subjects acting on the behalf of users	User security attributes	Values of security attributes
NEC group employee	NEC Group employee process	Type of user	NEC Group employee
		User identity	User identity
		User-URL	One-time URL
On-premise worker	On-premise worker process	Type of user	On-premise worker
		User identity	User identity
		User-URL	One-time URL
Customer	Customer process	Type of user	Customer
		User-URL	User identity

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

6.2.4. FMT: Security management

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1

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

[assignment: access control SFP, information flow control SFP]

Business operation access control policy

[selection: change_default, query, modify, delete, [assignment: other operations]]

See Table 17.

[assignment: other operations]

Register

[assignment: list of security attributes]

See Table 17.

[assignment: the authorised identified roles]

See Table 17.

Table 17 Management of security attributes

Security attributes	Selection: change_default, query, modify, delete and register	Authorised identified roles
Authorised area-user information	Query, delete and register	Area-user with administrator privileges
Authorised folder-user information	Query, modify, delete and register	Area-user with administrator privileges

FMT_MSA.3a Static attribute initialisation {authorised area-user information}

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]

Business operation access control policy

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

[assignment: other property]

The TSF shall specify the user identity of an NEC Group employee who created an area.

Refinement: security attributes → security attributes (authorised area-user information)

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]

None

FMT_MSA.3b Static attribute initialization {authorised user-URL and upload/download relevant user information}

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]

Business operation access control policy

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

[assignment: other property]

- The TSF shall specify a URL used to access the folder associated with an upload request and also specify an uploader.
- The TSF shall specify user(s) who download a business data file and also specify a URL used to access that file.

Refinement: security attributes → security attributes (authorised user-URL, upload/download relevant user information)

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]

None

FMT_SAE.1 Time-limited authorisation

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FPT_STM.1 Reliable time stamps

FMT_SAE.1.1

The TSF shall restrict the capability to specify an expiration time for [assignment: *list of security attributes for which expiration is to be supported*] to [assignment: *the authorised identified roles*].

[assignment: list of security attributes for which expiration is to be supported]

See Table 18.

[assignment: the authorised identified roles]

See Table 18.

FMT_SAE.1.2

For each of these security attributes, the TSF shall be able to [assignment: *list of actions to be taken for each security attribute*] after the expiration time for the indicated security attribute has passed.

[assignment: list of actions to be taken for each security attribute]

See Table 18.

Table 18 Security attributes and authorised roles for which expiration is to be supported

Security attributes	Authorised identified roles	Actions to be taken for each security attribute
Expiration date of one-time URL	System Administrator	The TSF shall invalidate one-time URLs that have passed the expiration date.

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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]

- The TSF allows area-users with administrator privileges to make a query about, delete and register the authorised area-user information.
- The TSF allows area-users with administrator privileges to make a query about, modify, delete and register the authorised folder-user information.

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: *the authorised identified roles*].

[assignment: the authorised identified roles]

- Area-user with administrator privileges
- System administrator

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.2.5. FTP: Trusted path/channels

FTP_ITC_EX.1 Trusted channel inside the TOE

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC_EX.1.1

The TSF shall provide a communication channel between two different TOE components that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

Refinement: two different TOE components → Web server and Web browser

FTP_ITC_EX.1.2

The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].

[assignment: list of functions for which a trusted channel is required]

- Area Maintenance
- User Maintenance
- Upload Request
- Upload
- Download
- Set Personal Information

6.3. Security assurance requirements

The following subsections describe the assurance requirements for each assurance requirement class.

6.3.1. 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

6.3.2. ADV: Development

ADV_FSP.1: Basic functional specification

6.3.3. AGD: Guidance documents

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

6.3.4. ALC: Life-cycle support

ALC_CMC.1: Labelling of the TOE
ALC_CMS.1: TOE CM coverage

6.3.5. ATE: Tests

ATE_IND.1: Independent testing - conformance

6.3.6. AVA: Vulnerability assessment

AVA_VAN.1: Vulnerability survey

6.4. Security requirements rationale

6.4.1. Security functional requirements rationale

Table 19 shows the correspondence between security functional requirements and security objectives. The “x” indicates that there exists a correspondence relation between them.

Table 19 Relation between security functional requirements and security objectives

	O.I&A	O.IDENTIFY	O.ADMIN_IDENTIFY	O.ACCESS_CONTROL	O.AUDIT	O.ENCRYPT
FAU_GEN.1					×	
FAU_GEN.2					×	
FAU_SAR.1					×	
FAU_SAR.2					×	
FAU_SAR.3					×	
FDP_ACC.1				×		
FDP_ACF.1				×		
FIA_AFL.1a	×					
FIA_AFL.1b		×				
FIA_ATD.1				×		
FIA_SOS.2a	×	×				
FIA_SOS.2b	×					
FIA_UAU.2	×					
FIA_UID.2a	×	×				
FIA_UID.2b		×				
FIA_UID.2c			×			
FIA_USB.1				×		
FMT_MSA.1				×		
FMT_MSA.3a				×		
FMT_MSA.3b				×		
FMT_SAE.1	×	×				
FMT_SMF.1				×		
FMT_SMR.1	×	×		×		
FTP_ITC_EX.1						×

This section shows the basis for claiming that the TOE security functional requirements fully satisfy each of these security objectives.

We first clarify details of countermeasures necessary to implement each of the security objectives. We then determine the required functions necessary to satisfy each of these countermeasures and demonstrate that each of the security objectives can be implemented by satisfying all of these required functions. Note that each of the required function is satisfied by at least one security functional requirements and these requirements are indispensable for implementing each of the security objectives. As for required functions, we further prove that at least one security functional requirements satisfy each required function and they are needed to support each security objective.

O.I&A (customer identification and authentication)

This security objective for the TOE demands that only authorised TOE users or area uses with customer privileges gain access to the TOE. Thus, it is required to determine if users are authorised area-users with customer privileges. Details of countermeasures and functions required for this security objective are as follows:

(a) Identification and authentication of area-users with customer privileges before they are allowed to use the TOE service functions

Each of area-users with customer privileges must be identified as an authorised user before they are allowed to use the TOE service functions. The identification and authentication of area-users with customer privileges requires a successful one-time URL identification and PIN authentication. Note that one-time URL has an expiration date that is defined by the System Administrator. Any expired one-time URL should be disabled, resulting in identification failure.

Thus, any area-users with customer privileges are not allowed access to the TOE service functions before they succeed in user identification and authentication attempts.

The security functional requirements corresponding to this countermeasure are FIA_UID.2a, FIA_UAU.2, FMT_SAE.1 and FMT_SMR.1.

(b) Disabling access to the TOE when a defined number of unsuccessful user identification and authentication attempts has been met

It is needed to regard area-users with customer privileges who failed in user identification and authentication attempts as an unauthorised TOE user. The TOE implements a predefined action (disabling a one-time URL) against area-users with customer privileges who failed in a predefined number of user identification and authentication attempts.

The security functional requirements corresponding to this countermeasure are FIA_AFL.1a.

(c) Generation of a different one-time URL before each use

Each one-time URL shall be temporarily generated for user identification and must be a different URL even for the same user. Thus, it is required to clearly define a necessary quality metric and provide a mechanism to generate URLs that meet the defined quality metric.

The security functional requirements corresponding to this countermeasure are FIA_SOS.2a.

(d) Generation of PINs that meet a defined quality metric

The PINs that are used for user identification and authentication must be hard to guess by other people. Thus, it is required to clearly define a necessary quality metric and provide a mechanism to generate PINs that meet the defined quality metric.

The security functional requirements corresponding to this countermeasure are FIA_SOS.2b.

In conclusion, satisfying all countermeasures (a), (b), (c) and (d) above is satisfying O.I&A. Therefore, O.I&A can be implemented by achieving the necessary security functional requirements, FIA_AFL.1a, FIA_SOS.2a, FIA_SOS.2b, FIA_UAU.2, FIA.UID.2a, FMT_SAE.1 and FMT_SMR.1.

O.IDENTIFY (internal user identification)

This security objective for the TOE demands that all NEC Group employees and on-premise workers who attempt to access the TOE identify themselves as authorised TOE users. Details of countermeasures and functions required for this security objective are as follows:

(a) Identification of NEC Group employees and on-premise workers before they are allowed access to the TOE service functions

All NEC Group employees and on-premise workers must be identified as authorised users before they are allowed access to the TOE service functions.

Thus, they are not allowed to use any of the TOE service functions before they are identified as authorised users.

The security functional requirements corresponding to this countermeasure are FIA_UID.2a and FIA_UID.2b.

(b) Disabling access to the TOE when a defined number of unsuccessful user identification and authentication attempts has been met

When area-users with NEC Group employee/on-premise worker privileges who attempt access to the TOE using a one-time URL failed in a predefined number of user identification and authentication attempts, the TOE implements a predefined action (disabling a one-time URL).

The security functional requirements corresponding to this countermeasure are FIA_AFL.1b.

(c) Generation of a different one-time URL before each use

Each one-time URL shall be temporarily generated for user identification and must be a different URL even for the same user. Thus, it is required to clearly define a necessary quality metric and provide a mechanism to generate URLs that meet the defined quality metric. Note that one-time URL has an expiration date that is defined by the System Administrator. Any expired one-time URL should be disabled, resulting in identification failure.

The security functional requirements corresponding to this countermeasure are FIA_SOS.2a, FMT_SAE.1 and FMT_SMR.1.

In conclusion, satisfying all countermeasures (a), (b) and (c) above is satisfying O.IDENTIFY. Therefore, O.IDENTIFY can be implemented by achieving the necessary security functional requirements, FIA_AFL.1b, FIA_SOS.2a, FIA.UID.2a, FIA_UID.2b, FMT_SAE.1 and FMT_SMR.1.

O.ADMIN_IDENTIFY (administrator identification)

This security objective for the TOE demands that all System Administrators and Auditors be identified as authorised TOE users. Details of countermeasures and functions required for this security objective are as follows:

(a) Identification of the System Administrator and the Auditor before they are allowed to use the TOE service functions

The System Administrator and the Auditor must identify themselves as authorised TOE users by means of URL before they are allowed to use the TOE service functions. Thus, they are not allowed to use any of the service functions before they are identified as authorised TOE users.

The security functional requirements corresponding to this countermeasure are FIA_UID.2c.

In conclusion, satisfying the countermeasure (a) is satisfying O.ADMIN_IDENTIFY. Therefore, O.ADMIN_IDENTIFY can be implemented by achieving the necessary security functional requirements FIA_UID.2c.

O.ACCESS_CONTROL (access control)
This security objective for the TOE demands to define access control policies and enforce business operational control over the protected assets in consideration of the fact that NEC Group employees, on-premise workers, and area-users with administrator privileges, NEC Group employee/on-premise worker privileges and customer privileges attempt to access only protected assets. Details of countermeasures and functions required for this security objective are as follows:

(a) Enforcement of access control rules

It is needed to define authorised operations and operational objects for NEC Group employees, on-premise workers, and area-users with administrator privileges, NEC Group employee/on-premise worker privileges and customer privileges. It is also needed to ensure that only authorised users can execute the TOE operations.

Consequently, dependent on user roles of NEC Group employees, on-premise workers and customers, access control should be implemented over the following operations concerning areas, folders and business data files.

- Creation of areas by NEC Group employees
- View and update of area names by NEC Group employees (area-users with administrator privileges)
- Delete of areas by NEC Group employees (area-users with administrator privileges)
- Creation of folders by NEC Group employees (area-users with administrator privileges)
- View of folder names by NEC Group employees (area-users with administrator privileges)
- View of folder names by NEC Group employees (area-users with NEC Group employee/on-premise worker privileges)
- Update of folder names by NEC Group employees (area-users with administrator privileges)
- Delete of folders by NEC Group employees (area-users with administrator privileges)
- Registration of upload requests by NEC Group employees (area-users with administrator privileges)
- Registration of upload requests by NEC Group employees (area-users with NEC Group employee/on-premise worker - privileges)
- Upload of business data files by NEC Group employees (area-users with administrator privileges)
- Upload of business data files by NEC Group employees (area-users with NEC Group employee/on-premise worker privileges)
- Delete of uploaded files by NEC Group employees (area-users with administrator privileges)
- Delete of uploaded files by NEC Group employees (area-users with NEC Group employee/on-premise worker privileges)
- Download of business data files and confirmation of those downloaded files by NEC Group employees (area-users with administrator privileges)
- Download or confirmation of uploaded files by NEC Group employees (area-users with NEC Group employee/on-premise worker privileges using one-time URL)
- View of folder names by on-premise workers (area-users with NEC Group employee/on-premise worker privileges)
- Registration of upload requests by on-premise workers (area-users with NEC Group employee/on-premise worker privileges)
- Upload of business data files by on-premise workers (area-users with NEC Group employee/on-premise worker privileges)

- Delete of uploaded files by on-premise workers (area-users with NEC Group employee/on-premise worker privileges)
- Download or confirmation uploaded files by on-premise workers (area-users with NEC Group employee/on-premise worker privileges)
- Download or confirmation of uploaded files by on-premise workers (area-users with NEC Group employee/on-premise worker privileges using one-time URL)
- View of folders by customers (area-users with customer privileges)
- Upload of business data files by customers (area-users with customer privileges using one-time URL)
- Delete of uploaded files by customers (area-users with customer privileges using one-time URL)
- Download of business data by customers (area-users with customer privileges using one-time URL)

The security functional requirements corresponding to this countermeasure are FDP_ACC.1 and FDP_ACF.1.

(b) Association of users with the process

To enforce access restrictions, it is required to associate user security attributes with the process (subject) acting on the behalf of that user when using the TOE. For this reason, all suthorised users should have a user security attribute of “type of user” and the TOE must provide a mechanism to associate type of user with a subject acting on the behalf that user.
The security functional requirements corresponding to this countermeasure are FIA_ATD.1 and FIA_USB.1.

(c) Access control dependent on each user role

To enforce access control over areas and folders, it is required to appropriately define security attributes such as authorised area-user information and authorised folder-user information. Only area-users with administrator privileges are allowed to query and delete the authorised area-user information, and to query, modify, register and delete the authorised folder-user information. When an NEC Group employee attempts to create an area, a default value to specify that NEC Group employee is set to the security attribute of authorised area-user information. When an area-user with NEC Group employee/on-premise worker privileges attempts to make an upload request or upload the business data to a specified folder, a default value to specify a URL used to access that folder or business data file is defined to the security attribute of authorised user-URL. Note that when the user attempt to upload the business data, users who are allowed to download that data are defined to the security attribute of download relevant user information, and the user who executed an upload is defined to the security attribute of upload relevant user information.
The security functional requirements corresponding to this countermeasure are FMT_MSA.1, FMT_MSA.3a, FMT_MSA.3b and FMT_SMR.1.

(d) Specification of the management functions affecting the TOE operations

The TOE specifies the management functions affecting the TOE operations so as to allow the management of the security attributes.
The security functional requirements corresponding to this countermeasure are FMT_SMF.1.

In conclusion, satisfying all the countermeasures (a), (b), (c) and (d) above, is satisfying O.ACCESS_CONTROL. Therefore, O.ACCESS_CONTROL can be implemented by achieving the necessary security functional requirements, FDP_ACC.1, FDP_ACF.1, FIA_ATD.1, FIA_USB.1, FMT_MSA.1, FMT_MSA.3a, FMT_MSA.3b, FMT_SMF.1 and FMT_SMR.1.

O.AUDIT (Audit)

This security objective for the TOE demands to collect and protect audit records. The audit records provide evidencing information necessary to monitor the TOE operational status at a later date. Thus, they must be accessible any time when needed. Consequently, the protection of audit records requires the consideration of the secure collection of audit records and the modification of them. Details of countermeasures and functions required for this security objective are as follows:

(a) Collection of information necessary to maintain an audit record

It is needed to record all necessary information that characterises auditable events occurred in the TOE operations. Specifically, it is needed to generate audit-related information including date and time of event, user ID, company code and department code concerning a user action such as identification, authentication and access control. At this time, audit (level of audit: not specified) is required before any use of the security mechanism. It is also needed to collect the exact information about date and time of that auditable event. As for the level of audit, in view of the fact that the audit measures are ex post measures and can prevent the unauthorised use of the TOE by means of identification/authentication and access control as TOE security measures, the level “not specified” is considered as appropriate.

The security functional requirements corresponding to this countermeasure are FAU_GEN.1.

In addition, it is needed to clarify the subject that caused an event. For this reason, each auditable event must be associated with the identity of the user that caused the event.

The security functional requirements corresponding to this countermeasure are FAU_GEN.2.

(b) Restriction on read and use of audit records

All authorised users can read audit records but only auditors can read and use them.

The security functional requirements corresponding to this countermeasure are FAU_SAR.1 and FAU_SAR.2.

Audit records must be offered in a searchable format based on specified criteria.

The security functional requirements corresponding to this countermeasure are FAU_SAR.3.

In conclusion, satisfying all the countermeasures (a) and (b) is satisfying O.AUDIT. Therefore, O.AUDIT can be implemented by achieving the necessary security functional requirements, FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2 and FAU_SAR.3.

O.ENCRYPT (encryption)

This security objective for the TOE demands the protection of communication data. For this reason, it is needed to encrypt and decrypt communication data. Details of countermeasures and functions required for this security objective are as follows:

(a) Encryption/decryption of communication data

Communication between an external user client and an external Web server and between an internal user client and an internal Web server is performed over a SSL channel that is logically distinct from other communication channels for protection against modification or disclosure of communication data.

The security functional requirements corresponding to this countermeasure are FTP_ITC_EX.1.

In conclusion, satisfying the countermeasure (a) is satisfying O.ENCRYPT. Therefore, O.ENCRYPT can be implemented by achieving the security functional requirements FTP_ITC_EX.1.

6.4.2. SFR Dependency Rationale

Dependencies between security functional components are shown in Table 20.

Table 20 SFR Dependency Rationale

Component	Dependency components in CC Part2	Dependency components in TOE	Components whose dependency is not satisfied	Rationale
FAU_GEN.1	FPT_STM.1	None	FPT_STM.1	*1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2	None	
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	None	
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	None	
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1	None	
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	None	
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3a FMT_MSA.3b	None *2	
FIA_AFL.1a	FIA_UAU.1	FIA_UAU.2 (hierarchical to FIA_UAU.1)	None	
FIA_AFL.1b	FIA_UAU.1	None	FIA_UAU.1	*3
FIA_ATD.1	None	None	None	
FIA_SOS.2a	None	None	None	
FIA_SOS.2b	None	None	None	
FIA_UAU.2	FIA_UID.1	FIA_UID.2a (hierarchical to FIA_UID.1)	None	
FIA_UID.2a	None	None	None	
FIA_UID.2b	None	None	None	
FIA_UID.2c	None	None	None	
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	None	
FMT_MSA.1	[FDP_ACC.1, FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	None	
FMT_MSA.3a	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1	FMT_SMR.1	*4
FMT_MSA.3b	FMT_MSA.1 FMT_SMR.1	None	FMT_MSA.1	*5
			FMT_SMR.1	*6
FMT_SAE.1	FMT_SMR.1 FPT_STM.1	FMT_SMR.1	FPT_STM.1	*7
FMT_SMF.1	None	None	None	
FMT_SMR.1	FIA_UID.1	FIA_UID.2a FIA_UID.2b FIA_UID.2c (hierarchical to FIA_UID.1)	None	
FTP_ITC_EX.1	None	None	None	

As shown in Table 16, the security functional requirements satisfy all necessary dependencies, other than the exceptions described below. The following provides the rationale that satisfying dependencies is unnecessary on all exceptions.

*1) FAU_GEN.1 → FPT_STM.1
The TOE provides a system clock using the OS functions outside the TOE based on OE.OS_TIMESTAMP. For this reason, the dependency between FAU_GEN.1 and FPT_STM.1 is unnecessary.

*2) About the security attribute of authorised folder-user information
As for the security attribute of authorised folder-user information in FDP_ACF.1, the TOE does not require the setting of a default value when a folder is created. For this reason, the dependency between FDP_ACF.1 and FMT_MSA.3 is unnecessary.

*3) FIA_AFL.1b → FIA_UAU.1
The TOE authenticates area-users with NEC employee/on-premise worker privileges using an internal authentication service outside the TOE based on OE.AUTHENTICATION. For this reason, the dependency between FIA_AFL.1b and FIA_UAU.1 is unnecessary.

*4) FMT_MSA.3a → FMT_SMR.1
The TOE does not define any authorised identified roles that are specified as a default value of the FMT_MSA.3a security attribute (authorised area-user information). For this reason, the dependency between FMT_MSA.3a and FMT_SMR.1 is unnecessary.

*5) FMT_MSA.3b → FMT_MSA.1
The TOE temporarily generates the FMT_MSA.3b security attribute (authorised user-URL) as a one-time URL and does not need to manage it. For this reason, the dependency between FMT_MSA.3b and FMT_MSA.1 is unnecessary.

*6) FMT_MSA.3b → FMT_SMR.1
The TOE does not define any authorised identified roles that are specified as a default value of the FMT_MSA.3b security attributes (authorised user-URL, upload relevant user information and download relevant user information). For this reason, the dependency between FMT_MSA.3b and FMT_SMR.1 is unnecessary.

*7) FMT_SAE.1 → FPT_STM.1
The TOE provides a system clock using the OS functions outside the TOE based on OE.OS_TIMESTAMP. For this reason, the dependency between FMT_SAE.1 and FPT_STM.1 is unnecessary.

6.4.3. Security Assurance Requirements Rationale

This TOE envisions low-level attackers from the assumed threats. Also, the TOE is an internal system that is used within the NEC group organization for information exchange with customers. For this reason, an assurance level requiring protection against known vulnerabilities is envisioned.
Therefore, this ST employs EAL1+ ASE_SPD.1, ASE_OBJ.2 and ASE_REQ.2.

7. TOE Summary Specification

This chapter describes the TOE security functionalities.

7.1. Identification and authentication function

The identification and authentication provides a function for identifying a user who attempts to access the TOE as an authorised user himself. The PIN used for authentication provides a mechanism to validate the quality metrics. The following subsections describe the identification and authentication function from the perspective of a method for implementing SFRs.

7.1.1. How to implement SFRs that correspond with the identification and authentication function

(1) FIA_UID.2a User identification before any action, FIA_UAU.2 User authentication before any action and FMT_SAE.1 Time-limited authorisation

The TOE identifies and authenticates area-users with customer privileges before permitting them to use TOE service functions. Identification is implemented using a one-time URL in compliance with the generation of secrets specified in (7) below and authentication is implemented using a PIN in compliance with the generation of secrets specified in (8) below. Note that this one-time URL is automatically disabled when the expiration time defined by the System Administrator has passed.

If the following processes have been successfully completed in that order, the identification and authentication for these area-users will be successful.

1. Identification by one-time URL
2. Verification of one-time URL expiration time
3. Authentication by PIN (the PIN that is input by a customer must match the PIN that has been preassigned to that customer)

Thus, FIA_UID.2a, FIA_UAU.2, FIA_SOS.2a, FIA_SOS.2b and FMT_SAE.1 can be implemented.

(2) FIA_UID.2a User identification before any action and FMT_SAE.1 Time-limited authorisation

The TOE identifies area-users with NEC employee/on-premise worker privileges before permitting them to use TOE service functions. Identification is implemented using a one-time URL in compliance with the generation of secrets specified in (7) below. Note that this one-time URL is automatically disabled when the expiration time defined by the System Administrator has passed.

If the following processes have been successfully completed in that order, the identification for these area-users will be successful.

1. Identification by one-time URL
2. Verification of one-time URL expiration time

Thus, FIA_UID.2a, FIA_SOS.2a and FMT_SAE.1 can be implemented.

(3) FIA_UID.2b User identification before any action

The TOE identifies NEC Group employees and on-premise workers before permitting them to use TOE service functions. This identification is implemented using a user ID.

If the following process is successfully completed, the identification for these users will be successful.

1. Identification by user ID

Thus, FIA_UID.2b can be implemented.

(4) FIA_UID.2c User identification before any action

The TOE identifies System Administrators and Auditors before permitting them to use TOE service functions. Identification is implemented using a URL on the System Administrator screen or the Auditor screen.

If the following process has been successfully completed, the identification for these users will be successful.

1. Identification by URL

Thus, FIA_UID.2c can be implemented.

(5) FIA_AFL.1a Authentication failure handling

The TOE provides the following function in association with the identification and authentication of area-users with customer privileges:

If the input PIN does not match the one-time URL used by the area-user with customer privileges, the TOE counts the number of incorrect PIN inputs for each one-time URL. When the cumulative number of incorrect PIN inputs reach the defined number of unsuccessful authentication attempts (fixed 3 times), the associated one-time URL will be disabled.

Thus, FIA_AFL.1a can be implemented.

(6) FIA_AFL.1b Authentication failure handling

The TOE provides the following function in association with the identification of area-users with NEC employee/on-premise worker privileges:

If these area-users failed in the authentication attempts using an internal authentication service via one-time URL, the TOE counts the number of unsuccessful authentication attempts in the internal authentication service. If the cumulative number of incorrect inputs reaches the predefined number of unsuccessful authentication attempts (fixed 3 times), the associated one-time URL will be disabled.

Thus, FIA_AFL.1b can be implemented.

(7) FIA_SOS.2a TSF generation of secrets

The TOE generates one-time URLs for identification and authentication that satisfy the following conditions:

1. A fixed 27-digit character string that is generated randomly
2. The following ASCII characters can be used:

Upper-alpha characters:	[A-Z] (26 characters)
Lower-alpha characters:	[a-z] (26 characters)
Numerical characters:	[0-9] (10 characters)
Symbol characters:	[+/] (2 characters)

Thus, FIA_SOS.2a can be implemented.

(8) FIA_SOS.2b TSF generation of secrets

The TOE generates PINs for identification and authentication that satisfy the following conditions:

1. A fixed 16-digit character string that is generated randomly
2. The following ASCII characters can be used:

Upper-alpha characters:	[A-Z] (26 characters)

Lower-alpha characters:	[a-z] (26 characters)
Numerical characters:	[0-9] (10 characters)
Symbol characters:	[+/] (2 characters)

Thus, FIA_SOS.2b can be implemented.

(9) FMT_SMR.1 Security roles

The TOE maintains the following authorised and identified roles to manage the expiration date for the one-time URL specified in (1) and (2) above.

- System Administrator

Thus, FMT_SMR.1 can be implemented.

7.2. Audit Function

The Audit provides a function to generate, view and search audit records for maintaining the stable TOE operations.

Only authorised auditors can be used the audit function.

The following subsections describe the audit function from the perspective of a method for implementing SFRs.

7.2.1. How to implement SFRs that correspond with the audit function

(1) FAU_GEN.1 Audit data generation

To collect the information necessary to ensure that the TOE operates securely and manage the collected information appropriately, if auditable events occur, the TOE generates audit records as audit trails of these events.

The TOE generates audit records when the following auditable events occur:

- Start and stop of audit functions
- View of audit records
- Unsuccessful attempt to view audit records
- Successful/unsuccessful attempt to create areas by NEC Group employees
- Successful/unsuccessful update or delete of areas by NEC Group employees
- Successful/unsuccessful creation, update or delete of folders by area-users with administrator privileges
- Successful/unsuccessful modification (register, update and delete) of internal user information (authorised area-user information and authorised folder-user information) by area-users with administer privileges
- Successful/unsuccessful register of upload requests by area-users with NEC Group employee/on-premise worker privileges
- Successful/unsuccessful register of upload requests by area-users with administrator privileges
- Successful/unsuccessful upload of business data by area-users with NEC Group employee/on-premise worker privileges
- Successful/unsuccessful upload of business data by area-users with customer privileges
- Successful/unsuccessful upload of business data by area-users with administrator privileges
- Successful/unsuccessful delete of uploaded files by area-users with NEC Group/on-premise workers
- Successful/unsuccessful delete of uploaded files by area-users with customer privileges
- Successful/unsuccessful delete of files within a folder by area-users with administrator privileges
- Successful/unsuccessful download of business data by area-users with NEC Group employee/on-premise worker privileges
- Successful/unsuccessful download of business data by area-users with customer privileges
- Successful/unsuccessful download of business data by area-users with administrator privileges

- Disabling of one-time URL when the cumulative number of unsuccessful authentication attempts reaches the predefined threshold
- Verification of the PIN quality metrics (success/unsuccess)
- Verification of the one-time URL quality metrics (success/unsuccess)
- Successful/unsuccessful authentication of area-users with customer privileges
- Successful/unsuccessful identification of area-users with NEC Group employee/on-premise worker privileges using one-time URL
- Successful/unsuccessful identification of area-users with customer privileges
- Modification of types of users
- Modification of mail addresses of area-users with administrator privileges
- Modification of mail addresses of area-users with NEC Group employee/on-premise worker privileges

Audit records consist of the following items:

- Date and time of events (OS based timestamp information)
- Types of events: classification of events
- Subject identity (user code)
- Event outcome (success or failure)
- Company code
- Department code

Thus, FAU_GEN.1 can be implemented.

(2) FAU_GEN.2 User identity association

When an auditable event occurs, the TOE associates that event with the identity of the user (subject identity) that caused the event and generates an audit record as audit trail. The TOE records a user code (that is the user identity) as the subject identity.

Thus, FAU_GEN.2 can be implemented.

(3) FAU_SAR.1 Audit review

The TOE provides the function to provide only authorised auditor the capability to obtain and interpret the collected audit information in a human understandable presentation. It also provides the function to identify the Auditor and read the following auditing items from the audit records.

- Subject identity (user code)
- Types of events
- Outcome of events (success or failure)
- Date and time of events
- Company code
- Department code

Thus, FAU_SAR.1 can be implemented.

(4) FAU_SAR.2 Restricted audit review

To provide a mechanism to prohibit users other than Auditor read access to the audit records, the TOE identifies all users to ensure that only authorised Auditor is permitted to perform the operations on audit records.

Thus, FAU_SAR.2 can be implemented.

(5) FAU_SAR.3 Selectable audit review

As a function to view audit records, the TOE provides authorised users with the capability to search intended audit data by specifying a specific date range for specific events.
Thus, FAU_SAR.3 can be implemented.

7.3. Access Control Function

The TOE provides the function to control operations on user data based on the privileges assigned to each TOE user role.
The following subsections describe the access control function from the perspective of a method for implementing SFRs.

7.3.1. Method to implement SFRs associated with access control functions

(1) FIA_ATD.1 User attribute definition

The TOE defines the requirements to associate user security attributes with individual users, including:

1. Types of users (NEC group employee, on-premise user and customer)
2. User identity
3. User-URL

Thus, FIA_ATD.1 can be implemented.

(2) FIA_USB.1 User-subject binding

To enable authenticated users to use the TOE, the TOE associates user security attributes with subjects acting on the behalf of that user as shown in Table 21.

Table 21 Relation between subjects and user security attributes

Subject	User security attributes	Security attribute item
NEC group employee process	Type of user	NEC Group employee
	User identity	Value of user identity
	User-URL	Value of one-time URL
On-premise worker process	Type of user	On-premise worker
	User identity	Value of user identity
	User-URL	Value of one-time URL
Customer process	Type of user	Customer
	User-URL	Value of one-time URL

Thus, FIA_USB1 can be implemented.

(3) FDP_ACC.1 Subset access control and FDP_ACF.1 Security attribute based access control

The TOE enforces business operation access control policy among those subjects and objects shown in Table 22.

Table 22 Operations among subjects and objects handled by the access control policies

Controlled subjects	Security attributes of subjects	Controlled operations	Controlled objects	Security attributes of objects
NEC group employee	- Type of user: NEC Group employee	Create areas	Areas	None

Controlled subjects	Security attributes of subjects	Controlled operations	Controlled objects	Security attributes of objects
process	- Type of user: NEC Group employee - User identity: same with authorised area-user information	View and update area names	Areas	- Authorised area-user information: same with user identity
		Delete areas	Areas	- Authorised area-user information: same with user identity
		Create folders	Areas	- Authorised area-user information: same with user identity
		View folder names	Folders	- Authorised area-user information: same with user identity
		Update folder names	Folders	- Authorised area-user information: same with user identity
		View/update mail addresses within the area	Folders	- Authorised area-user information: same with user identity
		Delete folders	Folders	- Authorised area-user information: same with user identity
		Request uploads	Folders	- Authorised area-user information: same with user identity
		Upload business data	Folders	- Authorised area-user information: same with user identity
		Delete uploaded files	Business data files	- Authorised area-user information: same with user identity
		Download/ confirmation of uploaded files	Business data files	- Authorised area-user information: same with user identity
	- Type of user: NEC Group employee - User identify: same with authorised folder-user	View folder names	Folders	- Authorised folder-user information: same with user identity
		View/update own mail address	Folders	- Authorised folder-user information: same with user identity
		Upload request	Folders	- Authorised folder-user information: same with user identity
		Upload	Folders	- Authorised folder-user information: same with user identity
	- Type of user: NEC group employee	Delete uploaded files	Business data files	- Uploader information: same with user identify

Controlled subjects	Security attributes of subjects	Controlled operations	Controlled objects	Security attributes of objects
	- User identify: same with uploaded user information			
	- Type of user: NEC group employee - User identify: same with downloaded user information	Download/ confirmation of uploaded files	Business data files	- Downloader information: same with user identity
	- Type of user: NEC group employee - User-URL: same with assigned URL	Download/ confirmation of uploaded using one-time URL	Business data files	- Authorised user-URL: same with user-URL
On-premise worker process	- Type of user: On-premise worker - User identity: same with authorised folder-user information	View folder names	Folders	- Authorised folder-user information: same with user identity
		View/update own mail address	Folders	- Authorised folder-user information: same with user identity
		Upload request	Folders	- Authorised folder-user information: same with user identity
		Upload business data	Folders	- Authorised area-user information: same with user identity
	- Type of user: On-premise worker - User identity: same with uploader information	Delete uploaded files	Business data files	- Uploader information: same with user identity
	- Type of user: On-premise worker - User identity: same with downloader information	Download/confirmation of uploaded files	Business data files	- Downloader information: same with user identity
	- Type of user: On-premise worker - User-URL: same with user-URL	Download/confirmation of uploaded files using one-time URL	Business data files	- Authorised user-URL: same with user-URL
Customer process	- Type of user: Customer - User-URL: same with authorised user-URL	Upload business data (one-time URL)	Folders	- Authorised user-URL: same with user-URL
	- Type of user: Customer	Delete uploaded files (one-time URL)	Business data files	- Uploader information: same with user-URL

Controlled subjects	Security attributes of subjects	Controlled operations	Controlled objects	Security attributes of objects
	- User-URL: same with uploader information			
	- Type of user: Customer - User-URL: same with authorised user-URL	Download/confirmation of uploaded files using one-time URL	Business data files	- Authorised user-URL: same with user-URL

* Only if the subject's security attribute matches the object's security attribute, the use of the TOE services is permitted.

Thus, FDP_ACC.1 and FDP_ACF.1 can be implemented.

(4) FMT_MSA.1 Management of security attributes and FMT_MSA.3a / FMT_MSA.3b Static attribute initialisation

In order to enforce access control based on user roles, the TOE permits only specific users to modify security objects as defined below:

1. Only area-users with administrator privileges can perform the security attribute related operations including:
   - Query, delete and register on authorised area-user information
   - Query, modify, delete and register on authorised folder-user information
2. Default values are registered for the following security attributes:
   - User identities of those NEC Group employees who created an area are registered in the Authorised Area-User Information
   - URLs for accessing the folders associated with upload requests are registered in the Authorised User-URL
   - URLs for accessing the uploaded business data are registered in the Authorised User-URL
   - User identities of those who are authorised to download the business data are registered in the Downloader Information
   - User identities of those who performed the upload are registered in the Uploader Information

Thus, FMT_MSA.1, FMT_MSA.3a and FMT_MSA.3b can be implemented.

(5) FMT_SMF.1 Specification of management functions

The TOE provides the following security management functions:

Inquiry, delete and register on authorised area-user information by area-users with administrator privileges

Inquiry, modify, delete and register on authorised folder-user information by area-users with administrator privileges

Thus, FMT_SMF.1 can be implemented.

(6) FMT_SMR.1 Security roles

The TOE maintains the following authorised and identified roles to manage the security attributes specified in the (4) above and to use the security attributes specified in the (5) above.

- Area-users with administrator privileges

Thus, FMT_SMR.1 can be implemented.

7.4. Cryptographic Functionality

The TOE provides the functionality to encrypt/decrypt communication data that flows between external user clients and the External Web server, and internal user clients and the Internal Web server.

The following subsections describe the cryptographic functionality from the perspective of a method for implementing SFRs.

7.4.1. How to implement SFRs that correspond with the cryptographic functionality

(1) FTP_ITC_EX.1 Inter-TOE trusted channel

The following defines the requirements for creating a trusted channel between itself and a remote TOE.

1. The TOE uses a SSL function for communication between internal/external user clients with Internet Explorer6.0/7.0 and the Internal Web server or the External Web server with Internet Information Server 6.0, and distinguishes these communications with other different communications using SSL server certificate.
2. The TOE uses a SSL for the following functions.
   - Area Maintenance
   - User Maintenance
   - Upload Request
   - Upload
   - Download
   - Set Personal Information

Thus, FTP_ITC_EX.1 can be implemented.