imagio MP 4000/5000 series, Aficio MP 4000/5000 series

Security Target

Authors : RICOH COMPANY, LTD. Yasushi FUNAKI, Hiroshi KAKII, Atsushi SATOH

Date : 2009-10-30

Version : 1.13

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

Revision History

Version	Date	Authors	Details
1.00	2008-12-16	Yasushi FUNAKI, Hiroshi KAKII, Astushi SATOH	First version
1.01	2009-02-10	Yasushi FUNAKI	Revised notes.
1.02	2009-03-31	Yasushi FUNAKI	Revised notes.
1.03	2009-04-10	Yasushi FUNAKI	Revised notes.
1.04	2009-04-14	Yasushi FUNAKI	Corrected clerical errors.
1.05	2009-04-23	Yasushi FUNAKI	Revised notes. Corrected clerical errors.
1.06	2009-06-02	Yasushi FUNAKI	Revised notes. Corrected clerical errors.
1.07	2009-06-11	Yasushi FUNAKI	Corrected clerical errors.
1.08	2009-06-15	Yasushi FUNAKI	Revised notes.
1.09	2009-07-10	Yasushi FUNAKI	Revised notes. Corrected clerical errors.
1.10	2009-10-06	Yasushi FUNAKI	Revised notes. Corrected clerical errors.
1.11	2009-10-07	Yasushi FUNAKI	Revised notes.
1.12	2009-10-23	Yasushi FUNAKI	Revised notes.
1.13	2009-10-30	Yasushi FUNAKI	Revised notes.

Table of Contents

List of Figures

List of Tables

1 ST Introduction

1.1 ST Identification

This section identifies the Security Target and the TOE by following information.

ST Title : imagio MP 4000/5000 series, Aficio MP 4000/5000 series Security Target

ST Version : 1.13

Date : 2009-10-30

Authors : RICOH COMPANY, LTD. Yasushi FUNAKI, Hiroshi KAKII, Atsushi SATOH

TOE :

[Japanese Name]

Ricoh imagio MP 4000/5000 series

[English Name]

Ricoh Aficio MP 4000/5000 series

Refer to Table 1 about product names for "Ricoh imagio MP 4000/5000 series" and "Ricoh Aficio MP 4000/5000 series".

TOE Version : "Ricoh imagio MP 4000/5000 series" and "Ricoh Aficio MP 4000/5000 series" are identified by following software and hardware.

Software	System/Copy	1.09
	Network Support	7.23
	Scanner	01.23
	Printer	1.09
	Fax	03.00.00
	Web Support	1.57
	Web Uapl	1.13.1
	Network Doc Box	1.09.3C
Hardware	Ic Key	1100
	Ic Hdd	01

Notes: When an "e" is suffixed to Printer version (described as X.YY), this "e" indicates the English printer version and it does not affect any security functions. (This "e" is suffixed only to English printer version and not suffixed to Japanese printer version.) Therefore "X.YY" is used for the identification of security functions.

Keywords : Digital MFP, Document, Copy, Print, Scanner, Fax, Network, Office

CC Version : Common Criteria for Information Technology Security Evaluation Ver2.3

Table 1: List of TOE

Series Name	Product Name/Model Name
Ricoh imagio MP 4000/5000 series	Ricoh imagio MP 4000SP Ricoh imagio MP 4000SPF Ricoh imagio MP 5000SP Ricoh imagio MP 5000SPF
Ricoh Aficio MP 4000/5000 series	Ricoh Aficio MP 4000SP Ricoh Aficio MP 4000SPF Ricoh Aficio MP 5000SP Ricoh Aficio MP 5000SPF Savin 9040SP Savin 9040SPF Savin 9050SP Savin 9050SPF Lanier LD040SP Lanier LD040SPF Lanier LD050SP Lanier LD050SPF Lanier MP 4000SP Lanier MP 4000SPF Lanier MP 5000SP Lanier MP 5000SPF Gestetner MP 4000SP Gestetner MP 4000SPF Gestetner MP 5000SP Gestetner MP 5000SPF Nashuatec MP 4000SP Nashuatec MP 4000SPF Nashuatec MP 5000SP Nashuatec MP 5000SPF Rex-Rotary MP 4000SP Rex-Rotary MP 4000SPF Rex-Rotary MP 5000SP Rex-Rotary MP 5000SPF Infotec MP 4000SP Infotec MP 4000SPF Infotec MP 5000SP Infotec MP 5000SPF

1.2 ST Overview

This Security Target describes the security requirements and specifications of the RICOH digital multi function product (hereafter called MFP) identified as the TOE in "1.1 ST Identification". An MFP is an image I/O device that incorporates the functionality of copier, scanner, fax and printer, is generally connected to an office LAN, and is used to input, store, and output Document Data. The MFP protects Document Data when stored internally and prevents Document Data from leakage when sent and received between the MFP and a client PC.

1.3 CC Conformance

This ST conforms to the following CC standards and Package Claims.

- CC part 2 conformant.

- CC part 3 conformant.

- Assurance level: EAL3.

This ST does not conform to any Protection Profiles.

1.4 Terminology

1.4.1 Terms in this ST

Table 2 shows the definitions of specific terms for clearly understanding of this ST.

Table 2: Specific Terms Used in this ST

Terms	Definitions
MFP	An abbreviation for digital multi function product. Also indicates the TOE in this ST.
MFP Control Software	Software installed in the TOE and has the elements that identify the TOE such as System/Copy, Network Support, Scanner, Printer, Fax, Web Support, Web Uapl and Network Doc Box. It manages the resources for units and devices that comprise the MFP and controls their operation.
HDD	An abbreviation for Hard Disk Drive. Indicates the HDD installed in the TOE.
Ic Key	A chip that contains a microprocessor for encryption processing and EEPROM that stores a private encryption key for secure communication. It keeps the keys for validity authentication and encryption processing and the random number generator.
Ic Hdd	A hardware device that encrypts the data to be written on HDD and decrypts the data to be read from HDD.

Terms	Definitions
Operation Panel	A display-input device that consists of a touch screen LCD, keyswitches, and LED indicators, and is used for MFP operation by users. Operation Panel Unit.
Internal Networks	Networks managed by an organization that has MFP. Normally indicates the office LAN environment established as the intranet.
External Networks	Networks that are not managed by the organization that manages the MFP. Generally, indicates the Internet.
SMTP Server	A server for sending E-mail using Simple Mail Transfer Protocol.
FTP Server	A server for sending files to client PC and receiving files from client PC using File Transfer Protocol.
SMB Server	A server for sharing files with client PC using Server Message Block protocol.
D-BOX	A storage area for Document Data on the HDD.
Print Data	The document files in client PC that are sent to the TOE from a client PC to be printed or faxed. It is necessary to install drivers into client PC in advance - printer driver for printing and fax driver for faxing. Print Data is taken into the TOE from Network Units or USB Ports.
Document Data	Electronic data that are loaded into MFP by authorized MFP users using either of the following operations. 1. Electronic data that are scanned from paper-based original and digitized by authorized MFP users' operation. 2. Electronic data that are sent to the MFP by authorized MFP users and converted by the MFP from received Print Data into a format that can be processed by the MFP.
Document Data ACL	An access control list of General Users that is set for each Document Data.
Customer Engineer (CE)	A person who is an expert in maintenance for the TOE and is employed by manufacturers, technical support service companies, or sales companies.
Responsible Manager for MFP	A person in an organization in which MFPs are placed and who has the authority to assign MFP Administrators and a Supervisor (or the person who is responsible for the organization). E.g., MFP purchasers, MFP owners, a manager of the department in which MFPs are placed, a person who is in charge of IT department.
Administrator	An authorized TOE user who manages the TOE. Administrators are given Administrator Roles and perform administrative operations accordingly. Up to four Administrators can be registered, and each Administrator is given one or more Administrator Roles.

Terms	Definitions
Administrator Role	Management functions given to Administrators. There are four types of Administrator Roles: User Administration, Machine Administration, Network Administration and File Administration. Each Administrator Role is assigned to at least one of the registered Administrators.
User Administration	The Administrator Role that manages General Users. The User Administrator is a person who has the user management role.
Machine Administration	The Administrator Role that manages machines and plays the role of performing the audit. The Machine Administrator is a person who has the machine management role.
Network Administration	The Administrator Role that manages the TOE network connections. The Network Administrator is a person who has the network management role.
File Administration	The Administrator Role that manages the D-BOX, which stores the Document Data stored in the TOE, and manages the Document Data ACL, which controls the access to the Document Data. The File Administrator is a person who has the role of File Administration.
Supervisor	The authorized TOE user who manages the passwords of Administrators.
General User	An authorized TOE user who uses the basic functions of the TOE.
Address Book	A database containing General User Information for each General User.
Back Up/Restore Address Book	To back up the Address Book to SD cards or to restore the backup copy of the Address Book from SD cards to the TOE.
General User Information	A record containing information about a General User. Data items include the General User IDs, General User authentication information, Document Data Default ACL, and S/MIME User Information.
S/MIME User Information	Information about each General User that is required for using S/MIME. Includes E-mail address, user certificates and specified value for S/MIME use.
Document Data Default ACL	One of the data items of General User Information. The default value that is set for the Document Data ACL of a new Document Data to be stored.
Document File Owner	General Users who are registered in the Document Data ACL as owners of the Document Data.
Document File User	General Users who are registered in the Document Data ACL and who are not owners of the Document Data.
Received and Stored Function	A function that stores the received fax data on HDD inside the TOE. Received and Stored Document Data is a fax data stored in the TOE.
Direct Print Function	A function that prints out the received Print Data by the TOE.

Terms	Definitions
Store and Print Function	A function that converts Print Data received by the TOE into Document Data and stores it in D-BOX. Document Data stored in D-BOX can be printed out according to users' instruction.
Immediate Transmission	A function that dials first, the faxes data while scanning the original.
Memory Transmission	A function that stores the scanned data of the original in memory, and then dials and faxes the data.
Stored Documents Fax Transmission	A function that faxes Document Data previously stored in D-BOX.
Fax Transmission from Computers	A function that faxes Document Data from a client PC via the TOE when connecting client PC to networks or with USB Ports.
IP-Fax	A function that sends and receives document files between two faxes directly via a TCP/IP network. It is also possible to send document files to a fax that is connected to a telephone line using this function.
Internet Fax	A function that converts scanned document images to e-mail format and transit the data over the Internet, and a machine that has an e-mail address can receive the e-mail sent using this function.
Sending by E-mail	A function that sends e-mail with the attached Document Data from the TOE.
Deliver to Folder	A function that sends the Document Data to folders in SMB Server or FTP Server from the TOE via networks.
Lockout	A function that prohibits the access for the specific user IDs to the TOE.
MFP Control Data	A generic term for a set of parameters that control the operation of MFP.
Device Control Data	MFP Control Data that is related to security functions and security behaviour.
Network Control Data	MFP Control Data that is used to connect MFP to networks.
Number of Attempts before Lockout	The number of consecutive failed password authentications using the same User ID that results in that user's Lockout.
Setting for Lockout Release Timer	Setting that enables or disables automatic timed release of Lockout with the time set in advance by Administrators. When this setting is inactive, Lockout can be released only by the direct operation by Administrators.
Lockout Flag	A data that is assigned to each authorized user. The Lockout Flag for the locked-out User is set to "Active", otherwise it is set to "Inactive". The Administrators or Supervisor who are authorized to operate the Lockout Flag can release the Lockout for the Locked out Users by setting the Lockout Flag for the Locked out Users to "Inactive".
Minimum Password Length	The minimum number of digits that can be registered for passwords.

Terms	Definitions
Complexity Setting for Password	The minimum combination of character types that can be registered for passwords. There are 4 character types: upper-case letters, lower-case letters, numbers, and symbols. There are two complexity setting levels for Complexity Setting for Password, Level 1 and Level 2. Level 1 requires passwords with a combination of more than two character types. Level 2 requires passwords with a combination of more than three character types.
Print Settings	Print Settings for printed output, including paper size, printing magnification and customized information (such as duplex and layout).
Stored Data Protection Function	A function that protects the Document Data stored on HDD from leakage.

2 TOE Description

This chapter outlines the type of the TOE, environment for the usage of the TOE, physical boundary of the TOE, the involved roles of the TOE, logical boundary of the TOE, and protected assets.

2.1 TOE Type

The TOE is an MFP, which is an IT product that provides the functions of copier, scanner, printer and fax (optional). Those functions are for digitising the paper document files, managing the document files, printing the document files.

2.2 Environment for Usage of TOE

The TOE is assumed to be placed in general offices. In offices, the TOE can be connected to IT products, networks, and telephone lines, depending on the needs of the users, and USB Ports can be also used. Users can operate the TOE from the Operation Panel of the TOE, client PCs that are connected to the Internal Networks, or client PCs that are connected to a USB Port. Figure 1 shows and describes an assumed environment for the usage of the TOE.

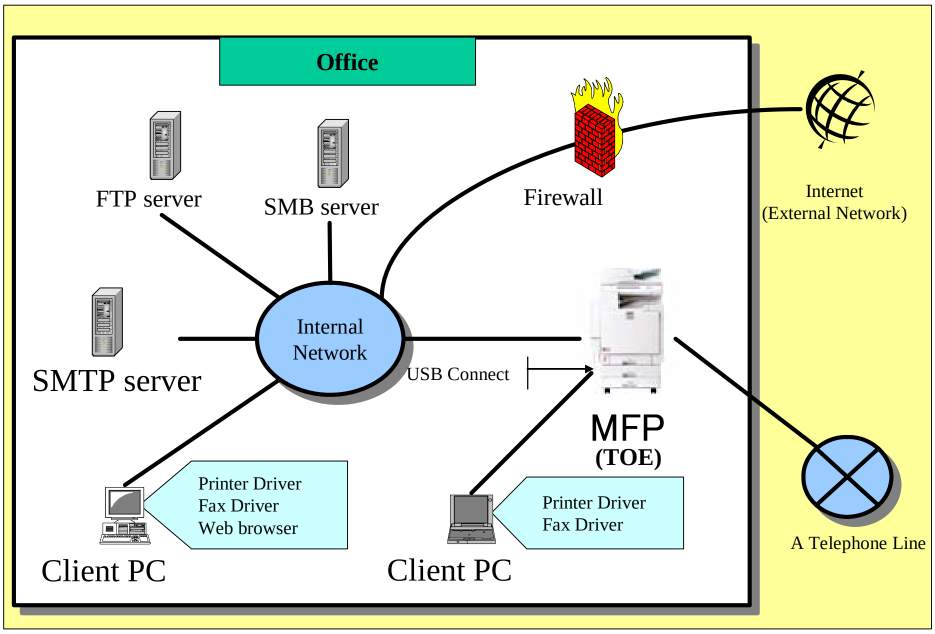

Figure 1: Environment for usage of TOE

Location for TOE

The TOE is assumed to be placed in general offices.

TOE Operation from Operation Panel

The Operation Panel is a user interface device that is equipped on the TOE and consists of keyswitches, LED indicators, and a touch screen LCD. Keyswitches have a role that users input information to the TOE, LED indicators have a role that displays users the information of the TOE, and the touch screen LCD has both of these roles.

Connecting TOE to Internal Network

Connecting the TOE to the Internal Networks allows the TOE to communicate with the IT products that are connected to the Internal Networks. The environment for the Internal Networks should be IPv4. The IT products with which the TOE communicates, and their intended purposes are described as follows.

[TOE operation from client PC]
It is valid for the TOE to be operated by users and to communicate data using a web browser on a client PC that is connected to the Internal Networks.
It is necessary to install Internet Explorer 6.0 or later on the client PC in advance.

[Printing from client PC]
It is valid for the TOE to print out the document files from a client PC that is connected to the Internal Networks. It is necessary to download and install RPCS printer driver into a client PC from the website described in Users Guidance.

[Faxing from client PC]

It is valid for the TOE to fax the document files from a client PC that is connected to the Internal Networks via the TOE. It is necessary to download and install the fax driver into a client PC from the website described in Users Guidance.

[Sending by e-mail from TOE to client PC]
It is valid for the TOE to send Document Data attached to an e-mail message to a client PC via an SMTP Server.

[FTP Server]
It is valid for the TOE to transfer Document Data to an FTP Server.

[SMB Server]
It is valid for the TOE to transfer Document Data to an SMB Server.

Connecting TOE to Telephone Line

Connecting the TOE to a telephone line allows the TOE to send and receive faxes.

Connecting TOE and Client PC with USB

Connecting the TOE and client PC with USB cable allows the TOE to print and fax from that client PC.

Connecting Internal and External Network

When connecting the Internal Networks and External Networks, the Internal Networks are protected from the External Networks by setting up firewalls between them.

2.3 Physical Boundary of TOE

The physical boundary of the TOE is the MFP, which consists of hardware (as shown in Figure 2): Operation Panel, Engine Unit, Fax Unit, Controller Board, Ic Hdd, HDD, Network Unit, USB Port and SD CARD Slot. Although the Fax Unit is optional among these, the configuration without the Fax Unit is also covered by the physical boundary. Figure 2 shows and outlines the configuration items of hardware of the TOE.

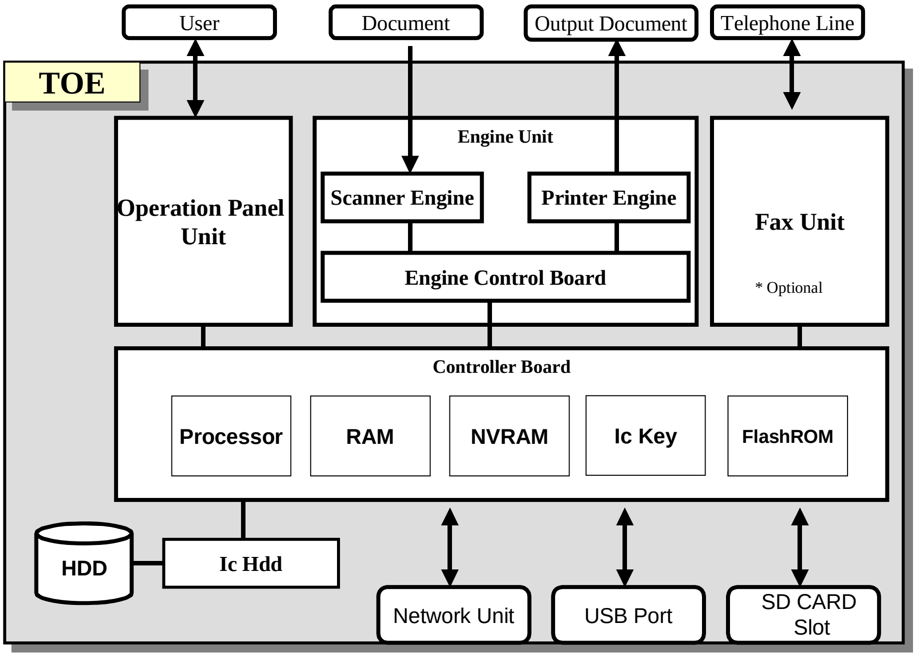

Figure 2: Hardware configuration of TOE

Operation Panel Unit (hereafter called Operation Panel)

The Operation Panel is an interface device that is equipped on the TOE and is used by TOE users for TOE operation. It is configured with keyswitches, LED indicators, touch screen LCD, and the Operation Panel Control Board. Operation Panel Control Software is installed in the Operation Panel Control Board. The Operation Panel Control Software puts on and off the LEDs, and displays information on the touch screen LCD after sending the input information from the keyswitches and touch screen LCD to MFP Control Software or in response to instructions from the MFP Control Software.

Engine Unit

The Engine Unit is configured with a Scanner Engine, Printer Engine and Engine Control Board. The Scanner Engine is an input device to read the paper documents. The Printer Engine is the output device to print and output the paper documents. Engine Control Software is installed in the Engine Control Board. The Engine Control Software sends information about the status of the Scanner Engine and the Printer Engine to the MFP Control Software, or operates the Scanner Engine and the Printer Engine according to the instruction from the MFP Control Software.

Fax Unit (optional)

The Fax Unit is a device that has a modem function to send and receive fax data when connected to a telephone line.

The Fax Unit has an interface to the MFP Control Software that provides the MFP Control Software with the information about the status of fax communication and controls the fax communication according to the instruction from the MFP Control Software.

Controller Board

The Controller Board contains processors, RAM, NVRAM, Ic Key and FlashROM. It is connected to the Operation Panel Unit, Engine Unit, Fax Unit, Network Unit, USB Port, SD CARD Slot and Ic Hdd. Ic Hdd is also connected with HDD. The functions of processors, RAM, NVRAM, Ic Key and FlashROM are described below:

[Processor]
A semiconductor chip that carries out the basic arithmetic processing of the MFP operation.

[RAM]
A volatile memory that is used for an image processing memory.

[NVRAM]
A non-volatile memory in which MFP Control Data to configure the MFP operation is stored.

[Ic Key]
A security chip that provides the functions of random number generation and encryption key generation, and is used to detect the tampering of MFP Control Software.

[FlashROM]
A memory in which MFP Control Software is installed.

Ic Hdd

Ic Hdd is a security chip that provides the functions to encrypt the information to be stored on HDD and to decrypt the information to be read from HDD.

HDD

HDD is a hard disk drive in which image data and user information for identification and authentication are stored.

Network Unit

The Network Unit is an interface board for Ethernet (100BASE-TX/10BASE-T) networks.

USB Port

The USB Port is used to connect a client PC to the TOE, and is used for printing or faxing from that client PC.

SD CARD Slot

The SD CARD Slot is a slot that is used by CEs for the maintenance work using SD CARD. It is located on the side of the TOE, and it is normally covered. When a CE performs maintenance work, he/she removes this cover to insert and remove the SD Card.

When installing the TOE, the CE installs an SD Card containing information to activate the Stored Data Protection Function into the SD CARD Slot to enable the Stored Data Protection Function.

2.4 Involved Roles of TOE

This section describes the roles involved in TOE operation.

2.4.1 Responsible Manager for MFP

The Responsible Manager for MFP is a person who belongs to the organization that uses the TOE and has the role to select the TOE Administrators and TOE Supervisor.

The Responsible Manager for MFP selects up to four Administrators and one Supervisor. When selecting Administrators, the Responsible Manager for MFP assigns each Administrator one or more of the following Administrator Roles: User Administration, Machine Administration, Network Administration and File Administration.

2.4.2 Administrator

An Administrator is a user who is registered on the TOE as an Administrator. There are one to four Administrators registered for the TOE. Administrator Roles for Administrators include User Administration, Machine Administration, Network Administration and File Administration. Administrators may have concurrent Administrator Roles, and Administrator Roles are assigned to one or more Administrators. One default Administrator is registered and is assigned all four Administrator Roles at the factory. When installing the TOE, the Administrators who are selected by the Responsible Manager for MFP change the settings of their own Administrator IDs, passwords and Administrator Roles. Table 3 describes the Administrator jobs for each Administrator Role.

Table 3: List of Administrator Roles

Administrator Roles	Explanations
User Administration	Manage General Users.
Machine Administration	Manage machines and perform the audit.
Network Administration	Manage the TOE network connections.
File Administration	Manage the document files stored in the TOE.

2.4.3 Supervisor

The Supervisor is a user who manages Administrator passwords and can change these passwords. One Supervisor shall be registered for the TOE. A default Supervisor is registered for the TOE at the factory. The person who is selected as a Supervisor by the Responsible Manager for MFP changes Supervisor ID and password of the default Supervisor.

2.4.4 General User

A General User is an authorized TOE user who is registered in the Address Book by the User Administrator, and can store the Document Data in the TOE and operate the Document Data stored in the TOE.

2.4.5 Customer Engineer

A Customer Engineer (hereafter called CE) is an expert in maintenance for the TOE who belongs to manufacturers, technical support service companies, or sales companies.

2.5 Logical Boundary of TOE

The logical boundary of the TOE comprises the functions provided by the TOE. This chapter describes the "basic functions", which is the service the TOE provides for the users, and the "security functions", which counters the threats of the TOE. These functions are illustrated in Figure 3.

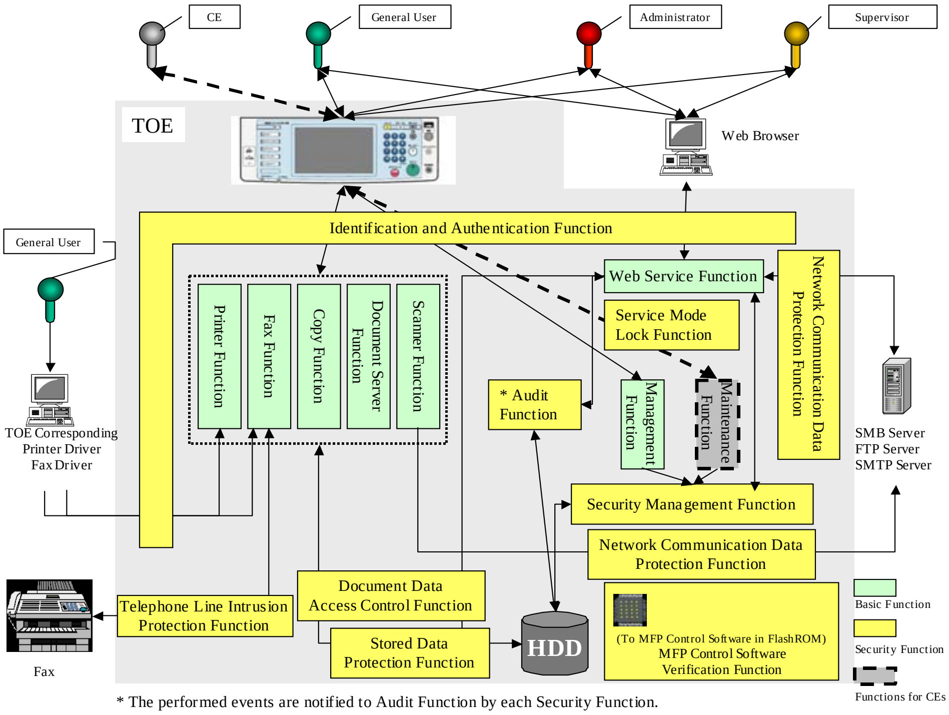
CE
General User
Administrator
Supervisor
TOE
Web Browser
General User
TOE Corresponding Printer Driver Fax Driver
Identification and Authentication Function
Printer Function
Fax Function
Copy Function
Document Server Function
Scanner Function
Web Service Function
Service Mode Lock Function
Network Communication Data Protection Function
* Audit Function
Management Function
Maintenance Function
SMB Server
FTP Server
SMTP Server
Security Management Function
Network Communication Data Protection Function
Fax
Telephone Line Intrusion Protection Function
Document Data Access Control Function
Stored Data Protection Function
HDD
(To MFP Control Software in FlashROM)
MFP Control Software Verification Function
Basic Function
Security Function
Functions for CEs
* The performed events are notified to Audit Function by each Security Function.

Figure 3: Logical boundary of TOE

2.5.1 Basic Functions

Basic functions include the Copy Function, Printer Function, Fax Function, Scanner Function, Document Server Function, Management Function and Web Service Function. This chapter describes these basic functions. Basic functions can be operated from the Operation Panel or web browser of a client PC.

When operating from the Operation Panel, users select functions from the Operation Panel shown in Figure 4. General Users use the functions of Copy, Document Server, Fax, Printer, and Scanner by pushing the buttons for "Copy", "Document Server", "Facsimile", "Printer" and "Scanner" which are on the left side of the panel. Administrators and a Supervisor use the Management Function by pushing the button "User Tools/Counter" which is on the upper left side of the Operation Panel.

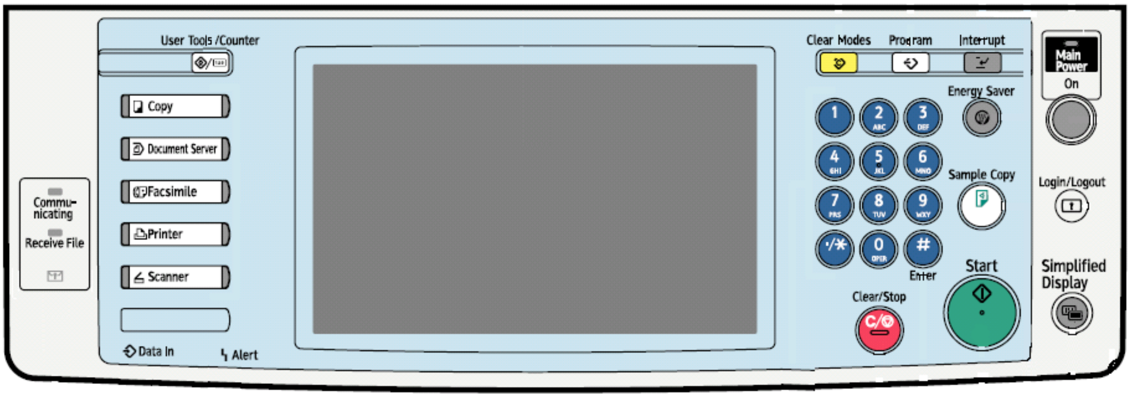

Figure 4: Operation Panel (for North America)

In addition, General Users, Administrators, and a Supervisor can use the functions corresponding to each user role by accessing to the Web Service Function of the TOE from web browser of a client PC. The basic functions are described in the following sections.

2.5.1.1 Copy Function

The Copy Function is used to scan the original and print out the scanned image data in accordance with the Print Settings specified by the user. Print Settings include the number of copies, magnification, and custom settings (e.g. specify to print multiple pages of original image on a single sheet). In addition, the scanned original images can be stored in D-BOX as Document Data. The Document Data stored in D-BOX using the Copy Function can be printed and deleted using the "2.5.1.5 Document Server Function".

2.5.1.2 Printer Function

The Printer Function is used to print out the Print Data sent from a client PC. The TOE receives Print Data from client PCs via networks or a USB Port. The TOE prints out the received Print Data with Direct Print Function or Store and Print Function. The Print Data can be stored in D-BOX as Document Data using the Store and Print Function, and the stored Document Data can be printed and deleted using the "2.5.1.5 Document Server Function".

2.5.1.3 Fax Function

The Fax Function is used to send and receive fax data to and from fax devices over a telephone line. The Fax Function includes the Fax Receive Function (hereafter called Fax Reception), the Fax Transmission Function (hereafter called Fax Transmission), and a function to print and delete Fax Transmission/Reception data.

Fax Reception either prints the received fax data, or converts the received fax data into the Fax Reception data and then stores it in D-BOX. The Fax Reception data stored in D-BOX can be printed and deleted using the Fax Function or "2.5.1.5 Document Server Function".

Fax Transmission includes Immediate Transmission, Memory Transmission, and Stored Document Fax Transmission, which are operated from the Operation Panel, and also includes PC Fax Transmission, which is operated from a client PC. Document Data stored in D-BOX for faxing can be printed and deleted using the "2.5.1.5 Document Server Function".

Although the MFP provides IP-Fax Function and Internet Fax Function as a part of Fax Function, these functions are not covered by this evaluation.

2.5.1.4 Scanner Function

The Scanner Function is used to scan paper-based originals and deliver the scanned image data to folders or send it as Document Data by e-mail via networks so that a client PC can handle. It can also store the scanned image data in D-BOX as Document Data. Document Data stored in D-BOX can be sent by e-mail, delivered to folders, and deleted using the Scanner Function.

2.5.1.5 Document Server Function

The Document Server Function is used to scan paper-based originals and store the scanned image data in D-BOX as Document Data. In addition, Document Data stored in D-BOX with Copy Function, Printer Function, Fax Function, and Document Server Function can be printed and deleted using the Document Server Function. However, the Document Data stored in D-BOX using Scanner Function cannot be printed or deleted using the Document Server Function.

2.5.1.6 Management Function

The Management Function is used to manage the following information: information to configure the operation of the machine, information to connect the TOE to networks, information about users, and information to restrict the use of the Document Data. A user's ability to manage this information is determined in accordance with that user's authorized role (General Users, Administrators, or Supervisor). The Management Function can be operated from the Operation Panel or by accessing to Web Service Function from a client PC. Some information can be managed only from either the Operation Panel or client PC. Among Management Functions, the functions related to security are described in "2.5.2.6 Security Management Function".

This evaluation does not cover Back Up/Restore Address Book that is limited its availability by this function.

2.5.1.7 Web Service Function

The Web Service Function is used to operate the TOE remotely from a client PC by authorized TOE users (General Users, Administrators or Supervisor). For remote operation, it is necessary to install a web browser on the client PC and to connect the TOE and client PC with networks. Users can use the Web Service Function by accessing to the web server of the TOE from web browser. The available TOE operations for remote operation are as follows:

1. Print, send, delete and download Document Data that is stored in D-BOX.
   However, only the Document Data stored with the Copy Function, Document Server Function, Fax Function, and Printer Function can be printed. Only the Document Data stored with Scanner Function can be sent. Only the Document Data stored with Scanner Function and Fax Function can be downloaded.
2. Subset of Management Functions.

3. Check the TOE status.

2.5.2 Security Functions

Security functions include the Audit Function, Identification and Authentication Function, Document Data Access Control Function, Stored Data Protection Function, Network Communication Data Protection Function, Security Management Function, Service Mode Lock Function, Telephone Line Intrusion Protection Function, and MFP Control Software Verification Function. This chapter describes these security functions.

2.5.2.1 Audit Function

The Audit Function is used to check the operation status of the TOE, or to record security-related events, which are required to detect the security intrusion, to the audit log. Only the Machine Administrator is allowed to read and delete the recorded audit logs. The Machine Administrator can use the Web Service Function for reading the audit logs, and the Operation Panel or Web Service Function for deleting the audit logs.

2.5.2.2 Identification and Authentication Function

The Identification and Authentication Function ensures that users are securely identified and authenticated. For users who attempt to use the TOE from the Operation Panel or client PC, this function requires users to enter a user ID and password and then it attempts to identify and authenticate the user. When printing or faxing from client PC, this function sends the user IDs and the authentication information to the TOE after users enter their user IDs and authentication information from printer or fax drivers, which are outside of the TOE. Then the TOE attempts to identify and authenticate the user with the received user ID and authentication information.

Identification and Authentication Function includes the following:

1. Account Lockout - If the number of consecutive unsuccessful attempts to identify and authenticate a particular user ID meets the Number of Attempts before Lockout, this prevents this user ID from logging in temporarily.
2. Authentication Feedback Area Protection - When users enter their passwords, this displays the passwords on the authentication feedback area with the protection character in order not to be viewed by others.
3. Password Quality Maintenance - When users set or change their passwords, this allows them to register only the passwords that satisfy the conditions of Minimum Password Length and Complexity Setting for Password, which the User Administrator has set in advance.

Although there are other Identification and Authentication Function that this TOE has, the Identification and Authentication Functions that are not listed above are not covered by this evaluation.

2.5.2.3 Document Data Access Control Function

The Document Data Access Control Function performs several operations to ensure that the users, who are authorized by Identification and Authentication Function, are permitted to access Document Data based on the permissions assigned to their user role or operation permission.
The three operations on Document Data are as follows:

1. Reading Document Data: Read Document Data stored in D-BOX.
2. Editing Document Data: Register Print Settings changes for Document Data stored in D-BOX.
3. Deleting Document Data: Delete Document Data stored in D-BOX.

The File Administrator is allowed to delete any Document Data stored in D-BOX. General Users are granted one of the following access rights for each Document Data: Read-only, Edit, Edit/Delete, Full Control, or no access rights. Table 4 describes the relation between the access rights and the operations by General Users on Document Data.

Table 4: Correspondence Table for Access Rights and Operations on Document Data

Operations on Document Data Access rights	Reading Document Data	Editing Document Data	Deleting Document Data
Read-only	X		
Edit	X	X	
Edit/Delete	X	X	X
Full Control	X	X	X

X: Granted permission to operate, Blank: Not granted permission to operate

2.5.2.4 Stored Data Protection Function

The Stored Data Protection Function protects Document Data recorded on HDD from leakage by making it difficult to understand unless the Document Data is accessed in the normal way.

2.5.2.5 Network Communication Data Protection Function

The Network Communication Data Protection Function protects Document Data and Print Data on networks from unauthorized access. The communication protocol that is used to protect the communication data differs according to the transmission methods for Document Data or Print Data.
The relation between the transmission methods and protection measures is described below:

The Network Administrator decides the communication protocol to use according to the environment where the TOE is placed and the intended purpose of the TOE.

1. Download the Document Data with the Web Service Function from a client PC: SSL protocol.
2. Print or fax from a client PC: SSL protocol.
3. Deliver Document Data to an FTP Server or SMB Server from the TOE: IPSec protocol.
4. Send Document Data attached to e-mail to a client PC from the TOE: S/MIME.

2.5.2.6 Security Management Function

The Security Management Function is used to allow the Administrators, Supervisor, and General Users, who are successfully authenticated with "2.5.2.2 Identification and Authentication Function", to perform the following operations for Security Management corresponding to their user role:

1. Management of the Document Data ACL

Management of the Document Data ACL is used to allow only specific users to modify the Document Data ACL. Modifying the Document Data ACL includes changing Document File Owners, registering new Document File Users for the Document Data ACL, deleting Document File Users who were previously registered for the Document Data ACL, and changing Document File Users' operation permissions. Among these, only the File Administrator is allowed to change the Document File Owners. The File Administrator, Document File Owners, and Document File Users who have full control permissions on Document Data are allowed to perform other operations.

When Document Data is stored, its Document Data ACL is set to the Document Data Default ACL.

2. Management of Administrator Information

Management of Administrator Information is used to allow the specific users to register and delete Administrators, to add and delete Administrator Roles, and to change Administrator IDs and passwords.

Only Administrators are permitted to register another Administrator and to add an Administrator Role to another Administrator. The concerned Administrator is permitted to delete the Administrator and Administrator Role and to change Administrator ID. The concerned Administrator and Supervisor are permitted to change Administrator passwords. And an Administrator is permitted to add an Administrator Role, and to delete his/her own Administrator Roles, provided that all such Administrator Roles are already assigned to other Administrators. Since Administrators are required to have one or more Administrator Roles, it is necessary to give (add) one or more roles of their own Administrator Roles to the new Administrator when they register other Administrators. In addition, if Administrators delete all the Administrator Roles of their own, their Administrator information will be automatically deleted.

3. Management of General User Information

Management of General User Information is used to allow only specific user roles to newly create, change and delete General User Information. The relation between the user roles and authorized operations is:

- The User Administrator is permitted to newly create, change and delete General User Information.
- General Users are permitted to change their own General User Information that is registered for Address Book, with the exception of their User ID even if it is their own General User Information.

4. Management of Supervisor Information

The Supervisor is permitted to change his/her Supervisor ID and password.

5. Management of Machine Control Data
Each Administrator is permitted to configure the data items of machine control data that corresponds to their Administrator Role (Machine Administrator, User Administrator and File Administrator).

2.5.2.7 Service Mode Lock Function

The Maintenance Function is used by CEs to perform the maintenance services for the TOE from the Operation Panel according to the request from the Machine Administrator. Service Mode Lock Function is used to prohibit the Maintenance Function from being operated. This ST covers this function set to "On" as the target of evaluation.

2.5.2.8 Telephone Line Intrusion Protection Function

The Telephone Line Intrusion Protection Function, for devices that are equipped with a Fax Unit, is used to restrict communication from a telephone line to the TOE so that only permitted data is received by the TOE.

2.5.2.9 MFP Control Software Verification Function

The MFP Control Software Verification Function is used to check the integrity of the executable code of the MFP Control Software that is installed in FlashROM, and to verify it is regular.

2.6 Protected Assets

The protected assets of the TOE are Document Data and Print Data. Document Data and Print Data are described below.

2.6.1 Document Data

Document Data is imported from the outside of the TOE in various ways and can be either stored in the TOE or output from the TOE. For Document Data stored in the TOE, Print Settings can be edited and Document Data can be deleted.

2.6.1.1 Importing Document Data

Document Data can be imported by the following two operations:

1. Import from Scanner Unit
   Read the image of a paper-based original with scanner of the TOE and generate Document Data.
2. Import from Networks/USB
   Convert Print Data that the TOE receives from networks or USB into a format that the TOE can process, and generate Document Data.

2.6.1.2 Storing Document Data

Document Data stored in the TOE is stored in D-BOX. Document Data stored in D-BOX is protected from unauthorized access and leakage.

2.6.1.3 Outputting Document Data

Document Data can be output by the following five operations:

1. Send the Document Data to a client PC (to its e-mail address)
2. Send the Document Data to an SMB Server or FTP Server
3. Download the Document Data from the TOE to a client PC
4. Print out the Document Data
5. Fax the Document Data

Document Data on communication path is protected from leakage during communication in methods 1 through 3, above, and if there is tampering, it is detected.

2.6.2 Print Data

Print Data is a printed or faxed output image that is generated from document files in a client PC by printer or fax drivers that are installed on the client PC when printing or faxing, respectively. Print Data is imported to the TOE via the Internal Networks or USB Port. Print Data is protected from leakage on the Internal Network path when it is sent from a client PC to the TOE, and if there is tampering, it is detected.

3 TOE Security Environment

This chapter describes the assumptions, threats and organizational security policy.

3.1 Assumptions

The assumptions related to the environment and use of the TOE is identified and described below.

A.ADMIN **(Assumption for Administrators)**

Administrators will have adequate knowledge to operate the TOE securely in the roles assigned to them, and guide General Users operate the TOE securely. Additionally, Administrators will not carry out any malicious acts using Administrator permissions.

A.SUPERVISOR **(Assumption for Supervisor)**

The Supervisor will have adequate knowledge to operate the TOE securely in the role assigned to him/her, and will not carry out any malicious acts using Supervisor permissions.

A.NETWORK **(Assumption for Network Connections)**

The Internal Networks will be protected from the External Networks when the TOE-connected networks are connected to the External Networks such as the Internet.

3.2 Threats

The assumed threats related to the use and environment of this TOE are identified and described below. The threats described in this chapter are attacks by persons who have the knowledge of disclosed information about the TOE operation, and the attackers will have the low level of attack potential.

T.ILLEGAL_USE **(Malicious Usage of TOE)**

Attackers may read or delete the Document Data by gaining unauthorized access to the TOE from the TOE external interfaces (Operation Panel, Network Interface, USB Interface or SD CARD interface).

T.UNAUTH_ACCESS **(Access Violation to Protected Assets Stored in TOE)**

Authorized TOE users may go beyond the bounds of the authorized usage and access to Document Data from the TOE external interfaces (Operation Panel, Network Interface or USB Interface) that are provided to the authorized TOE users.

T.ABUSE_SEC_MNG (Abuse of Security Management Function)

Persons who are not authorized to use Security Management Function may abuse the Security Management Function.

T.SALVAGE (Salvaging Memory)

Attackers may take HDD out of the TOE and disclose Document Data.

T.TRANSIT (Interceptions and Tampering on Communication Path)

Attackers may illegally obtain, leak, or tamper Document Data and Print Data that are sent or received by the TOE via the Internal Networks.

T.FAX_LINE (Intrusion from Telephone Line)

Attackers may gain unauthorized access to the TOE from telephone lines.

3.3 Organizational Security Policy

The following security policy is assumed for the organizations that demand the integrity of software installed in IT products:

P.SOFTWARE (Checking Integrity of Software)

Measures are provided for verifying the integrity of MFP Control Software, which is installed in FlashROM in the TOE.

4 Security Objectives

This chapter describes the security objectives for the TOE and security objectives for the environment for "3.1 Assumptions", "3.2 Threats", and "3.3 Organizational Security Policy".

4.1 Security Objectives for TOE

This chapter describes the security objectives for the TOE.

O.AUDIT **(Audit)**

The TOE shall record the security-function-relevant events as audit logs, and provide only the Machine Administrator with the function to read the audit logs so that the Machine Administrator can detect whether or not there was security intrusion.

O.I&A **(User Identification and Authentication)**

The TOE shall perform identification and authentication of users prior to their use of the TOE security functions, and allow the successfully authenticated user to use the functions for which the user has the operation permission.

O.DOC_ACC **(Access Control to Protected Assets)**

For General Users, the TOE shall ensure the access to Document Data according to the authorized users for Document Data set for each Document Data and their operation permissions for each Document Data. The TOE shall also allow the File Administrator to delete Document Data stored in D-BOX.

O.MANAGE **(Security Management)**

The TOE shall allow only specific users the TOE can maintain the security to manage the security functions behaviour, TSF data, and security attributes.

O.MEM.PROTECT **(Prevention of Data Disclosure Stored in Memory)**

The TOE shall make the format of Document Data stored on HDD difficult to decode.

O.NET.PROTECT **(Protection for Network Communication Data)**

The TOE shall protect Document Data and Print Data on communication paths from interceptions, and detect tampering.

O.GENUINE **(Protection of Integrity of MFP Control Software)**

The TOE shall provide the function to verify the integrity of MFP Control Software, which is installed in FlashROM with the TOE users.

O.LINE_PROTECT (Telephone Line Intrusion Protection)

The TOE shall prevent unauthorized access to the TOE from a telephone line connected to the Fax Unit.

4.2 Security Objectives for Environment

This chapter describes the security objectives for the environment.

OE.ADMIN (Trusted Administrator)

The Responsible Manager for MFP shall select trusted persons as Administrators, and provide them with the education programs according to their Administrator Roles. The educated Administrators shall instruct General Users to be familiar with the compliance rules for secure operation for General Users, as explicitly stated in Administrator guidance for the TOE.

OE.SUPERVISOR (Trusted Supervisor)

The Responsible Manager for MFP shall select a trusted person as the Supervisor and provide the Supervisor with the education programs according to the role of Supervisor.

OE.NETWORK (Network Environment for TOE Connection)

When connecting the Internal Networks, to which the TOE is connected, to External Networks such as the Internet, the organization that manages the operation of the Internal Networks shall close the unnecessary ports between the External and Internal Networks. (E.g., Firewall set up.)

5 IT Security Requirements

5.1 TOE Security Functional Requirements

This chapter describes the TOE security functional requirements to accomplish the security objectives defined in 4.1. The part with Assignment and Selection defined in the Common Criteria (CC) are identified with **[bold face and brackets].**

This chapter describes the dependencies required by the CC. Dependencies that are satisfied by this ST are described in Chapter 8.2.3.

5.1.1 Class 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:

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

b) All auditable events for the **[selection: not specified]** level of audit; and

c) **[assignment: auditable events of the TOE shown in Table 5]**.

Table 5 shows the actions (rules in the CC) that are recommended by the CC to be auditable for each functional requirement, and the corresponding auditable events of the TOE.

Table 5: List of Auditable Events

Functional Requirements	Actions which should be auditable	Auditable events of TOE
FAU_GEN.1	None	-
FAU_SAR.1	a) Basic: Reading of information from the audit records.	Auditable events are not recorded.
FAU_SAR.2	a) Basic: Unsuccessful attempts to read information from the audit records.	Auditable events are not recorded.
FAU_STG.1	None	-
FAU_STG.4	a) Basic: Actions taken due to the audit storage failure.	Auditable events are not recorded.
FCS_CKM.1	a) Minimal: Success and failure of the activity.	<Individually defined auditable events> 1. HDD cryptographic key generation

Functional Requirements	Actions which should be auditable	Auditable events of TOE
	b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	(Outcome: Success/Failure)
FCS_COP.1	a) Minimal: Success and failure, and the type of cryptographic operation. b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	<Individually defined auditable events> 1. Succeeding in storing the Document Data 2. Succeeding in reading the Document Data
FDP_ACC.1	None	-
FDP_ACF.1	a) Minimal: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by the SFP. c) Detailed: The specific security attributes used in making an access check.	<Individually defined auditable events> 1. Succeeding in storing the Document Data 2. Succeeding in reading the Document Data 3. Succeeding in deleting the Document Data
FDP_IFC.1	None	-
FDP_IFF.1	a) Minimal: Decisions to permit requested information flows. b) Basic: All decisions on requests for information flow. c) Detailed: The specific security attributes used in making an information flow enforcement decision. d) Detailed: Some specific subsets of the information that has flowed based upon policy goals (e.g. auditing of downgraded material).	a) Minimal 1. Fax Function: Reception
FIA_AFL.1	a) Minimal: the reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state	a) Minimal 1. Starting Lockout 2. Lockout release

Functional Requirements	Actions which should be auditable	Auditable events of TOE
	(e.g. re-enabling of a terminal).	
FIA_ATD.1	None	-
FIA_SOS.1	a) Minimal: Rejection by the TSF of any tested secret; b) Basic: Rejection or acceptance by the TSF of any tested secret; c) Detailed: Identification of any changes to the defined quality metrics.	b) Basic 1. Newly creating authentication information of General Users (Outcome: Success/Failure) 2. Changing authentication information of General Users (Outcome: Success/Failure) 3. Changing authentication information of Administrators (Outcome: Success/Failure) 4. Changing authentication information of Supervisor (Outcome: Success/Failure)
FIA_UAU.2	Minimal: Unsuccessful use of the authentication mechanism; Basic: All use of the authentication mechanism;	Basic 1. Login (Outcome: Success/Failure)
FIA_UAU.7	None	-
FIA_UID.2	a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided; b) Basic: All use of the user identification mechanism, including the user identity provided.	b) Basic 1. Login (Outcome: Success/Failure)
FIA_USB.1	a) Minimal: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject). b) Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).	b) Basic 1. Login (Outcome: Success/Failure)
FMT_MSA.1	a) Basic: All modifications of the values of security attributes.	<Individually defined auditable events> 1. Adding and deleting Administrator Roles 2. Changing the Document Data ACL
FMT_MSA.3	a) Basic: Modifications of the default setting of permissive or restrictive rules. b) Basic: All modifications of the initial values of security attributes.	Auditable events are not recorded.
FMT_MTD.1	a) Basic: All modifications to the values of TSF data.	<Individually defined auditable events> 1. Newly creating authentication

Functional Requirements	Actions which should be auditable	Auditable events of TOE
		information of General Users. 2. Changing authentication information of General Users. 3. Deleting authentication information of General Users. 4. Changing authentication information of Administrators. 5. Changing authentication information of Supervisor. 6. Changing time and date of system clock. 7. Deleting the entire audit logs
FMT_SMF.1	a) Minimal: Use of the Management Functions.	<Individually defined auditable events> 1. Adding and deleting Administrator Roles 2. Lockout release by the Unlocking administrator. 3. Changing time and date of system clock.
FMT_SMR.1	a) Minimal: modifications to the group of users that are part of a role; b) Detailed: every use of the rights of a role.	a) Minimal 1. Adding and deleting Administrator Roles.
FPT_RVM.1	None	-
FPT_SEP.1	None	-
FPT_STM.1	a) Minimal: changes to the time; b) Detailed: providing a timestamp.	a) Minimal 1. Changing time and date of system clock.
FPT_TST.1	a) Basic: Execution of the TSF self tests and the results of the tests.	-
FTP_ITC.1	a) Minimal: Failure of the trusted channel functions. b) Minimal: Identification of the initiator and target of failed trusted channel functions. c) Basic: All attempted uses of the trusted channel functions. d) Basic: Identification of the initiator and target of all trusted channel functions.	<Individually defined auditable events> 1. Communication with trusted IT products (Outcome: Success/Failure, Communication IP address)
FTP_TRP.1	a) Minimal: Failures of the trusted path functions. b) Minimal: Identification of the user associated with all	<Individually defined auditable events> 1. Communication with remote users (Outcome: Success/Failure)

Functional Requirements	Actions which should be auditable	Auditable events of TOE
	trusted path failures, if available. c) Basic: All attempted uses of the trusted path functions. d) Basic: Identification of the user associated with all trusted path invocations, if available.	

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[assignment: communication IP address, IDs of persons whose authentication information is created/changed/deleted, locking out Users, releasing User lockout, method of lockout release, IDs of object Document Data]**.

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: the Machine Administrator]** with the capability to read **[assignment: all log items]** from the audit records.

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_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

FAU_STG.1.2 The TSF shall be able to **[selection: prevent]** unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall **[selection: overwrite the oldest stored audit records]** and **[assignment: no other actions to be taken in case of audit storage failure]** if the audit trail is full.

5.1.2 Class FCS: Cryptographic support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: cryptographic key generation algorithm shown in** Table 6**]** and specified cryptographic key sizes **[assignment: cryptographic key size shown in** Table 6**]** that meet the following: **[assignment: standard shown in** Table 6**]**.

Table 6: List of Cryptographic Key Generation

Key type	Standard	Cryptographic key generation algorithm	Cryptographic key size
HDD cryptographic key	BSI-AIS31	TRNG	256 bit

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

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

FCS_COP.1.1 The TSF shall perform **[assignment: cryptographic operations shown in** Table 7**]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm**

shown in Table 7**]** and cryptographic key sizes **[assignment: cryptographic key size shown in** Table 7**]** that meet the following: **[assignment: standard shown in** Table 7**]**.

Table 7: List of Cryptographic Operations

Key type	Standard	Cryptographic algorithm	Cryptographic key size	Cryptographic operations
HDD cryptographic key	FIPS197	AES	256 bit	- Encryption when writing the Document Data on HDD - Decryption when reading the Document Data from HDD

5.1.3 Class 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: MFP access control SFP]** on **[assignment:** Table 8, **List of Subjects, Objects, and Operations among Subjects and Objects]**.

Table 8: List of Subjects, Objects, and Operations among Subjects and Objects

Subjects	Objects	Operations among subjects and objects
Administrator process	Document Data	Deleting the Document Data
General User process	Document Data	Storing the Document Data Reading the Document Data Editing the Document Data Deleting the Document Data

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_ACF.1.1 The TSF shall enforce the **[assignment: MFP access control SFP]** to objects based on the following: **[assignment: subjects or objects, and their corresponding security attributes shown in** Table 9**]**.

Table 9: Subjects, Objects and Security Attributes

Types	Subjects or objects	Security attributes
Subject	Administrator process	- Administrator IDs - Administrator Roles
Subject	General User process	- General User IDs - Document Data Default ACL
Object	Document Data	- A list of users for Document Data

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 subject's operations on objects and access on operations shown in** Table 10**]**.

Table 10: Rules Governing Access

Subject	Operations on objects	Rules governing access
General User process	Storing the Document Data	General Users can store the Document Data. The Document Data Default ACL associated with General User process is copied to the Document Data ACL associated with the storing Document Data when storing the Document Data.
	Reading the Document Data	When General User ID (associated with General User process) matches either the Document File Owner ID or a Document File User ID in the Document Data ACL (associated with the Document Data), and also the matched ID has permission for viewing, editing, editing/deleting or full control, the General User process is allowed to read the Document Data.
	Editing the Document Data	When General User ID (associated with General User process) matches either the Document File Owner ID or a Document File User ID in the Document Data ACL (associated with the Document Data), and also when the matched ID has permission for editing, editing/deleting or full control, the General User process is allowed to register the editing of Print Settings for the Document Data.
	Deleting the Document Data	When General User ID (associated with General User process) matches either the Document File Owner ID or a Document File User ID in the Document Data ACL (associated with the Document Data), and also when the matched ID has permission for editing/deleting or full control, the General User process is allowed to delete the Document Data.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules that explicitly authorize subject's operations on objects shown in** Table 11**]**.

Table 11: Rules Governing Access Explicitly

Subject	Operations on object	Rules governing access
Administrator process	Deleting the Document Data	When the File Administrator is included in Administrator Roles that are associated with Administrator process, the Administrator process is allowed to delete all Document Data stored in D-BOX.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the **[assignment: no rules, based on security attributes, that explicitly deny access of subjects to objects]**.

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the **[assignment: telephone line information flow SFP]** on **[assignment: subjects, information, and an operation listed in** Table 12**]**.

Table 12: List of Subjects, Information and Operation

Subjects	Information	Operation
- Fax process on Fax Unit - Fax reception process on Controller Board	Received data from a telephone line	Transferring

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the **[assignment: telephone line information flow SFP]** based on the following types of subject and information security attributes: **[assignment: subjects or information and their corresponding security attributes shown in** Table 13**]**.

Table 13: Security Attributes Corresponding to Subjects or Information

Types	Subjects or information	Security attributes
Subject	Fax process on Fax Unit	No security attributes
Subject	Fax reception process on Controller Board	No security attributes
Information	Received data from a telephone line	Data type

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[assignment: after the type of received data from a telephone line is recognized as the fax data, the fax process on the Fax Unit allows the fax reception process on the Controller Board to let the received data from a telephone line pass]**.

FDP_IFF.1.3 The TSF shall enforce the **[assignment: no additional information flow control SFP rules]**.

FDP_IFF.1.4 The TSF shall provide the following **[assignment: no list of additional SFP capabilities]**.

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: no rules, based on security attributes, that explicitly authorise information flows]**.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: **[assignment: no rules, based on security attributes, that explicitly deny information flows]**.

5.1.4 Class FIA: Identification and authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when **[selection: an administrator (refinement: the Machine Administrator) configurable positive integer within [assignment: 1 to 5]]** unsuccessful authentication attempts occur related to **[assignment: the consecutive numbers of times of authentication failure for each user in the authentication events shown in Table 14]**.

Table 14: List of Authentication Events

Authentication events
User authentication using control panel
User authentication using the TOE from web browser of client PC
User authentication when printing from client PC
User authentication when faxing from client PC

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[assignment: Lockout the user, who has failed the authentication attempts, until one of the Lockout release actions, shown in Table 15, is taken]**.

Table 15: Lockout Release Actions

Lockout release actions	Details
Auto Lockout Release	If the unsuccessful authentication attempts have met the defined number, and the Lockout Time set in advance (by the Machine Administrator between 1 and 9999 minutes) has elapsed, then Lockout is released by the first identification and authentication by the Locked out User. Although the Machine Administrator can also set the Lockout Time to an indefinite, in this case, Lockout cannot be released by the Lockout release operation of elapse of the time but can only by other Lockout release operations.
Manual Lockout Release	Regardless of the value set for the Lockout release time by the Machine Administrator, the Unlocking Administrators who are set for each User Role can release Locked out Users. FMT_MTD.1 defines the relation between the Locked out Users and Unlocking administrator. Also, as a special lockout release, if Administrators (all Administrator Roles) and a Supervisor are locked out, restarting the TOE has the same effect as the lockout release operation by the Unlocking Administrator.

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: General User IDs, Document Data Default ACL, Administrator IDs, Administrator Roles and Supervisor ID].**

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies

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

(1) Usable letters and its letter types:

Upper-case letters: [A-Z] (26 letters)
Lower-case letters: [a-z] (26 letters)
Numbers: [0-9] (10 letters)
Symbols: SP (spaces) ! " # $ % & ' ( ) * + - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ (33 letters)

(2) Registerable Password Length:

For General Users

No fewer than the Minimum Password Length set by the User Administrator (8-32 characters), nor more than 128 characters.

For Administrators and a Supervisor

No fewer than the Minimum Password Length set by the User Administrator (8-32 characters), nor more than 32 characters.

(3) Rules: It is allowed to register the passwords composed of a combination of letter types based on the Complexity Setting for Password set by the User Administrator. The User Administrator sets either Level 1 or Level 2 for Complexity Setting for Password.

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UID.1

Dependencies: FIA_UID.1 Timing of identification

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.

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only **[assignment: the display of a dummy letter (*: asterisk, or black circle) for each password character on the authentication feedback area]** to the user while the authentication is in progress.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

Dependencies: No dependencies

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

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: General User IDs, Document Data Default ACL, Administrator IDs, Administrator Roles and Supervisor ID]**.

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **[assignment: rules for the initial association of attributes listed in** Table 16**].**

Table 16: Rules for Initial Association of Attributes

Users	Subjects	Security attributes of users
General User	General User process	General User ID, Document Data Default ACL
Administrator	Administrator process	Administrator ID, Administrator Roles
Supervisor	Supervisor process	Supervisor ID

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: Administrators can add their own assigned Administrator Roles to other Administrators, and can delete their own Administrator Roles. However, if deleting the Administrator Role makes no Administrator covers that Administrator Role, it is not allowed to delete the Administrator Role.]**.

5.1.5 Class 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: MFP access control SFP]** to restrict the ability to **[selection: query, modify, delete, [assignment: newly create, change, add]]** the security attributes **[assignment: security attributes in** Table 17**]** to **[assignment: users/roles in** Table 17**]**.

Table 17: Management Roles of Security Attributes

Security attributes	Operations	User roles
General User IDs (data items of General User Information)	Query, newly create, delete	- User Administrator
	Query	- General Users
Administrator IDs	Newly create	- Administrators
	Query, change	- Concerned Administrators
	Query	- Supervisor
Administrator Roles	Query, add, delete	- Administrators who are assigned the concerned Administrator Roles
Supervisor ID	Query, change	- Supervisor
Document Data ACL	Query, modify	- File Administrator - Document File Owner - General Users who have full control operation permission for the concerned Document Data
Document Data Default ACL (data items of General User Information)	Query, modify	- User Administrators - Concerned General Users

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

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

FMT_MSA.3.1 The TSF shall enforce the **[assignment: MFP access control SFP]** to provide default values **[selection: [assignment: specified as shown in Table 18]]** for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **[assignment: no authorised identified roles]** to specify alternative initial values to override the default values when an object or information is created.

Table 18: Property of static attribute initialisation

Object	Security attribute associated to object	Default value and its property at time of object creation
Document Data stored by General Users	Document Data ACL	A value set in advance as the Document Data Default ACL for the concerned General User (Document File Owner). This value can be set arbitrarily by the User Administrator or the General User, and it has neither the restrictive nor permissive property but the specified property.

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to **[selection: query, modify, delete, [assignment: register, change, entirely delete, newly create]]** the **[assignment: List of TSF Data Management in** Table 19**]** to **[assignment: roles in** Table 19**]**.

Table 19: List of TSF Data Management

TSF data	Operations	User roles
Authentication information of General Users (data items of General User Information)	Newly create, change, delete	User Administrator
	Change	Concerned General Users of General User Information
Authentication information of Supervisor	Change	Supervisor
Authentication information of Administrators	Change	Supervisor, concerned Administrator
Number of Attempts before Lockout	Query, modify	Machine Administrator
Setting for Lockout Release Timer	Query, modify	Machine Administrator
Lockout time	Query, modify	Machine Administrator

TSF data	Operations	User roles
Date and time of system clock Date setting, time setting (hour, minute, second)	Query, modify	Machine Administrator
	Query	General Users, User Administrator, Network Administrator, File Administrator, Supervisor
Minimum Password Length	Query, modify	User Administrator
Complexity Setting for Password	Query, modify	User Administrator
HDD cryptographic key	Query, newly create	Machine Administrator
Audit logs	Query, delete entirely	Machine Administrator
Service Mode Lock setting	Query, modify	Machine Administrator
	Query	General Users, User Administrator, Network Administrator, File Administrator, Supervisor
Lockout Flag for General Users	Query, modify	User Administrator
Lockout Flag for Administrators	Query, modify	Supervisor
Lockout Flag for Supervisor	Query, modify	Machine Administrator
S/MIME User Information (data items of General User Information)	Query, newly create, delete, change	User Administrator, Concerned General User of S/MIME User Information
	Query	General User
Destination Information for Deliver to Folder	Query	User Administrator, General Users

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 Security Management Functions: **[assignment: List of Specification of Management Functions described in** Table 20**]**.

Table 20: List of Specification of Management Functions

Functional requirements	Management requirements	Management items
FAU_GEN.1	None	-
FAU_SAR.1	a) Maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.	a) Management of the Machine Administrator from Administrator Roles.
FAU_SAR.2	None	-
FAU_STG.1	None	-
FAU_STG.4	a) Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.	None: Actions are fixed and not an object of management.
FCS_CKM.1	a) The management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption).	None: Cryptographic key attributes are fixed and not an object of management.
FCS_COP.1	None	-
FDP_ACC.1	None	-
FDP_ACF.1	a) Managing the attributes used to make explicit access or denial based decisions.	a) Management of the File Administrator from Administrator Roles.
FDP_IFC.1	None	-
FDP_IFF.1	None	-
FIA_AFL.1	a) Management of the threshold for unsuccessful authentication attempts. b) Management of actions to be taken in the event of an authentication failure.	a) Security Management Function (Management of Machine Control Data): management of Number of Attempts before Lockout by the Machine Administrator. b) Management of the Unlocking administrators and Lockout release operations for the Locked out Users.
FIA_ATD.1	a) If so indicated in the assignment, the authorised Administrator might be able to define additional security attributes for users.	None: No functions to define additional security attributes for users
FIA_SOS.1	a) The management of the metric used to verify the secrets.	Security Management Function (Management of Machine Control Data): User Administrator manages the following settings of the machine control data:

		- Minimum Password Length - Complexity Setting for Password
FIA_UAU.2	Management of the authentication data by an Administrator; management of the authentication data by the user associated with this data.	- Security Management Function (Management of General User Information): management of authentication information of General Users by the User Administrator and management of own authentication information of General Users by General Users - Security Management Function (Management of Administrator Information): management of own authentication information of Administrators by Administrators - Security Management Function (Management of Administrator Information): new registration of Administrators by Administrators - Security Management Function (Management of Administrator Information): management of authentication information of Administrators by Supervisor - Security Management Function (Management of Supervisor Information): management of authentication information of Supervisor by Supervisor
FIA_UAU.7	None	-
FIA_UID.2	a) The management of the user identities.	- Security Management Function (Management of General User Information): management of user IDs by the User Administrator - Security Management Function (Management of Administrator Information): management of own Administrator IDs by Administrators - Security Management Function (Management of Administrator Information): new registration of Administrators by Administrators - Security Management Function (Management of Supervisor Information): management of Supervisor ID by Supervisor
FIA_USB.1	a) An authorised Administrator can define default subject security attributes. b) An authorised Administrator can change subject security attributes.	a) None: The default subject security attributes cannot be defined. b) Administrators can add their own assigned Administrator Roles to other

		Administrators and delete Administrator Roles.
FMT_MSA.1	a) Managing the group of roles that can interact with the security attributes.	Management of Administrator Roles by Administrators.
FMT_MSA.3	a) Managing the group of roles that can specify initial values; b) Managing the permissive or restrictive setting of default values for a given access control SFP.	a) None: No groups of roles that can specify the initial settings. b) Management of the Document Data Default ACL. - Allows the User Administrator to modify the Document Data Default ACL for all General User Information registered for Address Book. - Allows General Users to modify the Document Data Default ACL of their own General User Information.
FMT_MTD.1	a) Managing the group of roles that can interact with the TSF data.	None: No groups of roles that can interact with the TSF data.
FMT_SMF.1	None	-
FMT_SMR.1	a) Managing the group of users that are part of a role.	Management of Administrator Roles by Administrators.
FPT_RVM.1	None	-
FPT_SEP.1	None	-
FPT_STM.1	a) Management of the time.	- Security Management Function (Management of Machine Control Data): The Machine Administrator manages the following setting items for machine control data - Date of system clock, time (hour, minute and second)
FPT_TST.1	a) Management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions; b) Management of the time interval if appropriate.	a) None: The condition under which the TSF self testing occurs is fixed. b) None: No management of the time interval.
FTP_ITC.1	a) Configuring the actions that require trusted channel, if supported.	None: The actions that require the Inter-STF trusted channel are fixed.
FTP_TRP.1	a) Configuring the actions that require trusted path, if supported.	None: The actions that require trusted path are fixed.

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: General Users, Administrators (Machine Administrator, File Administrator, User Administrator and Network Administrator) and a Supervisor]**.

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

5.1.6 Class FPT: Protection of the TSF

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

Dependencies: No dependencies

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

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

Dependencies: No dependencies

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

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

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies

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

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: FPT_AMT.1 Abstract machine testing

FPT_TST.1.1 The TSF shall run a suite of self tests **[selection: during initial start-up]** to demonstrate the correct operation of **[selection: [assignment: Encryption Function of Ic Hdd]]**.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of **[selection: [assignment: HDD cryptographic key]]**.

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

5.1.7 Class FTP: Trusted path/channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies

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

FTP_ITC.1.2 The TSF shall permit **[selection: the TSF]** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **[assignment: Deliver to Folders service from the TOE to SMB Server (IPSec), Deliver to Folders service from the TOE to FTP Server (IPSec)]**.

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_TRP.1.1 The TSF shall provide a communication path between itself and **[selection: remote]** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 The TSF shall permit **[selection: the TSF, remote users]** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for **[selection: initial user authentication, [assignment: TOE web service, printing service from client PC, fax service from client PC, e-mail service to client PC from the TOE]]**.

Table 21 shows the services that require the trusted path described in FTP_TRP.1.3 and are used by each user who communicates via trusted path described in FTP_TRP.1.2.

Table 21: Services Requiring Trusted Path

Related persons for communication	Services which require trusted path
TSF	E-mail service to client PC from the TOE (S/MIME)
Remote users	Initial user authentication (SSL) TOE web service from client PC (SSL) Printing service from client PC (SSL) Fax service from client PC (SSL)

5.2 Minimum Strength of Function Claim

The minimum strength level of function for this TOE is SOF-basic. Among IT Security Requirements in Chapter 5, the TOE security functional requirements using the probabilistic or permutational mechanism are FIA_AFL.1, FIA_SOS.1 and FIA_UAU.2, and are relevant to the level of minimum strength of function. The algorithms specified with FCS_CKM.1 and FCS_COP.1 are cryptographic algorithms, and since its strength level is not covered by the scope of the CC, it is not an object for the minimum strength of function claim.

5.3 TOE Security Assurance Requirements

The evaluation assurance level of this TOE is EAL3. The assurance components of the TOE are shown in Table 22. These are a set of components defined by the evaluation assurance level, EAL3 and other requirements are not added.

Table 22: TOE Security Assurance Requirements (EAL3)

Assurance classes	Assurance components	
ACM: Configuration management	ACM_CAP.3	Authorisation controls
	ACM_SCP.1	TOE CM coverage
ADO: Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.2	Security enforcing high-level design
	ADV_RCR.1	Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
ALC: Life cycle support	ALC_DVS.1	Identification of security measures
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.1	Examination of guidance
	AVA_SOF.1	Strength of the TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

5.4 Security Requirements for the Environment

There are no security requirements for the environment.

6 TOE Summary Specification

This chapter describes the TOE security functions, the strength of function claim and assurance measures.

6.1 TOE Security Function

The TOE provides the following TOE security functions to satisfy the TOE Security Functional Requirements described in Chapter 5.1.

SF.AUDIT Audit Function

SF.I&A User Identification and Authentication Function

SF.DOC_ACC Document Data Access Control Function

SF.SEC_MNG Security Management Function

SF.CE_OPE_LOCK Service Mode Lock Function

SF.CIPHER Encryption Function

SF.NET_PROT Network Communication Data Protection Function

SF.FAX_LINE Protection Function for Intrusion from Telephone Line Interface

SF.GENUINE MFP Control Software Verification Function

These TOE security functions correspond to the security functional requirements described in Chapter 5.1 as shown in Table 23.

Table 23: Relation between TOE Security Functional Requirements and TOE Security Functions

	SF.AUDIT	SF.I&A	SF.DOC_ACC	SF.SEC_MNG	SF.CE_OPE_LOCK	SF.CIPHER	SF.NET_PROT	SF.FAX_LINE	SF.GENUINE
FAU_GEN.1	X								
FAU_SAR.1	X								
FAU_SAR.2	X								
FAU_STG.1	X								
FAU_STG.4	X								
FCS_CKM.1						X			
FCS_COP.1						X			
FDP_ACC.1			X						

	SF.AUDIT	SF.I&A	SF.DOC_ACC	SF.SEC_MNG	SF.CE_OPE_LOCK	SF.CIPHER	SF.NET_PROT	SF.FAX_LINE	SF.GENUINE
FDP_ACF.1			X						
FDP_IFC.1								X	
FDP_IFF.1								X	
FIA_AFL.1		X		X					
FIA_ATD.1		X							
FIA_SOS.1		X							
FIA_UAU.2		X							
FIA_UAU.7		X							
FIA_UID.2		X							
FIA_USB.1		X		X					
FMT_MSA.1				X					
FMT_MSA.3				X					
FMT_MTD.1	X			X	X	X			
FMT_SMF.1		X		X					
FMT_SMR.1		X		X					
FPT_RVM.1	X	X	X	X	X	X	X	X	X
FPT_SEP.1	X	X	X	X	X	X	X	X	X
FPT_STM.1	X								
FPT_TST.1						X			X
FTP_ITC.1							X		
FTP_TRP.1							X		

The following are descriptions of these TOE security functions.

6.1.1 SF.AUDIT Audit Function

The TOE starts the Audit Function when the power is supplied and the TOE starts up, and keeps running until the power is shut down. While the Audit Function runs, the TOE records the audit logs when auditable events occur. The recorded audit logs shall be protected from being lost before audit. Only the Machine Administrator is permitted to read the audit logs and delete the entire audit logs.

The TOE also ensures the reliable performance of Audit Function and protects the Audit Function from being interfered and tampered with outside of the Audit Function.

6.1.1.1 Audit logs generation

The TOE generates the audit logs when auditable events occur, and appends them to the audit log files. Audit logs consist of basic audit information and expanded audit information. The basic audit information is a data item recorded for the occurrence of any kinds of auditable events, and the expanded audit information is a data item recorded for the occurrence of the auditable events that require additional information for audit. Table 24 shows the audit information for each auditable event.

If there is no free space in the audit log files to append new audit logs, the oldest audit logs in terms of the time/date information are overwritten with new audit logs.

Table 24: Auditable Events and Auditable Information

Auditable events	Audit logs	
	Basic audit information	Expand audit information
Starting Audit Function (*1)	- Date/time of the events - Types of the events (Auditable events in this table) - Subject identity (*4) - Outcome	-
Login		-
Starting Lockout		Locked out User
Releasing Lockout (*2)		Locked out User who is to be released Release methods (Auto Lockout Release/Manual Lockout Release)
Lockout release at the TOE startup		-
HDD encryption key generation		-
Successful storage of Document Data		ID of object Document Data
Successful reading of Document Data (*3)		ID of object Document Data
Successful deletion of Document Data		ID of object Document Data
Receiving fax		-
Changing user password (includes newly creating and deleting password)		In the case of newly creating/changing/deleting the user authentication information of others, the ID of the person making the change
Deleting Administrator Role		-
Adding Administrator Role		-
Changing Document Data ACL		ID of object Document Data
Changing date and time of system clock		-

Communication with trusted IT product		Communication IP address
Communication with remote user		-
Deleting the entire audit log		-

-: No applicable individual audit information

*1: The starting of Audit Function is substituted with the event of the TOE startup. This TOE does not record the ending of Audit Function. The starting and ending of Audit Function audit the state of inactivity of Audit Function. Since Audit Function works as long as the TOE works and it is not necessary to audit the state of inactivity of Audit Function, it is appropriate not to record the ending of Audit Function.

*2: Lockout release for Administrators and Supervisor by the restarting the TOE, which is the special Lockout release operation, is substituted with the event of the TOE startup.

*3: For the successful reading of the Document Data, the objects to be recorded in ID of object Document Data are printing, sending by e-mail, delivering to folders and downloading from Web Service Function the Document Data stored in D-BOX.

*4: When the recording events occur due to the operations by users, User IDs are set as subject identities of common audit events, and when the recording events occur due to the TOE, IDs that do not duplicate the user IDs but can identify systems are set.

6.1.1.2 Reading Audit Logs

The TOE allows only the Machine Administrator to read the audit logs as text format.

6.1.1.3 Protection of Audit Logs

The TOE allows only the Machine Administrator to delete the entire audit logs from the Operation Panel and Web Service Function.

6.1.1.4 Time stamps

The TOE provides the date/time of the events of the audit logs by using the date and time of the system clock inside the TOE.

6.1.2 SF.I&A User Identification and Authentication Function

The TOE identifies and authenticates users prior to the use of the TOE security functions to allow the authorized users to operate the TOE according to their roles and authorization.

The TOE also ensures the reliable performance of User Identification and Authentication Function and protects the User Identification and Authentication Function from being interfered and tampered with outside of the User Identification and Authentication Function.

6.1.2.1 User Identification and Authentication

The TOE displays a login window to users who attempt to use the TOE security functions from the Operation Panel or Web Service Function, requires them to enter their user IDs and passwords, and then identifies and authenticates the users with the entered user IDs and passwords.

In addition, when receiving requests for printing or fax transmission, the TOE identifies and authenticates the users with the user IDs and passwords that are sent from the client PC.

The TOE binds the successfully authenticated users and their processes (General User process, Administrator process, or Supervisor process) according to their user roles (General Users, Administrators, or a Supervisor), associates each process with the security attributes of that role, and maintains those bindings and associations.

When the user is a General User, the TOE binds the General User with General User process, associates General User process with General User ID and Document Data Default ACL, and maintains those bindings and associations. When the user is an Administrator, the TOE binds the Administrator with Administrator process, associates Administrator process with Administrator ID and Administrator Roles, and maintains those bindings and associations. When the user is a Supervisor, the TOE binds the Supervisor with Supervisor process, associates Supervisor process with Supervisor ID, and maintains those bindings and associations.

The authentication methods vary by the user role. Table 25 shows the authentication methods for each user role.

Table 25: User Roles and Authentication Methods

User roles	Authentication methods
General User	Check if the user IDs and passwords entered into the TOE match the General User IDs and their passwords registered for Address Book.
Administrator	Check if the user IDs and passwords entered into the TOE match the Administrator IDs and their passwords registered for the TOE.
Supervisor	Check if the user IDs and passwords entered into the TOE match the Supervisor ID and password registered for the TOE.

6.1.2.2 Action in case of Identification and Authentication Failure

The TOE counts the number of times of each user ID's Identification and Authentication failure, described in "6.1.2.1 User Identification and Authentication". When a user ID's accumulated numbers of times of failure meets the Number of Attempts before Lockout, the user is locked out and the Lockout Flag for that user is set to "Active". The number of times for Number of Attempts before Lockout is set by the Machine Administrator to a value between 1 and 5.

In addition, when successfully authenticated with the Identification and Authentication described in "6.1.2.1 User Identification and Authentication

", the TOE resets the consecutive number of times of failure for that user to zero and starts counting from 0. When either of the two Lockout release actions described below is taken for a user whose Lockout Flags are set to "Active", the TOE sets the Lockout Flags for that user to "Inactive" and releases Lockout.

(1) Auto Lockout Release
After a user is locked out and Lockout release time elapses, that user's first identification and authentication releases his/her Lockout. The Lockout release time is set between 1 and 9999 minutes (by minutes) by the Machine Administrator. The Machine Administrator can also set the Lockout release time to an indefinite time. If the Lockout release time is set to an indefinite time, Lockout for users can only be released by Manual Lockout Release.

(2) Manual Lockout Release
The Unlocking administrators, who are set for each user role shown in Table 26, are allowed to release Lockout using the Web Service Function. As a special Lockout release operation, when Administrators (all Administrator Roles) and a Supervisor are locked out, Lockout is released by restarting the TOE.

Table 26: Unlocking Administrators for Each User Role

User roles (Locked out Users)	Unlocking administrators
General User	User Administrator
Administrator (all Administrator Roles)	Supervisor
Supervisor	Machine Administrator

6.1.2.3 Password Feedback Area Protection

The TOE displays a protection character (*: asterisk or black circle) in place of each password character entered on the Operation Panel or web browser of a client PC by General Users, Administrators, and a Supervisor.

6.1.2.4 Password Registration

The TOE provides the function to register and change the passwords of General Users, Administrators, and a Supervisor, from the Operation Panel and Web Service Function. This function uses the characters described below (1).
It checks if the password to be registered or changed meets the conditions (2) and (3) described below. If the password meets those conditions, it registers the password. If the password does not meet those conditions, it does not register password but displays an error message.

(1) Usable characters and character types:

Upper-case letters: [A-Z] (26 letters)
Lower-case letters: [a-z] (26 letters)
Numbers: [0-9] (10 letters)
Symbols: SP (space) ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ (33 letters)

(2) Registerable Password length:

For General Users

No fewer than the Minimum Password Length set by the User Administrator (8-32 digits), nor more than 128 digits.

For Administrators and a Supervisor

No fewer than the Minimum Password Length set by the User Administrator (8-32 digits), nor more than 32 digits.

(3) Rules: It is allowed to register the passwords composed of a combination of character types based on the Complexity Setting for Password set by the User Administrator. The User Administrator sets either Level 1 or Level 2 for Complexity Setting for Password.

6.1.3 SF.DOC_ACC Document Data Access Control Function

The TOE controls user access to operations that store, read, edit and delete Document Data. The access control to Document Data only displays the accessible Document Data on the Operation Panel or client PC, where the authorized users are authenticated, based on the authorization assigned to the user role of the authorized user with Identification and Authentication Function, or the authorization assigned to each user role. This chapter describes access control to Document Data for each user role.

The TOE also ensures the reliable performance of the Document Data Access Control Function and protects the Document Data Access Control Function from being interfered and tampered with outside of the Document Data Access Control Function.

6.1.3.1 Operations on Document Data by General Users

The TOE allows General Users to store the Document Data, and allows them to read, edit, and delete the stored Document Data according to the Document Data ACL. The Document Data ACL records the IDs for General Users who are allowed to perform operations on Document Data, and the access rights to each Document Data for each General User. If a General User ID associated with the General User process is registered for a Document Data ACL, the TOE allows that General User ID to perform the operations according to the access rights assigned to the user ID.

Table 4 shows the access rights and their corresponding operations on Document Data.

Table 27 shows the value of the Document Data ACL when storing Document Data.

Table 27: Initial Value for the Document Data ACL

Type of Document Data	The initial value for the Document Data ACL
Document Data stored by General User	Document Data Default ACL

6.1.3.2 Operations on Document Data by File Administrator

The TOE allows the File Administrators, logged in from the Operation Panel or Web Service Function, to display the list of Document Data, and allows the File Administrator to delete selected Document Data or to delete the entire displayed list of Document Data.

6.1.4 SF.SEC_MNG Security Management Function

The TOE provides the Security Management Function according to the user roles of users who are identified and authenticated with "SF.I&A User Identification and Authentication Function".
The TOE also ensures the reliable performance of Security Management Function and protects the Security Management Function for Document Data from being interfered and tampered with outside of the Security Management Function.

6.1.4.1 Management of the Document Data ACL

Management of the Document Data ACL allows only specific users to perform operations on the Document Data ACL from the Operation Panel or Web Service Function. Operations on the Document Data ACL include changing the Document File Owners and the access rights of the Document File Owners, newly registering and deleting the Document File Users, and changing the access rights of the Document File Users. The users who are authorized to perform each of these operations are specified. Table 28 shows the relation between operations on the Document Data ACL and the authorized users for the operations.

Table 28: Operations on the Document Data ACL and Authorized Operators

Operations on the Document Data	Authorized operators
Change the Document File Owners	- File Administrator
Change the access rights of the Document File Owners	- File Administrator - Document File Owners - General Users with full control authorization
Newly register the Document File Users	- File Administrator - Document File Owners - General Users with full control authorization
Delete the Document File Users	- File Administrator - Document File Owners - General Users with full control authorization
Change the access rights of the Document File Users	- File Administrator - Document File Owners - General Users with full control authorization

The TOE allows the login File Administrators to perform the operations on all Document Data ACLs including changing Document File Owners and the access rights of the Document File Owners, newly registering Document File Users, deleting Document File Users, and changing the access rights of Document

File Users.

The TOE allows the login General Users to perform the operations only on the Document Data ACL for which the General User is a full control authorized user, including changing the access rights of the Document File Owners, newly registering Document File Users, deleting Document File Users, and changing the access rights of Document File Users. However, even if the full control authorization is not set for Document File Owners, Document File Owners are allowed to change the access rights of Document File Owners, newly register and delete Document File Users, and change the access rights of Document File Users, in Document Data ACLs that the Document File Owners own.

6.1.4.2 Management of Administrator Information

Management of Administrator Information allows only specific users to perform operations on Administrator information from the Operation Panel or Web Service Function.

Administrator Information includes Administrator IDs, authentication information of Administrators, and Administrator Roles. The operations on Administrator information include newly registering Administrators, changing Administrator IDs and authentication information of Administrators, adding and deleting Administrator Roles. The users who are authorized to perform each of these operations are specified. Table 29 shows the relation between the operations on Administrator information and the authorized users for the operations on Administrator information.

Table 29: Access to Administrator Information

Operations on Administrator information	Authorized operators
Newly register Administrators	Administrators
Change Administrator IDs	The Administrator themselves
View Administrator IDs	Supervisor
Change authentication information of Administrators	The Administrator themselves, Supervisor
Add Administrator Roles	The Administrators who are already assigned that Administrator Role
Delete Administrator Roles	The Administrator who are already assigned that Administrator Role However, the operation cannot be performed if no other Administrators have the Administrator Role.

The TOE allows the login Administrator/Supervisor to perform the operations shown in Table 29.

6.1.4.3 Management of Supervisor Information

Management of Supervisor Information allows only the Supervisor to change Supervisor ID and Supervisor authentication information from the Operation Panel or Web Service Function. If the login user from the Operation Panel or client PC is a Supervisor, the TOE allows the Supervisor to change Supervisor ID and Supervisor authentication information.

6.1.4.4 Management of General User Information

Management of General User Information allows specific users to perform all or some of operations to newly create, change and delete General User Information from the Operation Panel or Web Service Function. General User Information includes the user IDs, user authentication information and the Document Data Default ACL.

The TOE allows the User Administrators or General Users, logged in from the Operation Panel or Web Service Function, to perform the operations shown in Table 30.

Table 30: Authorized Operations on General User Information

Operations on General User Information	Authorized operators
Newly create General User Information for Address Book	User Administrator
Edit General User Information registered for Address Book (User IDs, User authentication information, Document Data Default ACL, User certificates, S/MIME User Information)	User Administrator
Edit General User Information registered for Address Book (User authentication information, Document Data Default ACL, S/MIME User Information)	The General User themselves
Delete General User Information registered for Address Book	User Administrator

When newly creating the General User Information, the newly created General User ID is set to the value for the Document Data Default ACL as the Document File Owner, and the authorized operations on Document Data of that General User are to read the Document Data and to modify the Document Data ACL.

6.1.4.5 Management of Machine Control Data

Management of Machine Control Data allows only specific users to set Machine Control Data from specific operation interfaces.

The TOE allows the specific users to use the function that sets the Machine Control Data from the specific operation interfaces. Table 31 shows the authorized setter, the range of values that can be set, and the operation interfaces allowed by the TOE, for each Machine Control Data.

The TOE allows all authorized users to view the system clock, and allows the User Administrator and General Users to view the destination information for Deliver to Folder.

Table 31: List of Administrator for Machine Control Data

Machine control data items	Values	Authorized setters	Operation interfaces
Number of Attempts before Lockout	An integer 1-5 (times)	Machine Administrator	Web Service Function
Setting for Lockout Release Timer	Active or Inactive	Machine Administrator	Web Service Function
Lockout time	An integer 1-9999 (minutes)	Machine Administrator	Web Service Function
Minimum Password Length	An integer 8-32 (digits)	User Administrator	Operation Panel
Complexity Setting for Password	Level 1 or Level 2	User Administrator	Operation Panel
Date and time of system clock	Date, time (hour, minute, second)	Machine Administrator	Operation Panel, Web Service Function
Lockout Flag for General Users	Inactive	User Administrator	Web Service Function
Lockout Flag for Administrators	Inactive	Supervisor	Web Service Function
Lockout Flag for Supervisor	Inactive	Machine Administrator	Web Service Function

6.1.5 SF.CE_OPE_LOCK Service Mode Lock Function

Service Mode Lock Function controls the use of the maintenance functions for CEs according to the value of Service Mode Lock Function set by the Machine Administrator.

The TOE provides the Machine Administrator with the function to set Service Mode Lock Function from the Operation Panel, and provides all the authorized users with the function to view the setting value. If the Service Mode Lock Function is set to "Off", the TOE allows CE to operate the Maintenance Functions, and if the Service Mode Lock Function is set to "On", it does not.

The TOE also ensures the reliable performance of Service Mode Lock Function and protects the Service Mode Lock Function from being interfered and tampered with outside of the Service Mode Lock Function.

6.1.6 SF.CIPHER Encryption Function

The TOE encrypts the Document Data to be stored on HDD.

The TOE also ensures the reliable performance of Encryption Function and protects the Encryption Function from being interfered and tampered with outside of the Encryption Function.

6.1.6.1 Encryption of Document Data

The TOE encrypts the data with Ic Hdd before writing it on HDD, and decrypts the data with Ic Hdd after reading it from HDD. This process is performed for all the data to be written to and read from HDD, and the Document Data are encrypted and decrypted by the TOE in a similar way.

The HDD encryption keys are generated by the Machine Administrator. The TOE allows the login Machine Administrator to generate HDD encryption keys from the Operation Panel.

When the Machine Administrator gives the instruction to generate HDD encryption key from the Operation Panel, the TOE generates the 256 bit HDD encryption key with the encryption key generation algorithm TRNG complying with the Standard BSI-ATS31, and when writing the data on the HDD/reading the data from the HDD, it performs the encryption operations shown in Table 32.

Table 32: List of Encryption Operation on Stored Data on HDD

Triggers of encryption operation	Encryption operations	Standard	Encryption algorithm	Key size
Writing data on HDD	Encrypt	FIPS197	AES	256 bit
Reading data from HDD	Decrypt			

HDD encryption keys can be also printed. The TOE allows the login Machine Administrator to print the HDD encryption keys from the Operation Panel. The printed encryption keys are used to restore the encryption keys in case the encryption keys in the TOE are unavailable.

In addition, the TOE verifies that the encryption function of Ic Hdd operates normally at start-up and verifies the integrity of the HDD encryption keys. If the TOE is not able to verify the integrity of the HDD encryption keys, it indicates that the HDD encryption keys are changed.

6.1.7 SF.NET_PROT Network Communication Data Protection Function

Network Communication Data Protection Function protects Document Data and Print Data on the Internal Networks from leakage, and detects tampering of Document Data and Print Data.

The TOE also ensures the reliable performance of Network Communication Data Protection Function and protects the Network Communication Data Protection Function from being interfered and tampered with outside of the Network Communication Data Protection Function.

6.1.7.1 Use of Web Service Function from Client PC

When receiving requests to use the Web Service Function from a client PC, the TOE communicates with the client PC using the SSL protocol as a trusted path.

6.1.7.2 Printing and Faxing from Client PC

When receiving requests to print or transmit faxes from a client PC, the TOE communicates with the client PC using the SSL protocol as a trusted path.

6.1.7.3 Sending by E-mail from TOE

When sending Document Data by e-mail from the TOE to a client PC, the TOE attaches the Document Data to e-mail and sends the e-mail using S/MIME. The S/MIME destination information is managed as S/MIME User Information (part of General User Information), and users send S/MIME e-mail using only this managed destination information.

6.1.7.4 Deliver to Folders from TOE

When delivering data from the TOE to folders in an SMB Server or an FTP Server, the TOE connects itself with the SMB Server or FTP Server using the IPSec protocol as a trusted channel. The destination information for Deliver to Folders is registered in advance and managed by the TOE as Machine Control Data, and users deliver files to folders using only this managed destination information.

6.1.8 SF.FAX_LINE Protection Function for Intrusion from Telephone Line Interface

When the Fax Unit receives fax data from a telephone line, the TOE passes the received data to the Controller Board. When the Fax Unit receives data that is not fax data, the TOE does not pass the data to the Controller Board but instead it discards the data.

The TOE also ensures the reliable performance of Protection Function for Intrusion from Telephone Line Interface and protects the Protection Function for Intrusion from Telephone Line Interface from being interfered and tampered with outside of the Protection Function for Intrusion from Telephone Line Interface.

6.1.9 SF.GENUINE MFP Control Software Verification Function

The MFP Control Software Verification Function verifies the integrity of MFP Control Software, which is installed in FlashROM, during start-up of the TOE.

The TOE verifies the integrity of the executable code of MFP Control Software during start-up of the TOE. If the integrity is verified, it makes the TOE available for users. If not, it indicates that the MFP Control Software is not correct.

The TOE also ensures the reliable performance of MFP Control Software Verification Function and protects the MFP Control Software Verification Function from being interfered and tampered with outside of the MFP Control Software Verification Function.

6.2 Claims of Strength of Function

The TOE security function that is realised by a probabilistic or permutational mechanism related to the strength level of function is SF.I&A. The strength level of that TOE security function is SOF-basic.

6.3 Assurance Measures

This chapter describes the assurance measures for the TOE. The assurance measures shown below in Table 33 satisfy the TOE security assurance requirements described in Chapter 5.3. Assurance measures for Class

AGD depend on the region in which the TOE is sold. One of [Japanese ver.], [English ver.1], [English ver.2], or [English ver.3], which are categorized in Table 33, is enclosed with the TOE depending on its sales region.

Table 33: Assurance Requirements and Assurance Measures for EAL3

Assurance classes	Assurance components	Assurance measures
ACM: Configuration Management	ACM_CAP.3	- imagio MP 4000/5000 series, Aficio MP 4000/5000 series Configuration Management (written in Japanese) - imagio MP 4000/5000 series, Aficio MP 4000/5000 series Configuration Management List (written in Japanese)
	ACM_SCP.1	
ADO: Delivery and Operation	ADO_DEL.1	- imagio MP 4000/5000 series, Aficio MP 4000/5000 series Delivery Procedure (written in Japanese)
	ADO_IGS.1	- imagio MP 4000/5000 series , Aficio MP 4000/5000 series Installation, Generation, and Start-up Procedure (written in Japanese)
ADV: Development	ADV_FSP.1	- imagio MP 4000/5000 series Functional Specification (written in Japanese)
	ADV_HLD.2	- imagio MP 4000/5000 series High Level Design (written in Japanese)
	ADV_RCR.1	- imagio MP 4000/5000 series Expression Compliance Analysis (written in Japanese)

Assurance classes	Assurance components	Assurance measures
AGD: Guidance Documents	AGD_ADM.1	[Japanese ver] - imagio MP 4000/5000 series Operating Instructions <Security Reference> (D012-7950) (written in Japanese) - Notes for Security Functions (D011-7750A) (written in Japanese) - imagio MP 4000/5000 series Operating Instructions <About This Machine> (D012-7750) (written in Japanese) - Notes for Administrators: Using this Machine in a CC-Certified Environment (D011-7781) (written in Japanese) [English ver.1] - 9040/9040b/9050/9050b MP 4000/MP 4000B/MP 5000/MP 5000B LD040/LD040B/LD050/LD050B Aficio MP 4000/4000B/5000/5000B Operating Instructions About This Machine (D012-7753) - 9040/9040b/9050/9050b MP 4000/MP 4000B/MP 5000/MP 5000B LD040/LD040B/LD050/LD050B Aficio MP 4000/4000B/5000/5000B Operating Instructions About This Machine (D012-7757) - Manuals for Administrators Security Reference 9040/9040b/9050/9050b MP 4000/5000/4000B/5000B LD040/LD050/LD040B/LD050B Aficio MP 4000/5000/4000B/5000B(D009-7504A) - Manuals for Administrators Security Reference Supplement 9040/9040b/9050/9050b MP 4000/4000B/5000/5000B LD040/LD040B/LD050/LD050B Aficio MP 4000/4000B/5000/5000B(D011-7790A) - Notes for Administrators: Using this Machine in a CC-Certified Environment (D011-7782) - Notes for Administrators: Using this Machine in a CC-Certified Environment (D011-7784)

Assurance classes	Assurance components	Assurance measures
		[English ver.2] - Manuals for Administrators Security Reference MP 4000/5000/4000B/5000B Aficio MP 4000/5000/4000B/5000B(D009-7512A) - Manuals for Administrators Security Reference Supplement 9040/9040b/9050/9050b MP 4000/4000B/5000/5000B LD040/LD040B/LD050/LD050B Aficio MP 4000/4000B/5000/5000B(D011-7790A) - Notes for Administrators: Using this Machine in a CC-Certified Environment (D011-7783) [English ver.3] - MP 4000/MP 4000B/MP 5000/MP 5000B MP 4000/MP 4000B/MP 5000/MP 5000B Aficio MP 4000/4000B/5000/5000B MP 4000/MP 4000B/MP 5000/MP 5000B Operating Instructions About This Machine (D012-7755) - Manuals for Administrators Security Reference MP 4000/5000/4000B/5000B Aficio MP 4000/5000/4000B/5000B(D009-7508A) - Manuals for Administrators Security Reference Supplement 9040/9040b/9050/9050b MP 4000/4000B/5000/5000B LD040/LD040B/LD050/LD050B Aficio MP 4000/4000B/5000/5000B(D011-7790A) - Notes for Administrators: Using this Machine in a CC-Certified Environment (D011-7782)
	AGD_USR.1	[Japanese ver] - Notes for Users Back up/Restore Address Book (D015-7103) (written in Japanese) - imagio MP 4000/5000 series Operating Instructions <Troubleshooting> (D012-7800) (written in Japanese) - imagio MP 4000/5000 series supplied Operation Instructions (D012-7501) (written in Japanese) - imagio MP 4000/5000 series Quick Guide (D012-7658) (written in Japanese) - Operating Instructions, Drivers&Utilities imagio MP 5000/4000(D0097500A) (written in Japanese)

Assurance classes	Assurance components	Assurance measures
		[English ver.1] -9040/9040b/9050/9050b MP 4000/4000B/5000/5000B LD040/LD040B/LD050/LD050B Aficio MP 4000/4000B/5000/5000B Operating Instructions Troubleshooting (D012-7803) -9040/9040b/9050/9050b MP 4000/4000B/5000/5000B LD040/LD040B/LD050/LD050B Aficio MP 4000/4000B/5000/5000B Operating Instructions Troubleshooting (D012-7807) -Manuals 9040/9040b/9050/9050b MP 4000/MP 5000/MP 4000B/MP 5000B LD040/LD050/LD040B /LD050B Aficio MP 4000/5000/4000B/5000B(D009-7502A) - Notes for Users Back Up/Restore Address Book (D015-7108) - Notes for Users Back Up/Restore Address Book (D015-7105) [English ver.2] -Manuals General Setting Manuals MP 4000/5000/4000B/5000B Aficio MP 4000/5000/4000B/5000B(D009-7510) -Manuals Functions and Network Manuals MP 4000/5000/4000B/5000B Aficio MP 4000/4000B/5000/5000B(D009-7514A) - Notes for Users Back Up/Restore Address Book (D015-7109) [English ver.3] - MP 4000/MP 4000B/MP 5000/MP 5000B MP 4000/MP 4000B/MP 5000/MP 5000B Aficio MP 4000/4000B/5000/5000B MP 4000/MP 4000B/MP 5000/MP 5000B Operating Instructions Troubleshooting (D012-7805) -Manuals MP 4000/5000/4000B/5000B Aficio MP 4000/5000/4000B/5000B(D009-7506A) - Notes for Users Back Up/Restore Address Book (D015-7107)

Assurance classes	Assurance components	Assurance measures
ALC: Life cycle support	ALC_DVS.1	- imagio MP 4000/5000 series, Aficio MP 4000/5000 series Development Security (written in Japanese) - Development Security Omori Office (written in Japanese) - Development Security Shin-Yokohama Office (written in Japanese) - Development Security Technical Service Center (written in Japanese) - Development Security Gotemba Plant (written in Japanese) - Development Security RME (written in Japanese) - Development Security RCA (written in Japanese) - Development Security RAI (written in Japanese) - Development Security RPL (written in Japanese) - Development Security REI (written in Japanese) - Development Security Information Security (written in Japanese)
ATE: Tests	ATE_COV.2	- imagio MP 4000/5000 series, Aficio MP 4000/5000 series External Specification Test Plan (written in Japanese) - imagio MP 4000/5000 series, Aficio MP 4000/5000 series External Specification Test (written in Japanese) - imagio MP 4000/5000 series, Aficio MP 4000/5000 series External Specification Test Result Report (written in Japanese) - imagio MP 4000/5000 series, Aficio MP 4000/5000 series Internal Specification Test Plan (written in Japanese) - imagio MP 4000/5000 series, Aficio MP 4000/5000 series External Specification Test (written in Japanese) - imagio MP 4000/5000 series, Aficio MP 4000/5000 series Internal Specification Test Result Report (written in Japanese) - imagio MP 4000/5000 series, Aficio MP 4000/5000 series Test Coverage Analysis (written in Japanese) - imagio MP 4000/5000 series, Aficio MP 4000/5000 series Test Depth Analysis (written in Japanese)
	ATE_DPT.1	
	ATE_FUN.1	
	ATE_IND.2	-TOE
AVA: Vulnerability assessment	AVA_MSU.1	- imagio MP 4000/5000 series, Aficio MP 4000/5000 series Vulnerability Assessment (written in Japanese)

7 PP Claims

This ST does not claim conformance to any PP.

8 Rationale

This chapter describes the rationale for the security objectives, security requirements, TOE summary specification rationale, and PP claims.

8.1 Security Objectives Rationale

This chapter describes that one or more of "4.1 Security Objectives for TOE" or "4.2 Security Objectives for Environment" corresponds to "3.1 Assumptions", "3.2 Threats" and "3.3 Organizational Security Policy", as shown in Table 34. It also describes how the security objectives for "3.1 Assumptions", "3.2 Assumptions" and "3.3 Policy" are sufficient.

Table 34: Relation between Security Environment and Security Objectives

TOE Security Environment Security Objectives	A.ADMIN	A.SUPERVISOR	A.NETWORK	T.ILLEGAL_USE	T.UNAUTH_ACCESS	T.ABUSE_SEC_MNG	T.SALVAGE	T.TRANSIT	T.FAX_LINE	P.SOFTWARE
O.AUDIT				X		X	X	X	X	
O.I&A				X	X	X				
O.DOC_ACC					X					
O.MANAGE						X				
O.MEM.PROTECT							X			
O.NET.PROTECT								X		
O.GENUINE										X
O.LINE_PROTECT									X	
OE.ADMIN	X									
OE.SUPERVISOR		X								
OE.NETWORK			X							

A.ADMIN **(Administrators' assumption)**

A.ADMIN presupposes that Administrators have adequate knowledge to operate the TOE securely in the roles given to them, will instruct General Users to operate the TOE securely, and will not carry out any malicious acts using Administrator permissions.

By OE.ADMIN, Responsible Manager for MFP selects trusted persons as Administrators and provides them with the education programs corresponding to their Administrator Roles. The educated Administrators teach General Users the compliance rules and instruct them to follow the compliance rules that are for the secure operation for General Users and explicitly stated in Administrator guidance of the TOE. Therefore, A.ADMIN is accomplished.

A.SUPERVISOR (Supervisor's assumption)

A.SUPERVISOR presupposes that a Supervisor has adequate knowledge to operate the TOE securely in the roles given to a Supervisor and does not carry out any malicious acts using Supervisor permissions.

By OE.SUPERVISOR, Responsible Manager for MFP selects a trusted person as a Supervisor and provides the Supervisor with the education programs corresponding to the Supervisor role. Therefore, A.SUPERVISOR is accomplished.

A.NETWORK (Assumption of Network Connections)

A.NETWORK presupposes that the Internal Networks are protected from the External Networks when the networks to be connected to the TOE are connected to the External Networks such as the Internet.

By OE.NETWORK, when the Internal Networks connected to the TOE are connected to the External Networks such as the Internet, organizations that manage the operation on the Internal Networks close the unnecessary ports of the External and Internal Networks. Therefore, A.NETWORK is accomplished.

T.ILLEGAL_USE (Malicious Usage of the TOE)

To counter this threat, the TOE performs the identification and authentication with O.I&A prior to the use of the TOE security functions by users, and allows the only successfully authenticated user to use the functions for which the user has the operation permission. In addition, the performance of O.I&A is recorded as audit logs by O.AUDIT, and the function to read the audit logs is only provided to the Machine Administrator. The Machine Administrator detects afterwards whether or not there was security intrusion of O.I&A.

Therefore, the TOE can counter T.ILLEGAL_USE.

T.UNAUTH_ACCESS (Access Violation to the Protected Assets Stored in the TOE)

To counter this threat, the TOE allows the authorized users identified by O.I&A to access to the Document Data according to the access rights to Document Data which are assigned to the authorized users' roles and the authorized users by O.DOC_ACC. Specifically, the TOE allows the authorized General User to perform operations on Document Data according to the operation permissions for the Document Data which are given to the General User, and the TOE allows the File Administrator to delete the Document Data stored in D-BOX.

Therefore, the TOE can counter T.UNAUTH_ACCESS.

T.ABUSE_SEC_MNG (Abuse of Security Management Function)

To counter this threat, the TOE allows the users who are successfully authenticated with O.I&A to use the TOE security functions, and the TOE restricts the specific users to manage the security functions behaviour, TSF data, and security attributes by O.MANAGE. In addition, the performance of O.I&A and O.MANAGE is recorded as audit logs by O.AUDIT, and the function to read audit logs is only provided to the Machine

Administrator. The Machine Administrator detects afterwards whether or not there were security intrusion of O.I&A and O.MANAGE.
Therefore, the TOE can counter T.ABUSE_SEC_MNG.

T.SALVAGE **(Salvaging Memory)**

To counter this threat, the TOE converts the format of the Document Data by O.MEM.PROTECT which makes it difficult to read and decode if the HDD is installed in IT products other than the TOE. In addition, the performance of O.MEM.PROTECT is recorded as audit logs by O.AUDIT, and the function to read audit logs is only provided to the Machine Administrator. The Machine Administrator detects afterwards whether or not O.MEM.PROTECT was successfully performed.
Therefore, the TOE can counter T.SALVAGE.

T.TRANSIT **(Interceptions and Tampering of Communication Path)**

To counter this threat, the TOE protects Document Data and Print Data on communication path from leakage, and detects tampering. The performance of O.NET.PROTECT is recorded as audit logs by O.AUDIT, and the function to read audit logs is only provided to the Machine Administrator. The Machine Administrator verifies afterwards whether or not O.NET.PROTECT was performed.
Therefore, the TOE can counter T.TRANSIT.

T.FAX_LINE **(Intrusion from Telephone Line)**

To counter this threat, the TOE prevents the intrusion from a telephone line connected to Fax Unit to the TOE by O.LINE_PROTECT. In addition, the performance of O.LINE_PROTECT is recorded as audit logs by O.AUDIT, and the function to read audit logs is only provided to the Machine Administrator. The Machine Administrator detects afterwards whether or not O.LINE_PROTECT was successfully performed.
Therefore, the TOE can counter T.FAX_LINE.

P.SOFTWARE **(Checking Integrity of Software)**

To enforce this organizational security policy, the TOE enables TOE users to verify the integrity of the MFP Control Software installed in FlashROM by O.GENUINE.
Therefore, the TOE can enforce P.SOFTWARE.

8.2 Security Requirements Rationale

8.2.1 Rationale for Functional Requirements

Table 35 shows the relation between the TOE security functional requirements and TOE security objectives.

Table 35: Relation between Security Objectives and Functional Requirements

	O.AUDIT	O.I&A	O.DOC_ACC	O.MANAGE	O.MEM.PROTECT	O.NET.PROTECT	O.GENUINE	O.LINE_PROTECT
FAU_GEN.1	X							
FAU_SAR.1	X							
FAU_SAR.2	X							
FAU_STG.1	X							
FAU_STG.4	X							
FCS_CKM.1					X			
FCS_COP.1					X			
FDP_ACC.1			X					
FDP_ACF.1			X					
FDP_IFC.1								X
FDP_IFF.1								X
FIA_AFL.1		X						
FIA_ATD.1		X						
FIA_SOS.1		X						
FIA_UAU.2		X						
FIA_UAU.7		X						
FIA_UID.2		X						
FIA_USB.1		X						
FMT_MSA.1				X				
FMT_MSA.3				X				
FMT_MTD.1				X				
FMT_SMF.1				X				
FMT_SMR.1				X				
FPT_RVM.1	X	X	X	X	X	X	X	X
FPT_SEP.1	X	X	X	X	X	X	X	X
FPT_STM.1	X							
FPT_TST.1					X		X	
FTP_ITC.1						X		
FTP_TRP.1						X		

Table 35 shows that each TOE security functional requirement corresponds to one or more TOE security objectives.

The following describes how the TOE security objectives are accomplished by the TOE security functional requirements corresponding to the TOE security objectives in Table 35.

O. AUDIT Audit

The details of objectives required to accomplish O.AUDIT are listed below from a) to e). The following describes the security functional requirements that correspond to the objectives details, and this is the rationale for O.AUDIT being accomplished by the security functional requirements listed in Table 35.

a) Record audit logs

To accomplish O.AUDIT, it is necessary to record the performance of security functions in the audit logs.

For this, FAU_GEN.1 generates the audit information when starting and ending Audit Function, when performing the Identification and Authentication Function, when users operate the protected assets, when encrypting the protected assets, and when performing the major management functions. It also records the date and time of the event, type of event, subject identity and the outcome of the event.

b) Provide Audit Function

To accomplish O.AUDIT, it is necessary to provide only the Machine Administrator with access to audit logs and in a format that can be audited.

For this, FAU_SAR.1 makes it possible for the Machine Administrator to verify audit logs, and FAU_SAR.2 prohibits the persons other than the Machine Administrator to read audit logs.

c) Protect audit logs

To accomplish O.AUDIT, objectives to adequately protect audit logs are necessary.

For this, FAU_STG.4 protects audit logs from the unauthorized deletion and prevents the unauthorized tampering. If the auditable events occur and the audit log files are full, FAU_STG.4 also prevents the latest audit logs from being lost by writing the new audit log over the audit log that has the oldest time stamp.

d) Time of reliable events occurrence

To accomplish O.AUDIT, it is necessary to record the accurate time of events occurrence to adequately manage security intrusions.

For this, FPT_STM.1 provides the trusted time stamp.

e) Perform the audit surely.

To accomplish O.AUDIT, the objectives from a) to d) shall not be bypassed, and the security domains shall be protected from interference and tampering by untrusted subjects.

For this, the objectives from a) to d) are surely performed by FPT_RVM.1, and the security domains and the untrusted subjects are separated by FPT_SEP.1.

O.I&A User Identification and Authentication

The details of objectives required to accomplish O.I&A are listed below from a) to d). The following describes the security functional requirements that correspond to the objectives details, and this is the rationale for O.I&A being accomplished by the security functional requirements listed in Table 35.

a) Identify and authenticate users before users use the TOE.
To accomplish O.I&A, the identification and authentication shall be performed prior to the use of the TOE security functions by users.
For this, FIA_UID.2 identifies users prior to their use of the TOE security functions, and FIA_UAU.2 authenticates the identified users.

b) Allow the successfully identified and authenticated users to use the TOE.
To accomplish O.I&A, if users succeed in authentication that is performed prior to the use of the TOE security functions by users, the users shall be allowed to use the functions for which they have the operation permissions.
For this, FIA_ATD.1 and FIA_USB.1 bind the successfully identified and authenticated users with the subjects on behalf of that user. Additionally, they associate and maintain the subjects with the security attributes.

c) Make it difficult to decode passwords.
To accomplish O.I&A, the passwords for user authentication shall be protected from being viewed by others while users enter them, and from being easily guessed.
For this, FIA_UAU.7 prevents the passwords from being viewed by others by displaying protection characters (*: asterisk or black circle) in place of each password character entered by users on the authentication feedback area, and FIA_SOS.1 activates the only passwords that make it difficult to be guessed by registering only passwords that satisfy the Minimum Password Length and the combination of letter types for passwords set by the User Administrator, and FIA_AFL.1 reduces the chances to guess passwords by locking out the users whose consecutive numbers of times of failure for user authentication from the Operation Panel, the web browser of client PC, from client PC when printing, and from client PC when faxing meet the Number of Attempts before Lockout, which is set by the Machine Administrator.

d) Perform the identification authentication surely.
To accomplish O.I&A, the objectives from a) to c) shall not be bypassed, and the security domains shall be protected from interference and tampering by untrusted subjects.
For this, the objectives from a) to c) are surely performed by FPT_RVM.1, and the security domains and the untrusted subjects are separated by FPT_SEP.1.

O. DOC_ACC Access Control to Protected Assets

The details of objectives required to accomplish O.DOC_ACC are listed below from a) to b). The following describes the security functional requirements that correspond to the objectives details, and this is the rationale for O.DOC_ACC being accomplished by the security functional requirements listed in Table 35.

a) Specify the access control to the Document Data and perform.
To accomplish O.DOC_ACC, each user shall be allowed to perform operations on Document Data according to the operation permissions for Document Dataset for each type of subjects associated with

the users, and each security attribute associated with the subjects.

For this, if the Administrator Role associated with Administrator process is the File Administrator, FDP_ACC.1 and FDP_ACF.1 allow Administrator process to delete the Document Data. For General Users, FDP_ACC.1 and FDP_ACF.1 allow the General User process to store Document Data, and when the General User IDs which are associated with General User process are registered for the Document Data ACL of each Document Data, then FDP_ACC.1 and FDP_ACF.1 allow the General User process to perform operations on Document Data in accordance with the access rights set for each General User ID in the Document Data ACL.

b) Perform the access controls to the protected assets surely.

To accomplish O.DOC_ACC, the objective a) shall not be bypassed, and the security domains shall be protected from interference and tampering by untrusted subjects.

For this, the objective a) is surely performed by FPT_RVM.1, and the security domains and the untrusted subjects are separated by FPT_SEP.1.

O. MANAGE Security Management

The details of objectives required to accomplish O.MANAGE are listed below from a) to e). The following describes the security functional requirements that correspond to the objectives details, and this is the rationale for O.MANAGE being accomplished by the security functional requirements listed in Table 35.

a) Management of security attributes

To accomplish O.MANAGE, the management of the security attributes shall be limited to the specific users. In addition, a limited value shall be set as the default value of the Document Data ACL, which is one of the security attributes.

For this, FMT_MSA.1 allows:

- The User Administrator to inquire, newly create, and change General User IDs,
- General Users to inquire General User IDs,
- Administrators to inquire and newly create Administrator IDs,
- Administrators to inquire and change their own Administrator IDs,
- Supervisor to inquire Administrator IDs,
- Administrators to inquire, add, and delete the same Administrator Roles assigned to them,
- Supervisors to inquire and change Supervisor ID,
- The File Administrators, Document File Owners and the General Users who have the full control operation permission for the Document Data to inquire and modify its Document Data ACL, and
- The User Administrators and the General Users who have the full control operation permission for the Document Data to inquire and modify its Document Data Default ACL.

FMT_MSA.3 set a specified value for the default value of the Document Data ACL for storing the new Document Data.

b) Management and Protection of TSF data

To accomplish O.MANAGE, the access to the TSF data shall be limited to the specific users.

For this, FMT_MTD.1 allows:

- Machine Administrators to inquire and set the Number of Attempts before Lockout, Setting for Lockout Release Timer, Lockout time, and Lockout Flag for Supervisor, to set the date and time of the system clock, Service Mode Lock setting, to newly create and inquire HDD cryptographic keys, and to inquire audit logs and delete the entire audit logs,
- Authorized TOE users to inquire the date and time of system clock and Service Mode Lock setting,
- User Administrators to inquire and set the Minimum Password Length, Complexity Setting for Password, and Lockout Flag for General Users,
- User Administrators and the General Users to set the authentication information of the General Users, to newly create, delete, and change S/MIME User Information,
- User Administrators and the General Users to inquire S/MIME User Information and destination information for Deliver to Folder,
- Supervisor to inquire and set Lockout Flag for Administrators and set authentication information of Supervisor, and to change authentication information of Administrators, and
- Administrators to change their own authentication information.

c) Specify management functions
To accomplish O.MANAGE, the Security Management Functions for the implemented TSF shall be performed.
For this, FMT_SMF.1 specifies the required Security Management Functions for the security functional requirements.

d) Authorized use of Security Management Functions
To accomplish O.MANAGE, the authorized users shall be associated with the security management roles and the operation permissions and be maintained to ensure the use the Security Management Functions according to the authorized user roles.
FMT_SMR.1 associates the authorized users with one of four Administrators Roles (User Administrator, Machine Administrator, File Administrator and Network Administrator), and the Supervisor role, and maintains such associations.

e) Perform the security management surely.
To accomplish O.MANAGE, the objectives from a) to d) shall not be bypassed, and the security domains shall be protected from interference and tampering by untrusted subjects.
For this, the objectives from a) to d) are surely performed by FPT_RVM.1, and the security domains and the untrusted subjects are separated by FPT_SEP.1.

O.MEM.PROTECT Prevention of Data Disclosure Stored in Memory

The details of objectives required to accomplish O.MEM.PROTECT are listed below from a) to b). The following describes the security functional requirements that correspond to the objectives details, and this is the rationale for O.MEM.PROTECT being accomplished by the security functional requirements listed in Table 35.

a) Generate the encryption keys and perform encryption operations adequately.
To accomplish O.MEM.PROTECT, the format of the Document Data stored on HDD shall be made difficult so that the decoding is difficult unless Document Data is read with the regular methods using

the TOE.

For this, FCS_CKM.1 generates the encryption keys at the key size of 256 bit with TRNG for the encryption key generation algorithm based on BSI-AIS31, and FCS_COP.1 encrypts Document Data when it is stored on HDD, and decrypts Document Data when it is read from HDD using the generated encryption keys with the encryption algorithm AES which corresponds to FIPS197. At the TOE start-up, FTP_TST.1 tests the validity of encryption keys and the performance of Ic Hdd that performs the encryption operation, and it prevents storing Document Data on HDD without being encrypted.

b) Perform the encryption and decryption surely.

To accomplish O.MEM.PROTECT, the objective a) shall not be bypassed, and the security domains shall be protected from interference and tampering by untrusted subjects.

For this, the objective a) is surely performed by FPT_RVM.1, and the security domains and the untrusted subjects are separated by FPT_SEP.1.

O.NET.PROTECT Protection for Network Communication Data

The details of objectives required to accomplish O.NET.PROTECT are listed below from a) to b). The following describes the security functional requirements that correspond to the objectives details, and this is the rationale for O.NET.PROJECT being accomplished by the security functional requirements listed in Table 35.

a) Protect the assets on communication path.

To accomplish O.NET.PROTECT, Document Data or Print Data on the communication path shall be protected from leakage, and tampering shall be detected.

For Deliver to Folders on either an FTP Server or SMB Server from the TOE, FTP_ITC.1 protects Document Data on networks from leakage and detects tampering by using the IPSec protocol. FTP_TRP.1 also protects Document Data on networks from leakage and detects the tampering by requiring a trusted path between the TOE and the remote users, which is described later. For sending by e-mail from the TOE to client PC, Document Data or Print Data on networks is protected from leakage and tampering is detected using S/MIME in the mailing service. For use of web service, print service, and fax service from client PC, Document Data on networks is protected from leakage and tampering is detected by using the SSL protocol.

b) Protect the network communication data surely.

To accomplish O.NET.PROTECT, the objective a) shall not be bypassed, and the security domains shall be protected from interference and tampering by untrusted subjects.

For this, the objective a) is surely performed by FPT_RVM.1, and the security domains and the untrusted subjects are separated by FPT_SEP.1.

O.GENUINE Protection of Integrity of MFP Control Software

The details of objectives required to accomplish O.GENUINE are listed below from a) to b). The following describes the security functional requirements that correspond to the objectives details, and this is the rationale for O.GENUINE being accomplished by the security functional requirements listed in Table 35.

a) Check the integrity of MFP Control Software
To accomplish O.GENUINE, the integrity of MFP Control Software, which is installed in FlashROM, shall be verified.
For this, at the TOE start-up, FPT_TST.1 tests the integrity of the executable code of MFP Control Software, which is installed in FlashROM, and verifies its integrity.

b) Check the integrity of MFP Control Software securely
To accomplish O.GENUINE, the objective a) shall not be bypassed, and the security domains shall be protected from interference and tampering by untrusted subjects.
For this, the objective a) is surely performed by FPT_RVM.1, and the security domains and the untrusted subjects are separated by FPT_SEP.1.

O.LINE_PROTECT Protection for Intrusion from Telephone Line

The details of objectives required to accomplish O.LINE_PROTECT are listed below from a) to b). The following describes the security functional requirements that correspond to the objectives details, and this is the rationale for O.LINE_PROTECT being accomplished by the security functional requirements listed in Table 35.

a) Prohibit the intrusion of fax line
To accomplish O.LINE_PROTECT, the unauthorized access to the TOE over a telephone line by attackers shall be prevented.
For this, FDP_IFC.1 and FDP_IFF.1 allow only fax data received from a telephone line, which is connected to the Fax Unit, to pass from the fax process on the Fax Unit to the fax reception process on Controller Board.

b) Prohibit the intrusion of fax line securely.
To accomplish O.LINE_PROTECT, the objective a) shall not be bypassed, and the security domains shall be protected from interference and tampering by untrusted subjects.
For this, the objective a) is surely performed by FPT_RVM.1, and the security domains and the untrusted subjects are separated by FPT_SEP.1.

8.2.2 Rationale for Minimum Strength of Function

This TOE is placed on the premises for organizations such as offices, and connected to the Internal Networks, which are protected from the threats from the External Networks, and telephone lines. Therefore, the persons in offices including those who are not allowed to use the TOE could be the threat agents, and the risk of its assumed threats is low. Therefore, the level of attackers is low, and the appropriate minimum strength of function is SOF-basic.
This ST claims SOF-basic for the TOE as minimum strength of function, and is consistent.
FIA_AFL.1, FIA_SOS.1 and FIA_UAU.2 are the functional requirements that specify the stated strength of function.

8.2.3 Dependencies of Security Functional Requirements

On the TOE security functional requirements, Table 36 shows the correspondence status of the dependencies in this ST.

Table 36: Correspondence Table of Dependencies of TOE Security Functional Requirements

TOE Security Functional Requirements	Dependencies claimed by CC	Dependencies satisfied in ST	Dependencies not satisfied in ST
FAU_GEN.1	FPT_STM.1	FPT_STM.1	None
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	None
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	None
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	None
FAU_STG.4	FAU_STG.1	FAU_STG.1	None
FCS_CKM.1	[FCS_CKM.2 Or FCS_COP.1] FCS_CKM.4 FMT_MSA.2	FCS_COP.1	FCS_CKM.4 FMT_MSA.2
FCS_COP.1	[FDP_ITC.1 Or FDP_ITC.2 Or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	FCS_CKM.1	FCS_CKM.4 FMT_MSA.2
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	None
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3	None
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1	None
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3	None
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2	FIA_UAU.1
FIA_ATD.1	None	None	None
FIA_SOS.1	None	None	None
FIA_UAU.2	FIA_UID.1	FIA_UID.2	FIA_UID.1
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2	FIA_UAU.1
FIA_UID.2	None	None	None
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	None
FMT_MSA.1	[FDP_ACC.1 Or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	None

TOE Security Functional Requirements	Dependencies claimed by CC	Dependencies satisfied in ST	Dependencies not satisfied in ST
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1	None
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1	None
FMT_SMF.1	None	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2	FIA_UID.1
FPT_RVM.1	None	None	None
FPT_SEP.1	None	None	None
FPT_STM.1	None	None	None
FPT_TST.1	FPT_AMT.1	None	FPT_AMT.1
FTP_ITC.1	None	None	None
FTP_TRP.1	None	None	None

The rationale for satisfying no dependencies is listed and explained below.

Rationale for removing the dependencies for FCS_CKM.4

In this TOE, HDD encryption keys are stored in areas which cannot be accessed from outside Ic Hdd. In addition, after the Administrators generate encryption keys at the start of the TOE operation, deletion of encryption keys are not performed but only the change to overwrite the new encryption keys is performed. Therefore, the functional requirements for encryption key destruction using standard measures are not required.

Rationale for removing the dependencies for FMT_MSA.2

For this TOE, there are no attributes for generating keys such as HDD encryption keys, key types, or expiration date. Therefore, the functional requirements of management of the security attributes are not required.

Rationale for removing the dependencies for FIA_UAU.1

Since this TOE employs FIA_UAU.2, which is hierarchical to FIA_UAU.1, the dependency on FIA_UAU.1 is satisfied with FIA_AFL.1 and FIA_UAU.7.

Rationale for removing the dependencies for FIA_UID.1

Since this TOE employs FIA_UID.2, which is hierarchical to FIA_UID.1, the dependency on FIA_UID.1 is satisfied with FIA_UAU.2 and FMR_SMR.1.

Rationale for removing the dependencies for FPT_AMT.1

The TOE consists of both hardware and software, and there are no hardware and firmware outside of the TOE on which the TSF depends for its performance. Therefore, abstract machine testing by FPT_AMT.1 is not required.

8.2.4 Assurance Requirements Rationale

This TOE is a commercially available MFP. MFPs are assumed to be used in general offices, and this TOE does not assume the attackers have a moderate or greater level attack potential.

High-level design evaluation (ADV_HLD.2) is adequate to show the validity of commercially available products. A high attack potential is required for attacks that circumvent or tamper with the TSF, which is the target of this evaluation. Therefore, the obvious vulnerability analysis (AVA_VLA.1) is adequate for general needs.

On the other hand, it is required to protect the secrecy of relevant information to make the attacks more difficult and it is important to ensure a secure environment for the development environment. Therefore, the development security (ALC_DVS.1) is important.

Therefore, considering the time and cost for the evaluation, the evaluation assurance level of EAL3 is appropriate for this TOE.

8.2.5 Mutual Support of Security Requirements

Table 37 shows the relation of mutual support of security requirements.

Table 37: Mutual Support of Security Requirements

Functional Requirements	Bypass Prevention	De-activation Prevention	Tampering Prevention	Defeasance Detection
FAU_GEN.1	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FAU_SAR.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FAU_SAR.2	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FAU_STG.1	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FAU_STG.4	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FCS_CKM.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FCS_COP.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FDP_ACC.1	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FDP_ACF.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FDP_IFC.1	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FDP_IFF.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FIA_AFL.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FIA_ATD.1	N/A	N/A	FPT_SEP.1	N/A

Functional Requirements	Bypass Prevention	De-activation Prevention	Tampering Prevention	Defeasance Detection
FIA_SOS.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FIA_UAU.2	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FIA_UAU.7	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FIA_UID.2	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FIA_USB.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FMT_MSA.1	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FMT_MSA.3	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FMT_MTD.1	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FMT_SMF.1	N/A	N/A	FPT_SEP.1	FAU_GEN.1
FMT_SMR.1	N/A	N/A	FPT_SEP.1	FAU_GEN.1
FPT_RVM.1	N/A	N/A	FPT_SEP.1	N/A
FPT_SEP.1	N/A	N/A	N/A	N/A
FPT_STM.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FPT_TST.1	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FTP_ITC.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FTP_TRP.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1

8.2.5.1 Bypass Prevention

FAU_GEN.1, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.4, FCS_CKM.1, FCS_COP.1, FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1, FIA_AFL.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.7, FIA_UID.2, FIA_USB.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FPT_STM.1, FPT_TST.1, FTP_ITC.1, and FTP_TRP.1 do not perform their security functions properly if bypassed, but those functions are invoked by FPT_RVM.1 and that prevents the bypass.

Since FIA_ATD.1, FMT_SMF.1 and FMT_SMR.1 are the functional requirements that define and enumerate the security attributes, Security Management Functions and security roles, and there are no methods to bypass them, they are not the target of bypass prevention by FPT_RVM.1.

8.2.5.2 De-activation Prevention

Since FAU_GEN.1, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.4, FCS_CKM.1, FCS_COP.1, FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1, FIA_AFL.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.7, FIA_UID.2, FIA_USB.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FPT_RVM.1, FPT_SEP.1, FPT_STM.1, FPT_TST.1, FTP_ITC.1, FTP_TRP.1 are always performed and no methods are provided to stop these, the de-activation is not an issue.

FIA_ATD.1, FMT_SMF.1 and FMT_SMR.1 are the functional requirements that define and enumerate the security attributes, Security Management Functions and security roles, and de-activation is not an issue.

8.2.5.3 Tampering Prevention

Since FPT_SEP.1 prevents interference by untrusted subjects by keeping the security domains separated, the TOE security functional requirements are protected from tampering.

8.2.5.4 Defeasance Detection

For each security function, audit logs are generated for the use of the auditable events of security functions, marked as FAU_GEN.1 in the column of "Defeasance Detection" in Table 37. This enables the ex-post analysis on the performance status of security functions.

8.3 TOE Summary Specification Rationale

8.3.1 Rationale for TOE Security Function

This chapter demonstrates that the TOE security functions defined in Chapter 6.1 accomplish the TOE security functional requirements specified in Chapter 5.1.

Table 23 shows that the TOE security functions correspond to one or more TOE security functional requirements. The following describes that each security function is accomplished by the corresponding TOE security functions shown in Table 23.

FAU_GEN.1 (Audit data generation)

FAU_GEN.1 requires the auditable events of the TOE to be recorded in audit logs, and specifies the audit information that is recorded when the audit events occur.

SF.AUDIT ensures the audit information, required by FAU_GEN.1, is generated and recorded as audit logs when the auditable events, required by FAU_GEN.1, occur as shown in Table 24. While FAU_GEN.1 requires recording the starting and ending of the Audit Function, the starting of the Audit Function is substituted with the event of the TOE startup, but the ending of the Audit Function is not recorded in SF.AUDIT. Since Audit Function starts running under the same condition as the TOE, the starting of Audit Function can be substituted with the event of the TOE startup. The starting and ending of the Audit Function are recorded to audit the state of the inactivity of Audit Function. However, Audit Function of this TOE starts running when the TOE is powered on and keeps running until the power is shut down, and also while its power is down (while Audit Function is inactive), the entire function the TOE has does not work. In addition, while the status the auditable events occur, Audit Function of this TOE surely works, and it is not necessary for the TOE to record the state of the inactivity of Audit Function. Therefore, it is appropriate not to record the ending of Audit Function in SF.AUDIT. On Lockout release events at the TOE start-up, the Lockout release events at the TOE start-up can be substituted with the event of the TOE startup since the TOE start-up surely releases the Lockout for Administrators and a Supervisor whose Lockout Flag are set to "Active". In a mechanism of the TOE, the TOE surely encrypts Document Data when storing the Document Data, and decrypts the Document Data when reading Document Data, and additionally, it does not write the Document Data on HDD when failing to store Document Data, and makes the condition of Document Data undecodable when failing to read the Document Data, therefore the auditable events of Document Data encryption/decryption are the successful events for storing and reading the Document Data. For the successful reading of the Document Data, the recording objects of ID of object Document Data which are individual audit information are limited to printing, sending by e-mail, delivering to folder, downloading from Web Service Function the Document Data stored in D-BOX, and it is not included to fax the Document Data stored in D-BOX. For faxing the Document Data stored in D-BOX, even without the ID of object Document Data, the Machine Administrator can specify or limit the object Document Data for faxing out of the Document Data stored in D-BOX with other audit log information, and also can audit the fax operator and the outcome whether the faxing object Document Data have been sent or not based on those information. Therefore, FAU_GEN.1 is accomplished by implementing SF.AUDIT.

FAU_SAR.1 (Audit review), FAU_SAR.2 (Restricted audit review)

FAU_SAR.1 requires that the Machine Administrator can read the audit logs in the verifiable format, and FAU_SAR.2 requires that users other than the Machine Administrator cannot read audit logs.
SF.AUDIT allows only the Machine Administrator to read audit logs in the text format.
Therefore, FAU_SAR.1 and FAU_SAR.2 are accomplished by implementing SF.AUDIT.

FAU_STG.1 (Protected audit trail storage)

FAU_STG.1 requires that the audit logs are protected from the unauthorized deletion and the unauthorized modification is prevented.
SF.AUDIT allows only the Machine Administrator to delete the audit logs. On the modification of audit logs, since there are no interfaces for modifying the audit logs, unauthorized modification for audit the logs cannot be performed. The Machine Administrator who can delete the audit logs will not carry out any malicious acts using Administrator permissions. Thus, the audit logs are protected from unauthorized deletion and modifications.
Therefore, FAU_STG.1 is accomplished by implementing SF.AUDIT.

FAU_STG.4 (Prevention of audit data loss)

FAU_STG.4 requires overwriting the oldest audit logs if the audit log file area is full in order not to lose the newest audit logs.
SF.AUDIT writes the newest audit logs over the oldest ones if there is no remaining space to add new audit logs in the audit log file.
Therefore, FAU_STG.4 is accomplished by implementing SF.AUDIT.

FCS_CKM.1 (Cryptographic key generation)

On HDD cryptographic key generation, FCS_CKM.1 requires the conditions of standards, cryptographic key generation algorithm and cryptographic key sizes.
SF.CIPHER generates the HDD cryptographic keys at the key size of 256 bits with TRNG, the cryptographic key generation algorithm, based on the BSI-AIS31, to encrypt/decrypt the Document Data when storing the Document Data on HDD/reading the Document Data. The standard of HDD cryptographic key generation, cryptographic key generation algorithm, and cryptographic key size meet the requirements of FCS_CKM.1.
Therefore, FCS_CKM.1 is accomplished by implementing SF.CIPHER.

FCS_COP.1 (Cryptographic operation)

FCS_COP.1 requires the conditions of standards of cryptographic operation on HDD cryptographic keys, cryptographic algorithm and cryptographic key size.
SF.CIPHER encrypts/decrypts the Document Data with the cryptographic key at the key size of 256 bit and AES cryptographic algorithm based on FIPS 197 when storing the Document Data on HDD/reading the Document Data. This meets the requirements of FCS_COP.1.
Therefore, FCS_COP.1 is accomplished by implementing SF.CIPHER.

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

FDP_ACC.1 defines the relation between the user roles, which can store, read, edit and delete the Document Data, and the permitted operations for each user role as shown in Table 8. FDP_ACF.1 defines the rules between the user roles, which can access to the Document Data, and the permitted operations for each user role as shown in Table 9, Table 10, and Table 11.

SF.DOC_ACC allows the File Administrator to delete the Document Data, and General Users to store, read, edit and delete the Document Data according to the Document Data ACL of each Document Data.

Therefore, FDP_ACC.1 and FDP_ACF.1 are accomplished by implementing SF.DOC_ACC.

FDP_IFC.1 (Subset information flow control), FDP_IFF.1 (Simple security attributes)

FDP_IFC.1 and FDP_IFF.1 require the telephone line information flow control SFP is performed when the fax process on Fax Unit receives the data from a telephone line, and if the type of received data is the fax data, the data is passed over to the fax reception process on Controller Board.

If the type of data that the Fax Unit receives from a telephone line is the fax data, SF.FAX_LINE passes it over to Controller Board, and if Fax Unit receives data which is not fax data, the received data is not passed over to Controller Board but instead is discarded.

Therefore, FDP_IFC.1 and FDP_IFC.1 are accomplished by implementing SF.FAX_LINE.

FIA_AFL.1 (Authentication failure handling)

FIA_AFL.1 requires the detection of users whose consecutive numbers of times of failure for user authentication in Authentication Events shown in Table 14 meet the Number of Attempts before Lockout set by the Machine Administrator, and that such users are locked out until the Lockout release actions shown in Table 15 is taken.

SF.I&A counts the number of times of user authentication failure for Authentication Events in Table 14 as shown in "6.1.2.2 Action in case of Identification and Authentication Failure", and if the consecutive numbers of times of failure meet the Number of Attempts before Lockout, Lockouts the users and activates the Lockout Flag for the concerned user ID. When succeeding in authentication, the consecutive numbers of times of failure of that user is recounted from 0.is reset to zero.

Lockout release is performed by either Auto Lockout Release or Manual Lockout Release as defined in Table 15 Lockout Release Actions.

The value for Number of Attempts before Lockout is set with the value between 1 and 5, and the Lockout time is set with the value between 1 and 9999 minutes or an indefinite value. The Machine Administrator manages the Number of Attempts before Lockout and the Lockout time with SF.SEC_MNG.

Therefore, FIA_AFL.1 is accomplished by implementing SF.I&A and SF.SEC_MNG.

FIA_ATD.1 (User attribute definition)

FIA_ATD.1 requires the General User IDs, Document Data Default ACL, Administrator IDs, Administrator Roles, and Supervisor ID are maintained as security attributes that are attributed to each user.

SF.I&A associates the General Users with General User IDs and Document Data Default ACL, Administrators with Administrator IDs and Administrator Roles, and Supervisor with Supervisor ID as the

security attributes and maintains those attributes.
Therefore, FIA_ATD.1 is accomplished by implementing SF.I&A.

FIA_SOS.1 (Verification of secrets)

FIA_SOS.1 requires the quality of passwords of the authorized users meets the following contents.

- Usable characters and its character types:

  Upper-case letters: [A-Z] (26 letters)
  Lower-case letters: [a-z] (26 letters)
  Numbers: [0-9] (10 letters)
  Symbols: SP (space) ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ (33 letters)

- Registerable Password Length:

  For General Users
  No fewer than the Minimum Password Length set by the User Administrator (8-32 digits), nor more than 128 digits.
  For Administrators and a Supervisor
  No fewer than the Minimum Password Length set by the User Administrator (8-32 digits), nor more than 32 digits.

- Rule: It is allowed to register passwords with combination of the character types based on the Complexity Setting for Password set by the User Administrator. The User Administrator sets either Level 1 or Level 2 for Complexity Setting for Password.

Passwords are allowed to be registered by SF.I&A only when the password qualities described above are satisfied.
Therefore, FIA_SOS.1 is accomplished by implementing SF.I&A.

FIA_UAU.2 (User authentication before any action)

FIA_UAU.2 requires the users succeed in authentication prior to the use of the TOE security functions.
If no users are logged in from the Operation Panel, SF.I&A displays the screen on the Operation Panel to request users to enter their user IDs and passwords, and if there is an access to the Web Service Function from client PC which no users are logged in from, it displays the screen on the web browser screen to request users to enter their user IDs and passwords. It authenticates the users based on the user IDs and passwords entered by users.
For a print or a fax transmission request from client PC, it authenticates the users with the user IDs and passwords sent from client PC prior to the print or fax transmission request.
Therefore, FIA_SOS.1 is accomplished by implementing SF.I&A.

FIA_UAU.7 (Protected authentication feedback)

FIA_UAU.7 requires the display of protection characters (*: asterisk, or black circle) for each password character on the authentication feedback area while the TOE users enter their passwords.
SF.I&A displays one protection character (*: asterisk, or black circle) on the authentication feedback area when the TOE users enter one character of their passwords.
Therefore, FIA_UAU.7 is accomplished by implementing SF.I&A.

FIA_UID.2 (User identification before any action)

FIA_UID.2 requires that users are identified before the use of the TOE security functions.
If no users are logged in from the Operation Panel, SF.I&A displays the screen on the Operation Panel to request users to enter their user IDs and passwords, and if there is an access to the Web Service Function from client PC which no users are logged in from, it displays the screen on the web browser screen to request users to enter their user IDs and passwords. It identifies the users based on the user IDs entered by users.
For a print or a fax transmission request from client PC, it identifies the users with the user IDs sent from client PC prior to the print or fax transmission request. Therefore, FIA_UID.2 is accomplished by implementing SF.I&A.

FIA_USB.1 (User-subject binding)

FIA_USB.1 requires that the General User process is associated with the General User IDs and Document Data Default ACL on behalf of the General Users, the Administrator process is associated with the Administrator IDs and Administrator Roles on behalf of the Administrator, and the Supervisor process is associated with the Supervisor ID on behalf of the Supervisor. Administrators are allowed to add their own Administrator Roles to other Administrators, and Administrators are allowed to delete the Administrator Roles provided that such roles are already assigned to another Administrator.
If the successfully authenticated user is a General User, SF.I&A binds the General User with General User process, if it is an Administrator, it binds the Administrator with Administrator process, and if it is a Supervisor, it binds with Supervisor process. Additionally, it associates the General User process with the General User IDs and Document Data Default ACL, the Administrator process with the Administrator IDs and Administrator Roles, and the Supervisor process with the Supervisor ID as the security attributes and keeps.
SF.SEC_MNG also enforces the rules defined with FIA_USB.1.3 as a management of the security attributes of subjects (Administrator process), allows Administrators to add their own Administrator Roles to other Administrators, and it allows Administrators to delete the Administrator Roles provided that such roles are already assigned to another Administrator.
Therefore, FIA_UID.2 is accomplished by implementing SF.I&A.

FMT_MSA.1 (Management of security attributes)

FMT_MSA.1 requires the security attributes are managed as shown in Table 17.
For the security attributes shown in Table 17, SF.SEC_MNG allows the user roles shown in Table 17 to perform the operations shown in Table 17 by enforcing the access control SFP.
Therefore, FMT_MSA.1 is accomplished by implementing SF. SEC_MNG.

FMT_MSA.3 (Static attribute initialisation)

When a General User stores Document Data, FMT_MSA.3 requires that:

- The Document Data Default ACL of the General User who stores the Document Data is set to the Document Data ACL of the Document Data being stored, and
- The Document Data Default ACL has the specified property value which can be arbitrarily set by the User Administrator, and by General Users only for their own Document Data Default ACL.

SF.SEC_MNG provides the function to set the "Document Data Default ACL", which has the specified value defined in Table 18, as the security attributes for General Users. This function is provided as a default value of the security attributes to enforce the MFP access control SFP to the access control list for Document Data that is initialised when Document Data is generated by General Users. Setting this function is specified and provided only to the User Administrator, and to General Users for their own Document Data Default ACL.
Therefore, FMT_MSA.3 is accomplished by implementing SF. SEC_MNG.

FMT_MTD.1 (Management of TSF data)

FMT_MTD.1 requires the access to the TSF data is managed as shown in Table 19.
SF.SEC_MNG, SF.CIPHER, SF.AUDIT and SF.CE_OPE_LOCK allow the user roles shown in Table 19 to perform the operations shown in Table 19 for the TSF data listed in Table 19.
Therefore, FMT_MTD.1 is accomplished by implementing SF. SEC_MNG, SF.CIPHER, SF.AUDIT and SF.CE_OPE_LOCK.

FMT_SMF.1 (Specification of Management Functions)

FMT_SMF.1 requires the items to be the objectives of security management, specified by CC when selecting each functional requirement, and their corresponding items of the TOE security management as shown in Table 20.
SF.SEC_MNG and SF.I&A provide the security management items shown above in Table 20.
Therefore, FMT_SMF.1 is accomplished by implementing SF. SEC_MNG and SF.I&A.

FMT_SMR.1 (Security roles)

FMT_SMR.1 requires that when registering the users for the TOE, one of the security roles (General User, Administrator, or Supervisor) is assigned to the user, and when the registered user uses the TOE, the user is associated with a security role that is maintained during use of the TOE.
SF.I&A binds successfully authenticated users with the process that associated with their user roles, and maintains those roles. SF.SEC_MNG assigns the user roles (General User, Administrator, and Supervisor) to user when registering users for the TOE. It also maintains the security roles by allowing only the User Administrator to newly create the General User Information in the Address Book and delete the General User Information in the Address Book, by allowing only Administrators to register and delete Administrators, by allowing only Administrators who have a particular Administrator Role to add and delete that Administrator Role, and by allowing only Supervisor to change the Supervisor.
Therefore, FMT_SMR.1 is accomplished by implementing SF.I&A and SF. SEC_MNG.

FPT_RVM.1 (Non-bypassability of the TSP)

FPT_RVM.1 requires that the TSP enforcement functions are invoked before each function is allowed to proceed and its success is assured.
SF.AUDIT, SF.I&A, SF.DOC_ACC. SF.SEC_MGN, SF.CE_OPE_LOCK, SF.CIPHER, SF.NET_PROT, SF.FAX_LINE AND SF.GENUINE are implemented to perform surely without being bypassed.
Therefore, FPT_RVM.1 is accomplished by implementing SF.AUDIT, SF.I&A, SF.DOC_ACC, SF.SEC_MNG, SF.CE_OPE_LOCK, SF.CIPHER, SF.NET_PROT, SF.FAX_LINE and SF.GENUINE.

FPT_SEP.1 (TSF domain separation)

FPT_SEP.1 requires that the TSF maintains security domains to protect its operation from interference and tampering by untrusted subjects.
SF.AUDIT, SF.I&A, SF.DOC_ACC, SF.SEC_MNG, SF_CE_OPE_LOCK, SF.CIPHER, SF.NET_PROT, SF.FAX_LINE and SF.GENUINE protect themselves from interference and tampering by untrusted subjects.
Therefore, FPT_SEP.1 is accomplished by implementing SF.AUDIT, SF.I&A, SF.DOC_ACC, SF.SEC_MNG, SF_CE_OPE_LOCK, SF.CIPHER, SF.NET_PROT, SF.FAX_LINE and SF.GENUINE.

FPT_STM.1 (Reliable time stamps)

FPT_STM.1 requires the TSF is provided with reliable time stamps.
SF.AUDIT provides the date (year, month, day) and time of the system clock to record the date and time when the auditable events occur.
Therefore, FPT_STM.1 is accomplished by implementing SF.AUDIT.

FPT_TST.1 (TSF testing)

FPT_TST.1 requires that the TSF perform self testing.
SF.CIPHER tests the operation of HDD encryption function of Ic Hdd and the integrity of HDD cryptographic keys when the TOE is powered on.
SF.GENUINE checks the integrity of the executable code of MFP Control Software and verifies that MFP Control Software is regular when the TOE is powered on.
Therefore, FPT_TST.1 is accomplished by implementing SF.CIPHER and SF. GENUINE.

FTP_ITC.1 (Inter-TSF trusted channel)

FTP_ITC.1 requires that a trusted channel between the TSF and IT products is used when the TSF and IT products communicate.
SF.NET_PROT supports IPSec as trusted channel for Deliver to Folders between the TOE and FTP Server or between the TOE and SMB Server.
Therefore, FTP_ITC.1 is accomplished by implementing SF.NET_PROT.

FTP_TRP.1 (Trusted path)

FTP_TRP.1 requires that a trusted path is used for when the TSF and remote users communicate.
SF.NET_PROT supports S/MIME protocol as trusted path for e-mail service from the TOE to client PC, and supports SSL protocol as trusted path for the use of web service, print service and fax transmission service from client PC.
Therefore, FTP_TRP.1 is accomplished by implementing SF.NET_PROT.

8.3.2 Strength of Functions Rationale

For this TOE, the security functions which include the probabilistic or permutational mechanism are the authentication using the passwords for SF.I&A. SOF-basic is specified for the strength of these security functions in Chapter 6.2. In addition, SOF-basic is specified for the minimum strength of function level in Chapter 5.2. Therefore, both of these are consistent.

8.3.3 Rationale for Assurance Measures

The documents, which are provided as assurance measures for all security assurance required by EAL3, and the TOE are listed in Chapter 6.3 and it shows those correspondence. Those documents cover the evidence required by security assurance requirements. Therefore, the TOE security assurance requirements are satisfied.

8.4 PP Claims Rationale

This ST does not conform to any PPs.