imagio MP 2550/3350 series, Aficio MP 2550/3350 series

Security Target

Authors : RICOH COMPANY, LTD., Yoshihiko KAMEKURA, Yasushi FUNAKI, Fumi TAKITA
Date : 2010-02-08
Version : 1.05

Update History

Version	Date	Authors	Details
1.05	2010-02-08	Yoshihiko KAMEKURA, Yasushi FUNAKI, Fumi TAKITA	Released documents

Table of Contents

List of Figures

List of Tables

1 ST Introduction

This chapter describes the ST Reference, TOE Reference, TOE Overview and TOE Description.

1.1 ST Reference

The following are the identification information for this ST.

ST Title : imagio MP 2550/3350 series, Aficio MP 2550/3350 series Security Target

ST Version : 1.05

Date : 2010-02-08

Authors : RICOH COMPANY, LTD., Yoshihiko KAMEKURA, Yasushi FUNAKI, Fumi TAKITA

1.2 TOE Reference

The following are the identification information for this TOE.

Manufacturer : RICOH COMPANY, LTD.

TOE Name : <Japanese name> Ricoh imagio MP 2550/3350 series

<English name> Ricoh Aficio MP 2550/3350 series

Refer to Table 1 about product names for "Ricoh imagio MP 2550/3350 series" and "Ricoh Aficio MP 2550/3350 series".

TOE Version : "Ricoh imagio MP 2550/3350 series" and "Ricoh Aficio MP 2550/3350 series" are identified by following software and hardware.

Software	System/Copy	1.14
	Network Support	7.23
	Scanner	1.11
	Printer	1.05
	Fax	05.00.00
	Web Support	1.52
	Web Uapl	1.10
	Network Doc Box	1.10C
Hardware	Ic Key	1100
	Ic Hdd	01

Notes: When an "e" is suffixed to the 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

Table 1: List of TOE

Series Name	Series Details
Ricoh imagio MP 2550/3350 series	Ricoh imagio MP 2550SP Ricoh imagio MP 2550SPF Ricoh imagio MP 3350SP Ricoh imagio MP 3350SPF
Ricoh Aficio MP 2550/3350 series	Ricoh Aficio MP 2550 Ricoh Aficio MP 2550SP Ricoh Aficio MP 2550SPF Ricoh Aficio MP 3350 Ricoh Aficio MP 3350SP Ricoh Aficio MP 3350SPF Savin 9025 Savin 9025SP Savin 9025SPF Savin 9033 Savin 9033SP Savin 9033SPF Lanier LD425 Lanier LD425SP Lanier LD425SPF Lanier LD433 Lanier LD433SP Lanier LD433SPF Lanier MP 2550 Lanier MP 3350 Gestetner MP 2550 Gestetner MP 2550SP Gestetner MP 2550SPF Gestetner MP 3350 Gestetner MP 3350SP Gestetner MP 3350SPF nashuatec MP 2550 nashuatec MP 2550SP nashuatec MP 3350 nashuatec MP 3350SP RexRotary MP 2550 RexRotary MP 2550SP RexRotary MP 3350 RexRotary MP 3350SP infotec MP 2550 infotec MP 2550SP infotec MP 3350 infotec MP 3350SP

1.3 TOE Overview

This chapter describes the TOE Type, TOE Usage and Major Security Features, and Environment for TOE Usage and Non-TOE Configuration Items.

1.3.1 TOE Type

The TOE is a digital 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.

1.3.2 TOE Usage and Major Security Features of TOE

The TOE has the functions; input function to input the paper document files or electronic document files into the TOE, storage function to store the input Document Data, and output function to output the input or stored Document Data. The paper document files are input with the scanner device that the MFP has, and the electronic document files are input by receiving them from the network-connected client PCs or USB-connected client PCs, or receiving from faxes. The output function includes the printing, fax transmission and transferring to the servers or client PCs that are connected to networks. The TOE incorporates some of these functions and provides as the Copy Function, Scanner Function, Printer Function and Fax Function.
Users can use these functions from the Operation Panel. Users can also operate some of these functions remotely.

The major security functions of this TOE in this ST are as follows;

1. Audit Function
2. Identification and Authentication Function
3. Document Data Access Control Function
4. Stored Data Protection Function
5. Network Communication Data Protection Function
6. Security Management Function
7. Service Mode Lock Function
8. Telephone Line Intrusion Protection Function
9. MFP Control Software Verification Function

For the security functions described above, the contents of each function are described in "1.4.4.2 Security Functions".

1.3.3 Environment for TOE Usage and Non-TOE Configuration Items

The TOE is assumed to be placed in offices. In offices, the TOE can be connected to other IT products via networks, and telephone lines, depending on the needs of the users, and USB connection is also available. Users can operate the TOE from the Operation Panel of the TOE, client PCs that are connected to the

Internal Networks, or USB-connected client PCs. Figure 1 shows and describes an assumed environment for the usage of the TOE.

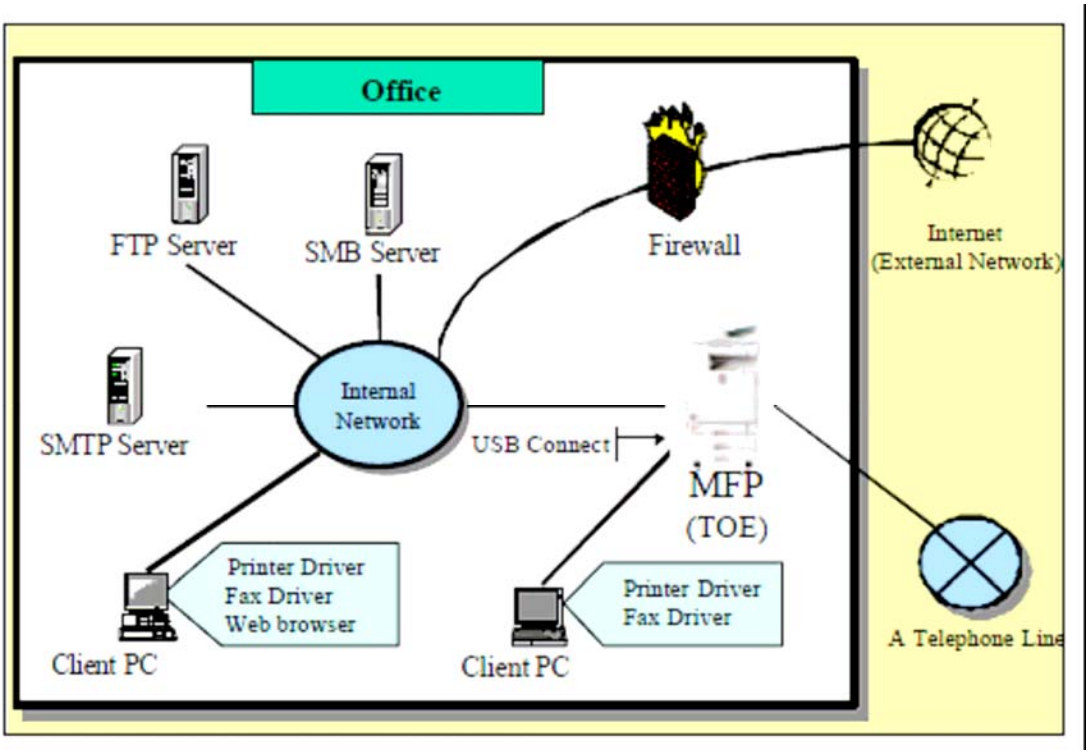

Figure 1: Environment for Usage of TOE

The following describes the non-TOE configuration items.

Internal Network

The Internal Network connects the TOE with various types of servers (FTP server, SMB server and SMTP server) and client PCs. It is connected to the Internet via firewall. IPv4 is used for the Internal Networks.

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.

It is necessary to download and install RPCS printer driver and fax driver into a client PC from the website described in the Operational user guidance when printing or faxing from a client PC that is connected to the Internal Network, or from a USB-connected client PC.

FTP Server

An FTP server is used to deliver the Document Data, which is stored in the TOE, to folders in an FTP server.

SMB Server

An SMB server is used to deliver the Document Data, which is stored in the TOE, to folders in an SMB server.

SMTP Server

An SMTP server is used to send the Document Data to a client PC by e-mail.

Telephone Line

A telephone line is a line used to send and receive the fax data from the external fax when the optional fax is equipped.

Firewall

A firewall is a device that is set between the Internal Network and External Network, and protects the Internal Network from the External Network.

1.4 TOE Description

This chapter describes the Physical Scope of TOE, Guidance Documents, User Roles, Logical Scope of TOE, and Protected Assets.

1.4.1 Physical Scope of TOE

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

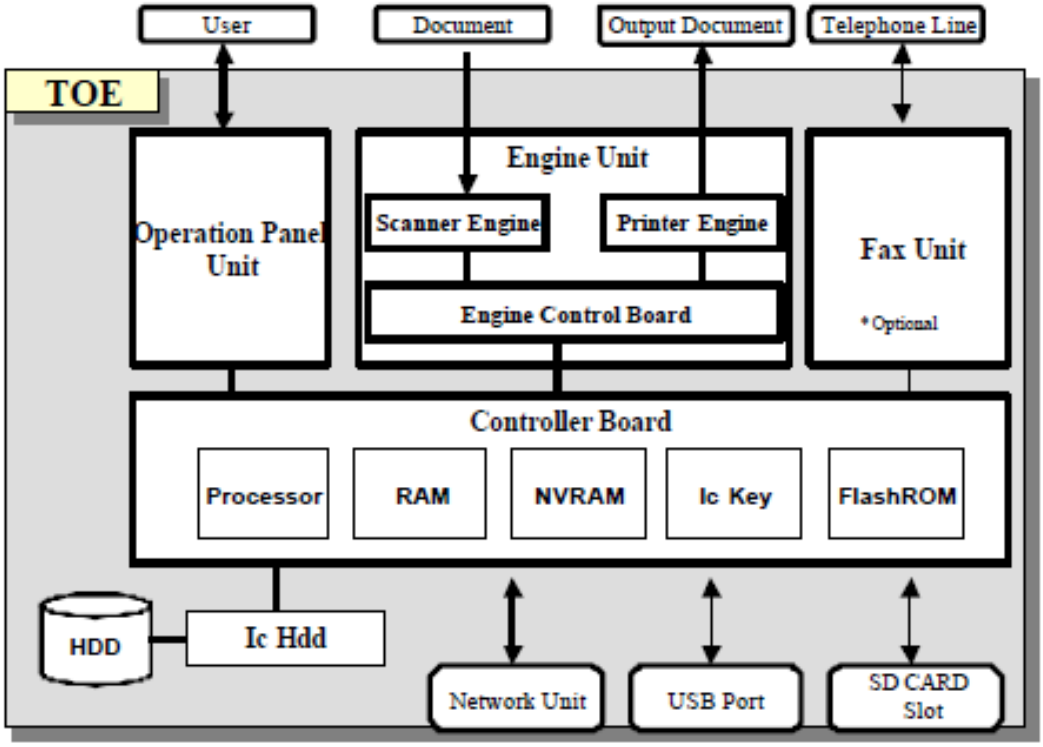

Figure 2: Hardware Configuration of TOE

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 key switches, 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 key switches and touch screen LCD to MFP Control Software or receiving the 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, FlashROM, RAM, NVRAM, and Ic Key. 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 outlines of processors, FlashROM, RAM, NVRAM, and Ic Key are described below:

[Processor]

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

[FlashROM]

A memory in which MFP Control Software is installed.

[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 has the functions of random number generation and encryption key generation, and is used to detect the tampering of MFP Control Software.

Ic Hdd

Ic Hdd is a security chip that has 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 the Customer Engineer (hereafter called CE) 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 inserts an SD Card containing information to activate the Stored Data Protection Function into this SD CARD Slot to enable the Stored Data Protection Function.

1.4.2 Guidance Documents

The following are the guidance documents attached with this TOE. One of the guidance documents, [Japanese version.], [English version.1], [English version.2] or [English version.3], is supplied, and the name of each document corresponds to the product name (in Table 1), which depends on the sales area.

[Japanese version]

- imagio MP 3350/2550 series Operating Instructions <Security Reference> (written in Japanese)
- Notes for Users (written in Japanese)
- For imagio MP 3350/2550 series Users (written in Japanese)
- imagio MP 3350/2550 series Manuals for This Machine (written in Japanese)
- imagio MP 3350/2550 series Quick Guide (written in Japanese)
- imagio MP 3350/2550 series Operating Instructions <About This Machine> (written in Japanese)
- imagio MP 3350/2550 series Operating Instructions <Troubleshooting> (written in Japanese)
- Operating Instructions, Drivers & Utilities imagio MP 3350/2550 (written in Japanese)
- Notes for Security Functions (written in Japanese)
- Notes for Administrators: Using this Machine in a CC-Certified Environment (written in Japanese)

[English version.1]

- 9025/9025b/9033/9033b
  MP 2550/MP 2550B/MP 3350/MP 3350B
  LD425/LD425B/LD433/LD433B
  Aficio MP 2550/2550B/3350/3350B
  Operating Instructions
  About This Machine
- 9025/9025b/9033/9033b
  MP 2550/MP 2550B/MP 3350/MP 3350B
  LD425/LD425B/LD433/LD433B
  Aficio MP 2550/2550B/3350/3350B
  Operating Instructions
  Troubleshooting
- Manuals
  9025/9033/9025b/9033b
  MP 2550/ 3350/ 2550B/ 3350B
  LD425/LD433/LD425B/LD433B
  Aficio MP 2550/3350/2550B/3350B

- Manuals for Administrators
  Security Reference
  9025/9033/9025b /9033b
  MP 2550/3350/2550B/3350B
  LD425/LD433/LD425B /LD433B
  Aficio MP 2550/3350/2550B/3350B
- Manuals for Administrators
  Security Reference Supplement
  9025/9025b/9033/9033b
  MP 2550/MP 2550B/MP 3350/MP 3350B
  LD425/LD425B/LD433/LD433B
  Aficio MP 2550/2550B/3350/3350B
- Notes for Users Back Up/Restore Address Book
- Notes for Administrators: Using this Machine in a CC-Certified Environment

[English version.2]

- Manuals for This Machine
- Manuals
  General Setting Manuals
  MP 2550/3350/2550B /3350B
  Aficio MP 2550/3350/2550B/3350B
- Manuals
  Functions and Network Manuals
  MP 2550/3350/2550B /3350B
  Aficio MP 2550/3350/2550B/3350B
- Manuals for Administrators
  Security Reference
  MP 2550/3350/2550B/3350B
  Aficio MP 2550/3350/2550B/3350B
- Manuals for Administrators
  Security Reference Supplement
  9025/9025b/9033/9033b
  MP 2550/MP 2550B/MP 3350/MP 3350B
  LD425/LD425B/LD433/LD433B
  Aficio MP 2550/2550B/3350/3350B
- Notes for Users Back Up/Restore Address Book
- Notes for Administrators: Using this Machine in a CC-Certified Environment

[English version.3]

- MP 2550/MP 2550B/MP 3350/MP 3350B
  MP 2550/MP 2550B/MP 3350/MP 3350B

Aficio MP 2550/2550B/3350/3350B
MP 2550/MP 2550B/MP 3350/MP 3350B
Operating Instructions
About This Machine

- MP 2550/MP 2550B/MP 3350/MP 3350B
  MP 2550/MP 2550B/MP 3350/MP 3350B
  Aficio MP 2550/2550B/3350/3350B
  MP 2550/MP 2550B/MP 3350/MP 3350B
  Operating Instructions
  Troubleshooting
- Manuals
  MP 2550/3350/2550B/3350B
  Aficio MP 2550/3350/2550B/3350B
- Manuals for Administrators
  Security Reference
  MP 2550/3350/2550B/3350B
  Aficio MP 2550/3350/2550B/3350B
- Manuals for Administrators
  Security Reference Supplement
  9025/9025b/9033/9033b
  MP 2550/MP 2550B/MP 3350/MP 3350B
  LD425/LD425B/LD433/LD433B
  Aficio MP 2550/2550B/3350/3350B
- Notes for Users Back Up/Restore Address Book
- Notes for Administrators: Using this Machine in a CC-Certified Environment

1.4.3 User Roles

This chapter describes the roles of the involved persons for this TOE operation.

1.4.3.1 Responsible Manager for MFP

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

1.4.3.2 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 shall be assigned to one or more Administrators. One Administrator is registered and is assigned all four Administrator Roles at the factory default. 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 2 describes the Administrator jobs for each Administrator Role.

Table 2: List of Administrator Roles

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

1.4.3.3 Supervisor

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

1.4.3.4 General User

A General User is an authorised TOE user who is registered for 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.

1.4.3.5 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.

1.4.4 Logical Scope of TOE

The logical scope 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 and described in Figure 3.

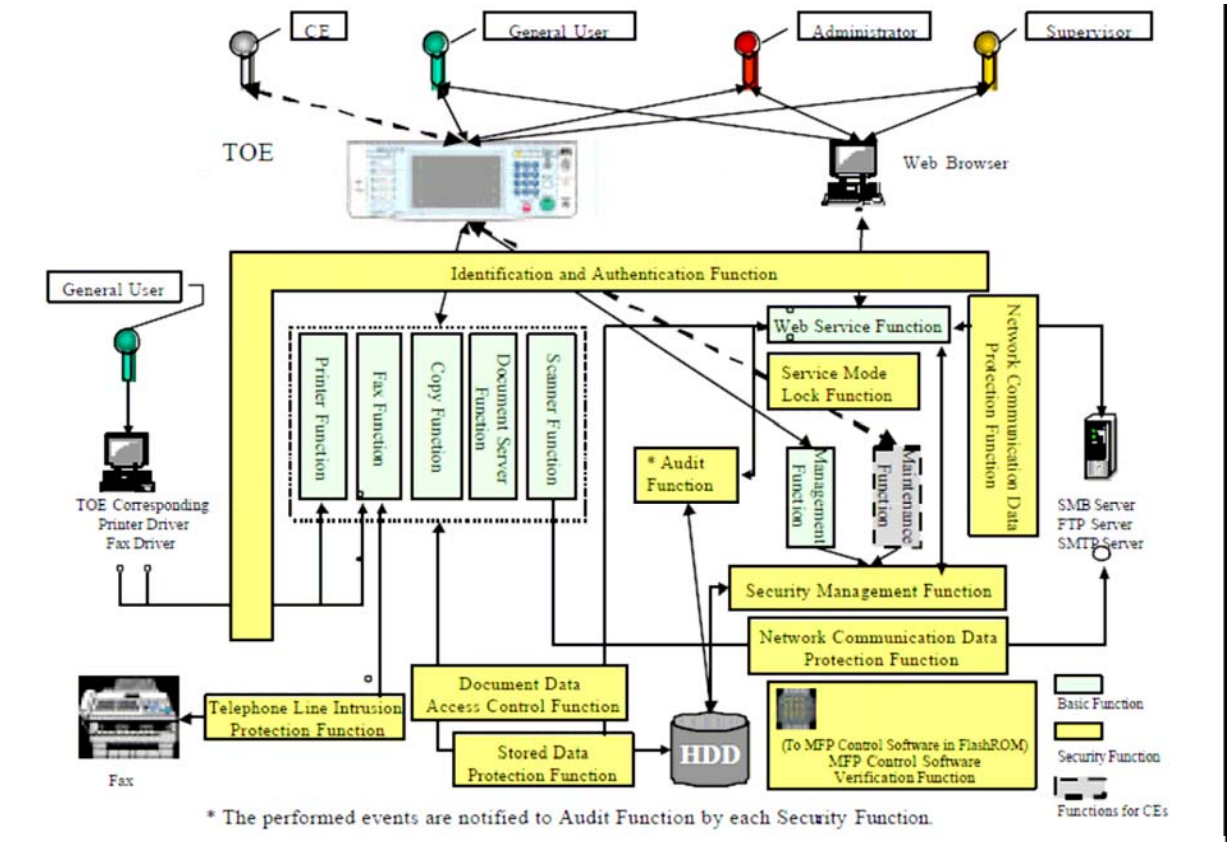

Figure 3: Logical Scope of TOE

1.4.4.1 Basic Functions

Basic functions include 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 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.

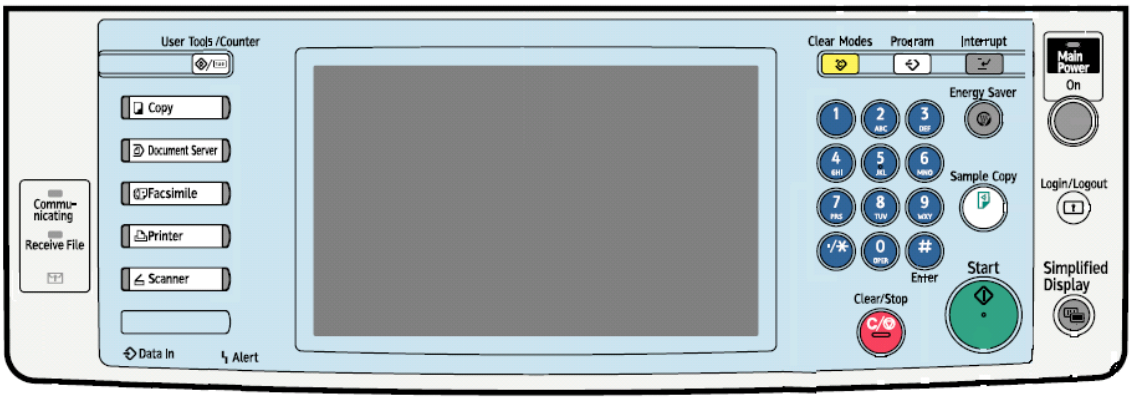

Figure 4: Operation Panel (for North America)

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 client PC. The following describes the outlines of basic functions.

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 "Document Server Function", which is also one of the basic functions and described later.

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 using 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 "Document Server Function", which is also one of the basic functions and described later.

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 out the received fax data, or converts the received fax data into the Fax Reception data and then store it in D-BOX.
The Fax Reception data stored in D-BOX can be printed and deleted using the Fax Function or "Document Server Function", which is also one of the basic functions and described later.
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 "Document Server Function", which is also one of the basic functions and described later.

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

Scanner Function

The Scanner Function is used to scan and digitise 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.

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 using 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 and deleted using the Document Server Function. When printing Document Data, the Print Settings for the stored Document Data is updated according to the operating users.

Management Function

The Management Function is used to set 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. The configurable information depends on each user role of the authorised TOE user (General User, Administrator, 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 later in "Security Management Function" in "1.4.4.2 Security Functions".

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

Web Service Function

The Web Service Function is used to operate the TOE remotely from a client PC by authorised 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 the stored Document Data in D-BOX.
   The Document Data stored using Copy Function, Document Server Function, Fax Function, and Printer Function can be printed. When printing Document Data, the Print Settings for the stored Document Data is updated according to the operating users
2. Send the stored Document Data in D-BOX.
   The Document Data stored using Scanner Function can be sent.

3. Delete the stored Document Data in D-BOX.
4. Download the stored Document Data in D-BOX.
   The Document Data stored using Scanner Function or Fax Function can be downloaded.
5. Subset of Management Functions.
6. Check the TOE status.

1.4.4.2 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.

Audit Function

The Audit Function is used to check the operation status of the TOE, or to record events, which are required to detect the security intrusion, to the audit log when the events occur. Only the Machine Administrator is allowed to read and delete the recorded audit logs. It is valid to read the audit logs using the Web Service Function, and to delete the audit logs using the Operation Panel or Web Service Function.

Identification and Authentication Function

The Identification and Authentication Function is used to make the users who attempt to use the TOE from the Operation Panel or client PC enter their user IDs and authentication information, specify and confirm the users. However, 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:

- Account Lockout: If the number of consecutive unsuccessful attempts with the same particular user ID meets the Number of Attempts before Lockout, this prevents this user ID from logging in temporarily.
- 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.
- Password Quality Maintenance: This allows the users to register only the passwords that satisfy the conditions of Minimum Password Length and Password Complexity Setting, which the User Administrator has set in advance.

Although this TOE also has other Identification and Authentication Functions, this evaluation does not cover the Identification and Authentication Functions that are not listed above.

Document Data Access Control Function

The Document Data Access Control Function is used to allow only the specific users to perform the operations on the Document Data stored in D-BOX.

The operations on Document Data include the reading operation and deleting operation. Each of these operations is as follows:

Reading Document Data: Read Document Data stored in D-BOX.

Deleting Document Data: Delete Document Data stored in D-BOX.

The File Administrator and General Users are the specific users the TOE allows to perform the operations on Document Data.

The File Administrator is allowed to delete any Document Data.

General Users are allowed to perform only the operations authorised by the operation permission on Document Data. The operation permission on Document Data includes Read-only, Edit, Edit/Delete, Full Control. Among these, the operation permission on Document Data for Edit operation is same as the Read-only operation, and updating the Print Settings is also permitted. Table 3 shows the relation between the operation permissions on Document Data and the operations on Document Data.

Table 3: Correspondence Table for Operation Permissions on Document Data and Operations on Document Data

Operation Permissions On Document Data \ Operations on Document Data	Reading Document Data	Deleting Document Data
Read-only	X	
Edit	X	
Edit/Delete	X	X
Full Control	X	X

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

The operation permission on each Document Data can be set for each General User.

Stored Data Protection Function

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

Network Communication Data Protection Function

The Network Communication Data Protection Function is used to protect Document Data and Print Data on networks from unauthorised 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.

And 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 Document Data using 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.

Security Management Function

The Security Management Function is used to allow the Administrators, Supervisor and General Users, who are successfully authenticated with "Identification and Authentication Function", which is also one of the security functions and described previously, to perform the following operations for Security Management corresponding to their user roles.

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, newly registering Document File Users for the Document Data ACL, deleting Document File Users who were previously registered for the Document Data ACL, and changing operation permissions on Document Data. 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 allowed to register another Administrator and to add an Administrator Role to another Administrator. The applicable Administrator is allowed to delete the Administrator and Administrator Role and to change Administrator ID. The applicable Administrator and Supervisor are allowed to change Administrator passwords. And an Administrator is allowed 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 user roles and authorised operations is:
   - The User Administrator is allowed to newly create, change and delete General User

Information.

- General Users are allowed to change their own General User Information that is registered for Address Book, with the exception of their user IDs even if it is their own General User Information.

4. Management of Supervisor Information
   The Supervisor is allowed to change his/her Supervisor ID and password.
5. Management of Machine Control Data
   Each Administrator is allowed to configure the data items of machine control data that corresponds to their Administrator Role (Machine Administrator, User Administrator and File Administrator).

Service Mode Lock Function

The Maintenance Function is used by CEs who receive the request from the Machine Administrator to perform the maintenance service for the TOE from the Operation Panel. 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.

Telephone Line Intrusion Protection Function

The Telephone Line Intrusion Protection Function, for the 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.

MFP Control Software Verification Function

The MFP Control Software Verification Function is used to verify the MFP Control Software is regular by checking the integrity of its executable code that is installed in FlashROM.

1.4.5 Protected Assets

This chapter describes the protected assets of this TOE (Document Data and Print Data).

1.4.5.1 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. The Document Data stored in the TOE can be deleted.

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 handle, and generate Document Data.

Storing Document Data

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

Outputting Document Data

Document Data can be output by the following five operations:

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

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

1.4.5.2 Print Data

Print Data is data in which the printed or faxed output image is written, and is generated from the 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 on the Internal Network path is protected from leakage when it is sent from a client PC to the TOE, and if there is tampering, it is detected.

2 Conformance Claims

This chapter describes the conformance claim.

2.1 CC Conformance Claim

The CC conformance claim of this ST and TOE as follows:

- CC Version for which this ST claims the conformance

  Part 1:

  Introduction and general model September 2006 Version 3.1 Revision 1 (Japanese translation Ver.1.2) CCMB-2006-09-002

  Part 2:

  Security functional components September 2007 Version 3.1 Revision 2 (Japanese translation Ver.2.0) CCMB-2007-09-002

  Part 3:

  Security assurance components September 2007 Version 3.1 Revision 2 (Japanese translation Ver.2.0) CCMB-2007-09-003

- Functional requirements: Part 2 conformant
- Assurance requirements: Part 3 conformant

2.2 PP Claims, Package Claims

This ST and TOE do not conform to any PPs.
This ST claims to be conformant to the following package shown below.

Package: EAL3 conformant.

2.3 Conformance Rationale

Since this ST does not conform to any PPs, there is no applicable PP rationale.

3 Security Problem Definition

This chapter describes the Threats, Organisational Security Policies and Assumptions.

3.1 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 the attacks by persons who have the knowledge of disclosed information about the TOE operation, and the attackers will have the basic level of attack potential.

T.ILLEGAL_USE (Malicious Usage of TOE)

Attackers may read or delete the Document Data by gaining unauthorised 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)

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

T.ABUSE_SEC_MNG (Abuse of Security Management Function)

Persons who are not authorised 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 unauthorised access to the TOE from telephone lines.

3.2 Organisational Security Policies

The following security policy is assumed for the organisations 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.

3.3 Assumptions

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

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

The Administrators will have adequate knowledge to operate the TOE securely in the roles assigned to them, and guide General Users to 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.

4 Security Objectives

This chapter describes the Security Objectives for TOE, Security Objectives for Operational Environment and Security Objectives Rationale.

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 **(Identification and Authentication for Users)**

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 operation permission for 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 of 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 (Prevention of Intrusion from Telephone Line)

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

4.2 Security Objectives for Operational Environment

This chapter describes the security objectives for the operational environment.

OE.ADMIN (Trusted Administrator)

The Responsible Manager for MFP shall select trusted persons as Administrators, and provide them with the education programmes 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 programmes 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 the External Networks such as the Internet, the organisation that manages the operation of the Internal Networks shall close the unnecessary ports between the External and Internal Networks. (E.g., Firewall set up.)

4.3 Security Objectives Rationale

This chapter describes the security objectives rationale.

By the following description, if all security objectives are achieved, the security problems as defined in "3 Security Problem Definition" are solved: all threats are countered, all organisational security policies are achieved, and all assumptions are accomplished.

4.3.1 Tracing

This chapter describes the correspondence relation between the previously described "3.1 Threats", "3.2 Organisational Security Policies" and "3.3 Assumptions", and either "4.1 Security Objectives for TOE" or "4.2 Security Objectives for Operational Environment" with Table 4. The "X" in the table indicates that each of the following TOE Security Environments and the security objectives correspond.

As Table 4 shows, it is obvious that each security objective corresponds to one or more threats,

organisational security policies and assumptions. And the security objectives do not correspond to the assumptions (as the shaded region in Table 4 shows).

Table 4: 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							

4.3.2 Tracing Validity

The following are the rationale for each security objective being appropriate to satisfy "3.1 Threats", "3.2 Organisational Security Policies" and "3.3 Assumptions".

A.ADMIN (Administrators' Assumption)

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

By OE.ADMIN, the Responsible Manager for MFP selects trusted persons as Administrators, and provides them with the education programmes according to their Administrator Roles. The educated Administrators 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. Therefore, A.ADMIN is accomplished.

A.SUPERVISOR (Supervisor's Assumption)

A.SUPERVISOR presupposes that the Supervisor has adequate knowledge to operate the TOE securely in the role assigned to him/her, and does not carry out any malicious acts using Supervisor permissions.
By OE.SUPERVISOR, Responsible Manager for MFP selects a trusted person as the Supervisor and provides the Supervisor with the education programmes according to the role of Supervisor. 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 TOE-connected networks are connected to the External Networks such as the Internet.
By OE.NETWORK, when connecting the Internal Networks, to which the TOE is connected, to the External Networks such as the Internet, the organisations that manage the operation of the Internal Networks close the unnecessary ports between 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 identification and authentication of users with O.I&A prior to their use of the TOE security functions, and allows the successfully authenticated user to use the functions for which the user has the operation permission. In addition, the TOE records the performance of O.I&A as audit logs by O.AUDIT, and provides only the Machine Administrator with the function to read the audit logs so that 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 authorised users identified by O.I&A to access to the Document Data according to the operation permission on Document Data that are assigned to the authorised users' roles and the authorised users by O.DOC_ACC. Specifically, if the authorised user is the General User, the TOE allows the General User to perform operations on Document Data according to the operation permissions for the Document Data that are assigned to the General User, and if the authorised user is the File Administrator, 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. The TOE also 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 so that 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 Document Data by O.MEM.PROTECT that 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 so that the Machine Administrator detects afterwards whether or not O.MEM.PROTECT was successfully performed.
Therefore, the TOE can counter T.SALVAGE.

T.TRANSIT (Interception 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. In addition, 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 so that 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 so that 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 counter this organisational security policy, the TOE provides the function to verify the integrity of MFP Control Software, which is installed in FlashROM, with the TOE users by O.GENUINE.
Therefore, the TOE can counter P.SOFTWARE.

5 Extended Components Definition

In this ST and TOE, there are no extended components, i.e., the new security requirements and security assurance requirements that are not described in the CC, which is claimed the conformance in "2.1 CC Conformance Claim".

6 Security Requirements

This chapter describes the Security Functional Requirements, Security Assurance Requirements, and Security Requirements Rationale.

6.1 Security Functional Requirements

This chapter describes the TOE security functional requirements to accomplish the security objectives defined in "4.1 Security Objectives for TOE". The security functional requirements are quoted from the ones defined in the CC Part 2.

The part with Assignment and Selection defined in the CC Part 2 are identified with **[bold face and brackets].**

6.1.1 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	<Individually defined auditable events>

Functional Requirements	Actions which should be auditable	Auditable events of TOE
	of the activity. b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	1. HDD cryptographic key generation (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 (e.g. re-enabling of a terminal).	a) Minimal 1. Starting Lockout 2. Lockout release
FIA_ATD.1	None	-

Functional Requirements	Actions which should be auditable	Auditable events of TOE
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 Administrator Authentication Information (Outcome: Success/Failure) 4. Changing Supervisor Authentication Information (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 information of General Users. 2. Changing authentication information of General Users.

Functional Requirements	Actions which should be auditable	Auditable events of TOE
		3. Deleting authentication information of General Users. 4. Changing Administrator Authentication Information. 5. Changing Supervisor Authentication Information. 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_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 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.	<Individually defined auditable events> 1. Communication with remote users (Outcome: Success/Failure)

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[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 in the audit trail 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 Action in case of possible audit data loss.

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.

6.1.2 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.

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 bits

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.

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 Operation

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

6.1.3 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: List of Subjects, Objects, and Operation among Subjects and Objects in** Table 8**]**.

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

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

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	- Document Data ACL

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 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 Document Data	When General User ID, associated with General User process, matches either 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 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 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 grant 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

(Notes: Transferring means that the Controller Board receives the data, which is received from a telephone line, from Fax Unit.)

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

(Notes: Data type is the type of data received from a telephone line and indicates either the fax data or non-fax data.)

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

FDP_IFF.1.5 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]**.

6.1.4 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 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 the 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 defined number of unsuccessful authentication attempts has been **[selection: met]**, 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 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 of the Locked out Users 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 digit numbers:

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) Rule:

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

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication.

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: displaying a dummy letter (*: asterisk, or -: black dot) for one letter of passwords on authentication feedback]** to the user while the authentication is in progress.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification.

Dependencies: No dependencies.

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

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].**

6.1.5 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 (a data item of General User Information)	Query, newly create, delete	- User Administrator
	Query	- General Users
Administrator IDs	Newly create	- Administrators
	Query, change	- Administrators who owns the applicable Administrator IDs
	Query	- Supervisor
Administrator Roles	Query, add, delete	- Administrators who are assigned the applicable 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 applicable Document Data
Document Data Default ACL (a data item of	Query, modify	- User Administrator - The General User who create the applicable

Security attributes	Operations	User roles
General User Information)		Document Data

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: 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: Characteristics of Static Attribute Initialisation

Object	Security attribute associated to object	Default value and its characteristic 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 applicable 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 (a data item of General User Information)	Newly create, change, delete	User Administrator

TSF data	Operations	User roles
	Change	Applicable General Users of General User Information
Supervisor Authentication Information	Change	Supervisor
Administrator Authentication Information	Change	Supervisor Applicable Administrator of Administrator Authentication Information
Number of Attempts before Lockout	Query, modify	Machine Administrator
Setting for Lockout Release Timer	Query, modify	Machine Administrator
Lockout time	Query, modify	Machine Administrator
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
Password Complexity Setting	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

TSF data	Operations	User roles
S/MIME User Information (a data item of General User Information)	Query, newly create, delete, change	User Administrator Applicable 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 Function

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **[assignment: List of 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	None	-
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	a) Managing the attributes used to make explicit access based decisions.	None: The attributes (data types) used to make explicit access based decisions are fixed, and there are also no interfaces to change.
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

Functional requirements	Management requirements	Management items
		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) Management of the metric used to verify the secrets.	Security Management Function (Management of Machine Control Data): The User Administrator manages the following setting of the machine control data: - Minimum Password Length - Password Complexity Setting
FIA_UAU.2	a) Management of the authentication data by an Administrator; b) 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 Administrator Authentication Information by Administrators. - Security Management Function (Management of Administrator Information): new registration of Administrators by Administrators. - Security Management Function (Management of Administrator Information): management of Administrator Authentication Information by Supervisor. - Security Management Function (Management of Supervisor Information): management of Supervisor Authentication Information by Supervisor.
FIA_UAU.7	None	-
FIA_UID.2	a) Management of the user identities.	- Security Management Function (Management of General User Information): management of General User IDs by the User Administrator. - Security Management Function

Functional requirements	Management requirements	Management items
		(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. b) Management of rules by which security attributes inherit specified values.	a) Management of Administrator Roles by Administrators. b) None: No rules by which security attributes inherit specified values.
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; c) Management of rules by which security attributes inherit specified values.	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. c) None: No rules by which security attributes inherit specified values.
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_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

Functional requirements	Management requirements	Management items
		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.

6.1.6 Class FPT: Protection of the TSF

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.

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

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.

6.1.7 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 another 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 **[selection: modification, 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 requiring 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)

6.2 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	
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.3	Authorisation controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

6.3 Security Requirements Rationale

This chapter describes the rationale for the security requirements.
As described below, if all security functional requirements are satisfied, the security objectives defined in "4.1 Security Objectives for TOE" are achieved.

6.3.1 Tracing

Table 23 shows the relation between the TOE security functional requirements and TOE security objectives. The "X" in the table indicates that the each of the TOE security functional requirements and the TOE security objectives correspond.

Table 23 shows that each TOE security functional requirement corresponds to one or more TOE security objectives.

Table 23: 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_STM.1	X							
FPT_TST.1					X		X	
FTP_ITC.1						X		
FTP_TRP.1						X		

6.3.2 Tracing Validity

This chapter describes how the TOE security objectives are accomplished by the TOE security functional requirements corresponding to the TOE security objectives in Table 23.

O. AUDIT Audit

The following are the rationale for the functional requirements that correspond to O.AUDIT in Table 23 being appropriate to satisfy O.AUDIT.

a) Record audit logs
To accomplish O.AUDIT, it is necessary to record the performance of security functions as 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 unauthorised deletion and prevents the unauthorised 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.

O.I&A User Identification and Authentication

The following are the rationale for the functional requirements that correspond to O.I&A in Table 23 being appropriate to satisfy O.I&A.

a) Identify and authenticate users before users use the TOE.
To accomplish O.I&A, 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 dot) 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.

O. DOC_ACC Access Control to the Protected Assets

The following are the rationale for the functional requirements that correspond to O.DOC_ACC in Table 23 being appropriate to satisfy O.DOC_ACC.

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 Data set for each type of subjects associated with the users, and each security attribute associated with the subject.
For this, if the Administrator Role associated with Administrator process is the File Administrator, FDP_ACC.1 and FDP_ACF.1 allow the Administrator process to delete 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 that 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. The permitted operations follow the operation permission on Document Data set for each General User ID in the Document Data ACL.

O. MANAGE Security Management

The following are the rationale for the functional requirements that correspond to O.MANAGE in Table 23 being appropriate to satisfy O.MANAGE.

a) Management of security attributes.

To accomplish O.MANAGE, the management of the security attributes shall be specified to the specific users. In addition, a specified 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 query, newly create, and change General User IDs,
- General Users to query General User IDs,
- Administrators to query and newly create Administrator IDs,
- Administrators to query and change their own Administrator IDs,
- Supervisor to query Administrator IDs,
- Administrators to query, add, and delete the same Administrator Roles assigned to themselves,
- Supervisor to query and change Supervisor ID,
- The File Administrator, Document File Owners and the General Users who have the full control operation permission for the Document Data to query and modify its Document Data ACL, and
- The User Administrator and the General Users who have the full control operation permission for the Document Data to query and modify its Document Data Default ACL.

FMT_MSA.3 sets 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:

- The Machine Administrator to query 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 query HDD cryptographic keys, and to query audit logs and delete the entire audit logs,
- Authorised TOE users to query the date and time of system clock and Service Mode Lock setting,
- The User Administrator to query and set the Minimum Password Length, Password Complexity Setting, and Lockout Flag for General Users,
- The User Administrator and the applicable General Users to set the authentication information of the General Users, newly create, delete, and change S/MIME User Information,

- The User Administrator and General Users to query S/MIME User Information and destination information for Deliver to Folder,
- Supervisor to query and set Lockout Flag for Administrators, and set Supervisor Authentication Information, and
- Supervisor and the applicable Administrators to change Administrator 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) Authorised use of Security Management Functions
To accomplish O.MANAGE, the authorised users shall be associated with the security management roles and the operation permissions for the Security Management Functions and be maintained since the use of the Security Management Functions depends on the authorised user roles.
FMT_SMR.1 associates the authorised users with General User, one of four Administrator Roles (User Administrator, Machine Administrator, File Administrator and Network Administrator), or the Supervisor role, and maintains such associations.

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

The following are the rationale for the functional requirements that correspond to O.MEM.PROTECT in Table 23 being appropriate to satisfy O.MEM.PROTECT.

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 the Document Data is read with the normal 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 that corresponds to FIPS197. Additionally, FTP_TST.1 tests the validity of encryption keys and the performance of Ic Hdd that performs the encryption operation at the TOE start-up, and it prevents storing Document Data on HDD without being encrypted.

O.NET.PROTECT Protection for Network Communication Data

The following are the rationale for the functional requirements that correspond to O.NET.PROTECT in Table 23 being appropriate to satisfy O.NET.PROTECT.

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 this, FTP_ITC.1 uses the IPSec protocol for Deliver to Folders on either an FTP server or SMB server from the TOE, protects Document Data on networks from leakage, and detects tampering.

FTP_TRP.1 also protects Document Data on networks from leakage and detects the tampering by using a trusted path, which is described later, between the TOE and the remote users. For sending by e-mail from the TOE to client PC, Document Data or Print Data on network is protected from leakage and tampering is detected by 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.

O.GENUINE Protection of Integrity of MFP Control Software

The following are the rationale for the functional requirements that correspond to O.GENUINE in Table 23 being appropriate to satisfy O.GENUINE.

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, FPT_TST.1 tests the integrity of the executable code of MFP Control Software, which is installed in FlashROM, and verifies its integrity at the TOE start-up.

O.LINE_PROTECT Protection for Intrusion from Telephone Line

The following are the rationale for the functional requirements that correspond to O.LINE_PROTECT in Table 23 being appropriate to satisfy O. LINE_PROTECT.

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

6.3.3 Dependency Analysis

Table 24 shows the correspondence status of the dependencies in this ST for the TOE security functional requirements.

Table 24: 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

TOE Security Functional Requirements	Dependencies claimed by CC	Dependencies satisfied in ST	Dependencies not satisfied in ST
	FCS_COP.1] FCS_CKM.4		
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1	FCS_CKM.4
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
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_STM.1	None	None	None
FPT_TST.1	None	None	None
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 the area that 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 destructions using standard measures 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.

6.3.4 Security Assurance Requirements Rationale

This TOE is a commercially available product. It is assumed that the TOE is used in general offices, and that the attackers have the basic attack potential for this TOE.

Architectural design (ADV_TDS.2) is adequate to show the validity of commercially available products. A high attack potential is required for attacks that circumvent or tamper the TSF, which is not covered by this evaluation. Therefore, the vulnerability analysis (AVA_VAN.2) 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 term and cost for the evaluation, the evaluation assurance level of EAL3 is appropriate for this TOE.

7 TOE Summary Specification

This chapter describes the summary specification of the security functions of this TOE.

7.1 TOE Security Function

The TOE provides the following TOE security functions to satisfy the Security Functional Requirements described in Chapter "6.1".

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 "6.1" as shown in Table 25.

Table 25: 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_STM.1	X								
FPT_TST.1						X			X
FTP_ITC.1							X		
FTP_TRP.1							X		

The following are the security functional requirements that correspond to these TOE security functions.

7.1.1 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 following are the explanations of each functional item in "SF.AUDIT Audit Function" and their corresponding security functional requirements.

7.1.1.1 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 generating auditable events that require additional information for audit. Table 26 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 26: Auditable Events and Auditable Information

Auditable events	Audit logs	
	Basic Audit Information	**Expanded Audit Information**
Starting Audit Function (*1)	- Date/time of the events - Types of the events (Auditable events in this table) - Subject identity (*4) - Outcome	-
Ending Audit Function (*1)		-
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 (include 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 Expanded 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 Basic Audit Information, and when the recording events occur due to the TOE, IDs that do not duplicate the user IDs but can identify systems are set.
Since there are no interfaces on the TOE for modifying audit logs, unauthorised modification for the audit logs are not performed and the Machine Administrator who can delete the audit logs will not carry out any malicious acts using Administrator privileges.
From the above, FAU_GEN.1 (Audit data generation), FAU_STG.1 (Protected audit trail storage) and FAU_STG.4 (Prevention of audit data loss) are accomplished.

7.1.1.2 Reading Audit Logs

The TOE allows only the Machine Administrator to read the audit logs as text format from Web Service Function.
From the above, FAU_SAR.1 (Audit review), FAU_SAR.2 (Restricted audit review) and FMT_MTD.1 (Management of TSF data) are accomplished.

7.1.1.3 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.
From the above, FAU_SAR.1 (Audit review), FAU_SAR.2 (Restricted audit review) and FMT_MTD.1 (Management of TSF data) are accomplished.

7.1.1.4 Time stamps

The TOE provides the data/time of the events of the audit logs by using the date and time of the system clock inside the TOE.
From the above, FPT_STM.1 (Reliable time stamps) is accomplished.

7.1.2 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 authorised users to operate the TOE according to their roles and authorisation.
The following are the explanations of each functional item in "SF.I&A User Identification and Authentication Function" and their corresponding security functional requirements.

7.1.2.1 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 27 shows the authentication methods for each user role.

Table 27: User Roles and Authentication Methods

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

From the above, FIA_ATD.1 (User attribute definition), FIA_UAU.2 (User authentication before any action), FIA_UID.2 (User identification before any action), FIA_USB.1 (User-subject binding), FMT_SMF.1 (Specification of Management Functions) and FMT_SMR.1 (Security Roles) are accomplished.

7.1.2.2 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 "7.1.2.1 User Identification and Authentication". When a user ID's consecutive numbers of times of failure

meets the Number of Attempts before Lockout, the TOE Lockouts the user 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 "7.1.2.1 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, (1) or (2), 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 28, are allowed to release Lockout using 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 28: Unlocking Administrators for Each User Role

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

From the above, FIA_AFL.1 (Authentication failure handling) and FMT_SMF.1 (Specification of Management Functions) are accomplished.

7.1.2.3 Password Feedback Area Protection

The TOE displays a protection character (*: asterisk or -: black dot) in place of each password character entered from the Operation Panel or web browser of client PC by General Users, Administrators, and a Supervisor.
From the above, FIA_UAU.7 (Protected authentication feedback) is accomplished.

7.1.2.4 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 using the characters described below (1).
It checks if the password to be registered or changed meets the condition (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 screen.

(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) Rule:

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

From the above, FIA_SOS.1 (Verification of secrets) and FMT_SMF.1 (Specification of Management Functions) are accomplished.

7.1.3 SF.DOC_ACC Document Data Access Control Function

The TOE controls the access to the operations by users to store, read and delete the Document Data. The access control to the Document Data displays the only accessible Document Data on the Operation Panel or client PC, where the authorised users are authenticated, based on the assigned authorisation to user roles of the authorised users, who are authenticated with Identification and Authentication Function, or on the assigned authorisation to each user. This chapter describes the access control to the Document Data for each user role.
The following are the explanations of each functional item in "SF.DOC_ACC Document Data Access Control Function" and their corresponding security functional requirements.

7.1.3.1 Operations on Document Data by General Users

The TOE allows General Users to store Document Data, and allows them to read 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 operation permissions for Document Data. If a General User ID associated with the General User process is registered for the Document Data ACL, the TOE allows that General User ID to perform the operations according to the user ID's operation permission for Document Data.
Table 3 shows the relation between the operation permissions on Document Data and the operations on

Document Data.
Table 29 shows the value of the Document Data ACL when storing Document Data.

Table 29: Initial Value for Document Data ACL

Type of Document Data	Initial value for Document Data ACL
Document Data stored by General User	Document Data Default ACL

From the above, FDP_ACC.1 (Subset access control) and FDP_ACF.1 (Security attribute based access control) are accomplished.

7.1.3.2 Operations on Document Data by File Administrator

If the login user from the Operation Panel or Web Service Function is the File Administrator, the TOE allows the File Administrator 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.
From the above, FDP_ACC.1 (Subset access control) and FDP_ACF.1 (Security attribute based access control) are accomplished.

7.1.4 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 following are the explanations of each functional item in "SF.SEC_MNG Security Management Function" and their corresponding security functional requirements.

7.1.4.1 Management of Document Data ACL

Management of the Document Data ACL allows only specific users to perform operation 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 operation permission on Document Data of Document File Owners, newly registering and deleting the Document File Users, and changing the operation permission on Document Data of Document File Users. The users who are authorised to perform each of these operations are specified. Table 30 shows the relation between operations on the Document Data ACL and the authorised users for the operations.

Table 30: Operations on the Document Data ACL and Authorised Operators

Operations on Document Data ACL	Authorised operators
Change the Document File Owners	- File Administrator
Change the operation permission on Document Data of Document File Owners	- File Administrator - Document File Owners - General Users with full control authorisation
Newly register the Document File Users	- File Administrator

	- Document File Owners - General Users with full control authorisation
Delete the Document File Users	- File Administrator - Document File Owners - General Users with full control authorisation
Change the operation permission on Document Data of Document File Users	- File Administrator - Document File Owners - General Users with full control authorisation

If the login user is the File Administrator, the TOE allows the File Administrator 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.
If the login user is a General User, it allows the General User to perform the operations only on the Document Data ACL for which the General User is set as the full control authorised user, including changing the operation permission on Document Data of the Document File Owners, newly registering Document File Users, deleting Document File Users, and changing the operation permission on Document Data of Document File Users. However, even if the full control authorisation is not set for Document File Owners, Document File Owners are allowed to perform the operations on the Document Data ACL of the Document Data owned by the Document File Owners, including changing the operation permission on Document Data of the Document File Owners, newly registering and delete Document File Users, and changing the operation permission on Document Data of Document File Users.
From the above, FMT_MSA.1 (Management of security attributes), FMT_MSA.3 (Static attribute initialisation) and FMT_SMF.1 (Specification of Management Functions) are accomplished.

7.1.4.2 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, Administrator Authentication Information, and Administrator Roles. The operations on Administrator Information include newly creating, querying and changing Administrator IDs, changing Administrator Authentication Information, querying, adding and deleting Administrator Roles. The users who are authorised to perform each of these operations are specified. Table 31 shows the relation between the operations on Administrator Information and the authorised users for the operations on Administrator Information.

Table 31: Access to Administrator Information

Operations on Administrator Information	Authorised operators
Newly create Administrator IDs	Administrators
Change Administrator IDs	The Administrator themselves
Query Administrator IDs	The Administrator themselves, Supervisor
Change Administrator	The Administrator themselves, Supervisor

Operations on Administrator Information	Authorised operators
Authentication Information	
Add and query Administrator Roles	The Administrators who are already assigned that Administrator Role
Delete Administrator Roles	The Administrators who are already assigned that Administrator Role However, the operation cannot be performed if no other Administrators have the Administrator Role.

If the login user is the Administrator or Supervisor, the TOE allows the Administrator/Supervisor to perform the operations shown in Table 31, respectively.
From the above, FIA_USB.1 (User-subject binding), FMT_MSA.1 (Management of security attributes), FMT_MTD.1 (Management of TSF data), FMT_SMF.1 (Specification of Management Functions) and FMT_SMR.1 (Security roles) are accomplished.

7.1.4.3 Management of Supervisor Information

Management of Supervisor Information allows only the Supervisor to query and change Supervisor ID, and to change Supervisor authentication information from the Operation Panel or Web Service Function.
If the login user from the Operation Panel or client PC is the Supervisor, the TOE allows the Supervisor to query and change Supervisor ID and to change Supervisor authentication information.
From the above, FMT_MSA.1 (Management of security attributes), FMT_MTD.1 (Management of TSF data), FMT_SMF.1 (Specification of Management Function) and FMT_SMR.1 (Security roles) are accomplished.

7.1.4.4 Management of General User Information

Management of General User Information allows the specific users to perform the all or some of operations to newly create, change and delete General User Information from the Operation Panel or Web Service Function and General User Information includes the General User IDs, authentication information of General Users, Document Data Default ACL and S/MIME User Information.
If the login user from the Operation Panel or Web Service Function is the User Administrator or General User, the TOE allows the User Administrator/General User to perform the operations shown in Table 32.

Table 32: Authorised Operations on General User Information

Operations on General User Information	Authorised operators
Newly Create General User Information for Address Book (General User ID, authentication information of General Users and S/MIME User Information)	User Administrator
Edit General User Information registered for Address Book (Authentication information of General Users, Document	User Administrator The General User themselves

Operations on General User Information	Authorised operators
Data Default ACL, S/MIME User Information)	
Query General User Information registered for Address Book (General User ID, Document Data Default ACL, S/MIME User Information)	User Administrator The General User themselves
Query General User Information registered for Address Book (General User ID, S/MIME User Information)	General User
Delete General User Information registered for Address Book (General User ID, authentication information of General Users, S/MIME User Information)	User Administrator
Delete General User Information registered for Address Book (S/MIME User Information)	The General User who owns the applicable S/MIME User Information

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 authorised operations on Document Data of that General User are to read the Document Data and to modify the Document Data ACL.

From the above, FMT_MSA.1 (Management of security attributes), FMT_MTD.1 (Management of TSF data), FMT_SMF.1 (Specification of Management Function) and FMT_SMR.1 (Security roles) are accomplished.

7.1.4.5 Management of Machine Control Data

Management of Machine Control Data allows only the 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 33 shows the range of values that can be set, the operations, the authorised setter, and the operation interfaces allowed by the TOE, for each Machine Control Data.

The TOE allows the User Administrator and General Users to query the destination information for Deliver to Folder.

Table 33: List of Administrator for Machine Control Data

Machine control data items	Range of values	Operations	Authorised setter	Operation interfaces
Number of Attempts before Lockout	An integer 1-5 (times)	Query, modify	Machine Administrator	Web Service Function
Setting for Lockout Release Timer	Active or Inactive	Query, modify	Machine Administrator	Web Service Function
Lockout time	An integer 1-9999 (minutes)	Query, modify	Machine Administrator	Web Service Function
Minimum Password	An integer 8-32	Query,	User Administrator	Operation

Machine control data items	Range of values	Operations	Authorised setter	Operation interfaces
Length	(digits)	modify		Panel
Password Complexity Setting	Level 1 or Level 2	Query, modify	User Administrator	Operation Panel
Date and time of system clock	Date, time (hour, minute, second)	Query, modify	Machine Administrator	Operation Panel Web Service Function
		Query	General Users, User Administrator, Network Administrator, File Administrator, Supervisor	
Lockout Flag for General Users	Inactive	Query, modify	User Administrator	Web Service Function
Lockout Flag for Administrators	Inactive	Query, modify	Supervisor	Web Service Function
Lockout Flag for Supervisor	Inactive	Query, modify	Machine Administrator	Web Service Function

From the above, FIA_AFL.1 (Authentication failure handling), FMT_MTD.1 (Management of TSF data), FMT_SMF.1 (Specification of Management Function) and FMT_SMR.1 (Security roles) are accomplished.

7.1.5 SF.CE_OPE_LOCK Service Mode Lock Function

Service Mode Lock Function controls the use of the maintenance functions by CEs according to the value of Service Mode Lock Function settings 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 authorised users with the function to view the setting value. If the Service Mode Lock Function is set to "Off", the TOE allows CEs to operate the Maintenance Functions, and if the Service Mode Lock Function is set to "On", it does not.

From the above, FMT_MTD.1 (Management of TSF data) is accomplished.

7.1.6 SF.CIPHER Encryption Function

The TOE encrypts the Document Data to be stored on HDD.
The following are the explanations of each functional item in "SF.CIPHER Encryption Function" and their corresponding security functional requirements.

7.1.6.1 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 on HDD and to be read from HDD, and Document Data are encrypted and decrypted by the TOE in a similar way.

The HDD encryption keys are generated by the Machine Administrator. If the login user is the Machine Administrator, the TOE provides the screen to generate the 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-AIS31, and when writing the data on the HDD/reading the data from the HDD, it performs the encryption operations shown in Table 34.

Table 34: 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 bits
Reading data from HDD	Decrypt			

The HDD encryption keys can be also printed. If the login user is the Machine Administrator, the TOE provides the Machine Administrator with the screen 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.
From the above, FCS_CKM.1 (Cryptographic key generation), FCS_COP.1 (Cryptographic operation), FMT_MTD.1 (Management of TSF data) and FPT_TST.1 (TSF testing) are accomplished.

7.1.7 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 following are the explanations of each functional item in "SF.NET_PROT Network Communication Data Protection Function" and their corresponding security functional requirements.

7.1.7.1 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.
From the above, FTP_TRP.1 (Trusted path) is accomplished.

7.1.7.2 Printing and Faxing from Client PC

When receiving requests for printing or fax transmission from a client PC, the TOE communicates with the client PC using the SSL protocol as a trusted path.
From the above, FTP_TRP.1 (Trusted path) is accomplished.

7.1.7.3 Sending by E-mail from TOE

When sending Document Data by e-mail from the TOE to client PC, the TOE attaches the Document Data to e-mail and send the e-mail with S/MIME. The destination information of S/MIME is managed as S/MIME User Information of General User Information, and users send e-mail only using this managed destination information.
From the above, FTP_TRP.1 (Trusted path) is accomplished.

7.1.7.4 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 only using this managed destination information.
From the above, FTP_ITC.1 (Inter-TSF trusted channel) is accomplished.

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

When the type of received data from a telephone line is the fax data, the TOE passes the received data to the Controller Board. When the TOE receives the non-fax data, it does not pass the data to the Controller Board but instead it discards the data.

From the above, FDP_IFC.1 (Subset information flow control) and FDP_IFF.1 (Simple security attributes) are accomplished.

7.1.9 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, at the TOE start-up.
The TOE verifies the integrity of the executable code of MFP Control Software at the TOE start-up. If the integrity is verified, it makes the TOE available for users. If not, it indicates that the MFP Control Software is not correct.
From the above, FPT_TST.1 (TSF testing) is accomplished.

8 Appendix

8.1 Terminology Description

Table 35 shows the definitions of specific terms for clearly understanding of this ST.

Table 35: Specific Terms Used in this ST

Terms	Definitions
D-BOX	A storage area for Document Data on the HDD.
FTP Server	A server for sending files to client PC and receiving files from client PC using File Transfer Protocol.
HDD	An abbreviation for Hard Disk Drive. Indicates the HDD installed in the TOE.
Ic Hdd	A hardware device that encrypts the data to be written on HDD and decrypts the data to be read from HDD.
Ic Key	A chip that contains a microprocessor for encryption processing and EEPROM that stores a private key for secure communication. It keeps the keys for validity authentication and encryption processing and the random number generator.
IP-Fax	A function that sends and receives document files between two faxes that are directly connected to 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.
MFP	An abbreviation for digital multi function product. Also indicates the TOE in this ST.
Responsible Manager for MFP	A person in an organisation in which MFPs are placed and who has the authority to assign Administrators and a Supervisor for the MFP (or the person who is responsible for the organisation). 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.
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.
MFP Control Data	A generic term for a set of parameters that control the operation of MFP.
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.
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.
SMB Server	A server for sharing files with client PC using Server Message Block Protocol.
SMTP Server	A server for sending E-mail using Simple Mail Transfer Protocol.
Address Book	A database containing General User Information for each General User.

Terms	Definitions
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.
Internet Fax	A function that reads the fax original, then converts the scanned document images to e-mail format and transit the data over the Internet to the machine that has an e-mail address.
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.
Fax Reception Process on Controller Board	MFP Control Software that is on the Controller Board, receives the information about the status of fax communication from Fax Unit, and provides Fax Unit with the instruction on fax communication.
Supervisor	One of the authorised TOE users who uses the basic functions of the TOE.
Supervisor ID	One of the data items of Supervisor Information, and also an identification code to identify and authenticate the Supervisor. Indicates the Supervisor's login name for this TOE.
Supervisor Authentication Information	The password to identify and authenticate the Supervisor.
Network Administration	One of the Administrator Roles that manages the TOE network connections. The Network Administrator is a person who has the network management role.
Network Control Data	MFP Control Data that is used to connect MFP to networks.
Minimum Password Length	The minimum number of digits that can be registered for passwords.
Password Complexity Setting	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 Level 1 and Level 2 for Password Complexity Setting. 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.
Fax Process on Fax Unit	The Control Software on Fax Unit. It provides the MFP Control Software on Controller Board with the information about the status of fax communication, and controls the fax communication according to the instruction from the MFP Control Software on Controller Board.
Deliver to Folder	A function that sends the Document Data to folders in an SMB server or FTP server from the TOE via networks.
Sending by E-mail	A function that sends e-mail with the attached Document Data from the TOE.
Memory Transmission	A function that stores the scanned data of the original in memory, and then dials and faxes the data.
User Administration	One of the Administrator Role that manages General Users. The User Administrator is a person who has the user management role.
Number of Attempts before Lockout	The number of consecutive failed password authentications using the same user ID that results in that user's Lockout.

Terms	Definitions
Lockout	A function that prohibits the access for the specific user IDs to the TOE.
Lockout Flag	A data that is assigned to each authorised user. The Lockout Flag for the Locked out User is set to "Active", and the one for the released Locked out User is set to "Inactive". The Administrators or Supervisor who are allowed 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".
Setting for Lockout Release Timer	Setting that enables or disables the timed release operation 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.
General User	One of the authorised TOE users who uses the basic functions of the TOE.
General User ID	One of the data items of General User Information, and also an identification code to identify and authenticate the General Users. Indicates the General User's login name for this TOE.
General User Information	A database containing the information about the General Users as data item. The data items include the General User ID, General User Authentication Information, Document Data Default ACL, and S/MIME User Information.
General User Authentication Information	The password to identify and authenticate the General User.
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 Unit or USB Ports.
Print Settings	Print Settings for printed output, including paper size, printing magnification and customised information (such as duplex and layout). The Print Settings for stored Document Data is updated according to the user who prints out that Document Data.
External Networks	Networks that are not managed by the organisation that manages the MFP. Generally indicates the Internet.
Administrator	One of the authorised TOE users 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.
Administrator ID	One of the data items of Administrator Information, and also an identification code to identify and authenticate the Administrator. Indicates the Administrator's login name for this TOE.
Administrator Authentication Information	The password to identify and authenticate the Administrator.
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 one of the registered Administrators.

Terms	Definitions
Machine Administration	One of the Administrator Roles that manages machines and plays the role of performing the audit. The Machine Administrator is a person who has the machine management role.
Machine Control Data	MFP Control Data that is related to security functions and security behaviour.
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.
Stored Data Protection Function	A function that protects the Document Data stored on HDD from leakage.
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.
Stored Documents Fax Transmission	A function that faxes Document Data previously stored in D-BOX.
Direct Print Function	A function that prints out the received Print Data by the TOE.
Immediate Transmission	A function that dials first, then faxes data while scanning the original.
Internal Networks	Networks managed by an organisation that has MFP. Normally indicates the office LAN environment established as the intranet.
Document File Owner	General Users who are registered for the Document Data ACL as owners of the Document Data.
Document Data	Electronic data that are loaded into MFP by authorised MFP users using either of the following operations. 1. Electronic data that are scanned from paper-based original and digitised by authorised MFP users' operation. 2. Electronic data that are sent to the MFP by authorised MFP users and converted by the MFP from received Print Data into a format that can be processed by the MFP.
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 Data ACL	An access control list of General Users that is set for each Document Data.
File Administration	One of the Administrator Roles that manages the D-BOX, which stores the Document Data stored in the TOE, and manages the Document Data ACL, which is the access control list of Document Data. The File Administrator is a person who has the role of File Administration.
Document File User	General Users who are registered for the Document Data ACL and who are not owners of the Document Data.

8.2 Reference

The following are the referenced materials for making this document.

- CC Version 3.1 Revision 2

Evaluation Criteria:

"English version"

Common Criteria for Information Technology Security Evaluation Version3.1

Part 1: Introduction and general model Revision 1 (CCMB-2006-09-001)

Part 2: Security functional components Revision 2 (CCMB-2007-09-002)

Part 3: Security assurance components Revision 2 (CCMB-2007-09-003)

"Translated version"

Common Criteria for Information Technology Security Evaluation Version3.1

Part 1: Introduction and general model Revision 1 [Japanese translation Ver.1.2]

Part 2: Security functional components Revision 2 [Japanese translation Ver. 2.0]

Part 3: Security assurance components Revision 2 [Japanese translation Ver. 2.0]

Evaluation Methodology:

"English version"

Common Methodology for Information Technology Security Evaluation Version 3.1

Evaluation methodology Revision 2(CCMB-2007-09-0004)

"Translated version"

Common Methodology for Information Technology Security Evaluation version 3.1

Evaluation Methodology Revision 2 [Translated version 2.0]