Aficio MP 9001/8001/7001/6001 series

with DataOverwriteSecurity Unit Type H

Security Target

Author : RICOH COMPANY, LTD.
Date : 2011-04-12
Version : 1.00

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

Revision History

Version	Date	Author	Detail
1.00	2011-04-12	RICOH COMPANY, LTD.	Publication version.

Table of Contents

List of Figures

List of Tables

1 ST Introduction

This section describes ST Reference, TOE Reference, TOE Overview and TOE Description.

1.1 ST Reference

The following are the identification information of this ST.

Title : Aficio MP 9001/8001/7001/6001 series with DataOverwriteSecurity Unit Type H Security Target

Version : 1.00

Date : 2011-04-12

Author : RICOH COMPANY, LTD.

1.2 TOE Reference

This TOE is identified by the following: digital multi function product (hereafter "MFP"), Fax Controller Unit (hereafter "FCU"), Security Card (residual data overwrite option), and HDD Encryption Unit, all of which constitute the TOE. The MFP is identified by its product name and version. Although the MFP product names vary depending on sales areas and/or sales companies, the components are identical. MFP versions consist of software and hardware versions. The FCU and Security Card are identified by their names and versions, and HDD Encryption Unit is identified by its name. Some MFPs include the Scanner/Printer Function (hereafter, "S/P function") as a standard feature, and some include the S/P function as an optional feature. As for the MFP that includes the S/P function as an optional feature, to have the configuration equal to that of the TOE, Printer/Scanner Unit Type 9001 must be installed in the MFP. Table 1 shows the identification information of the TOE.

Table 1 : Identification Information of TOE

Names	Versions	
MFPs		
- MFPs with S/P function as a standard feature Ricoh Aficio MP 6001 SP, Ricoh Aficio MP 7001 SP, Ricoh Aficio MP 8001 SP, Ricoh Aficio MP 9001 SP, Gestetner MP 6001 SP, Gestetner MP 7001 SP, Gestetner MP 8001 SP, Gestetner MP 9001 SP, infotec MP 6001 SP, infotec MP 7001 SP,	Software	
	System/Copy	1.18
	Network Support	8.69.1
	Scanner(*1)	01.20
	Printer(*1)	1.16e
	Fax	03.00.00
	RemoteFax	03.00.00
	Web Support	1.13.1
	Web Uapl	1.05

Names	Versions	
infotec MP 8001 SP, infotec MP 9001 SP, Lanier LD360sp, Lanier LD370sp, Lanier LD380sp, Lanier LD390sp, nashuatec MP 6001 SP, nashuatec MP 7001 SP, nashuatec MP 8001 SP, nashuatec MP 9001 SP, Rex-Rotary MP 6001 SP, Rex-Rotary MP 7001 SP, Rex-Rotary MP 8001 SP, Rex-Rotary MP 9001 SP, Savin 9060sp, Savin 9070sp, Savin 9080sp, Savin 9090sp - MFPs with S/P function as an optional feature Ricoh Aficio MP 6001, Ricoh Aficio MP 7001, Ricoh Aficio MP 8001, Ricoh Aficio MP 9001, Gestetner MP 6001, Gestetner MP 7001, Gestetner MP 8001, Gestetner MP 9001, infotec MP 6001, infotec MP 7001, infotec MP 8001, infotec MP 9001, Lanier LD360, Lanier LD370, Lanier LD380, Lanier LD390, Lanier MP 6001, Lanier MP 7001, Lanier MP 8001, Lanier MP 9001, nashuatec MP 6001, nashuatec MP 7001, nashuatec MP 8001, nashuatec MP 9001, Rex-Rotary MP 6001, Rex-Rotary MP 7001, Rex-Rotary MP 8001, Rex-Rotary MP 9001, Savin 9060, Savin 9070,	Network DocBox	1.04
	animation	1.2.1
	Option PCL	1.02
	OptionPCLFont	1.02
	Engine	1.61:04
	OpePanel	1.04
	LANG0	1.03
	LANG1	1.03
	Hardware	
	Ic Key	1100
	Ic Ctlr	03

Names		Versions	
Savin 9080, Savin 9090			
Options			
FCU name	Fax Option Type 9001	GWFCU3-16(WW)	04.00.00
Security Card name	DataOverwriteSecurity Unit Type H	Data Erase Opt	1.01x
HDD Encryption Unit name	HDD Encryption Unit Type A	-	

(*1): As for the MFP that includes the S/P function as an optional equipment, the versions of Printer and Scanner are displayed only when Printer/Scanner Unit Type 9001 is installed.

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

1.3 TOE Overview

This section defines TOE Type, TOE Usage and Major Security Features of TOE.

1.3.1 TOE Type

This TOE is a digital multi function product (hereafter "MFP"), which is an IT device that inputs, stores, and outputs documents.

1.3.2 TOE Usage

The operational environment of the TOE is illustrated below and the usage of the TOE is outlined in this section.

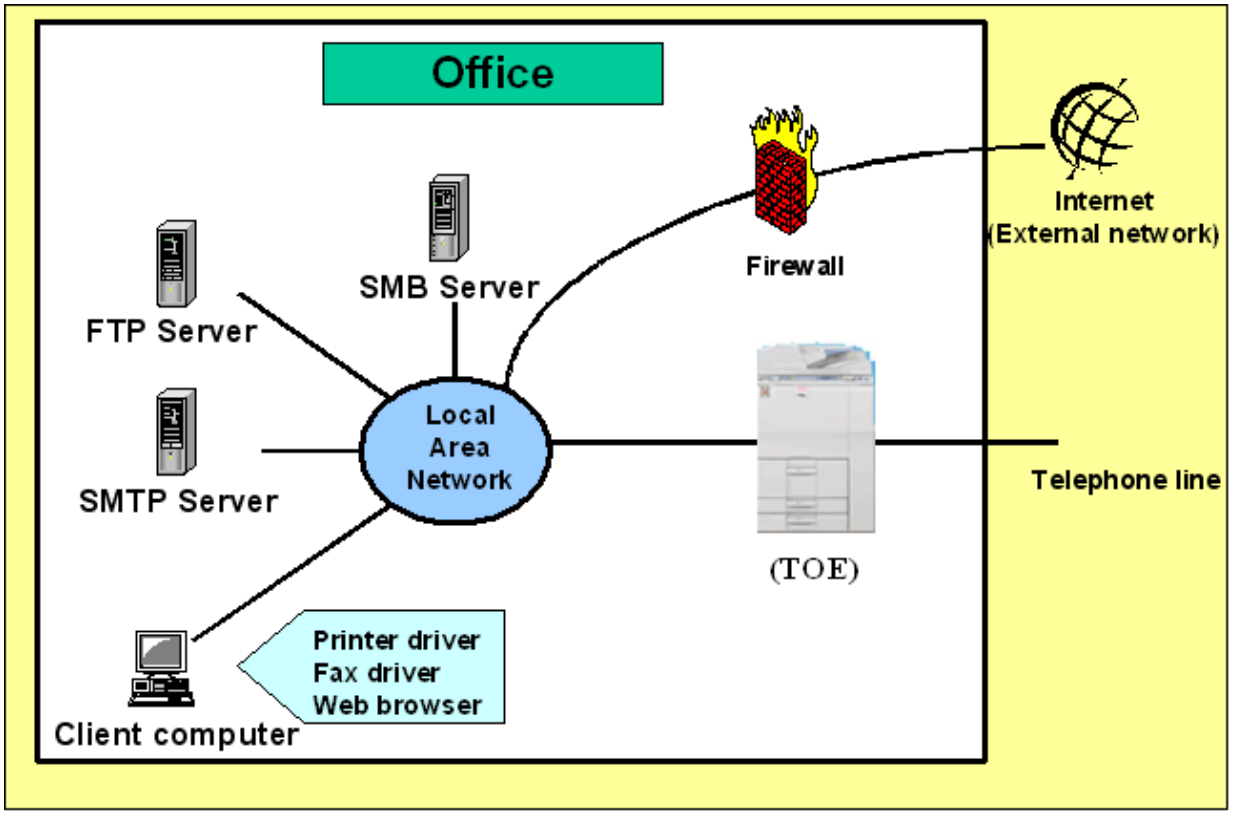

Figure 1 : Example of TOE Environment

The TOE is assumed to be used in an office environment, as shown in Figure 1. Users can operate the TOE from the Operation Panel of the TOE or a client computer connected to the local area network. The operational environment is described below:

[Local area network]

Indicates the local area network (hereafter "LAN") used in the office environment.

[MFP]

Indicates the TOE itself. It is connected to the office LAN, and users can perform the following operations from the Operation Panel of the MFP:

- Various settings for the MFP,
- Copy, fax, storage, and network transmission of paper documents,
- Print, fax, network transmission, and deletion of the stored documents.

Also, the TOE receives information via telephone lines and can store it as a document.

[Client computer]

Performs as a client of the TOE if it is connected to the LAN, and users can remotely operate the MFP from the client computer. The possible remote operations from the client computer are as follows:

- Various settings for the MFP using a Web browser,
- Print, fax, network transmission, and deletion of user documents using a Web browser,
- Store and print of documents using the printer driver,

- Store and fax of documents using the fax driver.

[Telephone line]

Indicates the public line for the TOE's communication with external faxes.

[Firewall]

A device to prevent the office environment from network attacks via the Internet.

[FTP Server]

A server used by the TOE for folder transmission of the stored documents in the TOE to its folders.

[SMB Server]

A server used by the TOE for folder transmission of the stored documents in the TOE to its folders.

[SMTP Server]

A server used by the TOE for e-mail transmission of the stored documents in the TOE.

1.3.3 Major Security Features of TOE

The TOE stores documents in it, and sends and receives documents to and from the IT devices connected to the LAN. To ensure provision of confidentiality and integrity for those documents, the TOE has the following security features:

- Audit Function
- Identification and Authentication Function
- Document Access Control Function
- Use-of-Feature Restriction Function
- Network Protection Function
- Residual Data Overwrite Function
- Stored Data Protection Function
- Security Management Function
- Software Verification Function
- Fax Line Separation Function

1.4 TOE Description

This section describes Physical Boundary of TOE, Guidance Documents, Definition of Users, Logical Boundary of TOE, and Protected Assets.

1.4.1 Physical Boundary of TOE

The physical boundary of the TOE is the MFP, which consists of the following hardware components (shown in Figure 2): Operation Panel Unit, Engine Unit, Fax Unit, Controller Board, HDD, Ic Ctlr, Network Unit, USB Port, SD Card Slot, and SD Card.

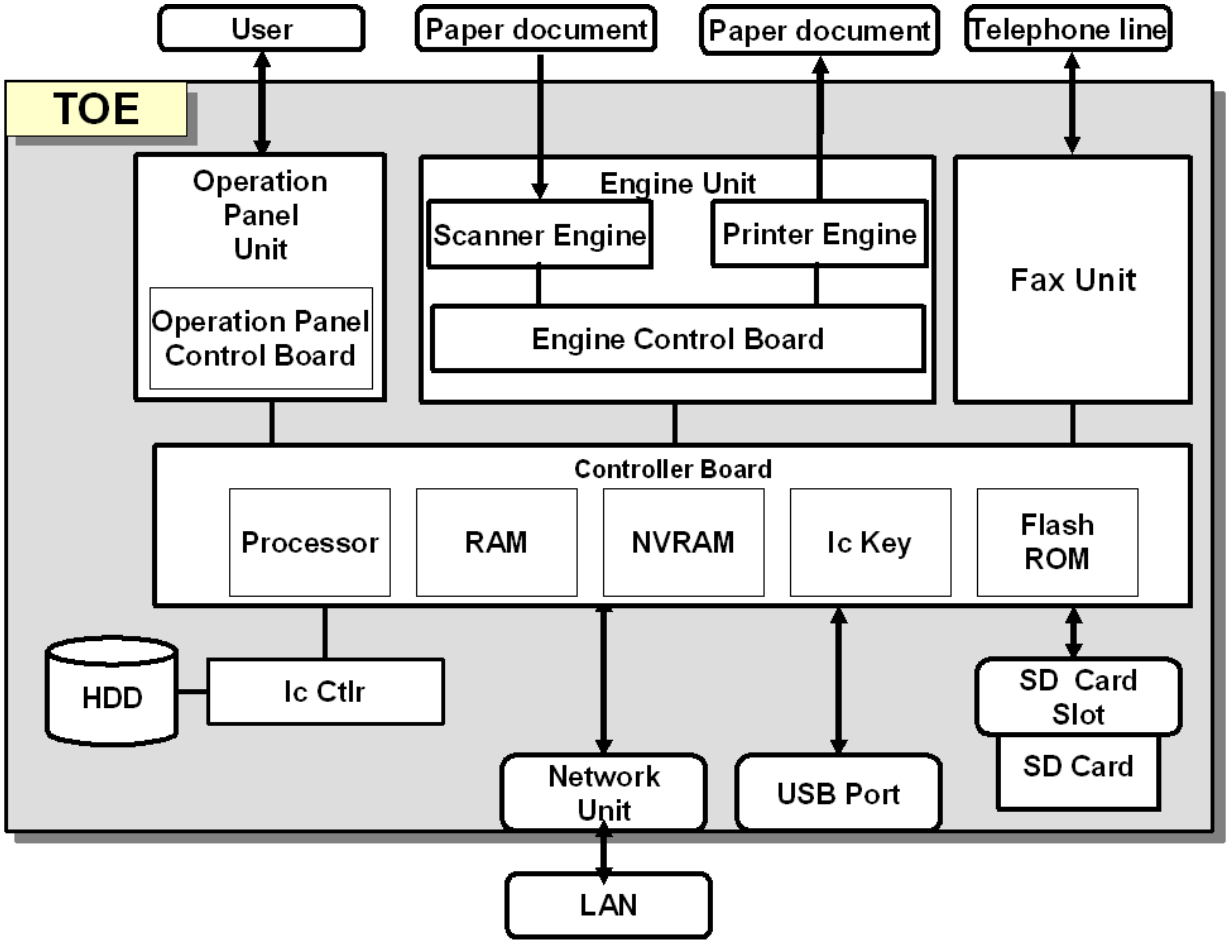

Figure 2 : Hardware Configuration of the TOE

Controller Board

The Controller Board is a device that contains Processors, RAM, NVRAM, Ic Key, and FlashROM. The following describes the components of the Controller Board:

- Processor

A semiconductor chip that performs basic arithmetic processing for MFP operations.

- RAM

A volatile memory medium which is used as a working area for image processing such as compressing/decompressing the image data. It can also be used to temporarily read and write internal information.

- NVRAM

A non-volatile memory medium in which TSF data for configuring MFP operations is stored.

- Ic Key

A security chip that has the functions of random number generation, cryptographic key generation and digital signature. It has the memory medium inside, and the signature root key is installed before the TOE is shipped.

- FlashROM

A non-volatile memory medium in which the following software components are installed:

System/Copy, Network Support, Fax, RemoteFax, Web Support, Web Uapl, Network DocBox, animation, Option PCL, OptionPCLFont, LANG0, and LANG1. These are part of the TOE and are included in the MFP Control Software.

Operation Panel Unit (hereafter "Operation Panel")

The Operation Panel is a user interface installed on the TOE and consists of the following devices: key switches, LED indicators, an LCD touch screen, and Operation Control Board. The Operation Control Board is connected to the key switches, LED indicators, and LCD touch screen. The Operation Panel Control Software is installed on the Operation Panel Control Board. The Operation Panel Control Software performs the following:

1. Transfers operation instructions from the key switches and the LCD touch screen to the MFP Control Software, which is on the Controller Board.
2. Controls the LEDs and displays information on the LCD touch screen according to display instructions from the MFP Control Software.

OpePanel, which is one of the components that constitute the TOE, is the identifier for the Operation Panel Control Software.

Engine Unit

The Engine Unit consists of Scanner Engine that is an input device to read paper documents, Printer Engine that is an output device to print and eject paper documents, and Engine Control Board. The Engine Control Software is installed in the Engine Control Board. The Engine Control Software sends status information about the Scanner Engine and Printer Engine to the MFP Control Software, and operates the Scanner Engine or Printer Engine according to instructions from the MFP Control Software. Engine, which is one of the components that constitute the TOE, is the identifier for the Engine Control Software.

Fax Unit

The Fax Unit is a unit that has a modem function for connection to a telephone line. It also sends and receives fax data to and from other fax devices using the G3 standard for communication. When connected to the Controller Board, the Fax Unit sends and receives control information about the Fax Unit and fax data to and from the MFP Control Software. FCU, which is one of the components that constitute the TOE, is the identifier of the Fax Unit.

HDD

The HDD is a hard disk drive that is a non-volatile memory medium. It stores user documents, deleted user documents, temporary documents and their fragments, login user names and login passwords of normal users.

Ic Ctlr

The Ic Ctlr is a board that implements data encryption and decryption functions. It is provided with functions for HDD encryption realisation.

The HDD encryption is an optional function, however, Ic Ctlr is a standard feature of this TOE.

Network Unit

The Network Unit is an external interface to an Ethernet (100BASE-TX/10BASE-T) LAN.

USB Port

The USB Port is an external interface to connect a client computer to the TOE for printing directly from the client computer. During installation, this interface is disabled.

SD Card/SD Card Slot

The SD Card is a memory medium in which Scanner, Printer and Data Erase Opt (MFP Control Software) are stored. When used, the SD Card is inserted into the SD Card Slot that is inside the MFP. Only the customer engineer is allowed to open the cover and insert the SD Card into the SD Card Slot during installation.

1.4.2 Guidance Documents

The following sets of user guidance documents are available for this TOE: [English version-1], [English version-2], [English version-3], and [English version-4]. Selection of the guidance document sets depends on the sales area and/or sales company. Guidance document sets will be supplied with individual products that constitute the TOE. Details of the document sets are as follows.

[English version-1]

Table 2 : Guidance for English Version-1

TOE Components	Guidance Documents for Product
MFP	- 9060/9070/9080/9090 MP 6001/MP 7001/MP 8001/MP 9001 LD360/LD370/LD380/LD390 Aficio MP 6001/7001/8001/9001 Operating Instructions About This Machine - 9060/9070/9080/9090 MP 6001/MP 7001/MP 8001/MP 9001 LD360/LD370/LD380/LD390 Aficio MP 6001/7001/8001/9001 Operating Instructions Troubleshooting - 9060/9070/9080/9090 MP 6001/MP 7001/MP 8001/MP 9001 LD360/LD370/LD380/LD390 Aficio MP 6001/7001/8001/9001 Operating Instructions Copy and Document Server Reference - Quick Reference Copy Guide - Quick Reference Printer Guide - Quick Reference Scanner Guide - Manuals for Users 9060/9060sp/9070/9070sp/9080/9080sp/9090/9090sp MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP

	LD360/LD360 sp/LD370/LD370 sp/LD380/LD380 sp/LD390/LD390 sp Aficio MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP - Manuals for Administrators 9060/9060sp/9070/9070sp/9080/9080sp/9090/9090sp MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP LD360/LD360 sp/LD370/LD370 sp/LD380/LD380 sp/LD390/LD390 sp Aficio MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP - Manuals for Administrators Security Reference Supplement - Notes for Users D060-7789A - Notes for Users D062-7183 - To Users of This Machine - Notes on Energy Saving Functions - Operating Instructions Notes on Security Functions - Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1™-2009 - Help(83NHBHENZ)
FCU	- Quick Reference Fax Guide
Security Card	- Manuals DataOverwriteSecurity Unit Type H/I
HDD Encryption Unit	-

[English version-2]

Table 3 : Guidance for English Version-2

TOE Components	Guidance Documents for Product
MFP	- Quick Reference Copy Guide - Quick Reference Fax Guide - Quick Reference Printer Guide - Quick Reference Scanner Guide - Manuals for This Machine - Manuals for Users

	MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP Aficio MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP A - Manuals for Administrators Security Reference MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP Aficio MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP - Manuals for Administrators Security Reference Supplement - Notes for Users D060-7782 - Notes for Users D062-7155 - To Users of This Machine - Safety Information for Aficio MP 6001/Aficio MP 7001/Aficio MP 8001/Aficio MP 9001 - Operating Instructions Notes on Security Functions - Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1™-2009 - Help(83NHBHENZ)
FCU	-
Security Card	- Manuals DataOverwriteSecurity Unit Type H/I
HDD Encryption Unit	-

[English version-3]

Table 4 : Guidance for English Version-3

TOE Components	Guidance Documents for Product
MFP	- Quick Reference Copy Guide - Quick Reference Fax Guide - Quick Reference Printer Guide - Quick Reference Scanner Guide - Manuals for This Machine - Manuals for Users

	MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP Aficio MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP A - Manuals for Administrators Security Reference MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP Aficio MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP - Manuals for Administrators Security Reference Supplement - Notes for Users D060-7782 - Notes for Users D062-7155 - To Users of This Machine - Safety Information for MP 6001/MP 7001/MP 8001/MP 9001 - Operating Instructions Notes on Security Functions - Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1™-2009 - Help(83NHBHENZ)
FCU	-
Security Card	- Manuals DataOverwriteSecurity Unit Type H/I
HDD Encryption Unit	-

[English version-4]

Table 5 : Guidance for English Version-4

TOE Components	Guidance Documents for Product
MFP	- MP 6001/MP 7001/MP 8001/MP 9001 MP 6001/MP 7001/MP 8001/MP 9001 Aficio MP 6001/7001/8001/9001 Operating Instructions About This Machine - MP 6001/MP 7001/MP 8001/MP 9001

	MP 6001/MP 7001/MP 8001/MP 9001 Aficio MP 6001/7001/8001/9001 Operating Instructions Troubleshooting - MP 6001/MP 7001/MP 8001/MP 9001 MP 6001/MP 7001/MP 8001/MP 9001 Aficio MP 6001/7001/8001/9001 Operating Instructions Copy and Document Server Reference - Quick Reference Copy Guide - Quick Reference Printer Guide - Quick Reference Scanner Guide - Manuals for Users MP 6001/MP 7001/MP 8001/MP 9001 Aficio MP 6001/MP 7001/MP 8001/MP 9001 - Manuals for Administrators MP 6001/MP 7001/MP 8001/MP 9001 Aficio MP 6001/MP 7001/MP 8001/MP 9001 - Manuals for Administrators Security Reference Supplement - Notes for Users D060-7782 - Notes for Users D062-7155 - To Users of This Machine - Notes On Energy Saving Functions - Operating Instructions Notes on Security Functions - Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1™-2009 - Help(83NHBHENZ)
FCU	- Quick Reference Fax Guide
Security Card	- Manuals DataOverwriteSecurity Unit Type H/I
HDD Encryption Unit	-

1.4.3 Definition of Users

This section defines the users related to the TOE. These users include those who routinely use the TOE (direct users) and those who do not (indirect users). The direct users and indirect users are described as follows:

1.4.3.1. Direct User

The "user" referred to in this ST indicates a direct user who has privileges to use the TOE. This user consists of normal users and administrators. The following table (Table 6) shows the definitions.

Table 6 : Definition of Users

Definition of Users	Explanation
Normal user	A user who is allowed to use the TOE. A normal user is provided with a login user name and can use Copy Function, Fax Function, Scanner Function, Printer Function, and Document Server Function.
Administrator	A user who is allowed to manage the TOE. An administrator performs management operations, which include issuing login names to normal users.

The administrator means the user registered for TOE management. According to its roles, the administrator can be classified as the supervisor and the MFP administrator. Up to four MFP administrators can be registered and selectively authorised to perform user management, machine management, network management, and file management. Therefore, the different roles of the management privilege can be allocated to multiple MFP administrators individually. The "MFP administrator" in this ST refers to the MFP administrator who has all management privileges (Table 7).

Table 7 : List of Administrative Roles

Definition of Administrator	Management Privileges	Explanation
Supervisor	Supervisor	Authorised to delete and register the login password of the MFP administrator.
MFP administrator	User management privilege	Authorised to manage normal users. This privilege allows configuration of normal user settings.
	Machine management privilege	Authorised to specify MFP device behaviour (network behaviours excluded). This privilege allows configuration of device settings and view of the audit log.
	Network management privilege	Authorised to manage networks and configure LAN settings. This privilege allows configuration of network settings.
	File management privilege	Authorised to manage user documents. This privilege allows access management of user documents.

1.4.3.2. Indirect User

Responsible manager of MFP

The responsible manager of MFP is a person who is responsible for selection of the TOE administrators in the organisation where the TOE is used.

Customer engineer

The customer engineer is a person who belongs to the organisation which maintains TOE operation. The customer engineer is in charge of installation, setup, and maintenance of the TOE.

1.4.4 Logical Boundary of TOE

The Basic Functions and Security Functions are described as below:

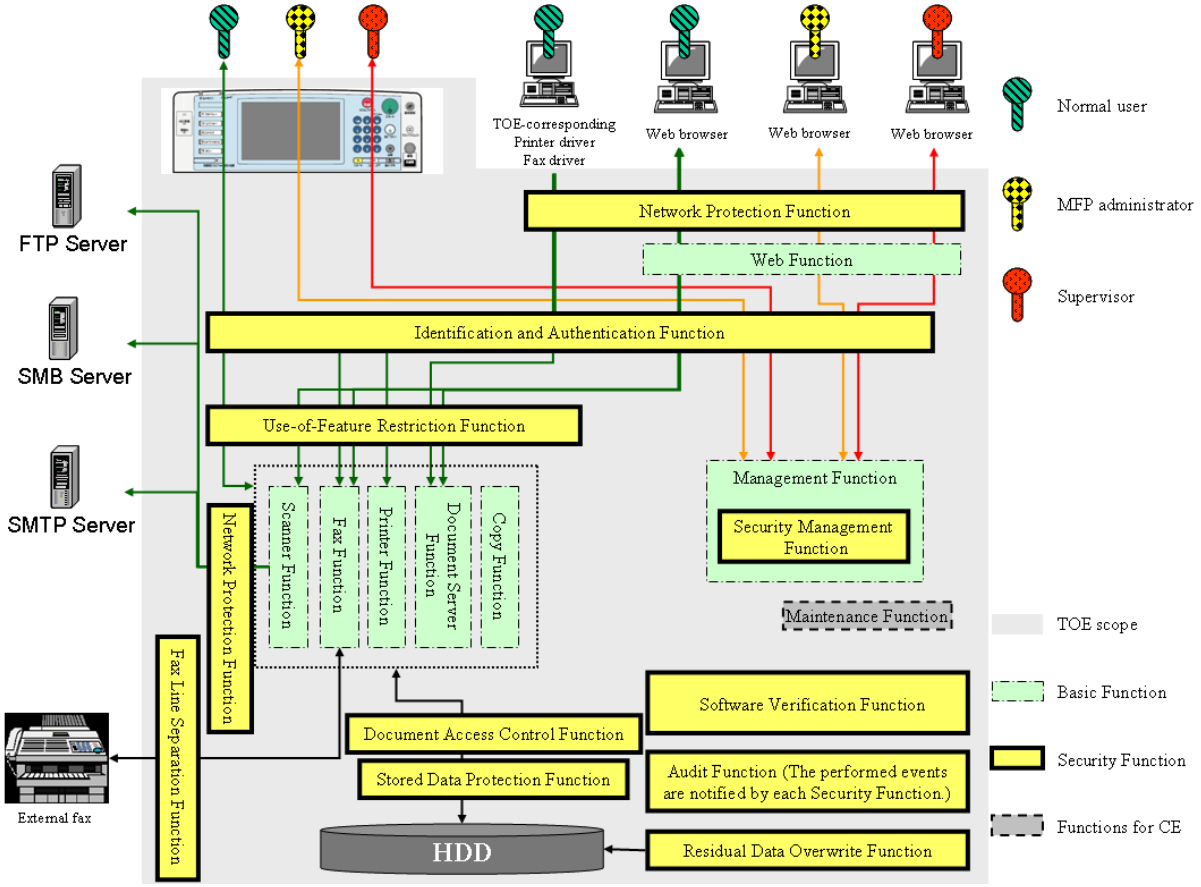

Figure 3 : Logical Scope of the TOE

1.4.4.1. Basic Functions

The overview of the Basic Functions is described as follows:

- Copy Function

The Copy Function is to scan paper documents and print scanned image data according to the specified number of copies, magnification, and custom settings. It can also be used to store scanned image data in the

MFP as a user document. User documents that are stored using this function are the Document Server user documents. Normal users can use this function from the Operation Panel.

- Printer Function

The Printer Function consists of the following:

- A function used to store print data as a Document Server user document when the print data is received from client computers via networks.
- A function used to directly print the print data from client computers via networks.

According to the guidance document, normal users shall first install the specified printer driver in their own client computers, and then use this function.

To use the Printer Function, normal users shall select documents to print on their client computers and send instructions to specify either document storage or direct printing.

- Scanner Function

The Scanner Function is to scan paper documents and create electronic documents from the scanned data. Once created, the electronic documents will be delivered to folders, sent by e-mail, or stored in the TOE as scanner user documents. The stored scanner user document will also be delivered to folders, sent by e-mail, or deleted using Scanner Function. Normal users operate this function from the Operation Panel.

Folder transmission can be applied only to the destination folders in a server that the MFP administrator pre-registers in the TOE and with which secure communication can be ensured. E-mail transmission is possible only with the mail server and e-mail addresses that the MFP administrator pre-registers in the TOE and with which secure communication can be ensured.

- Fax Function

The Fax Function is for sending and receiving fax data to and from external faxes over a telephone line. This function consists of the following:

- Fax Data Storage Function
  Normal users can store fax documents in the TOE. The fax document is the user document that is stored in the TOE for fax transmission. To store fax documents, normal users scan paper documents from the Operation Panel and create fax documents. Also, they create fax documents by receiving information from the fax driver installed on the client computers.
- Fax Transmission Function
  A function to send documents to external fax devices. Sendable documents include: paper documents, received information from the fax driver installed on the client computer, and fax documents stored in the TOE using the Fax Data Storage Function. Paper documents can be sent by fax using the Operation Panel to scan paper documents. Received information from the fax driver installed on the client computer can be sent by fax using the fax driver installed on the client computer. Fax documents can be sent by fax using the Operation Panel to access the TOE. Fax transmission is allowed only for the telephone numbers that are pre-registered in the TOE.

- Operation Function for Fax Documents
  A function to print or delete fax documents. Normal users operate this function using the Operation Panel.
- Folder Transmission Function of Fax Data
  A function to send fax documents to folders using the Operation Panel. The destination server must be pre-registered by the MFP administrator so that secure communication with the TOE can be ensured. Users select the destination server from the servers that the MFP administrator pre-registers, and send data to the folder.
- Fax Reception Function
  A function to receive information from external faxes via the telephone line and store the received information in the TOE. The stored documents in the TOE are called received fax documents.
- Operation Function for Received Fax Documents
  A function for normal users to operate the received fax documents from the Operation Panel or a Web browser. Normal users can print and delete the documents from the Operation Panel. Also, normal users can print, delete and download those documents from a Web browser.

- Document Server Function

Normal users can use this function from the Operation Panel and a Web browser.
From the Operation Panel, normal users can store, print and delete Document Server user documents. Also, they can print and delete fax documents.
From a Web browser, normal users can print and delete Document Server user documents, fax, print, download, and delete fax documents. Also, normal users can send scanner user documents to folders, send them by e-mail, download, and delete them.

- Management Function

The Management Function is to control the MFP's overall behaviour. This function can be implemented using the Operation panel or a Web browser.

- Maintenance Function

The Maintenance Function is to perform maintenance service for the MFP if it is malfunctioning. When analysing causes of the malfunction, a customer engineer performs this function from the Operation Panel. The customer engineer will implement this function following the procedures that are allowed to customer engineers only. If the MFP administrator sets the Service Mode Lock Function to "ON", the customer engineer cannot use this function.

In this ST, the Service Mode Lock Function is set to "ON" for the target of evaluation.

- Web Function

A function for the TOE user to remotely control the TOE from the client computer. To control the TOE remotely, the TOE user needs to install the designated Web browser on the client computer following the guidance documents and connect the client computer to the TOE via the LAN.

1.4.4.2. Security Functions

The Security Functions are described as follows:

- Audit Function

The Audit Function is to generate the audit log when security events occur so that the operation status of the TOE can be checked and any security intrusion can be detected. Also, this function can be used only by the MFP administrator to view and delete the recorded audit log. To view and delete the audit log, the Web Function will be used.

- Identification and Authentication Function

The Identification and Authentication Function is to identify and authenticate persons when they use the TOE, to lockout persons who consecutively fail authentication attempts, and to protect the authentication feedback area where the login password is entered using the Operation Panel. To use the Printer or Fax Function from the printer or fax driver, users will be identified and authenticated by entering the login user name and login password received from the printer or fax drivers.

- Document Access Control Function

The Document Access Control Function is to control the operations for user documents and user jobs by the authorised TOE users who are authenticated by Identification and Authentication Function. It controls user's operation on the user documents and user jobs based on the privileges for the user role, or the operation permissions for each user.

- Use-of-Feature Restriction Function

The Use-of-Feature Restriction Function is to control the operations of functions (Copy Function, Printer Function, Scanner Function, Document Server Function and Fax Function) by the authorised TOE users who are authenticated by Identification and Authentication Function. It controls the use of functions based on the privileges for the user role, or the operation permissions for each user.

- Network Protection Function

The Network Protection Function is to prevent information leakage through wiretapping on the LAN and detect data tampering. The protection function can be enabled using a Web browser to specify the URL for possible encrypted communication. If the Printer Function is used, the protection function can be enabled using the printer driver to specify encrypted communication. If the folder transmission function of Scanner Function is used, the protection function can be enabled through encrypted communication. If the e-mail transmission function of Scanner Function is used, the protection function can be enabled through encrypted communication with communication requirements that are specified for each e-mail address. If the LAN-Fax Transmission Function of Fax Function is used, the protection function can be enabled using the fax driver to specify encrypted communication.

- Residual Data Overwrite Function

The Residual Data Overwrite Function is to completely delete the residual data of deleted user documents, temporary documents and their fragments on the HDD by overwriting the specific pattern.

- Stored Data Protection Function

The Stored Data Protection Function is to encrypt the data on the HDD and protect the data so that data leakage can be prevented.

- Security Management Function

The Security Management Function indicates overall functions that are related to security management implemented by authorised users.

- Software Verification Function

The Software Verification Function is to check the integrity of the executable codes of the MFP Control Software and FCU Control Software in order to confirm the MFP Control Software and FCU Control Software are genuine.

- Fax Line Separation Function

The Fax Line Separation Function is to receive only faxes as input information from the telephone lines so that unauthorised intrusion from the telephone lines (same as the "fax line") can be prevented. Also, this function can be used to control fax transmissions so that unauthorised intrusion from the telephone lines to the LAN can be prevented.

1.4.5 Protected Assets

The TOE shall protect the following protected assets: user data, TSF data and functions.

1.4.5.1. User Data

The user data is classified into two types: document data and function data. Table 8 defines user data according to these data types.

Table 8: Definition of User Data

Type	Description
Document data	Digitised user documents, deleted documents, temporary documents and their fragments, which are managed by the TOE.
Function data	Jobs specified by users. In this ST, a "user job" is referred to as a "job".

1.4.5.2. TSF Data

The TSF data is classified into two types: protected data and confidential data. Table 9 defines TSF data according to these data types.

Table 9: Definition of TSF Data

Type	Description
Protected data	This data must be protected from changes by unauthorised persons. No security threat will occur even this data is exposed to the public. In this ST, "protected data", listed below, is referred to as "TSF protected data". Login user name, Number of Attempts before Lockout, settings for Lockout Release Timer, lockout time, year-month-day settings, time settings, Minimum Password Length, Password Complexity Setting, S/MIME user information, destination folder, stored and received document user, document user list, and available function list.
Confidential data	This data must be protected from changes by unauthorised persons and reading by users without viewing permissions. In this ST, "confidential data", listed below, is referred to as "TSF confidential data". Login password, audit log, and HDD cryptographic key.

1.4.5.3. Functions

The MFP applications (Copy Function, Document Server Function, Printer Function, Scanner Function, and Fax Function) that are for management of the document data of user data are classified as protected assets, whose use is subject to restrictions.

1.5 Glossary

1.5.1 Glossary for This ST

For clear understanding of this ST, Table 10 provides the definitions of specific terms.

Table 10: Specific Terms Related to This ST

Terms	Definitions
MFP Control Software	A software component installed in the TOE. This component is stored in FlashROM and SD Card. The components that identify the TOE include System/Copy, Network Support, Scanner, Printer, Fax, RemoteFax, Web Support, Web Uapl, Network DocBox, animation, Option PCL, OptionPCLFont, LANG0, LANG1 and Data Erase Opt.
Login user name	An identifier assigned to each user. The TOE identifies users by this identifier.
Login password	A password associated with each login user name.
Lockout	A type of behaviour to deny login of particular users.

Terms	Definitions
Auto logout	A function for automatic user logout if no access is attempted from the Operation Panel or Web Function before the predetermined auto logout time elapses. Auto logout time for the Operation Panel: Auto logout time specified by the MFP administrator (180 seconds) Auto logout time for the Web Function: 30 minutes (this cannot be changed by users). This auto logout time is also referred to as "fixed auto logout time".
Minimum Password Length	The minimum number of registrable password digits.
Password Complexity Setting	The minimum combination of the characters and symbols that can be used as registrable passwords. There are four types of characters: uppercase and lower case alphabets, digits and symbols. There are Level 1 and Level 2 Password Complexity Settings. Level 1 requires a password to be a combination of two or more types of characters and symbols specified above. Level 2 requires a password to be a combination of three or more types of characters and symbols specified above.
HDD	An abbreviation of hard disk drive. In this document, unless otherwise specified, "HDD" indicates the HDD installed on the TOE.
User job	A sequence of operations of each TOE function (Copy Function, Document Server Function, Scanner Function, Printer Function and Fax Function) from beginning to end. A user job may be suspended or cancelled by users during operation. If a user job is cancelled, the job will be terminated.
Documents	TOE digital image data that is generated through application of Copy Function, Printer Function, Scanner Function, Fax Function, and Document Server Function. "Document" is a general term for documents (or "user documents", so explicitly referred to in this ST) operated by users from the Operation Panel or a Web browser, deleted documents, temporary documents and their fragments.
Document user list	A list of the login user names of the normal users who are allowed to access a user document. This list is assigned as an attribute of each user document. The login user names of the MFP administrators are not included in this list, although access privileges are provided for them.
Document type	One of the attributes associated with user documents. Determining which access control rules or operations can be applied to user documents depends on document types, which include the following: - Document Server user document: The value for the documents stored in the Document Server using Copy Function, Document Server Function, and Printer Function. - Scanner user document: The value for the documents stored using Scanner Function. - Fax document: The value for the documents scanned and stored using Fax Function, and those stored using the LAN Fax. - Received fax document: The value for the fax data received and stored. This document is externally received, and its user cannot be identified.

Terms	Definitions
MFP application	A general term for each function the TOE provides: Copy Function, Document Server Function, Scanner Function, Printer Function, and Fax Function.
Application type	An attribute associated with normal user processes. This attribute is to identify the MFP application operated by a normal user. This attribute can also be applicable when a normal user is operating no MFP applications.
Available function list	A list of the functions (Copy Function, Printer Function, Scanner Function, Document Server Function, and Fax Function) that normal users are authorised to access. This list is assigned as an attribute of each normal user.
Operation Panel	Consists of a touch screen LCD and key switches. The Operation Panel is used by users to operate the TOE.
Users for stored and received documents	A list of the normal users who are authorised to read and delete received fax documents.
Folder transmission	A function that sends documents from the TOE via networks to a shared folder in an SMB Server by using SMB protocol, or that sends documents to a shared folder in an FTP Server by using FTP protocol. The following documents can be delivered to folders: scanned documents using Scanner Function and Fax Function, and scanned and stored documents using Scanner Function and Fax Function. IPSec protects the communication for realising this function.
Destination folder	Destination information for the "folder transmission" function. The destination folder includes the path information to the destination server, the folder in the server, and identification and authentication information for user access. The destination folder is registered and managed by the MFP administrator.
E-mail transmission	A function to send documents by e-mail from the TOE via networks to the SMTP Server. The documents that can be delivered using this function include: scanned documents using Scanner Function, and scanned and stored user documents using Scanner Function. S/MIME protects the communication for realising this function.
S/MIME user information	This information is required for e-mail transmission using S/MIME. Also, this information consists of e-mail address, user certificate, and encryption setting (S/MIME setting). Uniquely provided for each e-mail address, the S/MIME user information is registered and managed by the MFP administrator.
LAN Fax	One of Fax Functions. A function that transmits fax data and stores the documents using the fax driver on client computer. Sometimes referred to as "PC FAX".

2 Conformance Claim

This section describes Conformance Claim.

2.1 CC Conformance Claim

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

- CC version for which this ST and TOE claim conformance

  Part 1:

  Introduction and general model July 2009 Version 3.1 Revision 3 Final (Japanese translation ver.1.0 Final) CCMB-2009-07-001

  Part 2:

  Security functional components July 2009 Version 3.1 Revision 3 Final (Japanese translation ver.1.0 Final) CCMB-2009-07-002

  Part 3:

  Security assurance components July 2009 Version 3.1 Revision 3 Final (Japanese translation ver.1.0 Final) CCMB-2009-07-003

- Functional requirements: Part 2 extended
- Assurance requirements: Part 3 conformance

2.2 PP Claims

The PP to which this ST and TOE are demonstrable conformant is:

PP Name/Identification : 2600.1, Protection Profile for Hardcopy Devices, Operational Environment A

Version : 1.0, dated June 2009

Notes: The PP name which is published in Common Criteria Portal is "IEEE Standard for a Protection Profile in Operational Environment A (IEEE Std 2600.1-2009)".

2.3 Package Claims

The SAR package which this ST and TOE conform to is EAL3+ALC_FLR.2.

The selected SFR Packages from the PP are:

2600.1-PRT conformant

2600.1-SCN conformant

2600.1-CPY conformant

2600.1-FAX conformant

2600.1-DSR conformant

2600.1-SMI conformant

2.4 Conformance Claim Rationale

2.4.1 Consistency Claim with TOE Type in PP

The targeted product type by the PP is the Hardcopy devices (hereafter, HCDs). The HCDs consist of the scanner device and print device, and have the interface to connect telephone line. The HCDs combine these devices and equip one or more functions of Copy Function, Scanner Function, Printer Function or Fax Function. The Document Server Function is also available when installing the non-volatile memory medium, such as hard disk drive, as additional equipments.

The MFP is the type of this TOE. The MFP has the devices the HCDs have, and equips the functions that HCDs equip including the additional equipments. Therefore, this TOE type is consistent with the TOE type in the PP.

2.4.2 Consistency Claim with Security Problems and Security Objectives in PP

Defining all security problems in the PP, P.STORAGE_ENCRYPTION was added to the security problem definitions in chapter 3.
Defining all security objectives in the PP, O.STORAGE.ENCRYPTED was added to the security objectives in chapter 4. P.STORAGE_ENCRYPTION and O.STORAGE.ENCRYPTED encrypt data on the HDD, and satisfy both other organisational security policies in the PP and security objectives of the TOE. Therefore, the security problems and security objectives in this ST are consistent with the ones in the PP.
Although the PP is written in English, the security problem definitions in chapter 3 and security objectives in chapter 4 are translated from English PP into Japanese. In translating into Japanese, if the literal translation of the PP was judged to make it difficult for readers to understand the PP, the translation was made easily comprehensible, however, its description is not deviated from the requirements of the PP conformance. Also, the description is neither increased nor decreased.

2.4.3 Consistency Claim with Security Requirements in PP

The SFRs for this TOE consist of those found in the Common Security Functional Requirements and SFR Packages 2600.1-PRT, 2600.1-SCN, 2600.1-CPY, 2600.1-FAX, 2600.1-DSR, and 2600.1-SMI, and conform to the PP.

FAU_STG.1, FAU_STG.4, FAU_SAR.1, and FAU_SAR.2 are added according to PP APPLICATION NOTE7 in order for the TOE to maintain and manage the audit logs.

For the authentication function of the TOE, FIA_AFL.1, FIA_UAU.7, and FIA_SOS.1 are added according to PP APPLICATION NOTE36.

For the ownership of the received fax documents, the TOE has the characteristic that the ownership of the document is assigned to the intended user. This is according to PP APPLICATION NOTE 93.

This TOE claims the data protection against the non-volatile memory medium that is not allowed to be attached nor removed by administrator, and FCS_CKM.1 and FCS_COP.1 are added.
While FDP_ACC.1(a) and FDP_ACF.1(a) in the PP require access control to D.DOC, this ST specifies that only user documents, which are included in the D.DOC equivalent document, shall be subject to access control, and it is not required that access control to the deleted documents, temporary documents and their fragments be implemented. Because the TOE does not provide any function to access those documents and fragments, and because the TOE's Residual Data Overwrite Function makes them unavailable before they are read by users, it is not necessary to provide access control to those documents and fragments. Therefore, FDP_ACC.1(a) and FDP_ACF.1(a) in this ST satisfy the requirements demanded in the PP.

While FDP_ACF.1.1(a) and FDP_ACF.1.2(a) in the PP require the access control SFP to the document data that is defined for each SFR package in the PP, this ST instantiates the abstract security attributes in the PP and describes the security attributes that are actually used for this TOE as access control to the user documents and user jobs. This is not deviated from the PP.

FDP_ACF.1.2(a) in ST, operations to user documents vary depending on the type of documents and each TOE function (application type). For this TOE, however, the access control process to user with permission is always the same even when operated from the Operation Panel, printer driver, Web browser or fax driver. This is not deviated from the PP but instantiated.

For FDP_ACF.1.4(a), a rule that rejects the operations of user documents and user jobs by supervisor is added. Supervisor is not identified in the PP and is the special user for this TOE.

The PP only allows the specified users to operate the user documents and user jobs, and this is not deviated from the PP.

While FDP_ACF.1.3(b) in the PP allows the user with administrator permission to operate the TOE function, this ST only allows the Fax Reception Function which is the one of this TOE functions. The TOE allows the MFP administrator to delete the user documents and user jobs (common access control SFP, FDP_ACC.1(a) and FDP_ACF.1(a)), and as a result, the TSF restrictively allows the MFP administrator to access to the TOE functions. Therefore, the requirement for FDP_ACF.1.3(b) in the PP is satisfied at the same time. The fax reception process, which is accessed when receiving from telephone line, is regarded as the user with administrator permission. Therefore, FDP_ACF.1.3(b) in this ST satisfies FDP_ACF.1.3(b) in the PP.

The TOE is 2600.1-PRT, 2600.1-SCN, 2600.1-CPY, 2600.1-FAX, 2600.1-DSR, and 2600.1-SMI conformant.

2600.1-NVS is not selected because this TOE does not have any non-volatile memory medium that can be detachable.

This TOE, in accordance with the PP, extends the functional requirement Part 2 due to the addition of the restricted forwarding of data to external interfaces (FPT_FDI_EXP).

For conforming to the PP, some sections in this document are literally translated to make it easier for readers to understand when translating English into Japanese. However, this translation is not beyond the requirements of the PP conformance.

Although some functional requirements which the PP claims do not correspond in pairs in Chapter 6, all functional requirements in the PP are satisfied. The functional requirements FCS_CKM.1 and FCS_COP.1 are added and their dependent functional requirements are also added and changed in order to realise O.STORAGE.ENCRYPTED, however, these changes do not interfere the functional requirements demanded in the PP.

3 Security Problem Definitions

This section describes Threats, Organisational Security Policies and Assumptions.

3.1 Threats

Defined and described below are the assumed threats related to the use and environment of this TOE. The threats defined in this section are unauthorised persons with knowledge of published information about the TOE operations and such attackers are capable of Basic attack potential.

T.DOC.DIS **Document disclosure**

Documents under the TOE management may be disclosed to persons without a login user name, or to persons with a login user name but without an access permission to the document.

T.DOC.ALT **Document alteration**

Documents under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the document.

T.FUNC.ALT **User job alteration**

User jobs under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the user job.

T.PROT.ALT **Alteration of TSF protected data**

TSF Protected Data under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the TSF Protected Data.

T.CONF.DIS **Disclosure of TSF confidential data**

TSF Confidential Data under the TOE management may be disclosed to persons without a login user name, or to persons with a login user name but without an access permission to the TSF Confidential Data.

T.CONF.ALT **Alteration of TSF confidential data**

TSF Confidential Data under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the TSF Confidential Data.

3.2 Organisational Security Policies

The following organisational security policies are taken:

P.USER.AUTHORIZATION **User identification and authentication**

Only users with a login user name shall be authorised to use the TOE.

P.SOFTWARE.VERIFICATION **Software verification**

Procedures shall exist to self-verify executable code in the TSF.

P.AUDIT.LOGGING **Management of audit log records**

The TOE shall create and maintain a log of TOE use and security-relevant events. The audit log shall be protected from unauthorised disclosure or alteration, and shall be reviewed by authorised persons.

P.INTERFACE.MANAGEMENT **Management of external interfaces**

To prevent unauthorised use of the external interfaces of the TOE (Operation Panel, LAN, USB and telephone lines), operation of those interfaces shall be controlled by the TOE and its IT environment.

P.STORAGE.ENCRYPTION **Encryption of storage devices**

The TOE shall encrypt the stored data on the HDD inside the TOE.

3.3 Assumptions

The assumptions related to this TOE usage environment are identified and described.

A.ACCESS.MANAGED **Access management**

According to the guidance document, the TOE is placed in a restricted or monitored area that provides protection from physical access by unauthorised persons.

A.USER.TRAINING **User training**

The responsible manager of MFP trains users according to the guidance document and users are aware of the security policies and procedures of their organisation and are competent to follow those policies and procedures.

A.ADMIN.TRAINING **Administrator training**

Administrators are aware of the security policies and procedures of their organisation, are competent to correctly configure and operate the TOE in accordance with the guidance document following those policies and procedures.

A.ADMIN.TRUST **Trusted administrator**

The responsible manager of MFP selects administrators who do not use their privileged access rights for malicious purposes according to the guidance document.

4 Security Objectives

This section describes Security Objectives for TOE, Security Objectives of Operational Environment and Security Objectives Rationale.

4.1 Security Objectives for TOE

This section describes the security objectives for the TOE.

O.DOC.NO_DIS **Protection of document disclosure**

The TOE shall protect documents from unauthorised disclosure by persons without a login user name, or by persons with a login user name but without an access permission to the document.

O.DOC.NO_ALT **Protection of document alteration**

The TOE shall protect documents from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the document.

O.FUNC.NO_ALT **Protection of user job alteration**

The TOE shall protect user jobs from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the job.

O.PROT.NO_ALT **Protection of TSF protected data alteration**

The TOE shall protect TSF Protected Data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the TSF Protected Data.

O.CONF.NO_DIS **Protection of TSF confidential data disclosure**

The TOE shall protect TSF Confidential Data from unauthorised disclosure by persons without a login user name, or by persons with a login user name but without an access permission to the TSF Confidential Data.

O.CONF.NO_ALT **Protection of TSF confidential data alteration**

The TOE shall protect TSF Confidential Data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the TSF Confidential Data.

O.USER.AUTHORIZED User identification and authentication

The TOE shall require identification and authentication of users and shall ensure that users are authorised in accordance with security policies before allowing them to use the TOE.

O.INTERFACE.MANAGED Management of external interfaces by TOE

The TOE shall manage the operation of external interfaces (Operation Panel, LAN, telephone lines and USB) in accordance with security policies. The TOE shall control the access to the Operation Panel, opened LAN ports and telephone lines. Also, the TOE shall forward from external interfaces only data that are processed by the TOE.

O.SOFTWARE.VERIFIED Software verification

The TOE shall provide procedures to self-verify executable code in the TSF.

O.AUDIT.LOGGED Management of audit log records

The TOE shall create and maintain a log of TOE use and security-relevant events in the MFP and prevent its unauthorised disclosure or alteration.

O.STORAGE.ENCRYPTED Encryption of storage devices

The TOE shall ensure the data is encrypted first and then stored on the HDD.

4.2 Security Objectives of Operational Environment

This section describes the security objectives of the operational environment.

4.2.1 IT Environment

OE.AUDIT_STORAGE.PROTECTED Audit log protection in trusted IT products

If audit logs are exported to a trusted IT product, the responsible manager of MFP shall ensure that those logs are protected from unauthorised access, deletion and modifications.

OE.AUDIT_ACCESS.AUTHORIZED Audit log access control in trusted IT products

If audit logs are exported to a trusted IT product, the responsible manager of MFP shall ensure that those logs can be accessed in order to detect potential security violations, and only by authorised persons.

OE.INTERFACE.MANAGED Management of external interfaces in IT environment

The IT environment shall provide protection from unmanaged access to TOE external interfaces (LAN). The responsible manager of MFP shall give an instruction to

appropriately configure the firewall according to the guidance document, and prevent the attacks to the LAN from the Internet. Also, the responsible manager of MFP shall instruct the MFP administrators to close the unused LAN ports and disable the USB use at the time of installation according to the guidance document.

4.2.2 Non-IT Environment

OE.PHYSICAL.MANAGED Physical management

According to the guidance document, the TOE shall be placed in a secure or monitored area that provides protection from physical access to the TOE by unauthorised persons.

OE.USER.AUTHORIZED Assignment of user authority

The responsible manager of MFP shall grant login user name, login password and user role (supervisor, MFP administrator or normal user) to persons who follow the security policies and procedures of their organisation to be authorised to use the TOE.

OE.USER.TRAINED User training

The responsible manager of MFP shall train users according to the guidance document and ensure that users are aware of the security policies and procedures of their organisation and have the competence to follow those policies and procedures.

OE.ADMIN.TRAINED Administrator training

The responsible manager of MFP shall ensure that administrators are aware of the security policies and procedures of their organisation; have the training, competence, and time to follow the guidance document; and correctly configure and operate the TOE according to those policies and procedures.

OE.ADMIN.TRUSTED Trusted administrator

The responsible manager of MFP shall select administrators who will not use their privileged access rights for malicious purposes according to the guidance document.

OE.AUDIT.REVIEWED Log audit

The responsible manager of MFP shall ensure that audit logs are reviewed at appropriate intervals according to the guidance document for detecting security violations or unusual patterns of activity.

4.3 Security Objectives Rationale

This section describes the rationale for security objectives. The security objectives are for upholding the assumptions, countering the threats, and enforcing the organisational security policies that are defined.

4.3.1 Correspondence Table of Security Objectives

Table 11 describes the correspondence between the assumptions, threats and organisational security policies, and each security objective.

Table 11: Rationale for Security Objectives

	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	OE.USER.AUTHORIZED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.STORAGE.ENCRYPTED	OE.AUDIT_STORAGE.PROTCTED	OE.AUDIT_ACCESS_AUTHORIZED	OE.AUDIT.REVIEWED	O.INTERFACE.MANAGED	OE.PHYSICAL.MANAGED	OE.INTERFACE.MANAGED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED	OE.USER.TRAINED
T.DOC.DIS	X						X	X												
T.DOC.ALT		X					X	X												
T.FUNC.ALT			X				X	X												
T.PROT.ALT				X			X	X												
T.CONF.DIS					X		X	X												
T.CONF.ALT						X	X	X												
P.USER.AUTHORIZATION							X	X												
P.SOFTWARE.VERIFICATION									X											
P.AUDIT.LOGGING										X		X	X	X						
P.INTERFACE.MANAGEMENT															X		X			
P.STORAGE.ENCRYPTION											X									
A.ACCESS.MANAGED																X				
A.ADMIN.TRAINING																		X		
A.ADMIN.TRUST																			X	
A.USER.TRAINING																				X

4.3.2 Security Objectives Descriptions

The following describes the rationale for each security objective being appropriate to satisfy the threats, assumptions and organisational security policies.

T.DOC.DIS

T.DOC.DIS is countered by O.DOC.NO_DIS, O.USER.AUTHORIZED and OE.USER.AUTHORIZED.

By OE.USER.AUTHORIZED, a permission for using the TOE as a user is granted to the persons who follow the security policies and procedures of their organisation. By O.USER.AUTHORIZED, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE. By O.DOC.NO_DIS, the TOE protects the documents from unauthorised disclosure by persons without a login user name, or by persons with a login user name but without an access permission to the document.

T.DOC.DIS is countered by these objectives.

T.DOC.ALT

T.DOC.ALT is countered by O.DOC.NO_ALT, O.USER.AUTHORIZED and OE.USER.AUTHORIZED.

By OE.USER.AUTHORIZED, a permission for using the TOE as a user is granted to the persons who follow the security policies and procedures of their organisation. By O.USER.AUTHORIZED, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE. By O.DOC.NO_ALT, the TOE protects the documents from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the document.

T.DOC.ALT is countered by these objectives.

T.FUNC.ALT

T.FUNC.ALT is countered by O.FUNC.NO_ALT, O.USER.AUTHORIZED and OE.USER.AUTHORIZED.

By OE.USER.AUTHORIZED, a permission for using the TOE as a user is granted to the persons who follow the security policies and procedures of their organisation. By O.USER.AUTHORIZED, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE. By O.FUNC.NO_ALT, the TOE protects the user jobs from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the user job.

T.FUNC.ALT is countered by these objectives.

T.PROT.ALT

T.PROT.ALT is countered by O.PROT.NO_ALT, O.USER.AUTHORIZED and OE.USER.AUTHORIZED.

By OE.USER.AUTHORIZED, a permission for using the TOE as a user is granted to the persons who follow the security policies and procedures of their organisation. By O.USER.AUTHORIZED, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE. By O.PROT.NO_ALT, the TOE protects the TSF protected

data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the TSF protected data.

T.PROT.ALT is countered by these objectives.

T.CONF.DIS

T.CONF.DIS is countered by O.CONF.NO_DIS, O.USER.AUTHORIZED and OE.USER.AUTHORIZED.

By OE.USER.AUTHORIZED, a permission for using the TOE as a user is granted to the persons who follow the security policies and procedures of their organisation. By O.USER.AUTHORIZED, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE. By O.CONF.NO_DIS, the TOE protects the TSF confidential data from unauthorised disclosure by persons without a login user name, or by persons with a login user name but without an access permission to the TSF confidential data.

T.CONF.DIS is countered by these objectives.

T.CONF.ALT

T.CONF.ALT is countered by O.CONF.NO_ALT, O.USER.AUTHORIZED and OE.USER.AUTHORIZED.

By OE.USER.AUTHORIZED, a permission for using the TOE as a user is granted to the persons who follow the security policies and procedures of their organisation. By O.USER.AUTHORIZED, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE. By O.CONF.NO_ALT, the TOE protects the TSF confidential data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the TSF confidential data.

T.CONF.ALT is countered by these objectives.

P.USER.AUTHORIZATION

P.USER.AUTHORIZATION is enforced by O.USER.AUTHORIZED and OE.USER.AUTHORIZED.

By OE.USER.AUTHORIZED, a permission for using the TOE as a user is granted to the persons who follow the security policies and procedures of their organisation. By O.USER.AUTHORIZED, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE.

P.USER.AUTHORIZATION is enforced by these objectives.

P. SOFTWARE.VERIFICATION

P.SOFTWARE.VERIFICATION is enforced by O.SOFTWARE.VERIFIED.

By O.SOFTWARE.VERIFIED, the TOE provides measures for self-verifying the executable code of the TSF.

P.SOFTWARE.VERIFICATION is enforced by this objective.

P. AUDIT.LOGGING

P.AUDIT.LOGGING is enforced by O.AUDIT.LOGGED, OE.AUDIT.REVIEWED, OE.AUDIT_STORAGE.PROTECTED and OE.AUDIT_ACCESS.AUTHORIZED.

By O.AUDIT.LOGGED, the TOE creates and maintains a log of TOE use and security-relevant events in the MFP and prevents its unauthorised disclosure or alteration.

By OE.AUDIT.REVIEWED, the responsible manager of MFP reviews audit logs at appropriate intervals for security violations or unusual patterns of activity according to the guidance document.

By OE.AUDIT_STORAGE.PROTECTED, if audit records are exported from the TOE to another trusted IT product, the responsible manager of MFP protects those records from unauthorised access, deletion and alteration. By OE.AUDIT_ACCESS.AUTHORIZED, the responsible manager of MFP ensures that those records can be accessed in order to detect potential security violations, and only by authorised persons.

P.AUDIT.LOGGING is enforced by these objectives.

P.INTERFACE.MANAGEMENT

P.INTERFACE.MANAGEMENT is enforced by O.INTERFACE.MANAGED and OE.INTERFACE.MANAGED.

By O.INTERFACE.MANAGED, the TOE manages the operation of the external interfaces (the Operation Panel, LAN, USB and telephone line) in accordance with the security policies. The TOE controls the access to the Operation Panel and the opened LAN ports, and limits the functions which are available from telephone line. By OE.INTERFACE.MANAGED, the TOE appropriately controls the access to the LAN and USB. Specifically,

(1) The responsible manager of MFP gives an instruction to appropriately configure the firewall to prevent attacks to the LAN from the Internet,
(2) The responsible manager of MFP instructs the MFP administrators to close the unused LAN ports,
(3) The use of USB is deactivated at the time of installation.

P.INTERFACE.MANAGEMENT is enforced by these objectives.

P.STORAGE.ENCRYPTION

P.STORAGE.ENCRYPTION is enforced by O.STORAGE.ENCRYPTED.

By OE.PHYSICAL.MANAGED, the TOE encrypts and decrypts the data written into/read from the HDD, and ensures that the only encrypted data is written into the HDD.

P.STORAGE.ENCRYPTION is enforced by this objective.

A.ACCESS.MANAGED

A.ACCESS.MANAGED is upheld by OE.PHYSICAL.MANAGED.

By OE.PHYSICAL.MANAGED, the TOE is located in a restricted or monitored environment according to the guidance documents and is protected from the physical access by the unauthorised persons.

A.ACCESS.MANAGED is upheld by this objective.

A.ADMIN.TRAINING

A.ADMIN.TRAINING is upheld by OE.ADMIN.TRAINED.

By OE.ADMIN.TRAINED, the responsible manager of MFP ensures that the administrators are aware of the security policies and procedures of their organisation. For this, the administrators have the training, competence, and time to follow the guidance documents, and correctly configure and operate the TOE in accordance with those policies and procedures.

A.ADMIN.TRAINING is upheld by this objective.

A.ADMIN.TRUST

A.ADMIN.TRUST is upheld by OE.ADMIN.TRUSTED.

By OE.ADMIN.TRUSTED, the responsible manager of MFP selects the administrators and they will not abuse their privileges in accordance with the guidance documents.

A.ADMIN.TRUST is upheld by this objective.

A.USER.TRAINING

A.USER.TRAINING is upheld by OE.USER.TRAINED.

By OE.USER.TRAINED, the responsible manager of MFP instructs the users in accordance with the guidance documents to make them aware of the security policies and procedures of their organisation, and the users follow those policies and procedures.

OE.USER.TRAINED is upheld by this objective.

5 Extended Components Definition

This section describes Extended Components Definition.

5.1 Restricted forwarding of data to external interfaces (FPT_FDI_EXP)

Family behaviour

This family defines requirements for the TSF to restrict direct forwarding of information from one external interface to another external interface.

Many products receive information on specific external interfaces and are intended to transform and process this information before it is transmitted on another external interface. However, some products may provide the capability for attackers to misuse external interfaces to violate the security of the TOE or devices that are connected to the TOE's external interfaces. Therefore, direct forwarding of unprocessed data between different external interfaces is forbidden unless explicitly allowed by an authorized administrative role. The family FPT_FDI_EXP has been defined to specify this kind of functionality.

Component levelling:

FPT_FDI_EXP: Restricted forwarding of data to external interfaces	1

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces provides for the functionality to require TSF controlled processing of data received over defined external interfaces before these data are sent out on another external interface. Direct forwarding of data from one external interface to another one requires explicit allowance by an authorized administrative role.

Management: FPT_FDI_EXP.1

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

a) Definition of the role(s) that are allowed to perform the management activities

b) Management of the conditions under which direct forwarding can be allowed by an administrative role

c) Revocation of such an allowance

Audit: FPT_FDI_EXP.1

There are no auditable events foreseen.

Rationale:

Quite often, a TOE is supposed to perform specific checks and process data received on one external interface before such (processed) data are allowed to be transferred to another external interface. Examples are firewall systems but also other systems that require a specific work flow for the incoming data before it can be transferred. Direct forwarding of such data (i.e., without processing the data first) between different external interfaces is therefore a function that—if allowed at all—can only be allowed by an authorized role.

It has been viewed as useful to have this functionality as a single component that allows specifying the property to disallow direct forwarding and require that only an authorized role can allow this. Since this is a function that is quite common for a number of products, it has been viewed as useful to define an extended component.

The Common Criteria defines attribute-based control of user data flow in its FDP class. However, in this Protection Profile, the authors needed to express the control of both user data and TSF data flow using administrative control instead of attribute-based control. It was found that using FDP_IFF and FDP_IFC for this purpose resulted in SFRs that were either too implementation-specific for a Protection Profile or too unwieldy for refinement in a Security Target. Therefore, the authors decided to define an extended component to address this functionality.

This extended component protects both user data and TSF data, and it could therefore be placed in either the FDP or the FPT class. Since its purpose is to protect the TOE from misuse, the authors believed that it was most appropriate to place it in the FPT class. It did not fit well in any of the existing families in either class, and this led the authors to define a new family with just one member.

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

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

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on **[assignment: the Operation Panel, LAN, telephone line]** from being forwarded without further processing by the TSF to **[assignment: the LAN and telephone line]**.

6 Security Requirements

This section describes Security Functional Requirements, Security Assurance Requirements and Security Requirements Rationale.

6.1 Security Functional Requirements

This section describes the TOE security functional requirements for fulfilling the security objectives defined in section 4.1. The security functional requirements are quoted from the requirement defined in the CC Part2. The security functional requirements that are not defined in CC Part2 are quoted from the extended security functional requirements defined in the PP (IEEE Standard for a Protection Profile in Operational Environment A (IEEE Std 2600.1-2009)).

The part with assignment and selection defined in the [CC] is 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 12]**.
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: types of job for FDP_ACF.1(a), all login user names that attempted the user identification for FIA_UID.1, communication direction of Web Function, communication IP address of the communication used for Web Function and folder transmission, and recipient's e-mail address used for e-mail transmission]**.

Table 12 shows the action (CC rules) recommended by the CC as auditable for each functional requirement and the corresponding auditable events of the TOE.

Table 12 : List of Auditable Events

Functional Requirements	Actions Which Should Be Auditable	Auditable Events
FDP_ACF.1(a)	a) Minimal: Successful requests to perform an operation on an object	Original: - Start and end operation of

	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.	storing user documents. - Start and end operation of printing user documents. - Start and end operation of downloading user documents. - Start and end operation of faxing user documents. - Start and end operation of user documents e-mail transmission. - Start and end operation of user documents folder transmission. - Start and end operation of deleting user documents. Above described "storing, printing, downloading, faxing, e-mail transmission, folder transmission and deleting" are the job types of additional information that are required by the PP.
FDP_ACF.1(b)	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.	Original: Not recorded.
FIA_UAU.1	a) Minimal: Unsuccessful use of the authentication mechanism; b) Basic: All use of the authentication mechanism; c) Detailed: All TSF mediated actions performed before authentication of the user.	b) Basic: Success and failure of login operation
FIA_UID.1	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: Success and failure of login operation. Also includes the user identification that is required by the PP as the additional information.
FMT_SMF.1	a) Minimal: Use of the management functions.	a) Minimal: Record of management items in Table 32.
FMT_SMR.1	a) Minimal: modifications to the	No record due to any

	group of users that are part of a role; b) Detailed: every use of the rights of a role.	modification.
FPT_STM.1	a) Minimal: changes to the time; b) Detailed: providing a timestamp.	a) Minimal: Settings of Year-Month-Day and Hour-Minute
FTA_SSL.3	a) Minimal: Termination of an interactive session by the session locking mechanism.	a) Minimal: Termination of session by auto logout.
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.	a) Minimal: Failure of communication with trusted channel.

FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

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**.

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 MFP administrators]** with the capability to read **[assignment: all of 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.

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 in Table 13]** and specified cryptographic key sizes **[assignment: cryptographic key sizes in Table 13]** that meet the following: **[assignment: standards in Table 13]**.

Table 13 : 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 14]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm shown in Table 14]** and cryptographic key sizes **[assignment: cryptographic key sizes shown in Table 14]** that meet the following: **[assignment: standards shown in Table 14]**.

Table 14: List of Cryptographic Operation

Key Type	Standard	Cryptographic Algorithm	Cryptographic Key Size	Cryptographic Operation
HDD cryptographic key	FIPS197	AES	256 bits	- Encryption when writing the data on HDD - Decryption when reading the data from HDD

6.1.3 Class FDP: User data protection

FDP_ACC.1(a) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(a) The TSF shall enforce the **[assignment: common access control SFP]** on **[assignment: list of subjects, objects, and operations among subjects and objects in Table 15]**.

Table 15: List of Subjects, Objects, and Operations among Subjects and Objects (a)

Subjects	Objects	Operations among Subjects and Objects
MFP administrator process	User document	Delete
Supervisor process	User document	None
Normal user process	User document	Delete, print, download, fax, e-mail transmission and folder transmission
MFP administrator process	User job	Delete
Normal user process	Applicable user job	Delete

FDP_ACC.1(b) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(b) The TSF shall enforce the **[assignment: TOE function access control SFP]** on **[assignment: list of subjects, objects, and operations among subjects and objects in Table 16]**.

Table 16: List of Subjects, Objects, and Operations among Subjects and Objects (b)

Subjects	Objects	Operations among Subjects and Objects
Normal user process	MFP application	Execute

FDP_ACF.1(a) Security attribute based access control

Hierarchical to: No other components.

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

FDP_ACF.1.1(a) The TSF shall enforce the **[assignment: common access control SFP]** to objects based on the following: **[assignment: subjects or objects, and their corresponding security attributes shown in Table 17]**.

Table 17: Subjects, Objects and Security Attributes (a)

Category	Subject or Object	Security Attributes
Subject	Normal user process	- Login user name of normal user - Application type
Subject	Supervisor process	- Login user name of supervisor
Subject	MFP administrator process	- Login user name of MFP administrator
Object	User document	- Type of document - Document user list
Object	User job	- Login user name of normal user

FDP_ACF.1.2(a) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[assignment: rules on user documents in Table 18 and rules on user jobs in Table 19]**.

Table 18: Rules on User Documents

<table>
<tr><th>Subject</th><th>Object</th><th>Rules Governing Access</th></tr>
<tr><td>Normal user process</td><td>User document</td><td>The TOE controls the operations on user documents in the following order 1) and 2).
1) Limit the document types by MFP applications
2) Limit the operation by each normal user

1) Limit the document types by MFP applications
The availability of a user document is determined by the operation interface for normal user, application type associated with the normal user process, and document type associated with the user document. The following table shows the relationship between the application type and available document type.
<table>
<tr><th>Operation Interfaces</th><th>Application Type</th><th>Available Document Type</th></tr>
<tr><td rowspan="3">Operation Panel</td><td>Document Server Function</td><td>Document Server user document, fax document</td></tr>
<tr><td>Scanner Function</td><td>Scanner user document</td></tr>
<tr><td>Fax Function</td><td>Fax document,
received fax document</td></tr>
<tr><td rowspan="2">Client computer (Web browser)</td><td>Document Server Function</td><td>Document Server user document, scanner user document (operation permission for Scanner Function is required for the applicable normal user),
fax document (operation permission for Fax Function is required for the applicable normal user)</td></tr>
<tr><td>Fax Function</td><td>Received fax document (operation permission for Document Server Function is required for the applicable normal user)</td></tr>
<tr><td>Client computer (printer driver)</td><td>Printer Function</td><td>Document Server user document</td></tr>
<tr><td>Client computer (fax driver)</td><td>Fax Function</td><td>Fax document</td></tr>
</table>
2) Limit the operation for each normal user
When the document user list associated with the user documents includes the login user name of the normal user associated with the normal user process, the user document operations of reading (print, download, fax, e-mail and folder transmission) and deletion are allowed for that normal user process.</td></tr>
</table>

Table 19: Rules on User Jobs (a)

Subject	Operation on Object	Rule Governing Access
Normal user process	Deletion of user job	When the login user name of normal user associated with the normal user process matches the login user name of normal user associated with the user job, deletion of user job is allowed for that normal user process.

FDP_ACF.1.3(a) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules that explicitly authorise access of subjects to objects shown in Table 20]**.

Table 20: Rules That Explicitly Authorise Access (a)

Subject	Operations on Object	Rules That Explicitly Authorise Access
MFP administrator process	Deletion of user document	Allows the MFP administrator process to delete all of the stored user documents.
MFP administrator process	Deletion of user job	Allows the MFP administrator process to delete all user jobs.

FDP_ACF.1.4(a) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[assignment: rules that deny the operations on the user documents and user jobs when logged in with login user name of supervisor]**.

FDP_ACF.1(b) Security attribute based access control

Hierarchical to: No other components.

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

FDP_ACF.1.1(b) The TSF shall enforce the **[assignment: TOE function access control SFP]** to objects based on the following: **[assignment: subjects or objects, and their corresponding security attributes shown in Table 21]**.

Table 21: Subjects, Objects and Security Attributes (b)

Category	Subject or Object	Security Attributes
Subject	Normal user process	Login user name of normal user, available function list
Object	MFP application	Function type

FDP_ACF.1.2(b) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[assignment: operations on objects by subjects and rules governing access to operations shown in Table 22]**.

Table 22: Rules Governing the Operation for MFP Application (b)

Subject	Operation on Object	Rule That Controls Operation
Normal user process	Execution of MFP application	When the function type associated with the MFP application is included in the available function list associated with the normal user process, execution of that MFP application is allowed for the normal user process. The MFP administrator registers the available MFP applications for each normal user on the available function list in advance.

FDP_ACF.1.3(b) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules that the Fax Reception Function operated using administrator permission is surely permitted]**.

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

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **[selection: deallocation of the resource from]** the following objects: **[assignment: user documents]**.

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 The TSF shall detect when **[selection: an administrator configurable positive integer within [assignment: 1 to 5]]** unsuccessful authentication attempts occur related to **[assignment: the authentication events shown in Table 23]**.

Table 23: List of Authentication Events and Unsuccessful Authentication Attempts

Authentication Events
User authentication using the Operation Panel
User authentication using the TOE from client computer Web browser
User authentication when printing from the client computer
User authentication when using LAN Fax from client computer

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **[selection: met]**, the TSF shall **[assignment: perform actions shown in Table 24]**.

Table 24: List of Actions for Authentication Failure

Unsuccessfully Authenticated User	Actions for Authentication Failure
Normal user	The lockout for the normal user is released by the lockout time (60 minutes by default) set by the MFP administrator, or release operation by the MFP administrator.
Supervisor	The lockout for a supervisor is released by the lockout time (60 minutes by default) set by the MFP administrator, release operation by the MFP administrator or the TOE's restart.
MFP administrator	The lockout for the MFP administrator is released by the lockout time (60 minutes by default) set by the MFP administrator, release operation by a supervisor or the TOE's restart.

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: the security attributes listed in Table 25 for each user in Table 25]**.

Table 25: List of Security Attributes for Each User That Shall Be Maintained

User	List of Security Attributes
Normal user	- Login user name of normal user - Available function list
Supervisor	- Login user name of supervisor
MFP administrator	- Login user name of MFP administrator

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: the following quality metrics]**.

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

(2) Registrable password length:
For normal users:
No fewer than the Minimum Password Length specified by MFP administrator (8-32 characters) and no more than 128 characters.
For MFP administrators and a supervisor:
No fewer than the Minimum Password Length specified by MFP administrator (8-32 characters) and no more than 32 characters.

(3) Rule:
Passwords that are composed of a combination of characters based on the Password Complexity Setting specified by the MFP administrator can be registered. The MFP administrator specifies either Level 1 or Level 2 for Password Complexity Setting.

FIA_UAU.1 Timing of authentication

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.1.1	The TSF shall allow **[assignment: the viewing of the list of user jobs, Web Image Monitor Help from a Web browser, system status, counter and information of inquiries, and execution of fax reception]** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

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 dummy letters as authentication feedback on the Operation Panel]** to the user while the authentication is in progress.

FIA_UID.1 Timing of identification

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	The TSF shall allow **[assignment: the viewing of the list of user jobs, Web Image Monitor Help from a Web browser, system status, counter and information of inquiries, and execution of fax reception]** on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	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: login user name of normal user, application type, login user name of supervisor, login user name of MFP administrator, and available function list]**.

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 26]**.

Table 26: Rules for Initial Association of Attributes

User	Subject	User Security Attribute
Normal user	Normal user process	- Login user name of normal user - Application type - Available function list
Supervisor	Supervisor process	- Login user name of supervisor
MFP administrator	MFP administrator process	- Login user name of MFP administrator

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: none]**.

6.1.5 Class FMT: Security management

FMT_MSA.1(a)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 Function

FMT_MSA.1.1(a) The TSF shall enforce the **[assignment: common access control SFP]** to restrict the ability to **[selection: query, modify, delete, [assignment: newly create]]** the security attributes **[assignment: security attributes in Table 27]** to **[assignment: the user roles in Table 27]**.

Table 27: User Roles for Security Attributes (a)

Security Attributes	Operations	User Roles
Login user name of normal user	Query, modify, newly create, delete	MFP administrator
	Query	Normal user who owns the applicable login user name
Application type	No operations permitted	-
Login user name of supervisor	Query,	Supervisor

	modify	
Login user name of MFP administrator	Newly create	MFP administrator
	Query, modify	MFP administrator who owns the applicable login user name
	Query	Supervisor
Document type	No operations permitted	-
Document user list of user documents including the following document types: Document Server user document, scanner user document and fax document.	Query, modify	MFP administrator, applicable normal user who stored the document
Document user list of user documents including received fax documents.	Query, modify	MFP administrator

-: No user roles are permitted for operations by the TOE.

FMT_MSA.1(b)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 Function

FMT_MSA.1.1(b)The TSF shall enforce the **[assignment: TOE function access control SFP]** to restrict the ability to **[selection: query, modify, delete, [assignment: newly create]]** the security attributes **[assignment: security attributes in Table 28]** to **[assignment: the user roles in Table 28]**.

Table 28: User Roles for Security Attributes (b)

Security Attributes	Operations	User Roles
Login user name of normal user	Query, modify, newly create, delete	MFP administrator
	Query	Normal user who owns the applicable login user name
Available function list	Query, modify	MFP administrator
	Query	Applicable normal user
Function type	No operations permitted	-

-: No user roles are permitted for operations by the TOE.

FMT_MSA.3(a)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(a) The TSF shall enforce the **[assignment: common access control SFP]** to provide **[selection: [assignment: the property for each security attribute shown in Table 29]]** default values for security attributes that are used to enforce the SFP.

Table 29: Properties of Static Attribute Initialisation (a)

Object	Security Attributes	Default Value	Property
User document	Type of document	The value of MFP application that was used when storing the user document. For the documents stored using Copy Function, Printer Function or Document Server Function, the value is "Document Server user document". For the documents stored using Scanner Function, it is "scanner user document". For the documents stored using Fax Data Storage Function, "fax document". For the documents stored using Fax Reception Function, "received fax documents".	Restrictive
User document (when its document type is any of the following: Document Server user document, scanner user document, or fax document)	Document user list	Login user name of the normal user who stored the user document	Restrictive
User document (received fax document)	Document user list	Login user name of the normal user who is listed in the users for stored and received documents.	Restrictive
User job	Login user name of normal user	Normal user who newly created the user job.	Restrictive

FMT_MSA.3.2(a) The TSF shall allow the **[assignment: authorised identified roles shown in Table 30]** to specify alternative initial values to override the default values when an object or information is created.

Table 30: Authorised Identified Roles Allowed to Override Default Values

Object	Security Attributes	Authorised Identified Role
User document	Type of document	- No authorised identified roles
User document (when its document type is any of the following: Document Server user document, scanner user document, or fax document)	Document user list	- MFP administrator - Normal user who stored the applicable user document
User document (received fax document)	Document user list	- No authorised identified roles
User job	Login user name of normal user	- No authorised identified roles

FMT_MSA.3(b) 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(b) The TSF shall enforce the **[assignment: TOE function access control SFP]** to provide **[selection: [assignment: the permissive to the available function list, restrictive to the function type]]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(b) The TSF shall allow the **[assignment: MFP administrator for the available function list, no authorised identified roles for the function type]** to specify alternative initial values to override the default values when an object or information is created.

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: newly create]]** the **[assignment: list of TSF data in Table 31]** to **[assignment: the user roles in Table 31]**.

Table 31: List of TSF Data

TSF Data	Operation	User Role
Login password of normal user	Newly create, modify	MFP administrator
	Modify	Normal user who owns the login password
Login password of supervisor	Modify	Supervisor
Login password of MFP administrator	Modify	Supervisor
	Newly create	MFP administrator
	Modify	MFP administrator who owns the login password
Number of Attempts before Lockout	Query	MFP administrator
Setting for Lockout Release Timer	Query	MFP administrator
Lockout time	Query	MFP administrator
Date setting (year, month, day), time setting (hour, minute)	Query, modify	MFP administrator
	Query	Supervisor, normal user
Minimum Password Length	Query	MFP administrator
Password Complexity Setting	Query	MFP administrator
Audit logs	Query, delete	MFP administrator
HDD cryptographic key	Newly create	MFP administrator
S/MIME user information	Newly create, modify, query, delete	MFP administrator
	Query	Normal user
Destination information for folder transmission	Newly create, modify, query, delete	MFP administrator
	Query	Normal user
Users for stored and received documents	Query, modify	MFP administrator

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **[assignment: management functions shown in Table 32]**.

Table 32: List of Specification of Management Functions

Management Functions
New creation, query, modification, and deletion of the login user name of normal user by MFP administrator
Query of own login user name by normal user
Query and modification of login user name of supervisor by supervisor
New creation of login user name of MFP administrator by MFP administrator
Query and modification of own login user name by MFP administrator
Query of login user name of MFP administrator by supervisor
New creation and modification of login password of normal user by MFP administrator
Modification of own login password by normal user
Modification of login password of supervisor by supervisor
Modification of login password of MFP administrator by supervisor
New creation of login password of MFP administrator by MFP administrator
Modification of own login password by MFP administrator
Query of Minimum Password Length by MFP administrator
Query of Password Complexity by MFP administrator
Query of Number of Attempts before Lockout by MFP administrator
Query of Lockout Release Timer Setting by MFP administrator
Query of lockout time by MFP administrator
Query and modification of document user list by MFP administrator
Query and modification of document user list by the normal user who stored the document
Query and modification of available function list by MFP administrator
Query of own available function list by normal user
Query and modification of date and time by MFP administrator
Query of date and time by supervisor
Query of date and time by normal user
Query and deletion of audit logs by MFP administrator
New creation of HDD encryption key by MFP administrator
New creation, modification, query and deletion of S/MIME user information by MFP administrator
Query of S/MIME user information by normal user
New creation, modification, query and deletion of destination information for folder transmission by MFP administrator
Query of destination information for folder transmission by normal user
Query and modification of users for stored and received documents by MFP administrator

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: normal user, supervisor and MFP administrator]**.

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: the MFP Control Software, FCU Control Software]]**.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of **[selection: [assignment: the audit log data file]]**.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of **[selection: [assignment: the stored TSF executable code]]**.

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on **[assignment: the Operation Panel, LAN, telephone line]** from being forwarded without further processing by the TSF to **[assignment: the LAN and telephone line]**.

6.1.7 Class FTA: TOE access

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a **[assignment: elapsed time of auto logout, completion of print data reception from the printer driver, and completion of transmission information reception from the fax driver]**.

6.1.8 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, another trusted IT product]** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **[assignment: communication via the LAN of document data, function data, protected data, and confidential data]**.

6.2 Security Assurance Requirements

The evaluation assurance level of this TOE is EAL3+ALC_FLR.2. Table 33 lists the assurance components of the TOE. ALC_FLR.2 was added to the set of components defined in evaluation assurance level 3 (EAL3).

Table 33: TOE Security Assurance Requirements (EAL3+ALC_FLR.2)

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 model
	ALC_FLR.2	Flaw reporting procedures
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

Assurance Classes	Assurance Components	
	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 section describes the rationale for security requirements.

If all security functional requirements are satisfied as below, the security objectives defined in "4 Security Objectives" are fulfilled.

6.3.1 Tracing

Table 34 shows the relationship between the TOE security functional requirements and TOE security objectives. Table 34 shows that each TOE security functional requirement fulfils at least one TOE security objective.

Table 34: Relationship between Security Objectives and Functional Requirements

	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.STORAGE.ENCRYPTED
FAU_GEN.1										X	
FAU_GEN.2										X	
FAU_STG.1										X	
FAU_STG.4										X	
FAU_SAR.1										X	
FAU_SAR.2										X	
FCS_CKM.1											X
FCS_COP.1											X
FDP_ACC.1(a)	X	X	X								

FDP_ACC.1(b)							X				
FDP_ACF.1(a)	X	X	X								
FDP_ACF.1(b)							X				
FDP_RIP.1	X	X									
FIA_AFL.1							X				
FIA_ATD.1							X				
FIA_SOS.1							X				
FIA_UAU.1							X	X			
FIA_UAU.7							X				
FIA_UID.1							X	X			
FIA_USB.1							X				
FPT_FDI_EXP.1								X			
FMT_MSA.1(a)	X	X	X								
FMT_MSA.1(b)							X				
FMT_MSA.3(a)	X	X	X								
FMT_MSA.3(b)							X				
FMT_MTD.1				X	X	X					X
FMT_SMF.1				X	X	X					X
FMT_SMR.1				X	X	X					X
FPT_STM.1										X	
FPT_TST.1									X		
FTA_SSL.3							X	X			
FTP_ITC.1	X	X	X	X	X	X					

6.3.2 Justification of Traceability

This section describes below how the TOE security objectives are fulfilled by the TOE security functional requirements corresponding to the TOE security objectives.

O.DOC.NO_DIS Protection of document disclosure

O.DOC.NO_DIS is the security objective to prevent the documents from unauthorised disclosure by persons without a login user name, or by persons with a login user name but without an access permission to the document. To fulfil this security objective, it is required to implement the following countermeasures.

(1) Specify and implement the access control to the user document.
FDP_ACC.1(a) and FDP_ACF.1(a) restrict the reading of user document by the user role. Additionally, the normal users are restricted to read the user document by the operation permission granted to them. To normal users, the available document type of the user document is restricted by the executing MFP application, and the normal user can read only user document for which the reading permission is granted. The MFP administrator and supervisor are not allowed to read the user documents.

(2) Prevent reading the deleted documents, temporary documents and their fragments.
Deleted documents, temporary documents and their fragments are prevented from being read by FDP_RIP.1.

(3) Use trusted channels for sending or receiving user documents.
The user documents sent and received from the LAN interface are protected by FTP_ITC.1.

(4) Management of the security attributes.
FMT_MSA.1(a) specifies the available operations (newly create, query, modify and delete) on the login user name, and available operations (query and modify) on the document user list, and a specified user is thus restricted to perform each operation.
FMT_MSA.3(a) sets the defined default value to the document user list and document type which are the security attributes of the user document (object) when the user document is generated.

By satisfying FDP_ACC.1(a), FDP_ACF.1(a), FDP_RIP.1, FTP_ITC.1, FMT_MSA.1(a) and FMT_MSA.3(a), which are the security functional requirements for these countermeasures, O.DOC.NO_DIS is fulfilled.

O.DOC.NO_ALT Protection of document alteration

O.DOC.NO_ALT is the security objective to prevent the documents from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the document. To fulfil this security objective, it is required to implement the following countermeasures.

(1) Specify and implement the access control to user document.
FDP_ACC.1(a) and FDP_ACF.1(a) restrict the deletion (there is no "editing operation" of user documents) of user document by the user role. Additionally, the normal users are restricted to delete the user document by the operation permission granted to them. To normal users, the available document type of user document is restricted by the executing MFP application, and the normal user can delete only user document for which the deleting permission is granted. The MFP administrator is allowed to delete the user documents. The supervisor is not allowed to delete the user documents.

(2) Prevent deleting the deleted documents, temporary documents and their fragments.
Deleted documents, temporary documents and their fragments are prevented from being used by FDP_RIP.1.

(3) Use trusted channels for sending or receiving user documents.
The user documents sent and received from the LAN interface are protected by FTP_ITC.1.

(4) Management of the security attributes.
FMT_MSA.1(a) specifies the available operations (newly create, query, modify and delete) on the login user name, and available operations (query and modify) on the document user list, and a specified user is thus restricted to perform each operation.
FMT_MSA.3(a) sets the defined default value to the document user list and document type which are the security attributes of the user document (object) when the user document is generated.

By satisfying FDP_ACC.1(a), FDP_ACF.1(a), FDP_RIP.1, FTP_ITC.1, FMT_MSA.1(a) and FMT_MSA.3(a), which are the security functional requirements for these countermeasures, O.DOC.NO_ALT is fulfilled.

O.FUNC.NO_ALT Protection of user job alteration

O.FUNC.NO_ALT is the security objective to prevent the user jobs from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the user job. To fulfil this security objective, it is required to implement the following countermeasures.

(1) Specify and implement the access control to user document.
FDP_ACC.1(a) and FDP_ACF.1(a) determine the accessible user jobs and permitted operation on the user job for each normal user, and consequently, this permits the access to the user job for each normal user.

(2) Use trusted channels for sending or receiving user jobs.
The user jobs sent and received from the LAN interface are protected by FTP_ITC.1.

(3) Management of the security attributes.
FMT_MSA.1(a) specifies the available operations (newly create, query, modify and delete) on the login user name, and available operations (query and modify) on the document user list, and a specified user is thus restricted to perform each operation.
FMT_MSA.3(a) associates the login user name of the normal user who generated the job as the defined default value with the document user list and document type which are the security attributes of the user document (object) when the user job is generated.

By satisfying FDP_ACC.1(a), FDP_ACF.1(a), FTP_ITC.1, FMT_MSA.1(a) and FMT_MSA.3(a), which are the security functional requirements for these countermeasures, O.FUNC.NO_ALT is fulfilled.

O.PROT.NO_ALT Protection of TSF protected data alteration

O.PROT.NO_ALT is the security objective to allow only users who can maintain the security to alter the TSF protected data. To fulfil this security objective, it is required to implement the following countermeasures.

(1) Management of the TSF protected data.
By FMT_MTD.1, only the MFP administrator is allowed to manage the date, time, S/MIME user information, destination folder and users for stored and received documents.

(2) Specification of the Management Function.
FMT_SMF.1 performs the required Management Functions for Security Function.

(3) Specification of the roles.
FMT_SMR.1 maintains the users who have the privileges.

(4) Use trusted channels for sending or receiving the TSF protected data.
The TSF protected data sent and received from the LAN interface are protected by FTP_ITC.1.

By satisfying FMT_MTD.1, FMT_SMF.1, FMT_SMR.1 and FTP_ITC.1, which are the security functional requirements for these countermeasures, O.PROT.NO_ALT is fulfilled.

O.CONF.NO_DIS Protection of TSF confidential data disclosure

O.CONF.NO_DIS is the security objective to allow only users who can maintain the security to disclose the TSF confidential data. To fulfil this security objective, it is required to implement the following countermeasures.

(1) Management of the TSF confidential data.
FMT_MTD.1 allows the MFP administrator and applicable normal user to operate the login password of normal user. A supervisor is allowed to operate the login password of supervisor. The supervisor and applicable MFP administrator are allowed to operate the login password of MFP administrator. The MFP administrator is only allowed to operate the audit log and HDD cryptographic key.

(2) Specification of the Management Function.
FMT_SMF.1 performs the required Management Functions for Security Function.

(3) Specification of the roles.
FMT_SMR.1 maintains the users who have the privileges.

(4) Use trusted channels for sending or receiving TSF confidential data.
The TSF confidential data sent and received from the LAN interface are protected by FTP_ITC.1.

By satisfying FMT_MTD.1, FMT_SMF.1, FMT_SMR.1 and FTP_ITC.1, which are the security functional requirements for these countermeasures, O.CONF.NO_DIS is fulfilled.

O.CONF.NO_ALT Protection of TSF confidential data alteration

O.CONF.NO_ALT is the security objective to allow only users who can maintain the security to alter the TSF confidential data. To fulfil this security objective, it is required to implement the following countermeasures.

(1) Management of the TSF confidential data.
FMT_MTD.1 allows the MFP administrator and applicable normal user to operate the login password of normal user. A supervisor is allowed to operate the login password of supervisor. The supervisor and applicable MFP administrator are allowed to operate the login password of MFP administrator. The MFP administrator is only allowed to operate the audit log and newly create an HDD cryptographic key.

(2) Specification of the Management Function.
FMT_SMF.1 performs the required Management Functions for Security Function.

(3) Specification of the roles.
FMT_SMR.1 maintains the users who have the privileges.

(4) Use trusted channels for sending or receiving TSF confidential data.
The TSF confidential data sent and received from the LAN interface are protected by FTP_ITC.1.

By satisfying FMT_MTD.1, FMT_SMF.1, FMT_SMR.1 and FTP_ITC.1, which are the security functional requirements for these countermeasures, O.CONF.NO_ALT is fulfilled.

O.USER.AUTHORIZED User identification and authentication

O.USER.AUTHORIZED is the security objective to restrict users so that only valid users can use the TOE functions. To fulfil this security objective, it is required to implement the following countermeasures.

(1) Identify and authenticate the users prior to the TOE use.
FIA_UID.1 identifies the users prior to the TOE use.
FIA_UAU.1 authenticates the users if the user is the registered user or not prior to the TOE use.

(2) Allow the successfully identified and authenticated user to use the TOE.
FIA_ATD.1 and FIA_USB.1 manage the access procedures to the protected assets of the users who are

defined in advance, and associate the users who are successfully identified and authenticated with the access procedures.
FDP_ACC.1(b) and FDP_ACF.1(b) allow the applicable normal user to use the MFP application according to the operation permission granted to the successfully identified and authenticated normal user.

(3) Complicate decoding of login password.
FIA_UAU.7 displays dummy letters as authentication feedback on the Operation Panel and prevents the login password from disclosure.
FIA_SOS.1 accepts only passwords that satisfy the Minimum Password Length and password character combination specified by the MFP administrator, and makes it difficult to guess the password.
FIA_AFL.1 does not allow the user who is unsuccessfully authenticated for certain times to access to the TOE for certain period.

(4) Terminate login automatically.
FTA_SSL.3 automatically logs out the user after no operation is performed from the Operation Panel and a Web browser for certain period and the auto logout time elapses. It also logs out the status of document data reception after the completion of document data reception from the printer driver or fax driver.

(5) Management of the security attributes.
According to FMT_MSA.1(b), the login user name and available function list of normal user are managed by the MFP administrator, and users are not allowed to operate the function type.
FMT_MSA.3(b) sets the permissive default value to the available function list, and sets the restrictive default value to the function type.

By satisfying FDP_ACC.1(b), FDP_ACF.1(b), FIA_UID.1, FIA_UAU.1, FIA_ATD.1, FIA_USB.1, FIA_UAU.7, FIA_AFL.1, FIA_SOS.1, FTA_SSL.3, FMT_MSA.1(b) and FMT_MSA.3(b), which are the security functional requirements for these countermeasures, O.USER.AUTHORIZED is fulfilled.

The function for 2600.1-SMI (F.SMI), selected SFR Package from the PP, is used in conjunction with the function whose access control is enforced by FDP_ACC.1(b) and FDP_ACF.1(b). Therefore, the access control for F.SMI is included with the access control by FDP_ACC.1(b) and FDP_ACF.1(b) and fulfilled.

O.INTERFACE.MANAGED Management of external interfaces by TOE

O.INTERFACE.MANAGED is the security objective to protect the communication path when the TOE sends and receives the protected assets. To fulfil this security objective, it is required to implement the following countermeasures.

(1) Identify and authenticate the users prior to use the Operation Panel and LAN interface.
FIA_UID.1 identifies the users prior to their use of the Operation panel and LAN interface.
FIA_UAU.1 authenticates the registered users prior to their use of the Operation Panel and LAN interface.

(2) Automatically terminate the connection to the Operation Panel and LAN interface.
FTA_SSL.3 terminates the session after no operation is performed from the Operation Panel or LAN interface for certain period.

(3) Restricted forwarding of data to external interfaces.
FPT_FDI_EXP.1 prevents the data received from the Operation Panel, LAN interface and telephone line from being transmitted from the LAN or telephone line without further processing by the TSF.

By satisfying FIA_UID.1, FIA_UAU.1, FTA_SSL.3 and FPT_FDI_EXP.1, which are the security functional requirements for these countermeasures, O.INTERFACE.MANAGED is fulfilled.

O.SOFTWARE.VERIFIED Software verification

O.SOFTWARE.VERIFIED is the security objective to ensure the MFP Control Software and FCU Control Software are verified. To fulfil this security objective, it is required to implement the following countermeasures.

(1) Self-check
FPT_TST.1 checks if the MFP Control Software and FCU Control Software are verified software at the start-up.

By satisfying FTP_TST.1, which is the security functional requirement for this countermeasure, O.SOFTWARE.VERIFIED is fulfilled.

O.AUDIT.LOGGED Management of audit log records

O.AUDIT.LOGGED is the security objective to record the audit log required to detect the security intrusion, and allow the MFP administrator to view the audit log. To fulfil this security objective, it is required to implement the following countermeasures.

(1) Record the audit log.
FAU_GEN.1 and FAU_GEN.2 record the events, which should be auditable, with the identification information of the occurrence factor.

(2) Protect the audit log.
FAU_STG.1 protects the audit logs from the alteration, and FAU_STG.4 deletes the audit logs that have the oldest time stamp, and records the new audit logs if auditable events occur and the audit log files are full.

(3) Provide Audit Function.
FAU_SAR.1 allows the MFP administrator to read audit logs in a format that can be audited. FAU_SAR.2 prohibits the persons other than the MFP administrator reading the audit logs.

(4) Reliable occurrence time of the event
FPT_STM.1 provides a trusted time stamp, and a reliable record of the times when events occurred are recorded in the audit log.

By satisfying FAU_GEN.1, FAU_GEN.2, FAU_STG.1, FAU_STG.4, FAU_SAR.1, FAU_SAR.2 and FPT_STM.1, which are the security functional requirements for these countermeasures, O.AUDIT.LOGGED is fulfilled.

O.STORAGE.ENCRYPTED Encryption of storage devices

O.AUDIT.LOGGED is the security objective to ensure the encryption when writing data into the HDD, and decryption when reading data from the HDD. To fulfil this security objective, it is required to implement the following countermeasures.

(1) Generate appropriate cryptographic keys.
FCS_CKM.1 generates the cryptographic key for encryption.

(2) Perform cryptographic operation.
FCS_COP.1 encrypts the data to be stored in the HDD, and decrypts the data to be read from the HDD.

(3) Manage the TSF data.
FMT_MTD.1 allows the MFP administrator to manage the cryptographic keys.

(4) Specification of Management Function.
FMT_SMF.1 performs the required Management Functions for Security Function.

(5) Specification of the roles.
FMT_SMR.1 maintains the users who have the privileges.

By satisfying FCS_CKM.1, FCS_COP.1, FMT_MTD.1, FMT_SMF.1 and FMT_SMR.1, which are the security functional requirements for these countermeasures, O.STORAGE.ENCRYPTED is fulfilled.

6.3.3 Dependency Analysis

Table 35 shows the result of dependency analysis in this ST for the TOE security functional requirements.

Table 35: Result of Dependency Analysis of TOE Security Functional Requirements

TOE Security Functional Requirements	Claimed Dependencies	Dependencies Satisfied in ST	Dependencies Not Satisfied in ST
FAU_GEN.1	FPT_STM.1	FPT_STM.1	None
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1	None
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	None
FAU_STG.4	FAU_STG.1	FAU_STG.1	None
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	None
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	None
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	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(a)	FDP_ACF.1(a)	FDP_ACF.1(a)	None
FDP_ACC.1(b)	FDP_ACF.1(b)	FDP_ACF.1(b)	None
FDP_ACF.1(a)	FDP_ACC.1(a) FMT_MSA.3(a)	FDP_ACC.1(a) FMT_MSA.3(a)	None
FDP_ACF.1(b)	FDP_ACC.1(b)	FDP_ACC.1(b)	None

	FMT_MSA.3(b)	FMT_MSA.3(b)	
FDP_RIP.1	None	None	None
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	None
FIA_ATD.1	None	None	None
FIA_SOS.1	None	None	None
FIA_UAU.1	FIA_UID.1	FIA_UID.1	None
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	None
FIA_UID.1	None	None	None
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	None
FPT_FDI_EXP.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1	None
FMT_MSA.1(a)	[FDP_ACC.1(a) or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1(a) FMT_SMR.1 FMT_SMF.1	None
FMT_MSA.1(b)	[FDP_ACC.1(b) or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1(b) FMT_SMR.1 FMT_SMF.1	None
FMT_MSA.3(a)	FMT_MSA.1(a) FMT_SMR.1	FMT_MSA.1(a) FMT_SMR.1	None
FMT_MSA.3(b)	FMT_MSA.1(b) FMT_SMR.1	FMT_MSA.1(b) FMT_SMR.1	None
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	None
FMT_SMF.1	None	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.1	None
FPT_STM.1	None	None	None
FPT_TST.1	None	None	None
FTA_SSL.3	None	None	None
FTP_ITC.1	None	None	None

The following explains the rationale for acceptability in all cases where a dependency is not satisfied:

Rationale for Removing Dependencies on FCS_CKM.4

Once the MFP administrator generates the cryptographic key that is used for the HDD encryption of this TOE at the start of TOE operation, the cryptographic key will be continuously used for the HDD and will not be deleted. Therefore, cryptographic key destruction by the standard method is unnecessary.

6.3.4 Security Assurance Requirements Rationale

This TOE is software for the MFP, which is a commercially available product. The MFP is assumed that it will be used in a general office and this TOE does not assume the attackers with the possibility of moderate or greater level attacks.

Architectural design (ADV_TDS.2) is adequate to show the validity of commercially available products. A high attack potential is required for the attacks that circumvent or tamper with the TSF, which is not covered in this evaluation. The vulnerability analysis (AVA_VAN.2) is therefore adequate for general needs.

However, protection of the secrecy of relevant information is required to make security attacks more difficult, and it is important to ensure a secure development environment. Development security (ALC_DVS.1) is therefore important also.

In order to securely operate the TOE continuously, it is important to appropriately remediate the flaw discovered after the start of TOE operation according to flow reporting procedure (ALC_FLR.2).

Based on the terms and costs of the evaluation, the evaluation assurance level of EAL3+ALC_FLR.2 is appropriate for this TOE.

7 TOE Summary Specification

This section describes the procedures and mechanisms for each functional requirement in which the TOE satisfies the functional requirements described in 6.1

FAU_GEN.1 (Audit data generation)

The TOE generates the audit logs shown in Table 36 at the occurrence of auditable events shown in Table 36, and adds to the audit log files. Basic audit information in Table 36 is data recorded when any kind of auditable event occurs. Expanded audit information is data recorded for the generation of auditable events that requires additional information for audit.

Table 36: Auditable Events and Audit Data

Auditable Events	Audit Logs	
	Basic Audit Information	Expanded Audit Information
Starting Audit Function (*1)	- Starting date/time of event - Ending date/time of event - Types of event - Subject identity - Outcome	-
Ending Audit Function (*1)		-
Success and failure of login operation		-
Table 32 Record of Management Function		-
Date setting (year, month, day), time setting (hour, minute)		-
Termination of session by auto logout.		-
Communication for Web Function		Direction of communication (IN/OUT) and communicating IP address
Folder transmission		Communicating IP address
E-mail transmission		Communicating e-mail address
Printing via networks		Communicating IP address
LAN Fax via networks		Communicating IP address
Storing user documents		-
Reading user documents (print, download, fax transmission, e-mail transmission, and folder transmission)		-
Deleting user documents		-
Success and failure of new creation, modification, and deletion of S/MIME user information		-

Success and failure of new creation, modification, and deletion of destination folder		-

-: No applicable expanded audit information

(*1): The starting of Audit Function is substituted with the event of the TOE start-up.

FAU_GEN.2 (User identity association)

The TOE records each auditable event with the identification information (login user name) of the occurrence factor.

FAU_SAR.1 (Audit review)

The TOE allows only MFP administrator who are successfully identified and authenticated to read the audit log in a text format. The TOE provides its Web Function with the MFP administrator to read the audit log.

FAU_SAR.2 (Restricted audit review)

The TOE allows only MFP administrator who are successfully identified and authenticated to read and delete the audit log. The TOE provides its Web Function with the MFP administrator to read the audit log.

FAU_STG.1 (Protected audit trail storage)

The TOE provides only MFP administrator who are successfully identified and authenticated with the function to read and delete the audit log. It does not provide the users other than the MFP administrator with the function to access to the audit log.

FAU_STG.4 (Prevention of audit data loss)

The TOE writes the new audit log over the oldest audit log when there is insufficient space in the audit log files to append the new audit log.

FCS_CKM.1 (Cryptographic key generation)

The TOE generates the HDD cryptographic keys after receiving the operation instruction from the MFP administrator. If the logged-in user is the MFP administrator, the TOE displays a screen on the Operation Panel that the MFP administrator can use to generate the HDD cryptographic keys.
The MFP administrator uses the Operation Panel to instruct the TOE to generate an HDD cryptographic key, and the TOE generates a 256 bit HDD cryptographic key using the TRNG cryptographic key generation algorithm (compliant with the BSI-AIS31 standard) and stores it in the memory area inside the TOE.

FCS_COP.1 (Cryptographic operation)

The TOE encrypts data before writing it to the HDD, and decrypts data after reading it from the HDD. This process is performed for all data written to and read from the HDD. The following are the specific cryptographic operations:

Table 37: List of Cryptographic Operations for Stored Data Protection

Encryption-triggering Operation	Cryptographic Operations	Standard	Cryptographic Algorithm	Key Size
Writing data to HDD	Encrypt	FIPS197	AES	256 bits
Reading data from HDD	Decrypt			

FDP_ACC.1(a) (Subset access control)

The TOE restricts the following: deleting operation on user documents by the MFP administrator process, operations including deleting, printing, downloading, e-mail transmission, folder transmission, and fax transmission on user documents by the normal user process, and operations on user documents by the supervisor process. It also restricts the deleting operation on user jobs by the MFP administrator process, and deleting operation on own user jobs by the normal user process.

FDP_ACC.1(b) (Subset access control)

The TOE restricts the execution of the MFP applications (Copy Function, Printer Function, Scanner Function, Fax Function and Document Server Function) by the normal user process.

FDP_ACF.1(a) (Security attribute based access control)

The TOE defines the rule between each user role that is allowed to access the user document and user job, and operations allowed to each user role as shown in Table 17, Table 18, Table 19 and Table 20. The TOE provides each user who is allowed to access to the user documents and user jobs with the appropriate operation according to this rule.

For the access to the user document by the normal user, the available document type of user document is determined by the operation interface for normal user, and MFP application executed by the normal user as follows:

- If the MFP application executed from the Operation Panel is the Document Server Function, it is allowed to print and delete the Document Server user document and fax document.
- If the MFP application executed from the Operation Panel is the Scanner Function, it is allowed to e-mail and delete the scanner user document and deliver the scanner user document to a folder.
- If the MFP application executed from the Operation Panel is the Fax Function, it is allowed to fax, print and delete the fax document and deliver the fax document to a folder, and to print and delete the received fax document from the Operation Panel.
- If the MFP application executed from a Web browser is the Document Server Function, it is allowed to print and delete the Document Server user document, to e-mail, download and delete the scanner user document and deliver the scanner user document to a folder, to fax, print, download and delete the fax document. The normal user is required the operation permission for Scanner Function to perform the operation on scanner user document. For the operation for fax document, operation permission for Fax Function is required.
- If the MFP application executed from a Web browser is the Fax Function, it is allowed to print, download and delete the received fax document. The normal user is required the operation permission for Document Server Function to perform the operation on received fax document.

- If the MFP application executed from printer driver is the Printer Function, it is allowed to store the Document Server user document.
- If the MFP application executed from fax driver is the Fax Function, it is allowed to store the fax document.

For access to the user document by the normal user process, the login user name of normal user associated with the normal user process and login user name of normal user in the document user list associated with the user document are checked, and if they match, the above-specified operations are allowed for the normal user process.

The TOE associates the user job with the login user name of the person who newly created the user job as a security attribute.

For access to the user job by the normal user process, the login user name of normal user associated with the normal user process and login user name of the person, who created the user job, associated with the user job are checked, and if they match, the access control is performed and it is allowed for the normal user process to delete the user job.

The access control is also performed for the MFP administrator process, and it is allowed for the MFP administrator process to delete all of the stored user documents and created user jobs.

For the supervisor process, the access control is performed and operations on all of the stored user documents and created user jobs are denied.

FDP_ACF.1(b) (Security attribute based access control)

The TOE defines the rule between the user role allowed to access the Copy Function, Printer Function, Scanner Function, Fax Function and Document Server Function, and operations allowed to each user role as shown in Table 21 and Table 22. It provides each user who is allowed to access to the MFP applications with the appropriate operation according to this rule.

The TOE associates the normal user process with the login user name of normal user, and available function list (the list of functions that the normal user is allowed to access) as a security attribute.

For access to the MFP application by the normal user process, the TOE checks if the available function list associated with the normal user process contains the function type (any of the following: Copy Function, Printer Function, Scanner Function, Fax Function and Document Server Function) that the normal user attempts to use as the attribute of the MFP application. If it does, the access control is performed and the normal user process is allowed to execute the function.
It is always allowed to execute the fax reception function that if it is operated using administrator permission.

FDP_RIP.1 (Subset residual information protection)

When a user deletes a user document, the TOE overwrites the area on the HDD where the digital image data of the user document exists with the specific pattern. It also overwrites the area on the HDD where the temporary document and its fragments that are created during the user job execution exist with the specific pattern after the user job completes.

FIA_AFL.1 (Authentication failure handling)

The TOE counts the number of failed identification and authentication attempts made under each login user name. When a user authenticates successfully, the TOE resets the number of available authentication attempts for that user to 0.

When the number of failed consecutive attempts reaches the MFP administrator-specified Number of Attempts before Lockout, the TOE locks out that user.

The MFP administrator specifies 1 to 5 as the Number of Attempts before Lockout.

The TOE releases the lockout for the user who satisfies any of the following:

(1) Lockout release by a time-based operation
If a user fails to authenticate after making the number of attempts specified to initiate lockout, and the lockout time has elapsed, then lockout will be released. The MFP administrator specifies the lockout time (60 minutes by default). The elapsed time from the initiation of lockout is timed for each locked out user.

(2) Lockout release by unlocking administrator
The unlocking administrator specified for each user role releases the lockout. Table 38 shows the unlocking administrators for each user role.

Table 38: Unlocking Administrators for Each User Role

User Roles (Locked out Users)	Unlocking Administrators
Normal user	MFP administrator
Supervisor	MFP administrator
MFP administrator	Supervisor

(3) Lockout release by turning on/off the TOE
If the administrators (MFP administrator and supervisor) are locked out, restarting the TOE releases the lockout for them.

FIA_ATD.1 (User attribute definition)

The TOE associates the normal user with a login user name of normal user and available function list, supervisor with a login user name of supervisor, and MFP administrator with a login user name of MFP administrator, as security attributes, and it maintains these associations.

FIA_SOS.1 (Verification of secrets)

The TOE provides a function for registering and changing the login passwords of normal users, MFP administrators, and supervisor. This function uses the characters described below in (1).
It checks if the registering or changing password meets the conditions (2) and (3). If it does, the TOE registers the login password. If it does not, it does not register the login password and displays an error message.

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

(2) Registrable password length:
- Normal users
No fewer than the Minimum Password Length specified by MFP administrator (8-32 characters) and no more than 128 characters.
- MFP administrators and a supervisor
No fewer than the Minimum Password Length specified by MFP administrator (8-32 characters) and no more than 32 characters.

(3) Rule:
Passwords that are composed of a combination of characters based on the Password Complexity Setting specified by MFP administrator can be registered. The MFP administrator specifies either Level 1 or Level 2 for Password Complexity Setting.

FIA_UAU.1 (Timing of authentication)

The TOE displays a window on the Operation Panel when no users log in from the Operation Panel. This window requires the users to enter their login user name and password. The TOE displays a window in a Web browser when the Web Function of the TOE is accessed from a client computer. This window also requires the users to enter their login user name and password. In both windows, the TOE authenticates users with the login user name and password entered by them.

When receiving a request from a client computer for printing or storing user documents using Printer Function, the TOE authenticates users with the login user name and password sent from a client computer before printing and storing the user documents. When receiving a request from a client computer for sending and storing user documents using LAN Fax, the TOE authenticates users with the login user name and password sent from a client computer before sending and storing the user documents.

When receiving faxes from telephone line, the TOE does not have the function to authenticate users prior to the function that stores the received data as received fax document. The TOE does not receive any authentication information from telephone line, but executes the fax reception function using the received data.

The TOE allows any users to refer Web Image Monitor Help regardless of the user authentication status when users access to a Web browser from client computer.

The TOE allows the following operations regardless of the user authentication status: reference of the list of user jobs, Web Image Monitor Help from a Web browser, system status, counter, and information of inquiries, and execution of fax reception.

Table 39 shows the identified user by Identification and Authentication Function, and authentication procedures.

Table 39: Functions Provided by the TOE, Identified User and Authentication Procedures

Identified User	Authentication Procedures
Normal user	Checks if the login user name and password of normal user entered from the Operation Panel, Web browser, printer driver and fax driver of the client computer match the login user name and password of normal user registered in the TOE.
Administrator	Checks if the login user name and password of administrator entered from the Operation Panel, Web browser of client computer match the login user name and password of administrator registered in the TOE.

FIA_UAU.7 (Protected authentication feedback)

The TOE displays dummy letters in place of the login password entered from the Operation Panel by users in the authentication feedback area.

FIA_UID.1 (Timing of identification)

The TOE displays a window on the Operation Panel when no users log in from the Operation Panel. This window requires the users to enter their login user name and password. The TOE displays a window in a Web browser when the Web Function of the TOE is accessed from a client computer with no users logged in. This window also requires the users to enter their login user name and password. In both windows, the TOE identifies users with the login user name and password entered by them.

When receiving a request from a client computer for printing or storing user documents using Printer Function, the TOE identifies users with the login user name of the user sent from a client computer before printing and storing the user documents. When receiving a request from a client computer for sending and storing user documents using LAN Fax, the TOE identifies users with the login user name of the user sent from a client computer before sending and storing the user documents.

When receiving faxes from telephone line, the TOE does not have the function to identify users prior to the function that stores the received data as received fax document. The TOE does not receive any identification information from telephone line, but executes the fax reception function using the received data.

The TOE allows any users to refer Web Image Monitor Help regardless of the user identification status when users access to a Web browser from client computer.

The TOE allows the following operations regardless of the user identification status: reference of the list of user jobs, Web Image Monitor Help from a Web browser, system status, counter, and information of inquiries, and execution of fax reception.

FIA_USB.1 (User-subject binding)

For the successfully identified and authenticated users, the TOE binds the normal user with the normal user process, supervisor with the supervisor process, and MFP administrator with the MFP administrator process. The normal user process is associated with the login user name of normal user, application type, and available function list as security attributes. The supervisor process is associated with the login user name of supervisor, and the MFP administrator process is associated with the login user name of MFP administrator as security attributes. These associations are reflected to the operation permissions for each user role.

The TOE also allows creating up to four new MFP administrators, and deleting the MFP administrators. An MFP administrator cannot be deleted if the MFP administrator is assigned to no other persons.

FMT_MSA.1(a) (Management of security attributes)

The TOE allows only specified users to operate the security attributes related to the common access control SFP from the specified operation interfaces. The operations (newly create, query, modify and delete) are available only on the security attributes that can be operated by the users.

Table 40 shows the list of security attributes that can be operated by the users, the permitted users to operate each security attribute and their permitted operations, and the available operation interfaces.

Table 40: Security Attributes Management of Common Access Control SFP

Security Attribute	Operation Interface	Operation	User
Login user name of normal user	Operation Panel Web browser	Newly create, query, modify, delete	MFP administrator
		Query	Normal user who owns the applicable login user name
Application type	No operation interfaces available	No operations permitted	-
Login user name of supervisor	Operation Panel Web browser	Query, modify	Supervisor
Login user name of MFP administrator	Operation Panel Web browser	Newly create	MFP administrator
		Query, modify	MFP administrator who owns the applicable login user name
		Query	Supervisor
Document type	No operation interfaces available	No operations permitted	-
Document user list of user documents including the following document types: Document Server user document, scanner user document and fax document.	Operation Panel Web browser	Query, modify	MFP administrator, applicable normal user who stored the document
Document user list of user documents including received fax documents. (*1)	Operation Panel Web browser	Query, modify	MFP administrator

-: No user roles are permitted for operations by the TOE.

(*1): If MFP administrator modifies the users for stored and received documents, and the document type of document user list of user documents is the received fax document, the list is modified to the value of the users for stored and received documents.

FMT_MSA.1(b) (Management of security attributes)

The TOE allows only specified users to operate the security attributes related to the TOE function access control SFP from the specified operation interfaces.

Table 41 shows the list of security attributes that can be operated by the users, the permitted users to operate each security attribute and their permitted operations, and the available operation interfaces.

Table 41: Security Attributes Management of TOE Function Access Control SFP

Security Attribute	Operation Interface	Operation	User
Login user name of normal user	Operation Panel Web browser	Newly create, query, modify, delete	MFP administrator
		Query	Normal user who owns the applicable login user name
Available function list	Operation Panel Web browser	Query, modify	MFP administrator
		Query	Applicable normal user
Function type	No operation interfaces available	No operations permitted	-

-: No user roles are permitted for operations by the TOE.

FMT_MSA.3(a) (Static attribute initialisation)

The TOE sets the default value for the security attribute in Table 42 that corresponds to the object in Table 42 when generating the object listed in Table 42.

Table 42: List of Static Initialisation for Security Attributes of Common Access Control SFP

Object	Security Attribute	Default Value
User document	Type of document	When any of the following MFP applications is used for storing user documents: Copy Function, Printer Function or Document Server Function, the default value is "Document Server user document". When Scanner Function is used, it is "scanner user document". For Fax Data Storage Function, "fax document". For Fax Reception Function, "received fax documents".
User document (when the document type is any of the following: Document Server user document, scanner user document, or fax document)	Document user list	Login user name of the normal user who stored the user document
User document (received fax document)	Document user list	Login user name of the normal user who is listed in the users for stored and received documents
User job	Login user name of normal user	Login user name of the normal user who newly created the user job

FMT_MSA.3(b) (Static attribute initialisation)

The TOE sets the default value to the available function list and the function type.

When newly creating a normal user, the value that allows any operations of the MFP applications is set to the available function list for the user.

The setting value for the function type is determined for each MFP application. The value set for each function is as follows:

- For Copy Function: the value that identifies the Copy Function.
- For Document Server Function: the value that identifies the Document Server Function.
- For Printer Function: the value that identifies the Printer Function.
- For Scanner Function: the value that identifies the Scanner Function.
- For Fax Function: the value that identifies the Fax Function.

FMT_MTD.1 (Management of TSF data)

The TOE allows only specified users to operate the information of the TSF (TSF data) from the specified operation interfaces as shown in Table 43.

Table 43: Management of TSF Data

TSF Data	Operation Interface	Operation	User Role
Login password of normal user	Operation Panel Web browser	Newly create, modify	MFP administrator
		Modify	Normal user who owns the login password
Login password of supervisor	Operation Panel Web browser	Modify	Supervisor
Login password of MFP administrator	Operation Panel Web browser	Modify	Supervisor
		Newly create	MFP administrator
		Modify	MFP administrator who owns the login password
Number of Attempts before Lockout	Operation Panel Web browser	Query	MFP administrator
Lockout Release Timer	Web browser	Query	MFP administrator
Lockout time	Web browser	Query	MFP administrator
Date (year, month, day)	Operation Panel Web browser	Query, modify	MFP administrator
		Query	Supervisor, normal user
Time	Operation Panel Web browser	Query, modify	MFP administrator
		Query	Supervisor, normal user
Minimum Password Length	Operation Panel	Query	MFP administrator
Password Complexity Setting	Operation Panel	Query	MFP administrator
Audit logs	Web browser	Query, delete	MFP administrator
HDD cryptographic key	Operation Panel	Newly create	MFP administrator
S/MIME user information	Operation Panel Web browser	Newly create, modify query, delete	MFP administrator
		Query	Normal user
Destination information for folder transmission	Operation Panel Web browser	Newly create, modify query, delete	MFP administrator
		Query	Normal user

TSF Data	Operation Interface	Operation	User Role
Users for stored and received documents	Operation Panel Web browser	Query, modify	MFP administrator

FMT_SMF.1 (Specification of Management Functions)

The TOE provides the following Security Management Functions from the Operation Panel and a Web browser:

- New creation, query, modification, and deletion of the login user name of normal user by MFP administrator
- Query of own login user name by normal user
- Query and modification of login user name of supervisor by supervisor
- New creation of login user name of MFP administrator by MFP administrator
- Query and modification of own login user name by MFP administrator
- Query of login user name of MFP administrator by supervisor
- New creation and modification of login password of normal user by MFP administrator
- Modification of own login password by normal user
- Modification of login password of supervisor by supervisor
- Modification of login password of MFP administrator by supervisor
- New creation of login password of MFP administrator by MFP administrator
- Modification of own login password by MFP administrator
- Query of Minimum Password Length by MFP administrator
- Query of Password Complexity by MFP administrator
- Query of Number of Attempts before Lockout by MFP administrator
- Query of Lockout Release Timer Setting by MFP administrator
- Query of lockout time by MFP administrator
- Query and modification of document user list by MFP administrator
- Query and modification of document user list by the normal user who stored the document
- Query and modification of available function list by MFP administrator
- Query of own available function list by normal user
- Query and modification of date and time by MFP administrator
- Query of date and time by supervisor
- Query of date and time by normal user
- Query and deletion of audit logs by MFP administrator
- New creation of HDD cryptographic key by MFP administrator
- New creation, modification, query and deletion of S/MIME user information by MFP administrator

- Query of S/MIME user information by normal user
- New creation, modification, query and deletion of destination folder for folder transmission by MFP administrator
- Query of destination folder for folder transmission by normal user
- Query and modification of users for stored and received documents by MFP administrator

FMT_SMR.1 (Security roles)

The TOE binds the successfully identified and authenticated users with the user role processes associated with them and maintains this binding. When registering users in the TOE, it assigns the user roles of normal user, supervisor or MFP administrator to the users.

The TOE allows only specified users to operate the login user name and password, and maintains the security roles.

MFP administrator is allowed the following operations:

- New creation, modification and deletion of the login user name of normal user
- New creation of login user name of MFP administrator
- New creation of login password of normal user
- New creation of login password of MFP administrator
- Management of users for stored and received documents
- Management of HDD cryptographic key
- New creation, modification and deletion of S/MIME user information
- New creation, modification and deletion of destination folder for folder transmission

An MFP administrator is allowed the following operations:

- Modification of that MFP administrator's login user name

A normal user and MFP administrator are allowed the following operations:

- Query of login user name of that normal user
- Modification of login password of that normal user
- Query of that normal user's S/MIME user information
- Query of that normal user's destination folder for folder transmission

An MFP administrator and supervisor are allowed the following operations:

- Query of login user name of that MFP administrator
- Modification of login password of that MFP administrator

A supervisor is allowed the following operations:

- Query and modification of login user name of supervisor
- Modification of login password of supervisor

FPT_STM.1 (Reliable time stamps)

The TOE records the date (year-month-day) and time (hour-minute-second) for the audit log using the system clock of the TOE.

FPT_TST.1 (TSF testing)

The TOE runs a suite of self tests during the initial start-up after the power is supplied.

For the FCU, the TOE provides the users with the verification information to verify the integrity of executable code of the control software. The users compare the verification information from the TOE to the verification information described in the guidance document, and verify the integrity of the FCU. If no errors are detected, the users can use the TOE.

For configurations other than the FCU, the integrity of executable code of the MFP Control Software and audit log data files is verified. If errors are detected by the integrity verification of executable code of the MFP Control Software, an error message appears on the Operation Panel. The TOE is deactivated and normal users cannot use the TOE. If errors are detected by the integrity verification of the audit log data files, an error message appears on the Operation Panel. The TOE is deactivated and normal users cannot use the TOE. If no errors are detected by both of these verifications, the TOE is activated and users can use it.

FPT_FDI_EXP.1 (Restricted forwarding of data to external interfaces)

The TOE inputs the information after the TSF identifies and authenticates the input information from the Operation Panel or LAN interface. Therefore, the input information cannot be forwarded without the TSF interaction. For the input information from the telephone line, the TOE specifies the Fax Reception Function as the only available function from the telephone lines, and denies the communication that does not conform to the fax protocol. Since the function, which conforms to the fax protocol, to forward data is prohibited at the initial setting, no data is forwarded.

The TSF restricts the Operation Panel, LAN interface and telephone line, therefore, the forwarding of data is not performed without any processing.

FTA_SSL.3 (TSF-initiated termination)

The TOE provides the function to forcibly logout after the user logs in from the Operation Panel and the auto logout time elapses from the last operation from the Operation Panel. The auto logout time (180 seconds by default) is specified by the administrator with machine management privilege.

The TOE provides the function to forcibly logout after the user logs in from a Web browser, and the fixed auto log out time (30 minutes by default) elapses from the last operation from a Web browser.

This TOE has the interface from the printer driver, and provides the function to forcibly logout after it receives the print data from the printer driver. It also has the interface from the fax driver, and provides the function to forcibly logout after it receives the transmission information from the fax driver.

FTP_ITC.1 (Inter-TSF trusted channel)

The TOE provides SSL encrypted communication as a trusted channel to protect the LAN communication between the TOE and a client computer, which is a trusted IT product, for the operations via a Web browser of client computer, and the operations of printing, fax transmission, and fax data storage from client

computer. The TOE provides IPSec communication as a trusted channel to protect the LAN communication between the TOE and a client computer, which is a trusted IT product, for delivering data to an FTP Server and SMB Server, both of which are trusted IT products.

The TOE provides S/MIME communication as a trusted channel of the TSF to protect the LAN communication between the TOE and servers for e-mailing to an SMTP Server, which are trusted IT products.