Aficio MP 2851/3351 series with Fax Option Type 3351

Security Target

Author : RICOH COMPANY, LTD., Yasushi FUNAKI
Date : 2010-06-17
Version : 1.00

Revision History

Version	Date	Author	Details
1.00	2010-06-17	Yasushi FUNAKI	Released version.

Table of Contents

List of Figures

List of Tables

1 ST Introduction

This section describes the ST reference, TOE reference, TOE overview, and TOE description.

1.1 ST Reference

The following are the identification information of this ST.

ST Title : Aficio MP 2851/3351 series with Fax Option Type 3351 Security Target

ST Version : 1.00

Date : 2010-06-17

Author : RICOH COMPANY, LTD., Yasushi FUNAKI

1.2 TOE Reference

This TOE is a digital multi function product (hereafter called an "MFP") with an optional product, Fax Controller Unit (hereafter called an "FCU"), and is identified by the name of the MFP, version of software/hardware, and the name and version of the FCU. The TOE is a combination of one of the following MFPs and an FCU, and also matches the following software/hardware version.

Manufacturer : RICOH COMPANY, LTD.

MFP Name :

Ricoh Aficio MP 2851, Ricoh Aficio MP 3351
Savin 9228, Savin 9233
Lanier LD528, Lanier LD533
Lanier MP 2851, Lanier MP 3351
Gestetner MP 2851, Gestetner MP 3351
nashuatec MP 2851, nashuatec MP 3351
Rex-Rotary MP 2851, Rex-Rotary MP 3351
infotec MP 2851, infotec MP 3351

MFP Software /Hardware Version :

Software	System/Copy	1.00
	Network Support	7.29.3
	Scanner	01.12
	Printer	1.01
	Fax	01.00.00
	Web Support	1.01
	Web Uapl	1.03
	Network Doc Box	1.00
Hardware	Ic Key	1100
	Ic Hdd	01

FCU Name : Fax Option Type 3351

FCU Version : GWFCU3-20(WW) 01.00.00

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

1.3 TOE Overview

This section defines the TOE type, TOE usage and major security features of the TOE, the environment for the TOE usage and non-TOE configuration items.

1.3.1 TOE Type

The TOE is a digital MFP, which is an IT device that provides the functions of a copier, scanner, printer, and fax (optional). These functions are for digitising paper documents and managing and printing them.

1.3.2 TOE Usage and Major Security Features of TOE

The TOE has functions for inputting paper and electronic documents into the TOE, storing the input document data, and outputting it. Paper documents are input using the MFP's scanning device, and electronic documents are input by receiving them from a client computer via a network, USB connection, or fax. The output function includes printing, Fax Transmission, and transferring to networked servers or client computers. The TOE incorporates some of these functions and provides a Copy Function, Scanner Function, Printer Function, and Fax Function.
Users can use these functions from the Operation Panel. Users can also use some of these functions remotely.

The following are the major Security Functions of the TOE in this ST:

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

For the Security Functions listed above, each function is described in "1.4.4.2 Security Functions".

1.3.3 Environment for TOE Usage and Non-TOE Configuration Items

The TOE is assumed to be located in a general office. The TOE can be connected to other devices over a network, telephone line, or USB connection, according to users' needs. Users can operate the TOE from the Operation Panel, a client computer connected to the local network, or a client computer connected to the TOE through USB. Figure 1 shows an example of the assumed TOE environment.

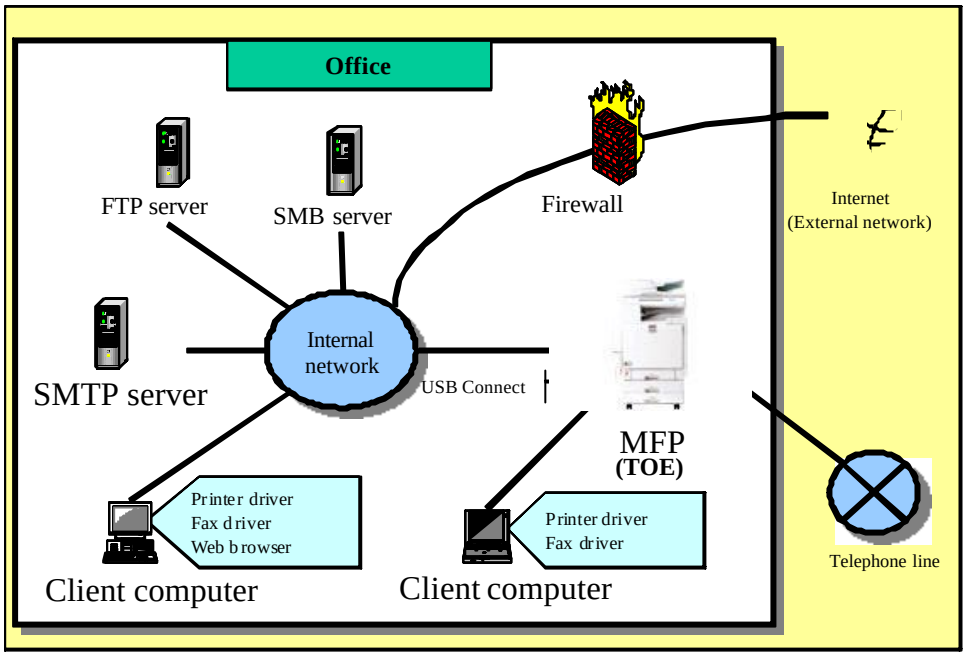

Figure 1: Example TOE environment

The following describes non-TOE configuration:

Internal Network

The internal network connects the TOE with various types of servers (FTP, SMB, and SMTP servers) and client computers. It is connected to the Internet via firewall. IPv4 is for the protocol of the internal network.

Client Computer

A Web browser of a client computer that is connected to the internal network allows users to access and operate the TOE, and permits data communications. Internet Explorer 6.0 or later must be pre-installed on the client computer.
To print and fax from the client computer via the internal network or USB connection, the PCL printer driver and fax driver must be downloaded and installed into the client computer from the website indicated in the user guidance.

FTP Server

An FTP server is used for the TOE to deliver the document data stored in the TOE to folders in the FTP server.

SMB Server

An SMB server is used for the TOE to send the document data stored in the TOE to folders in the SMB server.

SMTP Server

An SMTP server is used for the TOE to send the document data stored in the TOE to a client computer by e-mail.

Telephone Line

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

Firewall

A firewall is a device that is set between the internal and the external network and protects the internal network from the external network.

1.4 TOE Description

This section describes the Physical boundaries of the TOE, user guidance documents, user roles, logical boundaries of the TOE, and protected assets.

1.4.1 Physical Boundaries of TOE

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

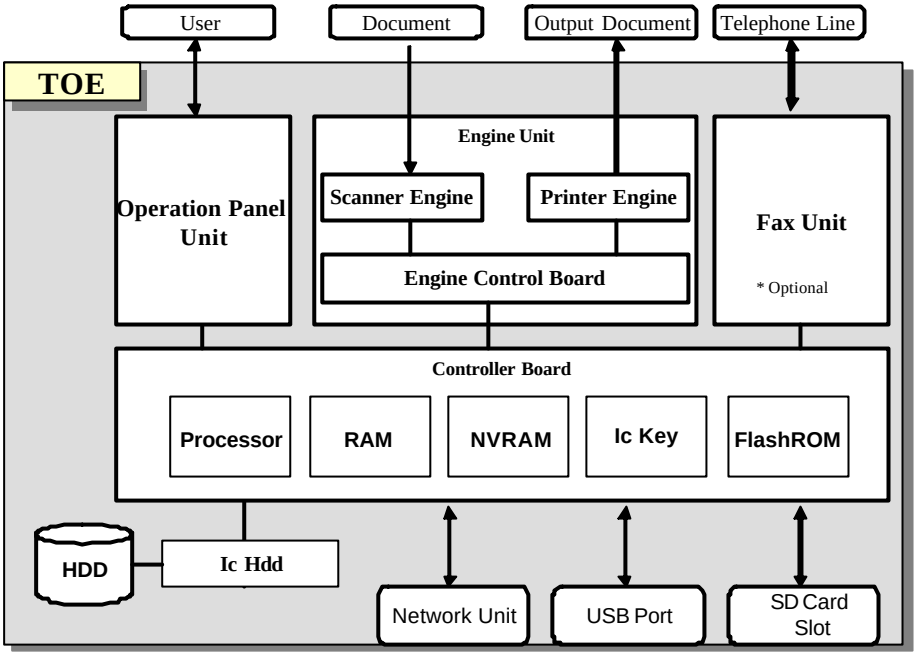

Figure 2: Hardware configuration of TOE

Operation Panel Unit (hereafter "Operation Panel ")

The Operation Panel is an interface device that is installed on the TOE for use by users. It features key switches, LED indicators, an LCD touch screen, and the Operation Panel Control Board. The Operation Panel Control Software is installed in the Operation Panel Control Board. The Operation Panel Control Software controls the LEDs and displays information on the LCD touch screen after input information has been sent from the key switches and LCD touch screen to the MFP Control Software, or in response to direct instructions from the MFP Control Software.

Engine Unit

The Engine Unit contains a Scanner Engine, Printer Engine, and the Engine Control Board. The Scanner Engine is an input device to read the paper documents. The Printer Engine is an output device for printing and outputting of paper documents. The Engine Control Software is installed in the Engine Control Board. The Engine Control Software sends information about the status of 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.

Fax Unit (optional)

The Fax Unit is a device that has a modem function to send and receive fax data when connected to a telephone line.
The Fax Unit has an interface to the MFP Control Software. The interface provides the MFP Control Software with information about the status of fax communications and controls the fax communications according to instructions from the MFP Control Software.

Controller Board

The Controller Board contains Processors, FlashROM, RAM, NVRAM, and Ic Key. It is connected to the Operation Panel Unit, Engine Unit, Fax Unit, Network Unit, USB Port, SD Card Slot, and Ic Hdd. The Ic Hdd is also connected to the HDD. The following are descriptions of these components:

[Processor]

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

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

[RAM]
A volatile memory medium used for image processing.

[NVRAM]
A non-volatile memory medium in which MFP Control Data for configuring the MFP operation is stored.

[Ic Key]
A security chip that generates random numbers and encryption keys, and detects any tampering with the MFP Control Software.

Ic Hdd

A security chip that encrypts information to be stored on the HDD and decrypts information to be read from the HDD.

HDD

The hard disk drive, where image data and user information for identification and authentication are stored.

Network Unit

Network Unit is an interface board for connection to an Ethernet (100BASE-TX/10BASE-T) network.

USB Port

The USB Port is used to connect a client computer to the TOE, print or fax from the client computer.

SD Card Slot

The SD Card Slot is a slot that is used by a customer engineers (hereafter called a "CE") for maintenance work using an SD card. It is located on the side of the TOE, and is normally covered. When a CE performs

maintenance work, s/he removes this cover to insert and remove the SD card.
When installingthe TOE, the CE inserts an SD card into the SD Card Slot to activate the Stored Data Protection Function.

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 characteristics of sales areas and/or companies. Details of the document sets are as follows:

[English version-1]

- 9228/9233
  MP 2851/3351
  LD528/LD533
  Aficio MP 2851/3351
  Operating Instructions
  About This Machine
- 9228/9233
  MP 2851/3351
  LD528/LD533
  Aficio MP 2851/3351
  Operating Instructions
  Troubleshooting
- Notes for Users
- App2Me Start Guide
- Manuals for Users
  9228/9233
  MP 2851/3351
  LD528/LD533
  Aficio MP 2851/3351
- Manuals for Administrators
  9228/9233
  MP 2851/3351
  LD528/LD533
  Aficio MP 2851/3351
- Manuals for Administrators
  Security Reference Supplement
  9228/9233
  MP 2851/3351
  LD528/LD533
  Aficio MP 2851/3351
- Notes for Administrators: Using this Machine in a CC-Certified Environment
- VM Card Manuals

[English version-2]

- Quick Reference Copy Guide
- Quick Reference Fax Guide
- Quick Reference Printer Guide
- Quick Reference Scanner Guide
- Manuals for This Machine
- Safety Information for Aficio MP 2851/Aficio MP 3351
- Notes for Users
- App2Me Start Guide
- Manuals for Users
  MP 2851/3351
  Aficio MP 2851/3351
  A
- Manuals for Administrators
  Security Reference
  MP 2851/3351
  Aficio MP 2851/3351
- Manuals for Administrators
  Security Reference Supplement
  9228/9233
  MP 2851/3351
  LD528/LD533
  Aficio MP 2851/3351
- Notes for Administrators: Using this Machine in a CC-Certified Environment
- VM Card Manuals

[English version-3]

- Quick Reference Copy Guide
- Quick Reference Fax Guide
- Quick Reference Printer Guide
- Quick Reference Scanner Guide
- Manuals for This Machine
- Safety Information for MP 2851/MP 3351
- Notes for Users
- App2Me Start Guide
- Manuals for Users
  MP 2851/3351
  Aficio MP 2851/3351
  A

- Manuals for Administrators
  Security Reference
  MP 2851/3351
  Aficio MP 2851/3351
- Manuals for Administrators
  Security Reference Supplement
  9228/9233
  MP 2851/3351
  LD528/LD533
  Aficio MP 2851/3351
- Notes for Administrators: Using this Machine in a CC-Certified Environment
- VM card Manuals

[English version-4]

- MP 2851/MP 3351
  MP 2851/MP 3351
  Aficio MP 2851/3351
  Operating Instructions
  About This Machine
- MP 2851/MP 3351
  MP 2851/MP 3351
  Aficio MP 2851/3351
  Operating Instructions
  Troubleshooting
- Quick Reference Copy Guide
- Quick Reference FAX Guide
- Quick Reference Printer Guide
- Quick Reference Scanner Guide
- Notes for Users
- App2Me Start Guide
- Manuals for Users
  MP 2851/3351
  Aficio MP 2851/3351
- Manuals for Administrators
  MP 2851/3351
  Aficio MP 2851/3351
- Manuals for Administrators
  Security Reference Supplement
  9228/9233
  MP 2851/3351
  LD528/LD533
  Aficio MP 2851/3351

- Notes for Administrators: Using this Machine in a CC-Certified Environment
- VM Card Manuals

1.4.3 User Roles

This section describes the roles involved in this TOE operation.

1.4.3.1 Responsible Manager of MFP

The "responsible manager" of the MFP is a person who belongs to the organisation that uses the TOE, and has the role of selecting the TOE administrators and TOE supervisor.
The responsible manager of the MFP selects up to four administrators and one supervisor. When selecting administrators, the responsible manager assigns each administrator one or more of the following administrator roles: user administration, machine administration, network administration, and/or file administration.

1.4.3.2 Administrator

An "administrator" is a user who is registered on the TOE as an administrator. One to four administrators can be registered for the TOE. Administrator roles for administrators include user administration, machine administration, network administration, and file administration. Administrators may have concurrent administrator roles, and administrator roles can be assigned to one or more administrators. One default administrator is registered and assigned all four administrator roles as a factory setting. When the TOE is being installed, the administrators who are selected by the responsible manager change the settings of their own administrator IDs, passwords, and administrator roles. Table 1 describes the duties involved in each administrator role.

Table 1: List of administrator roles

Administrator role	Explanation about duties involved
User administration	Managing general users.
Machine administration	Managing machines and performing audits.
Network administration	Managing the TOE's network connections.
File administration	Managing the documents stored in the TOE.

1.4.3.3 Supervisor

The "supervisor" is a user who manages administrator passwords and changes them. One supervisor must be registered for the TOE. A default supervisor is registered for the TOE as a factory setting. The person selected to be a supervisor by the responsible manager can change the supervisor ID and password of the default supervisor.

1.4.3.4 General User

A "general user" is an authorised TOE user who is registered in the Address Book by a user administrator. General users can store document data in the TOE and perform operations on the document data.

1.4.3.5 Customer Engineer

A customer engineer (hereafter "CE") is an expert in maintenance of the TOE and is employed by manufacturers, technical support service companies, and sales companies.

1.4.4 Logical Boundaries of TOE

The logical boundaries of the TOE comprise the functions provided by the TOE. This section describes the "Basic Functions", which is the service provided by the TOE to users, and the "Security Functions", which counter threats to the TOE. These functions are outlined in Figure 3.

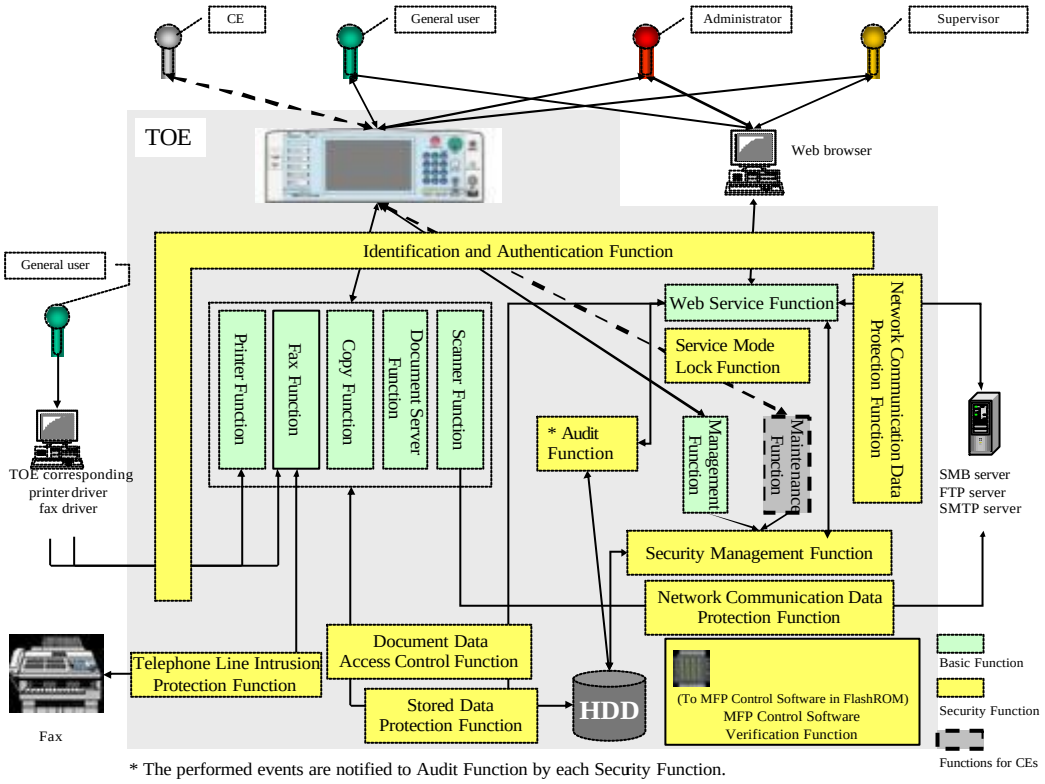

Figure 3: Logical boundaries of TOE

1.4.4.1 Basic Functions

Basic Functions include the Copy Function, Printer Function, Fax Function, Scanner Function, Document Server Function, and Management Function, which are operated from the Operation Panel, and the Web

Service Function, which is operated from the Web browser of a client computer.
General users are provided with the Copy Function, Document Server Function, Printer Function, Fax Function, and Scanner Function. Administrators and supervisors are provided with the Management Function. These functions are accessed by pushing the relevant buttons on the Operation Panel.
General users, administrators, and supervisors can use the Web Service Functions, depending on their role.

Copy Function

This function is for scanning originals and printing the scanned image according to the Print Settings specified by the user. Print Settings include the number of copies, magnification, and custom settings (e.g. printing multiple pages onto a single sheet). In addition, the scanned original images can be stored in the D-BOX. Document data stored in the D-BOX using the Copy Function can be printed and deleted using the "Document Server Function", which is part of the Basic Functions and described later.

Printer Function

This function is for printing out the print data sent from a client computer. The TOE receives the print data from a client computer on the network or directly connected to its USB Port. The TOE prints the received data using its Direct Print Function or Store and Print Function. The print data can be stored in the D-BOX as document data using the Store and Print Function, and the stored document data can be printed and deleted using the "Document Server Function", which is part of the Basic Functions and described later.

Fax Function

This function is for sending and receiving fax data over a telephone line. Fax Functions consists of the Fax Receive Function (hereafter called Fax Reception), the Fax Transmission Function (hereafter called "Fax Transmission"), and a function for printing and deleting fax data.
Fax Reception either prints received fax data, or converts received fax data into fax reception data and then stores it in the D-BOX.
Fax reception data stored in the D-BOX can be printed and deleted using the Fax Function or "Document Server Function", which is part of the Basic Functions and described later.
Fax Transmission includes Immediate Transmission, Memory Transmission, and stored document Fax Transmission, which are available from the Operation Panel, and also include LAN-Fax transmission, which is available from a client computer. Document data stored in the D-BOX for faxing can be printed and deleted using the "Document Server Function", which is part of the Basic Functions and described later.
Although the MFP provides IP-Fax and Internet Fax Function as a part of the Fax Function, no evaluation based on this document is applied to these functions.

Scanner Function

This function is for scanning and digitising paper originals and delivering scanned images to folders or sending them as document data by e-mail via networks. A client computer can process scanned data. This function can also be used for storing scanned images in the D-BOX as document data. Document data that is stored in the D-BOX using this function can be sent by e-mail, delivered to folders, and deleted using this function.

Document Server Function

This function is for scanning originals and storing scanned image data in the D-BOX as document data. In addition, document data stored in the D-BOX using the Copy Function, Printer Function, Fax Function, or Document Server Function can be printed and deleted using the Document Server Function. Document data stored in the D-BOX using the Scanner Function cannot be printed or deleted using the Document Server Function. When document data is printed, the Print Setting information for the stored document data will be updated according to the user's settings.

Management Function

This function is for setting the following information: information for configuring operation of the machine, information for connecting the TOE to networks, user information, and information on restriction of use of document data. The user's ability to manage this information depends on the user's role (general user, administrator, or supervisor). This function is available from the Operation Panel or by accessing the Web Service Function from a client computer. Some information can be managed from the Operation Panel, client computer, and both. As for Management Functions, security-related functions are described later in "Security Management Function" in "1.4.4.2 Security Functions".
Although the Management Function also provides Back Up/Restore Address Book functions, no evaluation based on this document is applied to these functions.

Web Service Function

This function is for allowing authorised TOE users (general users, administrators or supervisors) to operate the TOE remotely from a client computer. Remote operation is possible if a Web browser is installed on the client computer and the TOE and client computer are network-connected. Users can use this function by accessing the web server of the TOE from their computer's Web browser. The following TOE operations are available:

1. Printing document data stored in the D-BOX.
   Document data stored using the Copy Function, Document Server Function, Fax Function, or Printer Function can be printed. When document data is printed, the Print Setting information for the stored document data will be updated according to the user's settings.
2. Sending document data stored in the D-BOX.
   Document data stored using the Scanner Function can be sent.
3. Deleting document data stored in the D-BOX.
4. Downloading document data stored in the D-BOX.
   Document data stored using the Scanner Function or Fax Function can be downloaded.
5. Subset of Management Functions.
6. Checking the status of the TOE.

1.4.4.2 Security Functions

The Security Functions include the Audit Function, Identification and Authentication Function, Document Data Access Control Function, Stored Data Protection Function, Network Communication Data Protection

Function, Security Management Function, Service Mode Lock Function, Telephone Line Intrusion Protection Function, and MFP Control Software Verification Function. This section describes these functions.

Audit Function

This function is for checking the operational status of the TOE, and for recording events in the audit log, which is necessary for the detection of security breaches. Only the machine administrator is able to read and delete the recorded audit logs. The machine administrator can read the audit logs using the Web Service Function, and delete the audit logs using both the Operation Panel and the Web Service Function.

Identification and Authentication Function

This function is for those who attempt to use the TOE from the Operation Panel or a client computer. It prompts the users to enter their user IDs and authentication details for user identification and authentication. However, when printing or faxing from a client computer, this function sends the user's ID and authentication details to the TOE after the users enters their user ID and authentication details from printer or fax drivers, which are outside the TOE. The TOE then attempts to identify and authenticate the user with the received user ID and authentication information.

The Identification and Authentication Function includes the following:

- Account Lockout: If the number of consecutive unsuccessful attempts with the same particular user ID reaches the specified Number of Attempts before Lockout, this function temporarily prevents further login attempts from this user ID.
- Authentication Feedback Area Protection: When a user enters their password, this function masks the password with protection characters as it appears in the authentication feedback area, in order to prevent the password being viewed by others.
- Password Quality Maintenance: This forces users to register passwords that satisfy both the Minimum Password Length and Password Complexity Setting, which the user administrator sets in advance.

Although this TOE has other Identification and Authentication Functions, this evaluation does not cover the functions other than those listed above.

Document Data Access Control Function

This function restricts operations on document data stored in the D-BOX to specified users only. Operations on document data include reading and deleting. Each of these operations is as follows:

Reading document data: Read document data stored in the D-BOX.

Deleting document data: Delete document data stored in the D-BOX.

The TOE allows specified users, (file administrators, and general users) to perform operations on document data.
File administrators are allowed to delete any document data.
General users are allowed to perform only operations that are authorised by the permissions to process document data. The operation permissions in document data include read-only, edit, edit/delete, and full control. For editing permission, the same operation on document data is permitted as the read-only

permission, and changing the Print Settings is also permitted. Table 2 shows the relationship between the operation authorised by the permissions to process document data and the operations possible on the document data.

Table 2: Correspondence between operations authorised by permissions to process document data and operations possible on document data

Operations possible on document data / Operation permissions authorised by permissions to process document data	Reading document data	Deleting document data
Read-only	v	
Edit	v	
Edit/delete	v	v
Full control	v	v

v: possible

blank: impossible

The operation permissions for each document can be specified for each general user.

Stored Data Protection Function

The Stored Data Protection Function is for protecting document data stored on the HDD from leakage, by making it difficult to understand unless the document data is accessed and read in the normal way.

Network Communication Data Protection Function

This function is for protecting document data and print data in transit on the network from unauthorised access. The communication protocol that is used to protect the communication data differs according to the method by which the document or print data is sent.

The network administrator decides the communication protocol to apply based on the environment in which the TOE is operating and the intended usage of the TOE. The following explains the sending methods and their corresponding communication protocols.

1. Download document data using the Web Service Function from a client computer (SSL protocol)
2. Print or fax from a client computer (SSL protocol)
3. Deliver document data to an FTP server or SMB server from the TOE (IPSec protocol)
4. Send document data attached to e-mail to a client computer from the TOE (S/MIME)

Security Management Function

This function allows administrators, supervisors, and general users who have been successfully authenticated by the previously described "Identification and Authentication Function" to perform the following operations for security management according to user role.

1. Management of document data ACL
   Allows only specified users to modify the document Data ACL. Modifying the document data ACL includes changing document file owners, registering new document file users for the document data ACL, deleting document file users previously registered for document data ACL, and changingoperation permissions specified in document data. Only file administrators can change the document file owners. File administrators, document file owners, and document file users with full control permissions can perform other operations. When document data is stored, its document data ACL is set to the document data default ACL.
2. Management of administrator information
   Allows specified users to register and delete administrators, to add and delete administrator roles, and change administrator IDs and passwords.
   Only administrators are allowed to register another administrator or add an administrator role to another administrator. Such administrators can delete an administrator or an administrator role, and change an administrator's ID. Administrators and supervisors can change administrator passwords. An Administrator is permitted to add an Administrator Role to another Administrator, provided that the first Administrator is already assigned that Administrator Role, and an Administrator is permitted to delete one of his/her Administrator Roles, provided that at least one other Administrator is assigned that Administrator Role. Since administrators are required to have at least one administrator role, one or more of their roles must be given to a new administrator when they register another administrator. If administrators delete all of their own administrator roles, their administrator information will be automatically deleted.
3. Management of general user information
   Allows only users with specified user roles to newly create, change, and delete general user information. The relationship between user roles and authorised operations is:
   - User administrators can newly create, change, and delete general user information.
   - General users can change their own general user information that is registered to them in the Address Book, with the exception of their user IDs.
4. Management of supervisor information
   Supervisors can change their supervisor ID and password.
5. Management of machine control data
   Each administrator is allowed to configure the items of machine control data that correspond to their administrator role (machine administrator, user administrator, or and file administrator).

Service Mode Lock Function

The Maintenance Function is used by CEs who receive a request from the machine administrator to perform maintenance on the TOE from the Operation Panel. The Service Mode Lock Function prevents the Maintenance Function being used. In this evaluation, the Service Mode Lock Function set to "On".

Telephone Line Intrusion Protection Function

This function is for devices equipped with a Fax Unit. It restricts communication over a telephone line to the TOE, so that the TOE receives only permitted data.

MFP Control Software Verification Function

This function verifies the integrity of the MFP Control Software by checking the integrity of an executable code installed in the FlashROM.

1.4.5 Protected Assets

This section describes the protected assets of this TOE (document data and print Data).

1.4.5.1 Document Data

Document data is imported from outside the TOE by various methods, and can be either stored in the TOE or output by it. Document data stored in the TOE can be deleted.

Importing Document Data

Document data can be imported by the following two methods:

1. From a scanner
   Document data is created from the scanned image of a paper original that is imported to the TOE.
2. From the network or from a device connected to the USB Port
   Document data is created from print data received through the network or the USB Port that is then converted to a format that the TOE can handle.

Storing Document Data

Document data stored inside the TOE is stored in the D-BOX. The D-BOX protects the document data from unauthorised access and leakage.

Outputting Document Data

Document data can be output by the following five methods:

1. Sent by e-mail to a client computer (to the e-mail address).
2. Sent to an SMB or FTP server.
3. Downloaded by a client computer.
4. Printed out.

5. Sent as a fax.

When output using methods 1 to 3, document data is protected from leakage, and tampered data can be detected.

1.4.5.2 Print Data

Print data is data in which a print or fax image is written. It is generated from the document files in a client computer by the printer or fax drivers installed on the client computer when it is printed or faxed, respectively. Print data is imported to the TOE via the internal network or the USB Port. When passing from a client computer to the TOE through the internal network, print data is protected from leakage, and tampered data can be detected.

2 Conformance Claims

This section describes the 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 claims conformance

Part 1:

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

Part 2:

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

Part 3:

Security assurance components September 2007 Version 3.1 Revision 2 (Japanesetranslation ver.2.0) CCMB-2007-09-003

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

2.2 PP Claims, Package Claims

This ST and TOE do not conform to any PPs.
This ST claims conformance to the following package:

Package: EAL3 conformant

2.3 Conformance Rationale

Since this ST does not claim conformance to PPs, there is no rationale for PP conformance.

3 Security Problem Definitions

This section provides details of 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 attacks by unauthorised persons with knowledge of published information about TOE operations and such attackers are capable of potential security attacks.

T.ILLEGAL_USE (Abuse of TOE)

Attackers may read or delete document data by gaining unauthorised access to the TOE through the device's interfaces (the Operation Panel, network interface, USB Port, or SD card interface).

T.UNAUTH_ACCESS (Access violation to protected assets stored in TOE)

Authorised TOE users may breach the limits of authorised usage and access document data through the external TOE interfaces (the Operation Panel, network interface, or USB Port) that are provided for them.

T.ABUSE_SEC_MNG (Abuse of Security Management Function)

Persons not authorised to use Security Management Functions may abuse them.

T.SALVAGE (Salvaging memory)

Attackers may remove the HDD from the TOE and disclose document data.

T.TRANSIT (Interceptions and tampering on communication path)

Attackers may illegally obtain, leak, or tamper with document data or print data sent or received by the TOE via the internal network.

T.FAX_LINE (Intrusion from telephone line)

Attackers may gain access to the TOE through telephone lines.

3.2 Organisational Security Policies

The following security policy is assumed for organisations that demand integrity of the software installed in its IT products.

P.SOFTWARE **(Software integrity checking)**

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

3.3 Assumptions

Defined and described below are the assumptions related to the use and environment of this TOE:

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

Administrators shall have sufficient knowledge to operate the TOE securely in the roles assigned to them and will instruct general users to operate the TOE securely also. Additionally, administrators shall not abuse their permissions maliciously.

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

Supervisors shall have sufficient knowledge to operate the TOE securely in the roles assigned to them, and are shall not abuse their permissions maliciously.

A.NETWORK **(Assumption for network connections)**

When the network that the TOE is connected to (the internal network) is connected to an external network such as the Internet, the internal network shall be protected from the external network.

4 Security Objectives

This section describes the security objectives of the TOE and its security objectives of the operational environment and their rationale.

4.1 Security Objectives for TOE

The following define the security objectives of the TOE.

O.AUDIT **(Audit)**

The TOE shall record Security Function-related events in an audit log, and provides the machine administrator with a function for reading the audit logs, allowing the machine administrator to detect whether or not a security intrusion has occurred.

O.I&A **(Identification and authentication)**

The TOE shall perform identification and authentication of users prior to their use of the TOE Security Functions, and allows successfully authenticated users to use the functions for which they have permission.

O. DOC_ACC **(Access control to protected assets)**

The TOE shall ensure general users have access to document data according to their permissions to process document data. The TOE shall also allow the file administrator to delete document data stored in the D-BOX.

O. MANAGE **(Security management)**

The TOE shall only allow specified users to manage its Security Functions, TSF data, and security attributes. Such users are required to maintain the TOE security.

O.MEM.PROTECT **(Prevention of disclosure of data stored in memory)**

The TOE shall convert the format of the document data stored on the HDD into a format that is difficult to decode.

O. NET.PROTECT **(Protection of network communication data)**

The TOE shall protect document data and print data travelling over the communication network from interception, and detect any tampering.

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

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

O.LINE_PROTECT (Prevention of intrusion from telephone line)

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

4.2 Security Objectives of Operational Environment

The following describes the security objectives of the operational environment.

OE.ADMIN (Trusted administrators)

The responsible manager of the MFP shall select trusted persons as administrators and instructs them on their administrator roles. Once instructed, administrators then shall instruct general users, familiarising them with the compliance rules for secure TOE operation as defined in the administrator guidance for the TOE.

OE.SUPERVISOR (Trusted supervisor)

The responsible manager of the MFP shall select trusted persons as supervisors and instructs them on the role of supervisor.

OE.NETWORK (Network environment for TOE connection)

If the internal network, to which the TOE is connected, is connected to an external network such as the Internet, the organisation that manages operation of the internal network shall close any unnecessary ports between the external and internal networks (e.g. by employing a firewall)

4.3 Security Objectives Rationale

This section describes the rationale of the security objectives.

If all security objectives are fulfilled as explained in the following, the security problems defined in "3. Security Problem Definitions" are solved: all threats are countered, all organisational security policies enforced, and all assumptions upheld.

4.3.1 Tracing

This section describes the correspondence between the previously described "3.1 Threats", "3.2 Organisational Security Policies" and "3.3 Assumptions", and either "4.1 Security Objectives for TOE" or "4.2 Security Objectives of Operational Environment" with Table 3. The "v" in the table indicates that each of the elements of the TOE Security Environment is satisfied by security objectives.

Table 3 demonstrates that each security objective corresponds to at least one threat, organisational security policy, or assumption. As indicated by the shaded region in Table 3, assumptions are not upheld by TOE security objectives.

Table 3: Relationship between security environment and security objectives

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

4.3.2 Tracing Justification

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

A.ADMIN (Assumptions for administrators)

As specified by A.ADMIN, administrators shall have sufficient knowledge to operate the TOE securely in the roles assigned to them and instruct general users to operate the TOE securely also. Additionally, administrators are unlikely to abuse their permissions.
As specified by OE.ADMIN, the responsible manager of the MFP shall select trusted persons as administrators and instruct them on their administrator roles. Once instructed, administrators then shall instruct general users, familiarising them with the compliance rules for secure TOE operation as defined in the administrator guidance for the TOE. Therefore, A.ADMIN is upheld.

A.SUPERVISOR (Assumptions for supervisors)

As specified by A.SUPERVISOR, supervisors shall have sufficient knowledge to operate the TOE securely in the roles assigned to them, and be unlikely to abuse their permissions.
As specified by OE.SUPERVISOR, the responsible manager of the MFP shall select trusted persons as supervisors and instruct them on the role of supervisor. Therefore, A.SUPERVISOR is upheld.

A.NETWORK (Assumptions for network connections)

As specified by A.NETWORK, when the network that the TOE is connected to (the internal network) is connected to an external network such as the Internet, the internal network shall be protected from unauthorised communications originating from the external network.
As specified by OE.NETWORK, if the internal network, to which the TOE is connected, is connected to an external network such as the Internet, the organisation managing operation of the internal network shall close any unnecessary ports between the external and internal networks. Therefore, A.NETWORK is upheld.

T.ILLEGAL_USE (Malicious usage of the TOE)

To counter this threat, the TOE performs identification and authentication of users with O.I&A prior to their use of the TOE Security Functions, and allows the successfully authenticated user to use the functions for which the user has the operation permission. In addition, the TOE records the performance of O.I&A as audit logs by O.AUDIT, and provides only the Machine administrator with the function to read the audit logs so that the machine administrator detects afterwards whether or not there was security intrusion of O.I&A.
Therefore, the TOE can counter T.ILLEGAL_USE.

T.UNAUTH_ACCESS (Access violation of protected assets stored in the TOE)

To counter this threat, the TOE allows the authorised users identified by O.I&A to access to document data according to the operation permission on document data that are assigned to the authorised users' roles and the authorised users by O.DOC_ACC. For example, if the authorised user is the general user, the TOE allows the general user to perform operations on document data according to the operation permissions. If the authorised user is a file administrator, the TOE allows the file administrator to delete the document data stored in the D-BOX.
Therefore, the TOE can counter T.UNAUTH_ACCESS.

T.ABUSE_SEC_MNG (Abuse of Security Management Functions)

To counter this threat, the TOE allows only users who have successfully authenticated with O.I&A to use the TOE Security Functions. The TOE also restricts management of the Security Functions to specified users only, and control of TSF data, and security attributes by O.MANAGE. In addition, O.I&A and O.MANAGE events are recorded in audit logs by O.AUDIT, and the function for reading audit logs is available to the machine administrator only, so that the machine administrator can later identify whether or not security intrusion events involving O.I&A and O.MANAGE occurred.
Therefore, the TOE can counter T.ABUSE_SEC_MNG.

T.SALVAGE (Salvaging memory)

To counter this threat, the TOE converts the format of document data by O.MEM.PROTECT, making the document data difficult to read and decode if the HDD is installed in a device other than the TOE. In addition, the performance of O.MEM.PROTECT is recorded in audit logs by O.AUDIT, and the function for reading audit logs is available to the machine administrator only, so that the machine administrator can later identify whether or not O.MEM.PROTECT was performed successfully.
Therefore, the TOE can counter T.SALVAGE.

T.TRANSIT (Data interception and tampering with communication path)

To counter this threat, the TOE protects document data and Print Data on communication path from leakage, and detects tampering. In addition, the performance of O.NET.PROTECT is recorded as audit logs by O.AUDIT, and the function to read audit logs is only provided to the machine administrator so that the machine administrator verifies afterwards whether or not O.NET.PROTECT was performed.
Therefore, the TOE can counter T.TRANSIT.

T.FAX_LINE (Intrusion via telephone line)

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

P.SOFTWARE (Checking software integrity)

To enforce this organisational security policy, the TOE provides the function to verify the integrity of MFP Control Software, which is installed in FlashROM, with the TOE users by O.GENUINE.
Therefore, the TOE can enforce P.SOFTWARE.

5 Extended Components Definition

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

6 Security Requirements

This section describes the 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 "4.1 Security Objectives for TOE". The security functional requirements are quoted from the requirement defined in the CC Part2.

The part with assignment and selection defined in the CC Part2 are identified with [**bold face and brackets**].

6.1.1 Class FAU: Security audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps.

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

a) Start-up and shutdown of the Audit Functions;

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

c) **[assignment: auditable events of the TOE shown in** Table 4**].**

Table 4 shows the actions (CC rules) recommended by the CC as auditable for each functional requirement and the corresponding auditable events of the TOE.

Table 4: List of auditable events

Functional requirements	Actions which should be auditable	Auditable events of TOE
FAU_GEN.1	None	-
FAU_SAR.1	a) Basic: Reading of information from the audit records.	Auditable events not recorded.
FAU_SAR.2	a) Basic: Unsuccessful attempts to read information from the audit records.	Auditable events not recorded.
FAU_STG.1	None	-
FAU_STG.4	a) Basic: Actions taken due to the audit storage failure.	Auditable events not recorded.
FCS_CKM.1	a) Minimal: Success and failure of the activity. b) Basic: The object attribute(s), and object value(s) excluding any sensitive	<Individually-defined auditable events> 1. HDD cryptographic key generation (Outcome:

Functional requirements	Actions which should be auditable	Auditable events of TOE
	information (e.g. secret or private keys).	Success/Failure)
FCS_COP.1	a) Minimal: Success/failure, and type of cryptographic operation. b) Basic: Any applicable cryptographic mode(s) of operation, subject and object attributes.	<Individually-defined auditable events> 1. Storage of document data successful 2. Reading of document data successful
FDP_ACC.1	None	-
FDP_ACF.1	a) Minimal: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by the SFP. c) Detailed: The specific security attributes used in making an access check.	<Individually-defined auditable events> 1. Storage of document data successful 2. Reading of document data successful 3. Deletion of document data successful
FDP_IFC.1	None	-
FDP_IFF.1	a) Minimal: Decisions to permit requested information flows. b) Basic: All decisions on requests for information flow. c) Detailed: The specific security attributes used in making an information flow enforcement decision. d) Detailed: Some specific subsets of the information that has flowed based upon policy goals (e.g. auditing of downgraded material).	a) Minimal 1. Fax Function: Reception
FIA_AFL.1	a) Minimal: the reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).	a) Minimal 1. Lockout start 2. Lockout release
FIA_ATD.1	None	-
FIA_SOS.1	a) Minimal: Rejection by the TSF of any tested secret; b) Basic: Rejection or acceptance by the TSF of any tested secret; c) Detailed: Identification of any changes to the defined quality metrics.	b) Basic 1. Newly creating authentication information of general users (Outcome: Success/Failure) 2. Changing authentication information of general users (Outcome: Success/Failure)

Functional requirements	Actions which should be auditable	Auditable events of TOE
		3. Changing administrator authentication information (Outcome: Success/Failure) 4. Changing supervisor authentication information (Outcome: Success/Failure)
FIA_UAU.2	Minimal: Unsuccessful use of the authentication mechanism; Basic: All use of the authentication mechanism.	Basic 1. Login (Outcome: Success/Failure)
FIA_UAU.7	None	-
FIA_UID.2	a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided; b) Basic: All use of the user identification mechanism, including the user identity provided.	b) Basic 1. Login (Outcome: Success/Failure)
FIA_USB.1	a) Minimal: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject). b) Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).	b) Basic 1. Login (Outcome: Success/Failure)
FMT_MSA.1	a) Basic: All modifications of the values of security attributes.	<Individually-defined auditable events> 1. Adding and deleting administrator roles 2. Changing document data ACL
FMT_MSA.3	a) Basic: Modifications of the default setting of permissive or restrictive rules. b) Basic: All modifications of the initial values of security attributes.	Auditable events not recorded.
FMT_MTD.1	a) Basic: All modifications to the values of TSF data.	<Individually-defined auditable events> 1. Newly creating authentication information of general users. 2. Changing authentication information of general users. 3. Deleting authentication information of general users. 4. Changing administrator Authentication information. 5. Changing supervisor Authentication information.

Functional requirements	Actions which should be auditable	Auditable events of TOE
		6. Changing time and date of system clock. 7. Deleting entire audit logs.
FMT_SMF.1	a) Minimal: Use of the Management Functions.	<Individually defined auditable events> 1. Adding and deleting administrator roles. 2. Lockout release by the unlocking administrator. 3. Changing time and date of system clock.
FMT_SMR.1	a) Minimal: modifications to the group of users that are part of a role; b) Detailed: every use of the rights of a role.	a) Minimal 1. Adding and deleting administrator roles.
FPT_STM.1	a) Minimal: changes to the time; b) Detailed: providing a timestamp.	a) Minimal 1. Changing time and date of system clock.
FPT_TST.1	a) Basic: Execution of the TSF self tests and the results of the tests.	-
FTP_ITC.1	a) Minimal: Failure of the trusted channel functions. b) Minimal: Identification of the initiator and target of failed trusted channel functions. c) Basic: All attempted uses of the trusted channel functions. d) Basic: Identification of the initiator and target of all trusted channel functions.	<Individually-defined auditable events> 1. Communication with trusted IT products (Outcome: Success/Failure, Communication IP address)
FTP_TRP.1	a) Minimal: Failures of the trusted path functions. b) Minimal: Identification of the user associated with all trusted path failures, if available. c) Basic: All attempted uses of the trusted path functions. d) Basic: Identification of the user associated with all trusted path invocations, if available.	<Individually-defined auditable events> 1. Communication with remote users (Outcome: Success/Failure)

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[assignment: communication IP address, IDs of persons whose authentication information is created/changed/deleted, Locking out users, release of user Lockout, method of Lockout release, IDs of object document data].**

FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation.

FAU_SAR.1.1 The TSF shall provide **[assignment: the machine administrator]** with the capability to read **[assignment: all log items]** from the audit records.

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

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review.

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

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation.

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

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

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss.

Dependencies: FAU_STG.1 Protected audit trail storage.

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

6.1.2 Class FCS: Cryptographic support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: cryptographic key generation algorithm shown in** Table 5**]** and specified cryptographic key size **[assignment: cryptographic key size shown in** Table 5**]** that meet the following: **[assignment: standards shown in** Table 5**]**.

Table 5: 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 6**]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm shown in** Table 6**]** and cryptographic key sizes **[assignment: cryptographic key size shown in** Table 6**]** that meet the following: **[assignment: standards shown in** Table 6**]**.

Table 6: List of Cryptographic operations

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

6.1.3 Class FDP: User data protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control.

FDP_ACC.1.1 The TSF shall enforce the **[assignment: MFP access control SFP]** on **[assignment: List of Subjects, Objects, and Operation among Subjects and Objects in** Table 7**].**

Table 7: List of subjects, objects, and operations among subjects and objects

Subjects	Objects	Operations among subjects and objects
Administrator process	Document data	Deleting document data
General user process	Document data	Storing document data Reading document data Deleting document data

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation.

FDP_ACF.1.1 The TSF shall enforce the **[assignment: MFP access control SFP]** to objects based on the following: **[assignment: subjects or objects, and their corresponding security attributes shown** Table 8**].**

Table 8: Subjects, objects and security attributes

Types	Subjects or objects	Security attributes
Subject	Administrator process	- Administrator IDs - Administrator roles
Subject	General user process	- General user ID - Document data default ACL
Object	Document data	- Document data ACL

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[assignment: rules governing subject operations on objects and access to the operations shown in** Table 9**].**

Table 9: Rules governing access

Subject	Operations on objects	Rules governing access
General user process	Storing document data	General users can store document data. When the document data is stored, the document data default ACL associated with the general user process is copied to the document data ACL associated with the document data.
	Reading document data	A general user process has permission to read document data if the general user ID associated with the general user process matches either the document file owner ID or the document file user ID in the document data ACL associated with the document data, and if the matched ID has viewing, editing, editing/deleting, or full control permission.

	Deleting document data	A general user process has permission to delete document data if the general user ID associated with the general user process matches either the document file owner ID or a document file user ID in the document data ACL associated with the document data, and if the matched ID has permission for editing/deleting or full control permission.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules that explicitly grant subject's operations on objects shown in** Table 10**].**

Table 10: Rules governing access explicitly

Subject	Operations on object	Rules governing access
Administrator process	Deleting document data	When the file administrator is included in administrator roles that are associated with administrator process, the administrator process has permission to delete all document data stored in the D-BOX.

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

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes.

FDP_IFC.1.1 The TSF shall enforce the **[assignment: telephone line information flow SFP]** on **[assignment: subjects, information, and an operation listed in** Table 11**].**

Table 11: List of subjects, information and operation

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

(Note: "Transferring" means the Controller Board is receiving data through the Fax Unit from a telephone line.)

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation.

FDP_IFF.1.1 The TSF shall enforce the **[assignment: telephone line information flow SFP]** based on the

following types of subject and information security attributes: **[assignment: subjects or information and their corresponding security attributes shown in** Table 12**].**

Table 12: Security attributes corresponding to subjects or information

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

(Note: "Data type" means the type of data received from a telephone line and indicates whether this is fax or non-fax data.)

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

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

FDP_IFF.1.4 The TSF **shall** explicitly authorise an information flow based on the following rules: **[assignment: no rules, based on security attributes that explicitly authorise information flows]**.

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

6.1.4 Class FIA: Identification and authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication.

FIA_AFL.1.1 TSF shall detect when **[selection: an administrator (refinement: the machine administrator) configurable positive integer within [assignment: 1 to 5]]** unsuccessful authentication attempts occur related to **[assignment: the consecutive numbers of times of authentication failure for each user in the authentication events shown in** Table 13**].**

Table 13: List of authentication events

Authentication events
User authentication using the control panel

User authentication using TOE from client computer Web browser
User authentication when printing from client computer
User authentication when faxing from client computer

FIA_AFL.1.2 When defined number of unsuccessful authentication attempts has been **[selection: met]**, the TSF shall **[assignment: Lockout the user, who has failed the authentication attempts, until one of the Lockout release actions, shown in** Table 14**, is taken].**

Table 14: Lockout release actions

Lockout release actions	Details
Auto Lockout Release	If the user fails to authenticate after making the number of attempts specified for Lockout release, and the Lockout time (between 1 and 9999 minutes) set in advance by the machine administrator has elapsed, then Lockout will be released upon the first successful identification and authentication by the locked-out user. The machine administrator can set the Lockout time to indefinite, and in this case, Lockout cannot be released by a time-based operation but can be released by an operation other than a time-based operation.
Manual Lockout Release	Regardless of the time specified for the Lockout release by the machine administrator, an unlocking administrator specified for any user role of a locked-out user can release a locked-out user. FMT_MTD.1 defines the relationship between locked-out user and unlocking administrator. There is also a special Lockout release: If an administrator (any role) or a supervisor is locked out, restarting the TOE has the same effect as the Lockout release operation performed by an unlocking administrator.

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: **[assignment: general user IDs, document data default ACL, administrator IDs, administrator roles and supervisor ID].**

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

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

(1) Usable 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 (spaces) ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ (33 symbols)

(2) Registerable password length:

For general users

No fewer than the Minimum Password Length specified by the user administrator (8-32 characters) and no more than 128 characters.

For administrators and a supervisor

No fewer than the Minimum Password Length specified by the user 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 user administrator can be registered. The user administrator specifies either Level 1 or Level 2 for Password Complexity Setting.

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication.

Dependencies: FIA_UID.1 Timing of identification.

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

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication.

FIA_UAU.7.1 The TSF shall provide only **[assignment: displaying a dummy letter (*: asterisks, or •: bullets) for one letter of passwords on authentication feedback]** to the user while the authentication is in progress.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification.

Dependencies: No dependencies.

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

FIA_USB.1 User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition.

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **[assignment: general user IDs, document data default ACL,**

administrator IDs, administrator roles and supervisor ID].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **[assignment: rules for the initial association of attributes listed in** Table 15**].**

Table 15: Rules for initial association of attributes

Users	Subjects	Security attributes of users
General user	General user process	General user ID, Document data default ACL
Administrator	Administrator process	Administrator ID, Administrator roles
Supervisor	Supervisor process	Supervisor ID

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **[assignment: administrators can add their own assigned administrator roles to other administrators, and can delete their own administrator roles. However, the administrator cannot delete the assigned administrator role if that role is assigned to no other administrators].**

6.1.5 Class FMT: Security management

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1 The TSF shall enforce the **[assignment: MFP access control SFP]** to restrict the ability to **[selection: query, modify, delete, [assignment: newly create, change, add]]** the security attributes **[assignment: security attributes in** Table 16**] to [assignment: users/roles in** Table 16**].**

Table 16: Management roles of security attributes

Security attributes	Operations	User roles
General user IDs (a data item of general user information)	Query, newly create, delete	- User administrator

Security attributes	Operations	User roles
	Query	- General users
Administrator IDs	Newly create	- Administrators
	Query, change	- Administrators who own the administrator IDs
	Query	- Supervisor
Administrator roles	Query, add, delete	- Administrators who are assigned these administrator roles
Supervisor ID	Query, change	- Supervisor
Document data ACL	Query, modify	- File administrator - Document file owner - General users who have full control operation permissions for the relevant document data
Document data default ACL (a data item of general user information)	Query, modify	- User administrator - The general user who creates the applicable document data

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the **[assignment: MFP access control SFP]** to provide default values **[selection: [assignment: specified as shown in** Table 17**]** for security attributes that are used to enforce the SFP.

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

Table 17: Characteristics of static attribute initialisation

Object	Security attribute associated with object	Default value and its characteristic at time of object creation
Document data stored by general users	Document data ACL	A value set in advance as the document data default ACL for the applicable general user (document file owner). This value can be set arbitrarily by the user administrator or the general user, and it has neither a restrictive nor permissive property, only the specified property.

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to **[selection: query, modify, delete, [assignment: register, change, entirely delete, newly create]]** the **[assignment: list of TSF data management in** Table 18**]** to **[assignment: roles in** Table 18**].**

Table 18: List of TSF data management

TSF data	Operations	User roles
Authentication information of general users (a data item of general user information)	Newly create, change, delete	User administrator
	Change	Applicable general users of general user information
Supervisor authentication information	Change	Supervisor
Administrator authentication information	Change	Supervisor Applicable administrator of administrator authentication information
Number of Attempts before Lockout	Query, modify	Machine administrator
Setting for Lockout Release Timer	Query, modify	Machine administrator
Lockout time	Query, modify	Machine administrator
Date and time of system clock Date setting, time setting (hour, minute, second)	Query, modify	Machine administrator
	Query	General users, user administrator, network administrator, file administrator, supervisor
Minimum Password Length	Query, modify	User administrator
Password Complexity Setting	Query, modify	User administrator
HDD cryptographic key	Query, newly create	Machine administrator
Audit logs	Query, delete entirely	Machine administrator
Service mode lock setting	Query, modify	Machine administrator

TSF data	Operations	User roles
	Query	General users, User administrator, Network administrator, File administrator, Supervisor
Lockout Flag for general users	Query, modify	User administrator
Lockout Flag for administrators	Query, modify	Supervisor
Lockout Flag for supervisor	Query, modify	Machine administrator
S/MIME User Information (a data item of general user information)	Query, newly create, delete, change	User administrator Applicable general users of S/MIME user information
	Query	General users
Destination Information for Deliver to Folder	Query	User administrator, General users

FMT_SMF.1 Specification of Management Function

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following Management Functions: **[assignment: list of specifications of Management Functions described in** Table 19**].**

Table 19: List of specifications of Management Functions

Functional requirements	Management requirements	Management items
FAU_GEN.1	None	-
FAU_SAR.1	a) Maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.	a) Management of the machine administrator from administrator roles.
FAU_SAR.2	None	-
FAU_STG.1	None	-
FAU_STG.4	a) Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.	None: Actions are fixed and not an object of management.
FCS_CKM.1	None	-
FCS_COP.1	None	-
FDP_ACC.1	None	-

Functional requirements	Management requirements	Management items
FDP_ACF.1	a) Managing the attributes used to make explicit access or denial based decisions.	a) Management of the file administrator from administrator roles.
FDP_IFC.1	None	-
FDP_IFF.1	a) Managing the attributes used to make explicit access based decisions.	None: Attributes (data type) used to make explicit access-based decisions are fixed and there are no interfaces to change.
FIA_AFL.1	a) Management of the threshold for unsuccessful authentication attempts. b) Management of actions to be taken in the event of an authentication failure.	a) Security Management Function (management of machine control data): management of the Number of Attempts before Lockout by machine administrator. b) Management of unlocking administrators and Lockout release operations for locked-out users.
FIA_ATD.1	a) If so indicated in the assignment, the authorised administrator might be able to define additional security attributes for users.	None: No functions for defining additional security attributes for users.
FIA_SOS.1	a) Management of the metric used to verify the secrets.	Security Management Function (management of machine control data): The user administrator manages the following settings of the machine control data: - Minimum Password Length - Password Complexity Setting
FIA_UAU.2	a) Management of the authentication data by an administrator, b) Management of the authentication data by the user associated with this data.	- Security Management Function (management of general user information): management of authentication information of general users by the user administrator and management of own authentication information of general Users. - Security Management Function (management of administrator information): management of own administrator authentication information by administrators. - Security Management Function (management of administrator information): new registration of administrators by administrators. - Security Management Function (management of administrator information): management of administrator authentication information by supervisor.

Functional requirements	Management requirements	Management items
		- Security Management Function (management of supervisor information): management of supervisor authentication information by supervisor.
FIA_UAU.7	None	-
FIA_UID.2	a) Management of the user identities.	- Security Management Function (management of general user information): management of general user IDs by the user administrator. - Security Management Function (management of administrator information): management of own administrator IDs by administrators. - Security Management Function (management of administrator information): new registration of administrators by administrators. - Security Management Function (management of supervisor information): management of supervisor ID by supervisor.
FIA_USB.1	a) An authorised administrator can define default subject security attributes. b) An authorised administrator can change subject security attributes.	a) None: Default subject security attributes cannot be defined. b) Administrators can add own assigned administrator roles to other administrators and delete administrator roles.
FMT_MSA.1	a) Managing the group of roles that can interact with the security attributes; b) Management of rules by which security attributes inherit specified values.	a) Management of administrator roles by administrators. b) None: No rules by which security attributes inherit specified values.
FMT_MSA.3	a) Managing the group of roles that can specify initial values; b) Managing the permissive or restrictive setting of default values for a given access control SFP; c) Management of rules by which security attributes inherit specified values.	a) None: No groups of roles that can specify the initial settings. b) Management of the document data default ACL. - Allows the user administrator to modify the document data default ACL for all general user information registered to the Address Book. - Allows general users to modify the document data default ACL of their own general user information. c) None: No rules by which security attributes inherit specified values.

Functional requirements	Management requirements	Management items
FMT_MTD.1	a) Managing the group of roles that can interact with the TSF data.	None: No groups of roles can interact with TSF data.
FMT_SMF.1	None	-
FMT_SMR.1	a) Managing the group of users that are part of a role.	Management of administrator roles by administrators.
FPT_STM.1	a) Management of the time.	Security Management Function (management of machine control data): The machine administrator manages the following setting items for machine control data. - Data of system clock, time (hour, minute and second).
FPT_TST.1	a) Management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions. b) Management of the time interval if appropriate.	a) None: The condition under which TSF self-testing occurs is fixed. b) None: No management of time interval.
FTP_ITC.1	a) Configuring the actions that require trusted channel, if supported.	None: Actions that require Inter-STF trusted channels are fixed.
FTP_TRP.1	a) Configuring the actions that require trusted path, if supported.	None: Actions that require trusted paths are fixed.

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1 The TSF shall maintain the roles **[assignment: general users, administrators (machine administrator, file administrator, user administrator, and network administrator) and a supervisor]**.

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

6.1.6 Class FPT: Protection of the TSF

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

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

6.1.7 Class FTP: Trusted path/channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

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

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

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

Table 20 shows the services that require the trusted path defined in FTP_TRP.1.3 and used by each user who communicates via trusted path described in FTP_TRP.1.2.

Table 20: Services requiring trusted paths

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

6.2 Security Assurance Requirements

The evaluation assurance level of this TOE is EAL3. Table 21 lists the assurance components of the TOE. These components meet evaluation assurance level 3 (EAL3). Other requirements are not included.

Table 21: TOE Security assurance requirements (EAL3)

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

6.3 Security Requirements Rationale

This section describes the rationale behind the security requirements. If all security functional requirements are satisfied as below, the security objectives defined in "4.1Security Objectives for TOE" are fulfilled.

6.3.1 Tracing

Table 22 shows the relationship between the TOE security functional requirements and TOE security objectives. The "v" in the table indicates that the TOE security functional requirement fulfills the TOE security objective.

Table 22 shows that each TOE security functional requirement fulfills at least one TOE security objective.

Table 22: Relationship between security objectives and functional requirements

	O.AUDIT	O.I&A	O.DOC_ACC	O.MANAGE	O.MEM.PROTECT	O.NET.PROTECT	O.GENUINE	O.LINE_PROTECT
FAU_GEN.1	v							
FAU_SAR.1	v							
FAU_SAR.2	v							
FAU_STG.1	v							
FAU_STG.4	v							
FCS_CKM.1					v			
FCS_COP.1					v			
FDP_ACC.1			v					
FDP_ACF.1			v					
FDP_IFC.1								v
FDP_IFF.1								v
FIA_AFL.1		v						
FIA_ATD.1		v						
FIA_SOS.1		v						
FIA_UAU.2		v						
FIA_UAU.7		v						
FIA_UID.2		v						

	O.AUDIT	O.I&A	O.DOC_ACC	O.MANAGE	O.MEM.PROTECT	O.NET.PROTECT	O.GENUINE	O.LINE_PROTECT
FIA_USB.1		v						
FMT_MSA.1				v				
FMT_MSA.3				v				
FMT_MTD.1				v				
FMT_SMF.1				v				
FMT_SMR.1				v				
FPT_STM.1	v							
FPT_TST.1					v		v	
FTP_ITC.1						v		
FTP_TRP.1						v		

6.3.2 Justification of Traceability

This section describes how the TOE security objectives are fulfilled by the TOE security functional requirements corresponding to the TOE security objectives shown in Table 22.

O.AUDIT Audit

Following are the rationale behind the functional requirements corresponding to O.AUDIT in Table 22, and these requirements are included to fulfill the O.AUDIT specification.

a) Record audit logs
To fulfill O.AUDIT, the performance of Security Functions should be recorded as audit logs. For this, FAU_GEN.1 generates audit information whenever an Audit Function starts and ends, whenever an identification or authentication function is performed, whenever users operate protected assets, whenever protected assets are encrypted, and whenever a major Management Function is performed. The log also records the date, time, type, subject identity, and outcome of each event.

b) Provide Audit Function
To fulfill O.AUDIT, access to audit logs should be restricted to the machine administrator only, and in a format that can be audited. For this, FAU_SAR.1 allows only the machine administrator to read audit logs, and FAU_SAR.2 prohibits persons other than the machine administrator reading audit logs.

c) Protect audit logs
To fulfill O.AUDIT, audit logs should have adequate protection. For this, FAU_STG.4 protects audit logs from unauthorised deletion and prevents unauthorised tampering. If auditable events occur and the audit log files are full, FAU_STG.4 prevents loss of recent audit logs by writing the newer audit logs over audit logs that have the oldest time stamp.

d) Reliable record of time of event
To fulfill O.AUDIT, a reliable record of the times when events occurred should be available, as this will help identify security breaches.
For this, FPT_STM.1 provides a trusted time stamp.

O.I&A User identification and authentication

Following are the rationale behind the functional requirements corresponding to O.I&A in Table 22, and these requirements are included to fulfill the O.I&A specification.

a) Identify and authenticate users before they use the TOE.
To fulfill O.I&A, user identification and authentication shall be performed prior to allowing user access to the TOE Security Functions.
For this, FIA_UID.2 identifies users prior to their use of TOE Security Functions, and FIA_UAU.2 authenticates identified users.

b) Allow successfully identified and authenticated users to use the TOE.
To fulfill O.I&A, users who authenticate successfully before they use any TOE Security Functions shall be allowed use of the functions they have permission for.
For this, FIA_ATD.1 and FIA_USB.1 bind successfully identified and authenticated users with relevant subjects. Association and maintenance of the subjects with security attributes is also performed by FIA_ATD.1 and FIA_USB.1.

c) Complicate decoding of passwords.
To fulfill O.I&A, passwords for user authentication shall be protected from others while they are being entered, and must not be easily guessable.
For this, FIA_UAU.7 prevents passwords being viewed by displaying masking characters (*: asterisks or •: bullets) in place of each password character entered in the authentication feedback area.
FIA_SOS.1 accepts only passwords that satisfy the Minimum Password Length and password character combination specified by the user administrator, and it enables only passwords that are not easily guessable. FIA_AFL.1 also reduces the possibility of users guessing passwords by locking out users when their number of authentication attempts reaches the number specified by the machine administrator. The authentication attempts include user authentication attempts from the Operation Panel, the Web browser of a client computer, or a client computer when printing or faxing.

O.DOC_ACC Control of access to protected assets

Following are the rationale behind the functional requirements corresponding to O.DOC_ACC in Table 22, and these requirements are included to fulfill the O.DOC_ACC specification.

a) Specify access control to document data and perform operations.
To fulfill O.DOC_ACC, each user shall be allowed to perform operations on document data according to the operation permissions for document data set for each type of subject associated with the users and each security attribute associated with the subject.
For this, FDP_ACC.1 and FDP_ACF.1 allow the administrator to delete document data if the administrator's role associated with the administrator process is the file administrator. For general users, FDP_ACC.1 and FDP_ACF.1 allow storage of document data, and when the general user IDs associated with general user processes are registered in the document data ACL of a document,

FDP_ACC.1 and FDP_ADF.1 allow the general user to perform operations on document data. The operations that are permitted follow the operation permissions specified in the document data for each general user ID in the document data ACL.

O. MANAGE Security management

Following are the rationale behind the functional requirements corresponding to O.MANAGE in Table 22, and these requirements are included to fulfill the O.MANAGE specification.

a) Management of security attributes.

To fulfill O.MANAGE, management of security attributes shall be permitted to specified users only, and a default value shall be specified for the document data ACL, which is a security attribute. For this, FMT_MSA.1 allows:

- the user administrator to query, newly create, and change general user IDs;
- general users to query general user IDs;
- administrators to query and change their own administrator IDs;
- supervisors to query administrator IDs;
- administrators to query, add, and delete administrator roles assigned to themselves;
- supervisors to query and change supervisor IDs;
- the file administrator, document file owners, and general users with full control operation permission for the document data to query and modify its document data ACL; and
- the user administrator and general users with full control operation permission for the document data to query and modify the default ACLs of document data.

FMT_MSA.3 specifies the default value of the document data ACL for storage of new document data.

b) Management and protection of TSF data.

To fulfill O.MANAGE, access to TSF data shall be limited to specified users. For this, FMT_MTD.1 allows:

- the machine administrator to query and specify the Number of Attempts before Lockout, specify the setting of the Lockout release timer, specify a Lockout time, specify a Lockout Flag for supervisors, specify the date and time of the system clock, specify the service mode lock setting, newly create and query HDD cryptographic keys, and query and delete audit logs.

FMT_MTD.1 also allows:

- authorised TOE users to query the date and time of the system clock and the service mode lock setting;
- the user administrator to query and specify the Minimum Password Length, complexity setting, and a Lockout Flag for general users;
- the user administrator and applicable general users to specify the authentication information of general users, and newly create, delete, and change S/MIME user information;
- the user administrator and general users to query S/MIME user information and destination details when sending data to folders;
- supervisors to query and specify the Lockout Flag for administrators, and specify supervisor authentication information; and
- supervisors and applicable administrators to change administrator authentication information.

c) Specify Management Functions.

To fulfill O.MANAGE, the Security Management Functions for the implemented TSF shall be

performed.
For this, FMT_SMF.1 specifies the required Security Management Functions for the Security Function requirements.

d) Authorised use of Security Management Functions.
To fulfill O.MANAGE, authorised users shall be associated with the security management roles, and operation permissions for the Security Management Functions shall be maintained, since the use of the Security Management Functions depends on the authorised user roles.
FMT_SMR.1 associates authorised users with a general user, one of the four administrator roles (user administrator, machine administrator, file administrator, or network administrator), or the supervisor role, and maintains this association.

O.MEM.PROTECT Prevention of disclosure of data stored in memory

Following are the rationale behind the functional requirements corresponding to O.MEM.PROTECT in Table 22, and these requirements are included to fulfill the O.MEM.PROTECT specification.

a) Generate the encryption keys and perform encryption operations adequately.
To fulfill O.MEM.PROTECT, the document data stored on the HDD shall be sufficiently encrypted to make decoding difficult unless the document data is read with normal methods using the TOE.
For this, FCS_CKM.1 generates encryption keys at a key size of 256 bits with TRNG for the encryption key generation algorithm (based on BSI-AIS31); and FCS_COP.1 encrypts document data when it is stored on the HDD and decrypts it when it is read from the HDD using the encryption keys generated with the AES encryption algorithm (which corresponds to FIPS197). Additionally, FTP_TST.1 tests at the TOE start-up the validity of encryption keys and the performance of the Ic Hdd where encryption is performed, and this prevents storage of unencrypted document data on the HDD.

O.NET.PROTECT Protection of network communication data

Following are the rationale behind the functional requirements corresponding to O.NET.PROTECT in Table 22, and these requirements are included to fulfill the O.NET.PROTECT specification.

a) Protect assets on communication path.
To fulfill O.NET.PROTECT, document data and print data on the communication path shall be protected from leakage, and attempts at tampering with it shall also be detected.
For this, FTP_ITC.1 uses the IPSec protocol to protect data sent from the TOE to folders on FTP or SMB servers, to protect document data on the network from leakage, and also to detect attempts at tampering with document data.
FTP_TRP.1 also protects document data on networks from leakage and detects attempts at tampering by use of a trusted path (described later) between the TOE and remote users. The mail service is protected by S/MIME, which protects data sent by e-mail from the TOE to a client computer, protects document data or print data on the network from leakage, and detects attempts at tampering.
The SSL protocol protects document data and print data that are is travelling through a web service, print service, or fax service from a client computer from leakage and attempts at tampering.

O.GENUINE Protection of integrity of MFP Control Software integrity

Following are the rationale behind the functional requirements corresponding to O.GENUINE in Table 22, and these requirements are included to fulfill the O.GENUINE specification.

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

O.LINE_PROTECT Protection from intrusion via telephone line

Following are the rationale behind the functional requirements corresponding to O.LINE.PROTECT in Table 22, and these requirements are included to fulfill the O.LINE.PROTECT specification.

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

6.3.3 Dependency Analysis

Table 23 shows the correspondence of dependencies in this ST for the TOE security functional requirements.

Table 23: Correspondence of dependencies of TOE security functional requirements

TOE security functional requirements	Dependencies claimed by CC	Dependencies satisfied in ST	Dependencies not satisfied in ST
FAU_GEN.1	FPT_STM.1	FPT_STM.1	None
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	None
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	None
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	None
FAU_STG.4	FAU_STG.1	FAU_STG.1	None
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1	FCS_CKM.4
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1	FCS_CKM.4
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	None
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3	None

TOE security functional requirements	Dependencies claimed by CC	Dependencies satisfied in ST	Dependencies not satisfied in ST
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1	None
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3	None
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2	FIA_UAU.1
FIA_ATD.1	None	None	None
FIA_SOS.1	None	None	None
FIA_UAU.2	FIA_UID.1	FIA_UID.2	FIA_UID.1
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2	FIA_UAU.1
FIA_UID.2	None	None	None
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	None
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	None
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1	None
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1	None
FMT_SMF.1	None	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2	FIA_UID.1
FPT_STM.1	None	None	None
FPT_TST.1	None	None	None
FTP_ITC.1	None	None	None
FTP_TRP.1	None	None	None

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

Rationale for Removing Dependencies on FCS_CKM.4

In this TOE, the HDD encryption keys are stored in an area that cannot be accessed from outside the Ic Hdd. In addition, after the administrator generates the encryption keys at the start of TOE operation, deletion of the older encryption keys is not performed: they are overwritten with the new encryption keys. For these reasons, encryption key destruction by the standard method is unnecessary.

Rationale for Removing Dependencies on FIA_UAU.1

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

Rationale for Removing Dependencies on FIA_UID.1

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

6.3.4 Security Assurance Requirements Rationale

This TOE is a commercially available product. It is assumed that it will be used in general offices, and that the possibility of basic security attacks on this TOE exists. Architectural design (ADV_TDS.2) is adequate to show the validity of commercially available products. A high attack potential is required for attacks that circumvent or tamper 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 (ACL_DVS.1) is therefore important also.

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

7 TOE Summary Specification

This section provides a specification summary of the Security Functions of this TOE.

7.1 TOE Security Function

The TOE provides the following TOE Security Functions to satisfy the security functional requirements described in Section "6.1".

SF.AUDIT	Audit Function
SF.I&A	User Identification and Authentication Function
SF.DOC_ACC	Document Data Access Control Function
SF.SEC_MNG	Security Management Function
SF.CE_OPE_LOCK	Service Mode Lock Function
SF.CIPHER	Encryption Function
SF.NET_PROT	Network Communication Data Protection Function
SF.FAX_LINE	Protection Function for Intrusion via Telephone Line
SF.GENUINE	MFP Control Software Verification Function

As Table 24 shows, at least one TOE Security Function satisfies each security functional requirements described in section "6.1".

Table 24: Relationship between TOE security functional requirements and TOE security functions

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

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

Following are the security functional requirements that correspond to these TOE Security Functions.

7.1.1 SF.AUDIT Audit Function

The TOE starts the Audit Function when power is supplied and the TOE starts up, and keeps running the Audit Function until power down. While the Audit Function is running, the TOE creates audit logs whenever an auditable event occurs. These audit logs must be protected from loss before audit. Only the machine administrator is permitted to read audit logs and delete entire audit logs.

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

7.1.1.1 Generation of Audit Logs

The TOE generates audit log entries whenever an auditable event occurs, and appends these to audit log files. Audit logs consist of basic audit information and expanded audit information. Basic audit information is data

recorded when any kind of auditable event occurs. Expanded audit information is data recorded for the generation of auditable events that require additional information for audit. Table 25 shows the audit information for each auditable event.

If there is insufficient space in the audit log files to append new audit log files, older audit logs (identifiable by their time and date details) are overwritten with newer audit logs.

Table 25: Auditable events and auditable information

Auditable events	Audit logs	
	Basic audit information	**Expanded audit information**
Starting Audit Function (*1)	- Date/time of event - Types of event (auditable events in this table) - Subject identity (*4) - Outcome	-
Ending Audit Function (*1)		-
Login		-
Starting Lockout		Locked out user
Releasing Lockout (*2)		Locked out user who is to be released Release methods (auto Lockout release/manual Lockout release)
Lockout release at TOE startup		-
HDD encryption key generation		-
Successful storage of document data		ID of object document data
Successful reading of document data (*3)		ID of object document data
Successful deletion of document data		ID of object document data
Receiving fax		-
Changing user password (including new creation and deletion)		The ID of the user in the event of new creation/changing/deletion of another user's authentication details
Deletion of administrator role		-
Addition of administrator role		-
Changing document data ACL		ID of object document data
Changing date and time of system clock		-
Communication with trusted IT product		Communication IP address
Communication with remote user		-
Deletion of entire audit log		-

-: No applicable expanded audit information

*1: The starting of Audit Function is substituted with the event of the TOE startup. This TOE does not record the ending of Audit Function. The starting and ending of Audit Function audit the state of inactivity of Audit Function. Since Audit Function works as long as the TOE works and it is not necessary to audit the state of inactivity of Audit Function, it is appropriate not to record the ending of Audit Function.
*2: Lockout release for administrators and supervisor by the TOE's restart, which is the special Lockout release operation, is substituted with the event of the TOE startup.
*3: For the successful reading of the document data, the objects to be recorded in IDs for the operational object document data are printing, Sending by E-mail, Delivering to Folders and downloading from Web Service Function the document data stored in D-BOX
*4 When the recording events occur due to the operations by users, User IDs are set as subject identities of basic audit information, and when the recording events occur due to the TOE, IDs that do not duplicate the user IDs but can identify systems are set.
Since there are no interfaces on the TOE for modifying audit logs, unauthorised modification for the audit logs are not performed and the machine administrator who can delete the audit logs will not carry out any malicious acts using administrator privileges.
By the above, FAU_GEN.1 (Audit data generation), FAU_STG.1 (Protected audit trail storage), and FAU_STG.4 (Prevention of audit data loss) are satisfied.

7.1.1.2 Reading Audit Logs

The TOE allows only the machine administrator to read the audit logs in a text format using the Web Service Function.
By the above, FAU_SAR.1 (Audit review), FAU_SAR.2 (Restricted audit review), and FMT_MTD.1 (Management of TSF data) are satisfied.

7.1.1.3 Protection of Audit Logs

The TOE allows only the machine administrator to delete entire audit logs using the Operation Panel or the Web Service Function.
By the above, FAU_SAR.1 (Audit review), FAU_SAR.2 (Restricted audit review), and FMT_MTD.1 (Management of TSF data) are satisfied.

7.1.1.4 Time Stamps

The TOE logs the date and time of events by referencing the date and time of the internal system clock.
By the above, FPT_STM.1 (Reliable time stamps) is satisfied.

7.1.2 SF.I&A User Identification and Authentication Function

To allow authorised users to operate the TOE according to their roles and authorisation, the TOE identifies and authenticates users prior to their use of the TOE Security Functions.
Following are the explanations of each functional item in "SF.I&A User Identification and Authentication Function" and their corresponding security functional requirements.

7.1.2.1 User Identification and Authentication

The TOE displays a login window when users attempt to use the TOE Security Functions from the Operation Panel or the Web Service Function. This window requires the user to enter their ID and password, and then identifies and authenticates the user based on the entered user IDs and passwords.

The TOE also identifies and authenticates the user based on the user ID and password sent from the client computer when the TOE receives a request from the client computer for printing or transmitting faxes.
The TOE binds successfully authenticated users to the processes available to them (general user processes, administrator processes, or supervisor processes) according to their user roles (general users, administrators, or supervisors), associates each process with the security attributes of that role, and maintains those bindings and associations. If the user is a general user, the TOE binds the general user to general user processes, associates general user processes with a general user ID and the document data default ACL, and maintains those bindings and associations. If the user is an administrator, the TOE binds the administrator to administrator processes, associates administrator processes with the administrator ID and the administrator roles, and maintains those bindings and associations. If the user is a supervisor, the TOE binds the supervisor to supervisor processes, associates supervisor processes with the supervisor ID, and maintains those bindings and associations.
Authentication methods vary according to the user's role. Table 26 shows the authentication methods for each user role.

Table 26: User roles and authentication methods

User roles	Authentication methods
General users	Check if the general user ID and password entered by the user match a general user ID and corresponding password registered in the Address Book.
Administrators	Check if the administrator ID and password entered by the user match an administrator ID and corresponding password registered to the TOE.
Supervisor	Check if the supervisor ID and password entered by the user match a supervisor ID and corresponding password registered to the TOE.

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

7.1.2.2 Actions in Event of Identification and Authentication Failure

The TOE counts the number of failed identification and authentication attempts made under each ID, as described in "7.1.2.1 User Identification and Authentication". When the number of failed consecutive attempts reaches the machine administrator-specified Number of Attempts before Lockout, the TOE locks out the user, and sets the Lockout Flag for that user to "Active". The machine administrator can specify 1 to 5 as the Number of Attempts before Lockout.
When a user authenticates successfully, as described in "7.1.2.1 User Identification and Authentication", the TOE resets the number of available authentication attempts for that user to 0 and starts counting from 0.
When either of the following two Lockout release actions, (1) or (2), is performed by a user whose Lockout Flag is set to "Active", the TOE resets the Lockout Flag for that user to "Inactive" and releases the Lockout.

(1) Auto Lockout Release

If the 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 upon the first successful identification and authentication by the locked-out user. The machine administrator specifies the lockout time between 1 and 9999 minutes. If the machine administrator sets the lockout time to indefinite, lockout release will be performed only by manual lockout release. In this case, lockout release must be performed by manual lockout release.

(2) Manual Lockout Release

The unlocking administrators (specified for each user role, as shown in Table 27), have permission to release Lockout using the Web Service Function. If an administrator (any role) or a supervisor is locked out, as a special Lockout release operation, restarting the TOE releases Lockout.

Table 27: Unlocking administrators for each user role

User roles (locked out users)	Unlocking administrators
General users	User administrator
Administrators (all administrator roles)	Supervisor
Supervisor	Machine administrator

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

7.1.2.3 Password Feedback Area Protection

The TOE displays a string of masking characters (*: asterisks or •: bullets) in place of each letter of a password entered from the Operation Panel or the Web browser of a client computer by a general user, administrator, or supervisor.
From the above, FIA_UAU.7 (Protected authentication feedback) is satisfied.

7.1.2.4 Password Registration

The TOE provides a function for registering and changing the passwords of general users, administrators, and supervisors from the Operation Panel or the Web Service Function. This function uses a string of masking characters described in (1).
This function checks if the password to be registered or changed meets conditions (2) and (3). If it does, the password is registered. If it does not, the password is not registered and an error message appears.

(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) Registerable password length:

General users

No fewer than the Minimum Password Length specified by the user administrator (8-32 characters) and no more than 128 characters.

Administrators and supervisors

No fewer than the Minimum Password Length specified by the user 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 user administrator can be registered. The user administrator specifies either Level 1 or Level 2 for Password Complexity Setting.

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

7.1.3 SF.DOC_ACC Document Data Access Control Function

The TOE restricts user access to operations that store, read, and delete document data. The access control function displays only accessible document data on the Operation Panel or client computer where the user authenticated. Availability of document data is based on the roles assigned to the user who has been successfully authenticated by the Identification and Authentication Function, or the authorisation assigned to the individual user. This section describes the access control function that allows users to access document data based on their user role.

Following are the explanations of each functional item in "SF.DOC_ACC Document Data Access Control Function" and their corresponding security functional requirements.

7.1.3.1 General User Operations on Document Data

The TOE allows general users to store document data and to read and delete stored document data based on the document data ACL, which contains the IDs of general users who have permission to perform operations on the document data, and the operations permissions of the ID. If a general user ID that is associated with the general user process is registered for a document data ACL, the TOE allows that general user ID to perform operations on the document data according to the permissions assigned to the general user ID in the document data ACL.

Table 2 shows the relationship between the operation permissions for document data and operations on document data.

Table 28 shows the value of the document data ACL when storing document data.

Table 28: Default value for document data ACL

Type of document data	Default value for document data ACL
Document data stored by a general user	Document data default ACL

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

7.1.3.2 File Administrator Operations on Document Data

If the logged-in user from the Operation Panel or Web Service Function is a file administrator, the TOE allows that user to display a list of document data and to delete the document data in the list individually or all at once.
By the above, FDP_ACC.1 (Subset access control) and FDP_ACF.1 (Security attributebased access control) are satisfied.

7.1.4 SF.SEC_MNG Security Management Function

The TOE provides Security Management Functions according to the roles assigned to users who have been successfully identified and authenticated using the SF.I&A User Identification and Authentication Function". Following are explanations of each functional item in "SF.SEC_MNG Security Management Function" and their corresponding security functional requirements.

7.1.4.1 Management of Document Data ACL

Management of the document data ACL allows operations on the document data ACL from the Operation Panel or Web Service Function to be restricted to specified users only. Operations on the document data ACL include changing the document file owner and the document file owner's operation permissions for the document data, newly registering and deleting document file users, and changing document file users' operation permissions for the document data. These operations can be performed only by specified users who have been authorised for each operation. Table 29 shows the relationship between operations on the document data ACL and the users authorised for the operations.

Table 29: Operations on document data ACL and Authorised users

Operations on document data ACL	Authorised users
Changing of document file owners	- File administrators
Changing of Document file owners' operation permissions for document data	- File administrators - Document file owners - General users with full control authorisation
Registration of new document file users	- File administrators - Document file owners - General users with full control authorisation
Deletion of document file users	- File administrators - Document file owners - General users with full control authorisation
Changing of document file users' operation permissions for document data	- File administrators - Document file owners - General users with full control authorisation

If the logged-in user is a file administrator, the TOE allows that user to perform operations on all document data ACLs, including changing document file owners and their access rights, and newly registering and deleting document file users and changing their access rights.

If the logged-in user is a general user, the TOE allows that user to perform operations only on document data ACLs for which the user has full control authorisation. These operations are changing the document file owner's operation permissions for the document data, and newly registering and deleting document file users and changing their operation permissions. However, even if full control authorisation is not set for document file owners, document file owners can still perform operations on the document data ACLs of their own document data. These operations include changing the document file owner's operation permissions for the document data, newly registering and deleting document file users, and changing the document file users' operation permissions for the document data.
By the above, FMT_MSA.1 (Management of security attributes), FMT_MSA.3 (Static attribute initialisation), and FMT_SMF.1 (Specification of management functions) are satisfied.

7.1.4.2 Management of Administrator Information

Management of administrator information allows only specified users to perform operations on administrator information from the Operation Panel or Web Service Function. Administrator information includes administrator IDs, administrator authentication information, and administrator roles. Operations on administrator information include creation of new administrators, querying and changing administrator IDs, changing administrator authentication information, and querying, adding and deleting administrator roles. These operations can be performed only by specified users who have been authorised for each operation. Table 30 shows the relationship between the operations on administrator information and the users authorised for operations on administrator information.

Table 30: Access to administrator information

Operations on administrator information	Authorised users
Creation of new administrator IDs	Administrators
Change administrator IDs	Administrators themselves
Query administrator IDs	Administrators themselves, supervisors
Change administrator authentication information	Administrators themselves, supervisors
Add and query administrator roles	Administrators already assigned that administrator role
Delete administrator roles	Administrators already assigned that administrator role (However, no administrator roles can be deleted unless these roles are assigned to another administrator.)

If the logged-in user is an administrator or supervisor, the TOE allows that user to perform the operations shown in Table 30, respectively.
By the above, FIA_USB.1 (User-subject binding), FMT_MSA.1 (Management of security attributes), FMT_MTD.1 (Management of TSF data), FMT_SMF.1 (Specification of management functions) and FMT_SMR.1 (Security roles) are satisfied.

7.1.4.3 Management of Supervisor Information

Management of supervisor information allows only supervisors to query and change supervisor IDs, and to change supervisor authentication information from the Operation Panel or Web Service Function. If the logged-in user from the Operation Panel or a client computer is a supervisor, the TOE allows that user to query and change supervisor IDs and to change supervisor authentication information.
By the above, FMT_MSA.1 (Management of security attributes), FMT_MTD.1 (Management of TSF data), FMT_SMF.1 (Specification of management functions), and FMT_SMR.1 (Security roles) are satisfied.

7.1.4.4 Management of General User Information

Management of general user information allows only specified users to perform all or some of the operations involved in creating, changing, and deleting general user information from the Operation Panel or Web Service Function. General user information includes general user IDs, general user authentication information, document data default ACL, and S/MIME user information.
If the logged-in user from the Operation Panel and Web Service Function is a user administrator or general user, the TOE allows that user to perform the operations shown in Table 31.

Table 31: Authorised operations on general user information

Operations on general user information	Authorised user
Creation of new general user information to Address Book (general user ID, general user authentication information, and S/MIME user information)	User administrators
Edit general user information registered to Address Book (authentication information of general users, document data default ACL, S/MIME user information)	User administrators General users themselves
Query general user information registered to Address Book (general user ID, document data default ACL, S/MIME user information)	User administrators General users themselves
Query general user information registered to Address Book (general user ID, S/MIME user information)	General users
Delete general user Information registered to Address Book (general user ID, authentication information of general users, S/MIME user information)	User administrators
Delete general user information registered to Address Book (S/MIME user information)	General users identified as the S/MIME users

When new general user information is created, the new general user ID will be set to the value of the document data default ACL as the document file owner, and authorised operations on the document data will be reading document data and modifying the document data ACL.

By the above, FMT_MSA.1 (Management of security attributes), FMT_MTD.1 (Management of TSF data), FMT_SMF.1 (Specification of management functions), and FMT_SMR.1 (Security roles) are satisfied.

7.1.4.5 Management of Machine Control Data

Management of machine control data allows setting of machine control data by specified users only.
The TOE allows only specified users to use the functions that set the machine control data from specified operation interfaces. Table 32 shows for each item of machine control data, the range of values that can be set, the operations available, the authorised setter, and the operation interfaces allowed by the TOE.
The TOE also allows the user administrator and general users to query the destination information when using the Deliver to Folder function.

Table 32: Administrators authorised to specify machine control data

Machine control data items	Range of setting value	Operations	Authorised setter	Operation interfaces
Number of Attempts before Lockout	An integer 1-5 (times)	Query, modify	Machine administrators	Web Service Function
Setting for Lockout Release Timer	Active or Inactive	Query, modify	Machine administrators	Web Service Function
Lockout time	1-9999 (minutes)	Query, modify	Machine administrators	Web Service Function
Minimum Password Length	An integer 8-32 (digits)	Query, modify	User administrators	Operation Panel
Password Complexity Setting	Level 1 or Level 2	Query, modify	User administrators	Operation Panel
Date and time of system clock	Date, time (hour, minute, second)	Query, modify	Machine administrators	Operation Panel, Web Service Function
		Query	General users, user administrators, network administrators, file administrators, supervisors	
Lockout Flag for general users	Inactive	Query, modify	User administrators	Web Service Function
Lockout Flag for administrators	Inactive	Query, modify	Supervisors	Web Service Function
Lockout Flag for supervisors	Inactive	Query, modify	Machine administrators	Web Service Function

By the above, FIA_AFL.1 (Authentication failure handling), FMT_MTD.1 (Management of TSF data), FMT_SMF.1 (Specification of management function), and FMT_SMR.1 (Security roles) are satisfied.

7.1.5 SF.CE_OPE_LOCK Service Mode Lock Function

The Service Mode Lock Function restricts use of the Maintenance Functions to CEs only, based on the Service Mode Lock Function setting specified by the machine administrator.
The TOE allows the machine administrator to set the Service Mode Lock Function from the Operation Panel, and allows all authorised users to view the value of the setting. If the Service Mode Lock Function is set to "Off", the TOE allows only the CE to use the Maintenance Functions. If it is set to "On", the TOE does not allow the CE to use the Maintenance Functions.
By the above, FMT_MTD.1 (Management of TSF data) is satisfied.

7.1.6 SF.CIPHER Encryption Function

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

7.1.6.1 Encryption of Document Data

The TOE encrypts data with the Ic Hdd before writing it to the HDD. The TOE decrypts data with the Ic Hdd after reading it from the HDD. This process is performed for all data written to and read from the HDD. Document data is encrypted and decrypted by the TOE in a similar way.
The HDD encryption keys are generated by the machine administrator. If the logged-in user is the machine administrator, the TOE displays a screen on the Operation Panel that the administrator can use to generate the HDD encryption keys.
When the machine administrator uses the Operation Panel to instruct the TOE to generate an HDD encryption key, the TOE generates a 256-bit HDD encryption key using the TRNG encryption key generation algorithm (compliant with the BSI-AIS31 standard). When the TOE writes to or reads from the HDD, it performs the encryption operations shown in Table 33.

Table 33: List of encryption operations on data stored on the HDD

Encryption-triggering operation	Encryption operations	Standard	Encryption algorithm	Key size
Writing data to HDD	Encrypt	FIPS197	AES	256 bits
Reading data from HDD	Decrypt			

The HDD encryption keys can also be printed. If the logged-in user is the machine administrator, the TOE displays a screen on the Operation Panel that the administrator can use to print the HDD encryption keys. The printed encryption keys are used to restore the encryption keys in the event of the encryption keys in the TOE becoming unavailable.
In addition, the TOE verifies that the encryption function of the Ic Hdd operates normally at start-up and verifies the integrity of the HDD encryption keys. If the TOE is not able to verify the integrity of the HDD encryption keys, it will show that the HDD encryption keys have changed.

By the above, FCS_CKM.1 (Cryptographic key generation), FCS_COP.1 (Cryptographic operation), FMT_MTD.1 (Management of TSF data), and FPT_TST.1 (TSF testing) are satisfied.

7.1.7 SF.NET_PROT Network Communication Data Protection Function

This protects document data and print data in transit on internal networks from leakage, and also detects attempts at tampering.
Following are explanations of each functional item in "SF.NET_PROT Network Communication Data Protection Function" and their corresponding security functional requirements.

7.1.7.1 Use of Web Service Function from Client Computer

Whenever it receives a request from a client computer for use of the Web Service Function, the TOE communicates with the client computer using the SSL protocol to create a trusted path.
By the above, FTP_TRP.1 (Trusted path) is satisfied.

7.1.7.2 Printing and Faxing from Client Computer

Whenever it receives a request from a client computer for printing or transmitting faxes, the TOE communicates with the client computer using the SSL protocol to create a trusted path.
By the above, FTP_TRP.1 (Trusted path) is satisfied.

7.1.7.3 Sending by E-mail from TOE

When sending document data by e-mail to a client computer, the TOE attaches the document data to e-mail and sends the e-mail using S/MIME. The S/MIME destination information is registered as S/MIME user information within general user information. Users can send e-mail referring to the registered destination details only.
By the above, FTP_TRP.1 (Trusted path) is satisfied.

7.1.7.4 Delivering to Folders from TOE

When sending (delivering) data to folders on an SMB or FTP server, the TOE connects to the server using the IPSec protocol to create a trusted channel. The destination information for the Deliver to Folders function is registered in advance and managed by the TOE as machine control data. Users can send files referring to the registered folder information only.
By the above, FTP_ITC.1 (Inter-TSF trusted channel) is satisfied.

7.1.8 SF.FAX_LINE Protection Function for Intrusion via Telephone Line

When it receives fax data from the telephone line, the TOE passes the data to the Controller Board. If the received data is not fax data, the TOE discards it.
By the above, FDP_IFC.1 (Subset information flow control) and FDP_IFF.1 (Simple security attributes) are satisfied.

7.1.9 SF.GENUINE MFP Control Software Verification Function

At every TOE start-up, the MFP Control Software Verification Function verifies the integrity of the MFP Control Software that is installed in the FlashROM.
The TOE verifies the integrity of the executable code of the MFP Control Software each time the TOE starts up. The TOE becomes available for users only if the integrity of the control software can be verified. If integrity cannot be verified, it indicates that the MFP Control Software is not correct.
By the above, FPT_TST.1 (TSF testing) is satisfied.

8 Appendix

8.1 Definitions of Terminology

For ease of reader understanding, Table 34 provides definitions of the terms used in this ST.

Table 34: Specific terms used in this ST

Terms	Definitions
D-BOX	A storage area for document data on the HDD.
FTP server	A server for sending files to a client computer and receiving files from a client computer using File Transfer Protocol.
HDD	An abbreviation of "Hard Disk Drive". Refers to the HDD installed in the TOE.
Ic Hdd	A hardware device that encrypts data to be written on the HDD and decrypts data to be read from the HDD.
Ic Key	A chip that contains a microprocessor for encryption processing and EEPROM where a private key for secure communication is held. The Ic Key holds the keys for validity authentication and encryption processing, and a random number generator.
IP-Fax	A function that sends and receives document files between two faxes that are directly connected to a TCP/IP network. It can also send document files to a fax that is connected to a telephone line.
MFP	An abbreviation for digital "multi function product". In this ST, "MFP" also refers to the TOE
Responsible manager of MFP	A person in an organisation in which MFPs are used and who has authority to assign MFP administrators and supervisors. (Or the person who is responsible for the organisation). (Examples: MFP purchaser, MFP owner, manager of a department where MFPs are used, or a person in charge of an IT department.)
MFP Control Software	Software installed in the TOE that can identify TOE components such as system/copy, network support, scanner, printer, fax, Web support, Web Uapl, and Network Doc Box. Manages the resources for units and devices that comprise the MFP and controls their operation.
MFP Control Data	A generic term for a set of parameters that controls the operation of an MFP.
LAN-Fax Transmission	A function that faxes document data from a client computer via the TOE when the client computer is connected to the TOE via a network or USB Ports.
S/MIME user information	Information about each general user that is required for using S/MIME. Includes e-mail address, user certificates, and a specified value for S/MIME use.
SMB server	A server for sharing files with a client computer using Server Message Block Protocol.

Terms	Definitions
SMTP server	A server for sending e-mail using Simple Mail Transfer Protocol.
Address Book	A database containing general user information for each general user.
Back Up/Restore Address Book	A function for backing up the Address Book to SD cards and restoring the TOE Address Book from backups made on SD cards..
Internet Fax	A function that reads a fax original then converts the scanned image to an e-mail format for sending as data over the Internet to a machine with an e-mail address.
Customer engineer (CE)	An expert in TOE maintenance who is employed by a manufacturer, support service company, or a sales company.
Fax reception process on Controller Board	MFP Control Software embedded on the Controller Board. It receives information on the status of fax communications from the Fax Unit, and provides the Fax Unit with instructions for fax communication.
Supervisor	One of the authorised TOE users who manages a password of administrator.
Supervisor ID	An item of supervisor information. Also an identification code for identification and authentication of the supervisor. Indicates the supervisor's login name on this TOE.
Supervisor authentication information	A password for identification and authentication of the supervisor.
Network administration	An administrator role assigning responsibility for management of the TOEs network connections. The network administrator is a person with network management responsibility.
Network control data	MFP control data for connecting MFP to networks.
Minimum Password Length	The minimum number of digits that can be registered in passwords.
Password Complexity Setting	The minimum combination of character types that can be registered in passwords. There are Level 1 and Level 2 Password Complexity Settings. Level 1 requires passwords to include a combination of more than two types of character. Level 2 requires passwords to include a combination of more than three types of character.
Fax process on Fax Unit	The control software on the Fax Unit. It provides the MFP Control Software on the Controller Board with information on the status of fax communications, and controls fax communications according to instructions from the MFP Control Software on the Controller Board.
Deliver to Folder	A function that sends document data from the TOE to folders on an SMB or FTP server via a network.
Sending by E-mail	A function that sends e-mail with attached document data from the TOE.
Memory Transmission	A function that stores scanned data of an original in memory and then dials and faxes that data at a later time.
User administration	An administrator role assigning responsibility for management of general users. The user administrator is a person who has the user management role.

Terms	Definitions
Number of Attempts before Lockout	The number of consecutive failed authentication attempts that can be made using the same user ID before the user is locked out.
Lockout	A function that prohibits access to the TOE to the specific user IDs.
Lockout Flag	An item of data that is assigned to each authorised user. The Lockout Flag for a locked-out user is set to "Active", and the Lockout Flag for a Lockout-released user is set to "Inactive". Administrators and supervisors who are allowed to operate the Lockout Flag can release a Locked-out user by switching the Lockout Flag for the Locked-out user to "Inactive".
Setting for Lockout Release Timer	A setting that enables or disables the timed release of the Lockout function based on a time specified in advance by an administrator. When this setting is inactive, Lockout can be released only by a direct operation by an administrator.
General user	One of the authorised TOE users who uses the Basic Functions of the TOE.
General user ID	An item of general user information and an identification code for identification and authentication of general users. Indicates the general user's login name on this TOE.
General user information	A database containing information about general users as data items that include the general user ID, general user authentication information, document data default ACL, and S/MIME user information
General user authentication information	A password for identification and authentication of a general user.
Print data	The document files in a client computer that are sent to the TOE from a client computer to be printed or faxed. Drivers must be installed in the client computer in advance: a printer driver for printing and a fax driver for faxing. Print data is received by the TOE through the Network Unit or USB Port.
Print Settings	Print Settings for printed output, including paper size, printing magnification, and custom information (such as duplex or layout settings). Print Settings for stored document data can be updated by the user who prints the document data.
External networks	Networks that are not managed by the organisation that manages the MFP. Generally indicates the Internet.
Administrator	One of the authorised TOE users who manages the TOE. Administrators are given administrator roles and perform administrative operations accordingly. Up to four administrators can be registered, and each administrator is given one or more administrator roles.
Administrator ID	An item of administrator information and an identification code for identification and authentication of the administrator. Indicates the administrator's login name on this TOE.
Administrator authentication information	A password for identification and authentication of an administrator.

Terms	Definitions
Administrator role	Management Functions given to administrators. There are four types of administrator role: user administration, machine administration, network administration, and file administration. Each administrator role is assigned to a registered administrator.
Machine administration	An administrator role that assigns responsibility for machine management and performing audits. The machine administrator is a person who has the machine management role.
Machine Control Data	MFP Control Data related to Security Functions and security behaviour.
Operation Panel	A display-input device that consists of a touch screen LCD, key switches, and LED indicators, and is used for MFP operation by users. Also known as an "Operation Panel Unit".
Stored Data Protection Function	A function that protects document data stored on the HDD from leakage.
Store and Print Function	A function that converts print data received by the TOE into document data and stores it in the D-BOX. The document data stored in D-BOX can be printed at a later time.
Stored Documents Fax Transmission	A function that faxes document data stored earlier in the D-BOX.
Direct Print Function	A function that prints print data received by the TOE.
Immediate Transmission	A function that dials first then faxes data while scanning the original.
Internal networks	Networks managed by an organisation that has an MFP. Normally refers to an office LAN environment established as an intranet.
Document file owner	General users who are registered in the document data ACL as owners of the document data.
Document data	Electronic data sent to the MFP by authorised MFP users who perform either of the following operations. 1. Scanning from paper and digitising. 2. Received as print data and then converted by the MFP into a format that can be processed by the MFP.
Document data default ACL	An item of general user information. The default value that is set for the document data ACL of a new document data to be stored.
Document data ACL	An "access control list" of general users that is set for each document data.
File administration	An administrator role assigning responsibility for management of the D-BOX, where document data is stored on the TOE, and management of the document data ACL, which is the list that controls access to the document data. The file administrator is a person who has the role of file administration.
Document file user	General users who are registered in the document data ACL but are not owners of the document data.

8.2 References

Following are the documents referenced in this document.

- CC Version 3.1 Revision 2

  Evaluation Criteria:

  "English version"

  Common Criteria for Information Technology Security Evaluation Version3.1

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

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

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

  "Japanese-translated version"

  Common Criteria for Information Technology Security Evaluation Version3.1

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

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

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

  Evaluation Methodology:

  "English version"

  Common Methodology for Information Technology Security Evaluation Version 3.1

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

  "Japanese-translated version"

  Common Methodology for Information Technology Security Evaluation version 3.1

  Evaluation Methodology Revision 2 [Japanese translation ver. 2.0]