imagio MP 5000SP/4000SP with Security Card Type 9

Security Target

Authors : Ricoh Co., Ltd. Hiroshi Kakii, Tsuyoshi Shimizu, Tsuyoshi Sakuma, Fumi Takita
Date : 2010-02-18
Version : 1.00

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

Update History

Version	Date	Authors	Details
1.00	2010-02-18	Hiroshi Kakii, Tsuyoshi Shimizu, Tsuyoshi Sakuma, Fumi Takita	Release print

Table of Contents

Figure List

Table List

1 ST Introduction

This chapter describes ST references, TOE references, TOE overview and TOE descriptions.

1.1 ST References

The ST identification information shows as follows:

ST Title : imagio MP 5000SP/4000SP with Security Card Type 9 Security Target

ST Version : 1.00

Date : 2010-02-18

Authors : Ricoh Co., Ltd. Hiroshi Kakii, Tsuyoshi Shimizu, Tsuyoshi Sakuma, Fumi Takita

1.2 TOE References

The TOE identification information shows as follows:

Manufacturers : Ricoh Co., Ltd.

TOE Name : Ricoh imagio MP 5000SP/4000SP with Security Card Type 9

TOE Versions : The TOE is specified by 3 types of versions: Firmware Configuration System Version, ASIC Version and Option Version. Firmware Configuration is specified by System Version. The system version is a version which is given for combining multiple firmware versions built-in the device itself. ASIC and Option are specified by the list of each onboard version. This TOE version is as follows:

- Firmware Configuration

System Version : V2.16-00

Name and Version of Firmware Configuration	
System/Copy	1.11.1
Network Support	7.26
Network DocBox	1.10C
Web Support	1.59
Web Uapl	1.15
animation	1.3
Scanner	01.24
RPDL	7.33
Printer	1.11
MSIS	7.15.02

RPCS Font	1.01
Engine	1.04:05
OpePanel	1.01
LANG0	1.01
LANG1	1.01
ADF	15.000:15

- ASIC

  Ic Key Version : 1100

- Option

  Data Erase Opt Version : 1.01m

Keyword : Digital MFP, Document, Copy, Print, Scanner, Network, Office

1.3 TOE Overview

This chapter describes this TOE type and the major security functions, the TOE usage environment.

1.3.1 TOE Identification and Major Security Functions

This TOE is a digital MFP (as described below, MFP) which is an IT product. The major security functions in this TOE are as follows:

- Audit Function
- Identification and Authentication Function
- Access Control Function
- Network Protection Function
- Residual Data Overwrite Function
- Security Management Function
- Software Verification Function

1.3.2 TOE Usage Environment

The TOE usage environment is illustrated and described.

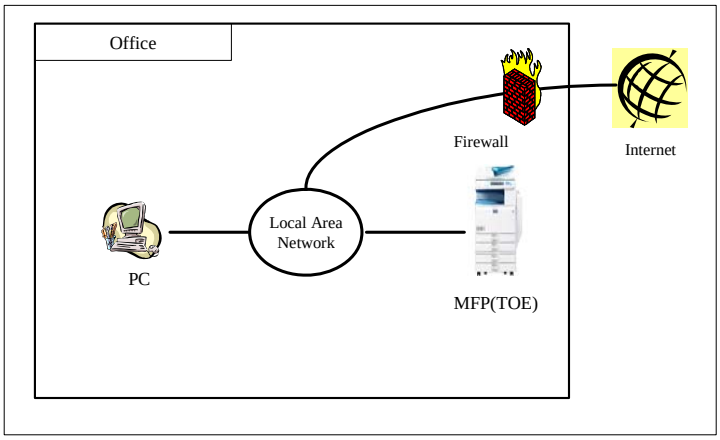


Figure 1 : TOE Usage Environment

It is assumed that the TOE is used in offices. The environment is described as follows:

[Local Area Network]

It indicates Local Area Network (as described below, LAN) used in offices.

[MFP]

It is a TOE, connected to Office LAN where users perform the following processing from Operation Panel:

- Each setting of the MFP itself
- Copy paper documents by copy operation
- Print user documents received by printer operation
- Store user documents into MFP with scanner operation
- Operate on user documents by document server operation

[PC]

It is operated as a client PC and it performs the following processing communicating with MFP via LAN:

- Each setting of the MFP itself via Web browser
- Operate on user documents via Web browser
- Store user documents via printer driver

[Firewall]

It is a device to prevent any attack in the office network from Internet

1.4 TOE Descriptions

This chapter describes the overview of: physical scope of the TOE, definitions of the related roles, logical scope of the TOE, and protected assets.

1.4.1 Physical Scope of the TOE

The physical scope of the TOE is a MFP which consists of hardware: Operation Panel Unit, Engine Unit, Controller Board, HDD, LAN Interface, USB Interface, SD Slot, and Panel Interface as shown in Figure 2.

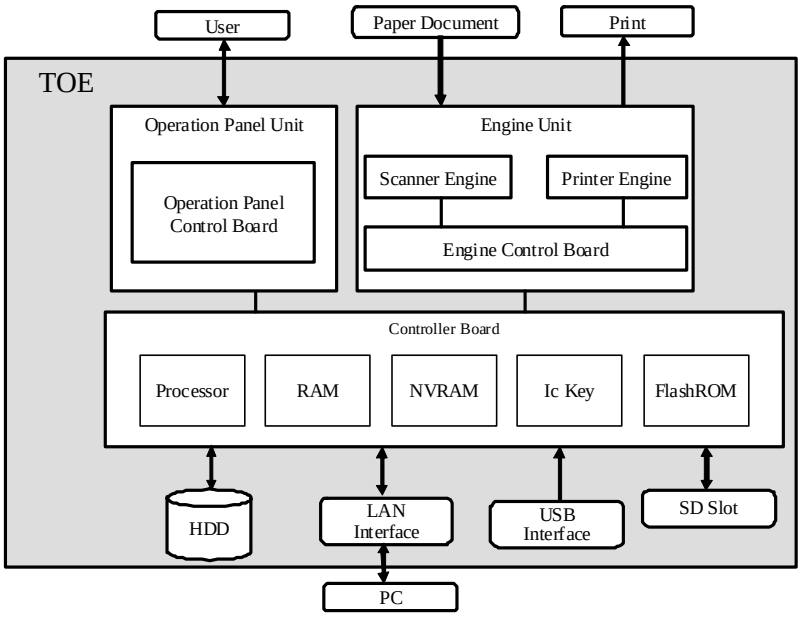


Figure 2 : Hardware Configuration of TOE

- Operation Panel Unit (hereinafter called Operation Panel)

  The Operation Panel Unit is a device which has the user interface function installed in the TOE, and consists of key switches, LED indicators, touch screen LCD, and operation panel control board which is connected with these devices. The operation panel control software is installed in the operation panel control board. The operation panel control software performs as follows:

  1. It transmits the instruction for operating from key switches and touch screen LCD into MFP control software.
  2. It turns ON / OFF LED indicators and the touch screen LCD displays messages by the instruction for displaying from MFP control software.

  The operation panel control software corresponds to 'OpePanel', 'LANG0', and 'LANG1' among the components which identify the TOE. LANG0 and LANG1 are character data displayed on the operation panel.

- Engine Unit

  The Engine Unit consists of scanner engine which is a device for reading paper documents, printer engine which is a device for printing the outgoing documents, and engine control board. The engine control software is installed in the engine control board. The engine control software transmits the status

of the scanner engine and the printer engine to MFP control software, or receives the instruction from the MFP control software and operates the scanner engine and the printer engine. Among the components which identify the TOE, the engine control software corresponds to 'Engine' and 'ADF'.

- Controller Board
  Device on which processor, RAM, NVRAM, IcKey, and FlashROM are assembled. The overview is described as follows:
  - Processor
    Semiconductor chip that performs the basic calculation processing for MFP operation
  - RAM
    Volatile memory which is used as a working area to process the image data for compressing / decompressing the processing information and to temporarily read and write the internal information.
  - NVRAM
    Non-volatile memory to store TSF information which determines the MFP operation
  - Ic Key
    Security chip which has functions of random number generation, cryptographic key generation, and electronic signature. It provides storage of the signature root key for maintenance when shipping from factories.
  - FlashROM
    Non-volatile memory that installs MFP control software itself. The MFP control software is software installed in the TOE, and among the components of the TOE, corresponds to System / Copy, Network Support, Scanner, Printer, Web Support, Web Uapl, Network Doc Box, animation, RPDL, MSIS, and RPCS Font. It performs the resource management of units and devices that comprise the MFP and controls their operation.
- HDD
  Hard Disk Drive which is non-volatile memory. It stores user documents, deleted user documents, temporary documents, fragments, login user names and login passwords of normal users.
- LAN Interface
  External interface for LAN to support Ethernet (100BASE-TX/10BASE-T)
- USB Interface
  If printing directly from PCs, it is an external interface to connect the TOE with client PCs. This interface is disabled during the installation / setup of the TOE.
- SD Slot
  Slot for inserting SD card, which keeps the residual data overwrite function software (Data Erase Opt). The SD slot is inside of the device, and only a customer engineer is allowed to open the cover and use it for installation.

1.4.2 Guidance

The guidance documents for configuring this TOE are as follows (written in Japanese):

- imagio MP 5000/4000 Series Operating Instructions (Security Reference)
- imagio MP 5000/4000 Series Operating Instructions (For Using this Machine)

- imagio MP 5000/4000 Series Operating Instructions (Q&A)
- imagio MP 5000/4000 Series Operating Instructions (Copy Function / Document Server Function Reference)
- imagio MP 5000/4000 Series Operating Instructions (Printer Function Reference)
- imagio MP 5000/4000 Series Operating Instructions (Scanner Function Reference)
- imagio MP 5000/4000 Series Operating Instructions (Network Guide)
- imagio MP 5000/4000 Series Operating Instructions (Initialisation Reference)
- imagio MP 5000/4000 Series Included Operating Instructions
- imagio MP 5000/4000 Series Quick Guide
- For Users of Security Function
- For Administrators who use the settings based on IEEE Std. 2600.1-2009 compliance
- Operating Instructions for imagio Security Card Type 7 and imagio Security Card Type 9

1.4.3 User Roles

This section defines users who directly use the TOE and users who indirectly do so.

1.4.3.1. Direct User

When this ST simply calls it 'User', it indicates this Direct User, who is permitted to use the TOE for any authorisations. Users consist of normal user and administrator, and the following Table (Table 1) shows its definitions.

Table 1 : User Definitions

User Definition	Explanation
Normal User	User, who is allowed to use the TOE, is granted login name and performs normal MFP functions.
Administrator	User, who is allowed to manage the TOE, performs the management operation included giving login name to normal user.

Administrator is a user who is registered for the purpose of the TOE management. According to the roles, they shall be identified as Supervisor and MFP Administrator. Up to 4 (maximum) MFP administrators can be registered to selectively authorise User Management, Device Management, Network Management and File Management. Therefore, it is possible for multiple MFP administrators to select the management authorisations, but, if this ST calls it 'MFP Administrator', it indicates that the MFP administrators have all management authorisations (Table 2).

Table 2 : List of Administrative Roles

Administrator Definition	Management Authorisation	Explanation
Supervisor	Supervisor	Authorises to delete and register a login password of MFP administrator
MFP Administrator	User management authorisation	Authorises to manage normal user. Enables to operate the setting for normal user.

	Device management authorisation	Authorises to determine the operation of MFP devices except for Network. Enables to operate the information for device settings and browse the audit log.
	Network management authorisation	Authorises to manage Network including LAN settings. Enables to operate the information for Network settings.
	File management authorisation	Authorises to manage user documents. Enables to operate the access management of user documents.

1.4.3.2. Indirect User

MFP Chief Administrator

MFP Chief Administrator is a person who has a role to select the TOE administrators in the organisation for using the TOE.

Customer Engineer

Customer Engineer is a person who belongs to the organisation which manages the maintenance of the TOE, and is in charge of installing the TOE, setup, and performing the maintenance.

1.4.4 Logical Scope of the TOE

The basic functions and the security functions are described as below:

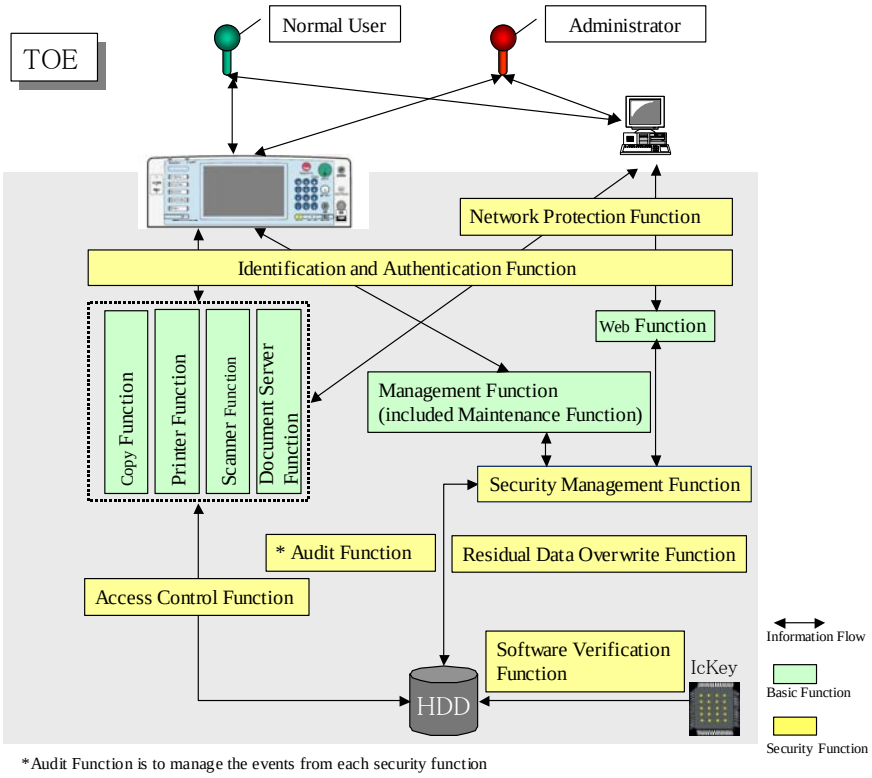


Figure 3 : Logical Scope of TOE

1.4.4.1. Basic Functions

The overview of the basic functions is described as follows:

- **Copy Function**

  Copy Function is to scan paper documents and then print the scanned image data according to the chosen number of copies, the printing magnification, and the custom settings. When using the copy function, normal users shall enter login from Operation Panel and perform the copy processing.

- **Printer Function**

  Printer Function consists of the following 3 functions:

  - A function to store as user document the print information from client PCs via Network
  - A function to perform the operation of printing the stored user documents
  - A function to directly print the print information from client PCs via Network

  According to the guidance, normal users shall install first the designated printer driver in their own client PCs, and then use it.

For using the printer function in practice, normal users shall select documents to print from their client PCs and instruct the storage of their documents, then perform the print processing from Operation Panel or Web browser, or they shall select documents to print from their client PCs and instruct the direct print, and then perform the print processing.

- **Scanner Function**

  Scanner Function is to scan paper documents and consists of the following 2 functions:

  - A function to scan and store user documents in the device itself
  - A function to download to client PCs the stored user documents

  For using the scanner function in practice, normal users shall perform the scan operation from Operation Panel, and then perform the download processing of the stored user documents via Web browser to their client PCs.

- **Document Server Function**

  Document Server Function is to perform operations on user documents stored in the HDD of the MFP device itself. Printing the user documents which are stored by the above printer function, and downloading to client PCs the user documents stored by the scanner function, are implemented using this document server function.

- **Management Function**

  Management Function is to control all of the operation of MFP devices. It is performed by Operation Panel or via Web browser.

- **Maintenance Function**

  Maintenance Function is to implement the maintenance service processing for machines malfunction. Customer Engineer performs to analyse the cause from Operation Panel. This function will be performed only by the procedures which Customer Engineer holds. If MFP administrator sets the service mode lock, Customer Engineer cannot use it.

  This ST covers the service mode lock function to ‘ON’ as the target of evaluation.

- **Web Function**

  Web Function is a function with which the TOE user operates a remote control for the TOE from a client PC. For the remote control, install the specified Web browser in the client PC according to the guidance, and then connect the TOE via LAN.

1.4.4.2. Security Functions

The security functions are described as follows:

- **Audit Function**

  Audit Function is to generate audit log for the occurrences of events in order to check the operation status of the TOE and detect the security intrusion. Only MFP administrators are allowed to read and delete the audit log generation. The operations of reading and deleting the audit log shall be performed by Web function.

- **Identification and Authentication Function**

  Identification and Authentication Function is to identify and authenticate persons who try to use the TOE, to lockout persons who consecutively fail in the authentication, and to protect the feedback area for authenticating login password when logging in using the Operation Panel. When using the printer function, it identifies and authenticates login user name and login password after entering in the printer driver.

- **Access Control Function**

  Access Control Function is to control based on the authorities for the authorised TOE users who are authenticated by Identification and Authentication Function or for the user roles, or based on the operation permissions allowed to each user.

- **Network Protection Function**

  Network Protection Function is to protect the information disclosure from monitoring on Networks when using LAN. The Web browser enables the protection function by designating the URL for encrypted communication. When using the printer function, MFP enables the protection function by selecting encrypted communication in the printer driver.

- **Residual Data Overwrite Function**

  Residual Data Overwrite Function is to completely delete the residual data by overwriting with specific pattern data all user documents deleted in HDD, temporary documents and fragments.

- **Security Management Function**

  Security Management Function is to provide all functions related to security management which the administrators perform.

- **Software Verification Function**

  Software Verification Function is to ensure the correctness of MFP control software by checking the integrity of executable codes for the MFP control software which is installed in FlashROM.

1.4.5 Protected Assets

This section defines assets which the TOE shall protect, shown as class, type, and the contents in Table 3 below. Table 4 summarizes where those assets exist. When simply representing Protected Assets later, all these information are intended in this document.

Table 3 : Assets Definitions

Class	Type	Content
User Data	Document Information	Digitalized user documents, deleted documents, temporary documents and fragments under the TOE control
	Function Information	Job information specified by users. In this ST, it is represented by 'User Job'.
TSF Data	Protected Information	Login user name, Status of user job, Allowance times of entering login password, Timer settings of lockout release, Lockout time, Year-month-day settings, Time settings, Service Mode Lock Function. In this ST, it is represented by 'TSF Protected Information'.
	Confidential Information	Login password, Audit log. In this ST, it is represented by 'TSF Confidential Information'.

Table 4 : Non-Volatile Memory and Stored Information

Non-Volatile Memory	Stored Information
HDD	User documents Deleted user documents, temporary documents and fragments Login password for normal user Audit log
NVRAM	Login user name of administrator Login password for administrator Login user name of normal user Device setting values, device counter information, adjusting values for devices, etc.
Flash ROM	MFP control software
SD Memory	Residual data overwrite function software
IcKey	Signature root key

1.5 Terminology

1.5.1 Terminology for this ST

For clearly understanding this ST, the meanings of the specific terms are defined in Table 5.

Table 5 : Specific Terms Related to this ST

Term	Definition
Login User Name	An identifier given to a user. The TOE specifies the user with the identifier.
Login Password	A password associated with each login user name
Lockout	A status of disallowing users to login
Auto Logout	A function to automatically logout if no activity during a given period of time after login from Operation Panel or Web browser
Minimal Password Length	The minimum number of characters that can be registered for passwords.
Password Complexity Setting	The minimum combination of character types that can be registered for passwords. There are 4 character types: alphabetic lowercase and uppercase letters, number, and symbols. There are Level 1 and Level 2 for Password Complexity Setting. Level 1 requires passwords with a combination of more than 2 character types. Level 2 requires passwords with a combination of more than 3 character types.
HDD	An abbreviation of Hard Disk Drive. In this document, it indicates that HDD is installed in the TOE if simply describing as HDD.
User Job	A job in which users require the operation for the TOE. The continuous work from start to end is regarded as 1 job. The intended operations are: Store, Print, Download, and Delete user documents.
Document	Information for digital image data under the TOE control which is generated by using the functions of Copier, Printer, and Scanner. The stored documents in the device are explicitly called 'User Documents' in this ST. If simply describing as document, it includes deleted documents for copying and printing, temporary documents and fragments.
Available Document User List	A login user name list of normal users who are allowed to access to user documents. It is granted as attributes of each user document. Even if allowed to access, the login user name of MFP administrator is not included in this list.
Available Function List	A list of the permitted functions (Copy Function, Printer Function, Scanner Function, and Document Server Function) to access for normal users. It is granted as attributes of each normal user.
Operation Panel	A display-input device that consists of a touch screen LCD and key switches. It is used by Users to perform MFP operation.

2 CC Conformance

This chapter describes conformance claims.

2.1 CC Conformance Claims

CC conformance claims in this ST and the TOE are described as follows:

- CC Versions which claim conformances

  Part 1:

  Introduction and general model, September 2006 Ver.3.1 Revision 1 (Japanese translation Ver.1.2) CCMB-2006-09-001

  Part 2:

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

  Part 3:

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

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

2.2 PP Claims

PP to which this ST and the TOE are demonstrable conformance is:

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

Version: 1.0, dated June 2009

Notes: PP name which is published in Common Criteria Portal is "U.S. Government Protection Profile for Hardcopy Devices in Basic Robustness Environments (IEEE Std. 2600.1-2009)".

2.3 Package Claims

The package which this ST and the TOE conform to is Evaluation Assurance Level EAL3+ALC_FLR.2.

The selected SFR Packages from PPs are:

2600.1-PRT conformant

2600.1-SCN conformant

2600.1-CPY conformant

2600.1-DSR conformant

2600.1-SMI conformant

2.4 Conformance Claims Rationale

This TOE selects as Common Security Functional Requirements and SFR Package in accordance with PP, 2600.1-PRT, 2600.1-SCN, 2600.1-CPY, 2600.1-DSR, and 2600.1-SMI.

For maintaining and managing the audit log, this TOE augments FAU_STG.1, FAU_STG.4, FAU_SAR.1, and FAU_SAR.2 in accordance with PP APPLICATION NOTE 7.

Implemented by this TOE, the authentication augments FIA_AFL.1, FIA_UAU.7, and FIA_SOS.1 in accordance with PP APPLICATION NOTE 36.

2600.1-PRT, 2600.1-SCN, 2600.1-CPY, 2600.1-DSR, and 2600.1-SMI are PP conformances.

2600.1-FAX is not selected because this TOE doesn't assemble Fax Function.

2600.1-NVS is not selected because this TOE doesn't have any removable, non-volatile memory media.

This TOE, in accordance with PP, extends the Functional Requirement Part 2 with adding the restricted forwarding of data to external interfaces (FPT_FDI_EXP).

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

Chapters 3 and 4 embodied the points that readers will not understand smoothly for literal translation. For threats, organisational security policies, assumptions, security objectives for the TOE and operational security policies, the items neither increase nor decrease.

In Chapter 6, some functional requirements which PP claims do not correspond in pairs, while it is concretely explained according to the implementation of the TOE in order to satisfy the claims for all functional requirements described in PP.

3 Security Problem Definition

This chapter describes threats, organisational security policies, and assumptions.

3.1 Threats

This section identifies and explains the assumed threats in this TOE usage and the usage environment. It is assumed that the threats stated in this chapter are users who have as knowledge the information that is published on the TOE operation. The attacker is a person who has the capability of attacking on basic level.

T.DOC.DIS **Document Disclosure**

User documents, deleted documents, temporary documents and fragments which the TOE manages may be referenced by persons who have no login user name or by unauthorised persons who have login user names but don't have any access to their documents.

T.DOC.ALT **User Document Alteration**

User documents which the TOE manages may be altered by persons who have no login user name or by unauthorised persons who have login user names but don't have any access to the user documents.

T.FUNC.ALT **User Job Alteration**

User job which the TOE manages may be altered by persons who have no login user name or by unauthorised persons who have login user names but don't have any access to the user job.

T.PROT.ALT **TSF Protected Information Alteration**

TSF Protected Information which the TOE manages may be altered by persons who have no login user name or by unauthorised persons who have login user names but don't have any access to the TSF Protected Information.

T.CONF.DIS **TSF Confidential Information Disclosure**

TSF Confidential Information which the TOE manages may be referenced by persons who have no login user name or by unauthorised persons who have login user names but don't have any access to the TSF Confidential Information.

T.CONF.ALT **TSF Confidential Information Alteration**

TSF Confidential Information which the TOE manages may be altered by persons who have no login user name or by unauthorised persons who have login user names but don't have any access to the TSF Confidential Information.

3.2 Organisational Security Policies

The organisational security policies are taken as follows:

P.USER.AUTHORIZATION User Authorization

The person who has a login user name only for the TOE usage shall be able to use the TOE.

P.SOFTWARE.VERIFICATION Software Verification

The TOE shall provide procedures to self-verify executable codes.

P.AUDIT.LOGGING Audit Log Management

The TOE shall be able to manage and maintain auditable events logs related to the TOE usage and security in order to prevent unauthorised persons from disclosure or alteration of the audit logs. Additionally, the authorised persons shall be able to reference the logs.

P.INTERFACE.MANAGEMENT External Interface Management

In order to prevent unauthorised persons from using the external interface of the TOE (Operation Panel, LAN, and USB), those interfaces shall be appropriately controlled by the TOE and the IT environment.

3.3 Assumptions

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

A.ACCESS.MANAGED Access Managed

According to the guidance, the TOE shall be installed in a safe place under control, and physically limit access to unauthorised persons.

A.USER.TRAINING User Training

MFP chief administrator trains users to be aware of their organisational security policies and procedures in accordance with the guidance. The users are regarded as following their policies and procedures.

A.ADMIN.TRAINING Administrator Training

Administrators are aware of the organisational security policies and the procedures and can perform the TOE settings and processing in accordance with the guidance.

A.ADMIN.TRUST Trust Administrator

MFP chief administrator does not use their privileged access rights for malicious purposes.

4 Security Objectives

This chapter describes security objectives for the TOE, security objectives for operational environment, and rationale.

4.1 Security Objectives for the TOE

This chapter describes security objectives for the TOE.

O.DOC.NO_DIS Protection of Document Disclosure

The TOE shall ensure that user documents, deleted user documents, temporary documents and fragments are protected from disclosure by persons who have no login user name or by unauthorised persons who have login user names but don't have any access to their documents.

O.DOC.NO_ALT Protection of User Document Alteration

The TOE shall ensure that user documents are protected from alteration by persons who have no login user name or by unauthorised persons who have login user names but don't have any access to the user documents.

O.FUNC.NO_ALT Protection of User Job Alteration

The TOE shall ensure that user job is protected from alteration by persons who have no login user name or by unauthorised persons who have login user names but don't have any access to the user job.

O.PROT.NO_ALT Protection of TSF Protected Information Alteration

The TOE shall ensure that TSF Protected Information is protected from alteration by persons who have no login user name or by unauthorised persons who have login user names but don't have any access to the TSF Protected Information.

O.CONF.NO_DIS Protection of TSF Confidential Information Disclosure

The TOE shall ensure that TSF Confidential Information is protected from disclosure by persons who have no login user name or by unauthorised persons who have login user names but don't have any access to the TSF Confidential Information.

O.CONF.NO_ALT Protection of TSF Confidential Information Alteration

The TOE shall ensure that TSF Confidential Information is protected from alteration by persons who have no login user name or by unauthorised persons who have login user names but don't have any access to the TSF Confidential Information.

O.USER.AUTHORIZED User Authorization

The TOE requires user identification and authentication, and the TOE shall ensure that the user is authenticated in accordance with the security policies prior to the permission for the TOE usage.

O.INTERFACE.MANAGED External Interface Management by TOE

The TOE shall ensure that the TOE manages the operation of the external interfaces (Operation Panel and LAN) in accordance with the security policies. It performs the access control to the operation panel and the opened LAN port by the TOE. And the TOE sends only data processed by the TOE to the external interfaces.

O.SOFTWARE.VERIFIED Software Verification

The TOE shall ensure the provision of the procedures to self-verify executable codes.

O.AUDIT.LOGGED Audit Log Management

The TOE shall ensure that the TOE maintains as audit log the auditable events logs related to the TOE usage and security in the device itself and that it manages to prevent unauthorised persons from disclosure or alteration of the audit logs.

4.2 Security Objectives for Operational Environment

This chapter describes the security objectives for operational environment.

4.2.1 IT Environment

OE.AUDIT_STORAGE.PROTECTED Audit Log for Trusted IT Products Protection

MFP chief administrator shall ensure that the exported audit log to trusted IT products are defended against access, deletion, and alteration from unauthorised persons.

OE.AUDIT_ACCESS.AUTHORIZED Audit Log Access of Trusted IT Products Restriction

MFP chief administrator shall ensure that the exported audit log to trusted IT products is accessible only for authorised persons and detects the potential security violations.

OE.INTERFACE.MANAGED External Interface Management in the IT Environment

The IT environment shall ensure to take the action for avoiding the unmanaged access to the TOE external interface (LAN). Therefore, according to the guidance, MFP chief administrator instructs to appropriately perform the firewall settings and protects the LAN interface from attack in Internet. Moreover, according to the guidance, the MFP chief administrator instructs MFP administrators to process the closing of the LAN port which is not used and to set the USB port to forbid installation.

4.2.2 Non-IT Environment

OE.PHYSICAL.MANAGED Physical Management

According to the guidance, The TOE shall be placed in a secure or monitored area that provides protection from unmanaged physical access to the TOE.

OE.USER.AUTHORIZED Grant Authorities to Users

MFP chief administrator shall ensure to give login user names, login passwords, and user roles (Supervisor, MFP Administrator, and Normal User) to those who follow the organisational security policies and procedures and to permit as user the authorities to use the TOE.

OE.USER.TRAINED Trained User

MFP chief administrator shall ensure that users, who are trained by the guidance to recognize the organisational security policies and the procedures, follow those policies and procedures.

OE.ADMIN.TRAINED Trained Administrator

MFP chief administrator shall ensure that administrators are aware of the organisational security policies and the procedures. Therefore, the MFP chief administrator shall ensure that the administrators are trained and competent, and they also have the time to follow the organisational security policies and the procedures in accordance with the guidance.

OE.ADMIN.TRUSTED Trust Administrator

MFP chief administrator does not use their privileged access rights for malicious purposes.

OE.AUDIT.REVIEWED Audit Log Review

MFP chief administrator shall ensure that audit logs are reviewed at appropriate intervals for security violations or unusual patterns of activity.

4.3 Security Objectives Rationale

This chapter indicates the security objectives rationale. The security objectives respond to the regulated assumptions, counter threats, and enforce organisational security policies.

4.3.1 Corresponding relation table for security objectives

Table 6 shows the corresponding relation for the assumptions of security objectives, the countering threats, and the enforcing organisational security policies.

Table 6 : Security Objectives Rationale

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

4.3.2 Security Objectives Descriptions

Each of the following security objectives shows the suitable rationale which satisfies threats, assumptions, and organisational security policies.

T.DOC.DIS

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

It is ensured that OE.USER.AUTHORIZED permits as an authorised user to use the TOE for a person who follows the organisational security policies and procedures. It is ensured that by O.USER.AUTHORIZED, the TOE requires the user identification and authentication, and authorise the user prior to the TOE usage permission in accordance with the security policies. From O.DOC.NO_DIS, the TOE ensures that user documents, deleted documents, temporary documents and fragments are not disclosed by persons who have no login user name, or by unauthorised persons who have login user names but don't have any access to their documents.

These objectives counter T.DOC.DIS.

T.DOC.ALT

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

It is ensured that OE.USER.AUTHORIZED permits as an authorised user to use the TOE for a person who follows the organisational security policies and procedures. It is ensured that by O.USER.AUTHORIZED, the TOE requires the user identification and authentication, and authorise the user prior to the TOE usage permission in accordance with the security policies. From O.DOC.NO_ALT, the TOE ensures that user document is not altered by persons who have no login user name, or by unauthorised persons who have login user names but don't have any access to the user document.

These objectives counter T.DOC.ALT.

T.FUNC.ALT

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

It is ensured that OE.USER.AUTHORIZED permits as an authorised user to use the TOE for a person who follows the organisational security policies and procedures. It is ensured that by O.USER.AUTHORIZED, the TOE requires the user identification and authentication, and authorise the user prior to the TOE usage permission in accordance with the security policies. From O.FUNC.NO_ALT, the TOE ensures that user job is not altered by persons who have no login user name, or by unauthorised persons who have login user names but don't have any access to the user job.

These objectives counter T.FUNC.ALT.

T.PROT.ALT

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

It is ensured that OE.USER.AUTHORIZED permits as an authorised user to use the TOE for a person who follows the organisational security policies and procedures. It is ensured that by O.USER.AUTHORIZED, the TOE requires the user identification and authentication, and authorise the user prior to the TOE usage permission in accordance with the security policies. From O.PROT.NO_ALT, the TOE ensures that TSF

Protected Information is not altered by persons who have no login user name, or by unauthorised persons who have login user names but don't have any access to the TSF Protected Information.

These objectives counter T.PROT.ALT.

T.CONF.DIS

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

It is ensured that OE.USER.AUTHORIZED permits as an authorised user to use the TOE for a person who follows the organisational security policies and procedures. It is ensured that by O.USER.AUTHORIZED, the TOE requires the user identification and authentication, and authorise the user prior to the TOE usage permission in accordance with the security policies. From O.CONF.NO_DIS, the TOE ensures that TSF Confidential Information is not disclosed by persons who have no login user name, or by unauthorised persons who have login user names but don't have any access to the TSF Confidential Information.

These objectives counter T.CONF.DIS.

T.CONF.ALT

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

It is ensured that OE.USER.AUTHORIZED permits as an authorised user to use the TOE for a person who follows the organisational security policies and procedures. It is ensured that by O.USER.AUTHORIZED, the TOE requires the user identification and authentication, and authorise the user prior to the TOE usage permission in accordance with the security policies. From O.CONF.NO_ALT, the TOE ensures that TSF Confidential Information is not altered by persons who have no login user name, or by unauthorised persons who have login user names but don't have any access to the TSF Confidential Information.

These objectives counter T.CONF.ALT.

P.USER.AUTHORIZATION

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

It is ensured that OE.USER.AUTHORIZED permits as an authorised user to use the TOE for a person who follows the organisational security policies and procedures. It is ensured that by O.USER.AUTHORIZED, the TOE requires the user identification and authentication, and authorise the user prior to the TOE usage permission in accordance with the security policies.

These objectives comply with P.USER.AUTHORIZATION.

P.SOFTWARE.VERIFICATIN

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

From O.SOFTWARE.VERIFIED, it is ensured that the TOE provides the procedures to self-verify the executable codes.

These objectives comply with P.SOFTWARE.VERIFICATION.

P.AUDIT.LOGGING

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

By O.AUDIT.LOGGED, it is ensured that the TOE maintains in the device itself as audit log the auditable events logs related to the TOE usage and security, and manages to prevent the unauthorised persons from disclosure or alteration of the audit logs. From OE.AUDIT.REVIEWED, it is ensured that MFP chief administrator enforces to review the audit logs at appropriate intervals in accordance with the guidance descriptions for detecting the security violations or unusual patterns of activity.

Meanwhile, by OE.AUDIT_STORAGE.PROTECTED, it is ensured that the MFP chief administrator prevents the unauthorised persons from access, deletion, and alteration of the audit log which is exported to trusted IT products. From OE.AUDIT_ACCESS.AUTHORIZED, the MFP chief administrator ensures that the audit log which is exported to trusted IT products is accessible only by authorised persons, and the potential security violations are detected.

These objectives comply with P.AUDIT.LOGGING.

P.INTERFACE.MANAGEMENT

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

From O.INTERFACE.MANAGED, it is ensured that the TOE controls the operation of the external interfaces (Operation Panel and LAN) in accordance with the security policies. It is ensured that the TOE enforces the access control to the operation panel and the opened LAN port, and OE.INTERFACE.MANAGED appropriately controls the access between LAN and USB. More specifically,

i. MFP chief administrator instructs to appropriately perform the firewall settings and to protect the LAN interface from attack in Internet.
ii. MFP chief administrator tells MFP administrators to close the LAN port which is not used.
iii. MFP chief administrator tells MFP administrators to set the USB port to forbid installation.

These objectives comply with P.INTERFACE.MANAGEMENT.

A.ACCESS.MANAGED

OE.PHYISCAL.MANAGED operates A.ACCESS.MANAGED.

According to the guidance, it is ensured that OE.PHYISCAL.MANAGED installs the TOE in a safe place under control and restricts physical access from unauthorised persons.

This objective fulfills A.ACCESS.MANAGED.

A.ADMIN.TRAINING

OE.ADMIN.TRAINED operates A.ADMIN.TRAINING.

From OE.ADMIN.TRAINED, MFP chief administrator ensures that administrators are aware of the organisational security policies and procedures. Therefore, it is ensured that the MFP chief administrator is responsible for that the administrators are trained and competent, and also have the time to follow those policies and procedures in accordance with the guidance.

This objective fulfills A.ADMIN.TRAINING.

A.ADMIN.TRUST

OE.ADMIN.TRUSTED operates A.ADMIN.TRUST.

By OE.ADMIN.TRUSTED, it is ensured that MFP chief administrator does not use their privileged access rights for malicious purposes.

This objective fulfills A.ADMIN.TRUST.

A.USER.TRAINING

OE.USER.TRAINED operates A.USER.TRAINING.

From OE.USER.TRAINED, MFP chief administrator ensures that users, who are trained by the guidance to recognize the organisational security policies and the procedures, follow those policies and procedures.

This objective fulfills OE.USER.TRAINED.

5 Extended Components Definition

This chapter describes the extended security functional requirements.

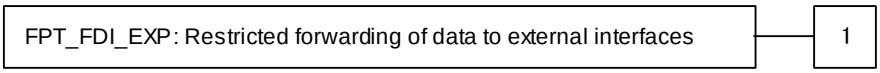
5.1 Restricted forwarding of data to external interfaces (FPT_FDI_EXP)

Family Behaviour

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

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

Component levelling



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

Management: FPT_FDI_EXP.1

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

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

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

c) revocation of such an allowance.

Audit: FPT_FDI_EXP.1

There are no auditable events foreseen.

Rationale:

Quite often a TOE is supposed to perform specific checks and process data received on one external interface before such (processed) data is allowed to be transferred to another external interface. Examples are firewall

systems but also other systems that require a specific work flow for the incoming data before it can be transferred. Direct forwarding of such data (i.e. without processing the data first) between different external interfaces is therefore a function that – if allowed at all – can only be allowed by an authorised role.

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

The Common Criteria defines attribute-based control of user data flow in its FDP class. However, in this Security Target, the authors needed to express the control of both user data and TSF data flow using administrative control instead of attribute-based control. It was found that using FDP_IFF and FDP_IFC for this purpose were inappropriate. Therefore, the authors decided to define an extended component to address this functionality.

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

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of Management Functions. FMT_SMR.1 Security roles
FPT_FDI_EXP.1.1	The TSF shall provide the capability to restrict data received on **[assignment: *list of external interfaces*]** from being forwarded without further processing by the TSF to **[assignment: *list of external interfaces*]**.

6 Security Requirements

This chapter describes security functional requirements, security assurance requirements, and security requirements rationale.

6.1 Security Functional Requirements

This chapter describes the TOE security functional requirements to enforce the security objectives specified in Clause 4.1. And the security functional requirements are referenced by the specified ones in CC Part2. The security functional requirements which are not specified in CC Part2 are referenced by the extended security functional requirements specified in PP (U.S. Government Protection Profile for Hardcopy Devices in Basic Robustness Environments (IEEE 2600.1 – 2009)).
And the parts which perform operations of assignments and selections defined in [CC] are identified in **[Bold and Parenthesis]**.

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: the TOE auditable events listed in Table 7]**
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: type of user job, IP address for communications, communication directions]**

Table 7 shows the actions that are recommended by the CC to be auditable for each functional requirement, and the corresponding auditable events of the TOE.

Table 7 : List of Auditable Events

Functional requirement	Action as auditable event	Auditable event
FDP_ACF.1(a)	a) Minimal: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by the SFP. c) Detailed: The specific security attributes used in making an access check.	Original: - Start and end operation of storing user documents. - Start and end operation of printing user documents. - Start and end operation of downloading user documents. - Start and end operation of deleting user documents.

FDP_ACF.1(b)	a) Minimal: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by the SFP. c) Detailed: The specific security attributes used in making an access check.	Original: No record
FIA_UAU.1	a) Minimal: Unsuccessful use of the authentication mechanism; b) Basic: All use of the authentication mechanism; c) Detailed: All TSF mediated actions performed before authentication of the user.	b)Basic: Success / Failure of login operation
FIA_UID.1	a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided; b) Basic: All use of the user identification mechanism, including the user identity provided.	b)Basic: Success / Failure of login operation
FMT_SMF.1	a) Minimal: Use of the management functions.	a)Minimal: Record the management items shown in Table 22
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.	No record due to no modification
FPT_STM.1	a) Minimal: Changes to the time; b) Detailed: providing a timestamp.	a)Minimal: Settings of Year-Month-Day and Hour-Minute
FTA_SSL.3	a) Minimal: Termination of an interactive session by the session locking mechanism.	a)Minimal: Termination of session by auto logout
FTP_ITC.1	a) Minimal: Failure of the trusted channel functions. b) Minimal: Identification of the initiator and target of failed trusted channel functions. c) Basic: All attempted uses of the trusted channel functions. d) Basic: Identification of the initiator and target of all trusted channel functions.	a)Minimal: Failure of SSL encrypted communications; b)Minimal: Communication directions (IN/OUT) and the target device IP address

FAU_GEN.2 User identity association

Hierarchical to: No other components.

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

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

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

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

FAU_STG.4 Prevention of audit data loss

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

Dependencies: FAU_STG.1 Protected audit trail storage

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

FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide **[assignment: MFP administrators]** with the capability to read **[assignment: All of log items]** from the audit records.

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

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

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

6.1.2 Class FDP: User data protection

FDP_ACC.1 (a) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 (a) The TSF shall enforce the **[assignment: common access control SFP]** on **[assignment: list of subjects, objects, and operations among subjects and objects in Table 8]**.

Table 8 : List of Subjects, Objects, and Operations among Subjects and Objects (a)

Subject	Object	Operation among subject and object
MFP administrator process	User document	Delete

Supervisor process	User document	None
Normal user process	User document	Delete, Print, and Download
MFP administrator process	User job	Delete
Normal user process	Applicable user job	Delete

FDP_ACC.1 (b) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control.

FDP_ACC.1.1 (b) The TSF shall enforce **[assignment: TOE functions access control SFP]** on **[assignment: list of subjects, objects, and operations among subjects and objects in Table 9]**.

Table 9 : List of Subjects, Objects, and Operations among Subjects and Objects (b)

Subject	Object	Operation among subject and object
Normal user process	Copy function	Execute
Normal user process	Printer function	Execute
Normal user process	Scanner function	Execute
Normal user process	Document server function	Execute

FDP_ACF.1 (a) Security attribute based access control

Hierarchical to: No other components.

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

FDP_ACF.1.1 (a) The TSF shall enforce the **[assignment: common access control SFP]** to objects based on the following: **[assignment: list of subjects and objects, and for each, the relevant security attributes shown in Table 10]**.

Table 10 : Subjects and Objects, and Security Attributes (a)

Category	Subject or Object	Security attribute
Subject	Normal user process	Login user name of normal user
Subject	Supervisor process	Login user name of supervisor
Subject	MFP administrator process	Login user name of MFP administrator
Object	User document	List of file users
Object	User job	Login user name which is created by the new user job

FDP_ACF.1.2 (a) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[assignment: rules governing access on operations, and operations on objects of subjects in Table 11]**.

Table 11 : Rules Governing Access (a)

Subject	Operation on Object	Rule governing access
Normal user process	Delete and print printer user document	If the login user name is identical to the login user name of normal user in the list of available document users which are associated with printer user documents, it is allowed to delete and print the printer user documents for the normal user process.
	Delete and download scanner user document	If the login user name is identical to the login user name of normal user in the list of available document users which are associated with scanner user documents, it is allowed to delete and download the scanner user documents for the normal user process.
Normal user process	Delete user job	If the login user name is identical to the login user name of job creator in the list of available document users which are associated with user jobs, it is allowed to delete the user job for the normal user process.

FDP_ACF.1.3 (a) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules that explicitly authorise operations on objects of subjects in Table 12**].

Table 12 : Rules Explicitly Authorising Access (a)

Subject	Operation on Object	Rule governing access
MFP administrator process	Delete user document	Allow the operation to delete all user documents stored for MFP administrator process.
MFP administrator process	Delete user job	Allow the operation to delete all user jobs for MFP administrator process.

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

FDP_ACF.1 (b) Security attribute based access control

Hierarchical to: No other components.

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

FDP_ACF.1.1 (b) The TSF shall enforce **[assignment: TOE functions access control SFP]** to objects based on the following: **[assignment: list of subjects or objects, and for each, the security attributes in Table 13]**.

Table 13 : Subjects and Objects, and Security Attributes (b)

Category	Subject or Object	Security attribute
Subject	Normal user process	Login user name of normal user, list of available functions
Object	Copy function	None
Object	Printer function	None
Object	Scanner function	None
Object	Document server function	None

FDP_ACF.1.2 (b) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[assignment: rules governing access on operations, and operations on objects of subjects in Table 14]**.

Table 14 : Rules Governing Access (b)

Subject	Operation on Object	Rule governing access
Normal user process	Performs copy function	If copy function exists in the list of available functions associated with login user name, the copy function is allowed to perform for normal user process.
Normal user process	Performs printer function	If printer function exists in the list of available functions associated with login user name, the printer function is allowed to perform for normal user process.
Normal user process	Performs scanner function	If scanner function exists in the list of available functions associated with login user name, the scanner function is allowed to perform for normal user process.
Normal user process	Performs document server function	If document server function exists in the list of available functions associated with login user name, the document server function is allowed to perform for normal user process.

FDP_ACF.1.3 (b) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: no rules, based on security attributes, that explicitly authorise access of subjects to objects]**.

FDP_ACF.1.4 (b) 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_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.1.3 Class FIA: Identification and authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when **[selection: an administrator configurable positive integer within [assignment: 1 to 5]]** unsuccessful authentication attempts occur related to **[assignment: authentication events in Table 15].**

Table 15 : List of Authentication Events and Unsuccessful Authentication Attempts

Authentication event
User authentication to use Operation Panel
User authentication to use the TOE from Web browser in client PCs
User authentication when printing from client PCs

FIA_AFL.1.2 When the defined number the unsuccessful authentication attempts has been **[selection: met]**, the TSF shall **[assignment: actions in Table 16].**

Table 16 : Action List of Authentication Failures

Unsuccessful authenticated user	Action of authentication failure
Normal user	Lockout time (60 minutes) set by MFP administrator or lockout until MFP administrator releases.
Supervisor	Lockout time (60 minutes) set by MFP administrator or lockout until MFP administrator releases or turns on / off the power.
MFP administrator	Lockout time (60 minutes) set by MFP administrator or lockout until supervisor releases or turns on / off the power.

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: login user names of normal user, supervisor, and MFP administrator]**.

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

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

(1) Available characters and types:

Alphabetical upper case characters: [A-Z] (26 letters)

Alphabetical lower case characters: [a-z] (26 letters)

Numbers: [0-9] (10 letters)

Symbols: SP (space)! ” # $ % & ‘ ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~ (33 letters)

(2) Registerable number of characters:

For Normal User

Minimal number of characters for password set by MFP administrator is more than (8 to 32 digits), less than 128 digits

For MFP Administrator and Supervisor

Minimal number of characters for password set by MFP administrator is more than (8 to 32 digits), less than 32 digits

(3) Rules: Login password must be created by the combination of character types based on password complexity set by MFP administrator. MFP administrator set Level 1 and 2 to password complexity.

FIA_UAU.1	**Timing of authentication**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.1.1	The TSF shall allow **[assignment: reference list of user jobs]** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
FIA_UAU.7	**Protected authentication feedback**
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_UAU.7.1	The TSF shall provide only **[assignment: display dummy letters as authentication feedback on Operation Panel]** to the user while the authentication is in progress.
FIA_UID.1	**Timing of identification**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	The TSF shall allow **[assignment: reference list of user jobs]** on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
FIA_USB.1	**User-subject binding**
Hierarchical to:	No other components.
Dependencies:	FIA_ATD.1 User attribute definition
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **[assignment: login user names of normal user, supervisor, and MFP administrator]**.
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 17]**

Table 17 : Rules for the Initial Association of Attributes

User	Subject	User security attribute
Normal user	Normal user process	Login user name of normal user
Supervisor	Supervisor process	Login user name of supervisor
MFP administrator	MFP administrator process	Login user name of MFP administrator

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **[assignment: up to 4 MFP administrators can be newly created and deleted. However, MFP administrators cannot be deleted if the result would be no MFP administrators with that role]**.

6.1.4 Class FMT: Security management

FMT_MSA.1 (a)Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1 (a) The TSF shall enforce the **[assignment: common access control SFP]** to restrict the ability to **[selection: query, modify, delete, [assignment: newly create]]** the security attributes **[assignment: security attributes in Table 18]** to **[assignment: user roles in Table 18]**.

Table 18 : User Roles of Security Attributes (a)

Security attribute	Operation	User role
Login User Name of Normal User	Query, Modify, Newly create, Delete	MFP administrator
	Query	Applicable normal user
Login User Name of Supervisor	Query, Modify	Supervisor
Login User Name of MFP Administrator	Newly create	MFP administrator
	Query, Modify	Applicable MFP administrator
	Query	Supervisor
List of File User	Query, Modify	MFP administrator, Applicable normal user who stored user documents

FMT_MSA.1 (b) Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1 (b) The TSF shall enforce the **[assignment: TOE functions access control SFP]** to restrict the ability to **[selection: query, modify, delete, [assignment: newly create]]** the security attributes **[assignment: security attributes in Table 19 : User Roles of** Security Attributes**]** to **[assignment: user roles in Table 19 : User Roles of** Security Attributes**]**.

Table 19 : User Roles of Security Attributes (b)

Security attribute	Operation	User role
Login User Name of Normal User	Query, Modify, Newly create, Delete	MFP administrator
	Query	Applicable normal user
Available Function List for Normal User	Query, Modify	MFP administrator
	Query	Applicable normal user

FMT_MSA.3 (a)Static attribute initialisation

Hierarchical to: No other components.

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

FMT_MSA.3.1 (a) The TSF shall enforce the **[assignment: common access control SFP]** to provide **[selection: [assignment: restrictive in Table 20]]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (a) 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 20 : Characteristics of Static Attributes Initialisation (a)

Object	Security attribute associated with object	Default values and the characteristics for object generation
User Document	List of file users	Default value is normal user who stores user documents, and has restrictive characteristics.
User Job	Login user name of normal user	Default value is normal user who creates a new user job and has restrictive characteristics.

FMT_MSA.3 (b) Static attribute initialisation

Hierarchical to: No other components.

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

FMT_MSA.3.1 (b) The TSF shall enforce the **[assignment: TOE functions access control SFP]** to provide **[selection: permissive]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (b) The TSF shall allow the **[assignment: MFP administrator]** to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF Data

Hierarchical to: No other components.

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

FMT_MTD.1.1 The TSF shall restrict the ability to **[selection: query, modify, delete, clear, [assignment: newly create]]** the **[assignment: list of TSF data in Table 21]** to **[assignment: user roles in Table 21]**.

Table 21 : List of TSF Data

TSF data	Operation	User role
Login Password of Normal User	Newly create, Modify	MFP administrator
	Modify	Applicable normal user
Login Password of Supervisor	Modify	Supervisor
Login Password of MFP Administrator	Modify	Supervisor
	Newly create	MFP administrator
	Modify	Applicable MFP administrator
Allowance Times of Entering Login Password	Query	MFP administrator
Timer Settings for Lockout Release	Query	MFP administrator
Lockout Time	Query	MFP administrator
Settings of Year-Month-Day-Hour-Minute	Query, Modify	MFP administrator
	Query	Supervisor, Normal user
Minimal Number of Characters for Password	Query	MFP administrator
Password Complexity	Query	MFP administrator
Audit Log	Query, Delete	MFP administrator
Service Mode Lock Function	Query	MFP administrator, Supervisor, Normal user

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **[assignment: list of specification of management functions in Table 22].**

Table 22 : List of Specification of Management Functions

Functional requirement	Management requirement	Management item
FAU_SAR.1	a) maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.	a) None: User group is fixed.
FAU_STG.4	a) maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.	a) None: Action is fixed.
FDP_ACF.1(a)	a) managing the attributes used to make explicit access or denial based decisions.	a) Management of MFP administrators
FDP_ACF.1(b)	a) managing the attributes used to make explicit access or denial based decisions.	None
FIA_AFL.1	a) management of the threshold for unsuccessful authentication attempts; b) management of actions to be taken in the event of an authentication failure.	a) None: After initial start-up, do not change the allowance time of entering login password by MFP administrator b) Persons who are intended for lockout (Normal user), persons who release lockout (MFP administrator), and user roles of persons who release lockout. - Persons who are intended for lockout (Normal user), persons who release lockout (MFP administrator) - Persons who are intended for lockout (MFP administrator), persons who release lockout (Supervisor) - Persons who are intended for lockout (Supervisor), persons who release lockout (MFP administrator)
FIA_ATD.1	a) if so indicated in the assignment, the authorised administrator might be able to define additional security attributes for users.	None
FIA_SOS.1	a) the management of the metric used to verify the secrets.	None: After initial start-up, do not change minimum number of characters for password and password complexity by MFP administrator
FIA_UAU.1	a) management of the authentication data by an administrator; b) management of the authentication data by the associated user; c) managing the list of actions that can be taken before the user is authenticated.	-Security management function (Normal user): Manage login password of normal user by MFP administrator, and manage login password of normal user by normal user -Security management function (MFP administrator): Manage password of MFP administrator by MFP administrator -Security management function (Administrator information management): New creation of administrator by administrator

		-Security management function (Administrator information management): Manage administrator authentication information by supervisor -Security management function (Supervisor):Manage login password of supervisor by supervisor
FIA_UID.1	a) the management of the user identities; b) if an authorised administrator can change the actions allowed before identification, the managing of the action lists.	-Manage login user name of normal user by MFP administrator -Security management function (Normal user): Manage login name of normal user by MFP administrator -Security management function (MFP administrator): Manage login name of MFP administrator by MFP administrator -Security management function (MFP administrator): New creation of MFP administrator by MFP administrator -Security management function (Supervisor): Manage login names of supervisor 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 b) None
FMT_MSA.1(a)	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) None b) None
FMT_MSA.1(b)	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) None b) None
FMT_MSA.3(a)	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 group of roles which can be specified by initial settings. b) Limit MFP administrators and the applicable normal users to authorise the default access rights. c) None
FMT_MSA.3(b)	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 group of roles which can be specified by initial settings b) None c) None

FMT_MTD.1	a) managing the group of roles that can interact with the TSF data.	a) None: After setting "Prohibit" for initialisation, do not change Service Mode Lock Function by MFP administrator
FMT_SMR.1	a) managing the group of users that are part of a role.	a) None
FPT_STM.1	a) management of the time.	a) Year-Month-Day settings and Hour-Minute settings
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 b) None
FTP_ITC.1	a) Configuring the actions that require trusted channel, if supported.	a) None
FTA_SSL.3	a) specification of the time of user inactivity after which termination of the interactive session occurs for an individual user; b) specification of the default time of user inactivity after which termination of the interactive session occurs.	a) None b) After initial start-up, do not change the auto logout time of panel operation
FPT_FDI_EXP.1	a) definition of the role(s) that are allowed to perform the management activities; b) management of the conditions under which direct forwarding can be allowed by an administrative role; c) revocation of such an allowance.	a) None b) None c) None

FMT_SMR.1 Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles **[assignment: normal user, supervisor, MFP administrator]**.
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.1.5 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: the TSF]**.

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

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

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to: No other components.

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

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

6.1.6 Class FTA: TOE access

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a **[assignment: the completion of receiving the print information from printer driver, in case of Operation Panel, the auto logout time (180 seconds) when an authorised administrator manages the devices, in case of Web browser, the fixed auto logout time (30 minutes) from the operation of the last time normal user and administrator enter from Operation panel, Web browser, or Printer driver]**.

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

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

6.2 Security Assurance Requirements

The Evaluation Assurance Level of this TOE is EAL3+ALC_FLR.2. Table 23 lists the TOE assurance components. This means that a set of components which is defined by EAL3 of the Evaluation Assurance Level is augmented with ALC_FLR.2.

Table 23 : TOE Security Assurance Requirements (EAL3+ALC_FLR.2)

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

6.3 Security Requirements Rationale

This chapter describes the security requirements rationale.

As shown below, if satisfying all security functional requirements, the TOE security objectives defined in “4 Security Objectives” are accomplished.

6.3.1 Tracing

The following Table 24 shows the corresponding relation of the security functional requirements (SFRs) for the TOE security objectives. As clearly in Table 24, the SFRs respond to at least more than 1 security objectives.

Table 24 : Relations between Security Objectives and Functional Requirements

	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED
FAU_GEN.1										✓
FAU_GEN.2										✓
FAU_STG.1										✓
FAU_STG.4										✓
FAU_SAR.1										✓
FAU_SAR.2										✓
FDP_ACC.1(a)	✓	✓	✓							
FDP_ACC.1(b)							✓			
FDP_ACF.1(a)	✓	✓	✓							
FDP_ACF.1(b)							✓			
FDP_RIP.1	✓									
FIA_AFL.1							✓			
FIA_ATD.1							✓			
FIA_SOS.1							✓			
FIA_UAU.1							✓	✓		
FIA_UAU.7							✓			
FIA_UID.1							✓	✓		
FIA_USB.1							✓			
FPT_FDI_EXP.1								✓		
FMT_MSA.1(a)	✓	✓	✓							
FMT_MSA.1(b)							✓			
FMT_MSA.3(a)	✓	✓	✓							
FMT_MSA.3(b)							✓			
FMT_MTD.1				✓	✓	✓				
FMT_SMF.1				✓	✓	✓				
FMT_SMR.1				✓	✓	✓				

FPT_STM.1										✓
FPT_TST.1									✓	
FTA_SSL.3							✓	✓		
FTP_ITC.1	✓	✓	✓	✓	✓	✓				

6.3.2 Justification of Tracing

As below, it is described that security objectives for the TOE is enforced by the corresponding security functional requirements of the TOE.

O.DOC.NO_DIS Protection of document from unauthorised disclosure

O.DOC.NO_DIS is the security objectives to prevent user documents, deleted documents, temporary documents and fragments from disclosure by persons who have no login user name or by unauthorised persons who have login user names but don't have any access to their documents. In order to fulfill these security objectives, it is necessary to satisfy the following actions:

(1) Specify and implement access control to user documents
FDP_ACC.1 (a) and FDP_ACF.1 (a) determine the accessible user documents for each normal user and the operations to permit for the user documents. According to the result, normal user is allowed to access to user documents.

(2) Prevent reading deleted documents, temporary documents and fragments.
FDP_RIP.1 prevents reading deleted documents, temporary documents and fragments.

(3) Use trusted channels for sending or receiving user documents.
FTP_ITC.1 protects the sending user documents from LAN interfaces, and the receiving user documents on LAN interfaces.

(4) Management of security attributes
According to FMT_MSA.3 (a), the permitted user for default to user documents is limited to normal user who stores the user documents.
According to FMT_MSA.1 (a), the list of available document users is managed by MFP administrator.

The necessary actions to fulfill O.DOC.NO_DIS are (1), (2), (3) and (4). Therefore, O.DOC.NO_DIS is fulfilled by accomplishing FDP_ACC.1 (a), FDP_ACF.1 (a), FDP_RIP.1, FTP_ITC.1, FMT_MSA.1 (a), and FMT_MSA.3 (a) considered as the necessary security functional requirements for these actions.

O.DOC.NO_ALT Protection of user document from unauthorised alteration

O.DOC.NO_ALT is the security objectives to prevent user documents, deleted documents, temporary documents and fragments from alteration by persons who have no login user name or by unauthorised persons who have login user names but don't have any access to their documents. In order to fulfill these security objectives, it is necessary to satisfy the following actions:

(1) Specify and implement access control to user documents
FDP_ACC.1 (a) and FDP_ACF.1 (a) determine the accessible user documents for each normal user and the operations to permit for the user documents. According to the result, normal user is allowed to access to user documents.

(2) Use trusted channels for sending or receiving user documents
FTP_ITC.1 protects the sending user documents from LAN interfaces, and the receiving user documents on LAN interfaces.

(3) Management of security attributes
According to FMT_MSA.3 (a), the permitted user for default to user documents is limited to normal user who stores the user documents.

According to FMT_MSA.1 (a), the list of available document users is managed by MFP administrator.

The necessary actions to fulfill O.DOC.NO_ALT are (1), (2) and (3). Therefore, O.DOC.NO_ALT is fulfilled by accomplishing FDP_ACC.1 (a), FDP_ACF.1 (a), FTP_ITC.1, FMT_MSA.1 (a), and FMT_MSA.3 (a) considered as the necessary security functional requirements for these actions.

O.FUNC.NO_ALT Protection of user job from unauthorised alteration

O.FUNC.NO_ALT is the security objectives to prevent user job from alteration by persons who have no login user name or by unauthorised persons who have login user names but don't have any access to their documents. In order to fulfill these security objectives, it is necessary to satisfy the following actions:

(1) Specify and implement access control to user jobs
FDP_ACC.1 (b) and FDP_ACF.1 (b) determine the accessible user job for each normal user and the operations to permit for the user job. According to the result, normal user is allowed to access to user documents.

(2) Use trusted channels for sending or receiving user jobs
FTP_ITC.1 protects the sending user job from LAN interfaces, and the receiving user job on LAN interfaces.

(3) Management of security attributes
According to FMT_MSA.3 (a), the person for default access to user job is limited to normal user who creates a new user job.

According to FMT_MSA.1 (a), the login user name of normal user is managed by MFP administrator.

The necessary actions to fulfill O.FUNC.NO_ALT are (1), (2), and (3). Therefore, O.FUNC.NO_ALT is fulfilled by accomplishing FDP_ACC.1 (a), FDP_ACF.1 (a), FTP_ITC.1, FMT_MSA.1 (a), and FMT_MSA.3 (a) considered as the necessary security functional requirements for these actions.

O.PROT.NO_ALT Protection of TSF protected information from unauthorised alteration

O.PROT.NO_ALT is the security objectives to allow only users who maintain the security to alter the TSF protected information. In order to fulfill these security objectives, it is necessary to satisfy the following actions:

(1) Management of TSF protected information
According to FMT_MTD.1, only MFP administrator is allowed to establish the settings of year-month-day and of the time.

(2) Specification of management function
FMT_SMF.1 performs the necessary management functions for the security functions.

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

(4) Use trusted channels for sending or receiving TSF protected information
FTP_ITC.1 protects the sending TSF protected information from LAN interfaces, and the receiving TSF protected information on LAN interfaces.

The necessary actions to fulfill O.PROT.NO_ALT are (1), (2), (3), and (4). Therefore, O.PROT.NO_ALT is fulfilled by accomplishing FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, and FTP_ITC.1 considered as the necessary security functional requirements for these actions.

O.CONF.NO_DIS Protection of TSF confidential information from unauthorised disclosure

O.CONF.NO_DIS is the security objectives to allow only users who maintain the security to disclose the TSF confidential information. In order to fulfill these security objectives, it is necessary to satisfy the following actions:

(1) Management of TSF confidential information
FMT_MTD.1 allows MFP administrators and the applicable normal users to access to login password of normal user. Supervisor is allowed to access to the login password of supervisor. Supervisor and the applicable MFP administrators are allowed to access to the login password of administrator. Only MFP administrator is allowed to access to audit log.

(2) Specification of management function
FMT_SMF.1 performs the necessary management functions for the security functions.

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

(4) Use trusted channels for sending or receiving TSF confidential information.
FTP_ITC.1 protects the sending TSF confidential information from LAN interfaces, and the receiving TSF confidential information on LAN interfaces.

The necessary actions to fulfill O.CONF.NO_DIS are (1), (2), (3), and (4). Therefore, O.CONF.NO_DIS is fulfilled by accomplishing FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, and FTP_ITC.1 considered as the necessary security functional requirements for these actions.

O.CONF.NO_ALT Protection of TSF confidential information from unauthorised alteration

O.CONF.NO_ALT is the security objectives to allow only users who maintain the security to alter the TSF confidential information. In order to fulfill these security objectives, it is necessary to satisfy the following actions:

(1) Management of TSF confidential information
FMT_MTD.1 allows MFP administrators and the applicable normal users to access to login password of normal user. Supervisor is allowed to access to the login password of supervisor. Supervisor and the applicable MFP administrators are allowed to access to the login password of administrators. Only MFP administrator is allowed to access to audit log.

(2) Specification of management functions
FMT_SMF.1 performs the necessary management functions for the security functions.

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

(4) Use trusted channels for sending or receiving TSF confidential information.
FTP_ITC.1 protects the sending TSF confidential information from LAN interfaces, and the receiving TSF confidential information on LAN interfaces.

The necessary actions to fulfill O.CONF.NO_ALT are (1), (2), (3), and (4). Therefore, O.CONF.NO_ALT is fulfilled by accomplishing FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, and FTP_ITC.1 considered as the necessary security functional requirements for these actions.

O.USER.AUTHORIZED User identification and authentication

O.USER.AUTHORIZED is the security objectives to authorise only normal users to use the TOE functions. In order to fulfill these security objectives, it is necessary to satisfy the following actions:

(1) Identify and authenticate users before using the TOE
FIA_UID.1 identifies users before using the TOE.
FIA_UAU.1 authenticates users who are registered before using the TOE.

(2) Allow users who succeed in identification and authentication to use the TOE
FIA_ATD.1 and FIA_USB.1 manage the access procedures to the protected assets of the users who are defined in advance, and associate the users who succeed in identification and authentication.
FDP_ACC.1 (b) and FDP_ACF.1 (b) determines the function available for users who succeed in identification and authentication and the operation to permit for the function.

(3) Make it difficult to analyse login password
According to FIA_UAU.7, displaying dummy letters as authentication feedback for Operation panel prevents login password from disclosure.
According to FIA_SOS.1, allowing only password registration which meets minimum number of characters for password and the combination of character types by MFP administrators make it difficult to guess the login password. FIA_AFL.1 doesn't allow continuous attempts to access the TOE for the users who authenticate unsuccessfully and repeatedly for certain times.

(4) Terminate login automatically
FTA_SSL.3 auto-logouts in case of no operation at constant intervals.

(5) Management of security attributes
According to FMT_MSA.1 (b), the login user name of normal user and the available function list of normal user are both managed by MFP administrator.

According to FMT_MSA.3 (b), a function which normal user performs is only limited to the function MFP administrator permits in the available function list of normal user.

The necessary actions to fulfill O.USER.AUTHORIZED are (1), (2), (3), (4) and (5). Therefore, O.USER.AUTHORIZED is fulfilled by accomplishing FIA_UID.1, FIA_UAU.1, FIA_ATD.1, FIA_USB.1, FIA_UAU.7, FIA_AFL.1, FIA_SOS.1, FTA_SSL.3, FMT_MSA.1 (a), and FMT_MSA.3 (b) considered as the necessary security functional requirements for these actions.

However, 2600.1-SMI function (F.SMI) which is the selected SFR Package from PP is a function used by FDP_ACC.1 (b) and FDP_ACF.1 (b) in the functions to perform access control. Therefore, access control of F.SMI is fulfilled, including access control by FDP_ACC.1 (b) and FDP_ACF.1 (b).

O.INTERFACE.MANAGED Interface management

O.INTERFACE.MANAGED is the security objectives to protect the communication path when the TOE sends or receives the protected assets. In order to fulfill these security objectives, it is necessary to satisfy the following actions:

(1) Operation panel and LAN interfaces identify and authenticate users before using.
According to FIA_UID.1, Operation panel and LAN interfaces identify users before using.
According to FIA_UAU.1, Operation panel or LAN interfaces authenticate users who are registered before using.

(2) Terminate connection to Operation panel or LAN interfaces automatically
FTA_SSL.3 terminates sessions in case of not operating Operation panel or LAN interfaces for some intervals of time.

(3) Restricted forwarding of data to external interfaces
FPT_FDI_EXP.1 prevents the received data on Operation panel and LAN interfaces from transmission via LAN without processing by TSF.

The necessary actions to fulfill O.INTERFACE.MANAGED are (1), (2), and (3). Therefore, O.INTERFACE.MANAGED is fulfilled by accomplishing FIA_UID.1, FIA_UAU.1, FTA_SSL.3, and FPT_FDI_EXP.1 considered as the necessary security functional requirements for these actions.

O.SOFTWARE.VERIFIED Software verification

O.SOFTWARE.VERIFIED is the security objectives to ensure that the software installed in FlashROM is the official MFP control software. In order to fulfill these security objectives, it is necessary to satisfy the following action:

(1) Self check
FPT_TST.1 confirms that the software installed in FlashROM is the official MFP control software for start-up.

The necessary action to fulfill O.SOFTWARE.VERIFIED is (1). Therefore, O.SOFTWARE.VERIFIED is fulfilled by accomplishing FTP_TST.1 considered as the necessary security functional requirement for this action.

O.AUDIT.LOGGED Audit log management

O.AUDIT.LOGGED is the security objectives to allow MFP administrators to generate the necessary audit log for verifying security intrusions and further reviewing the audit logs. In order to fulfill these security objectives, it is necessary to satisfy the following actions:

(1) Generate audit logs
FAU_GEN.1 and FAU_GEN.2 generate auditable events with the identification information which describes the causes when the events occur.

(2) Protect audit log
FAU_STG.1 protects audit logs from alteration. If auditable events occur in the status of audit log files being full by FAU_STG.4, delete the oldest audit log of time stamps and generate a new audit log.

(3) Provide audit function
FAU_SAR.1 makes it possible for MFP administrator to read audit log in a verifiable method. FAU_SAR.2 forbids persons except for MFP administrator to read the audit log.

(4) Occurrence time of reliable events
Reliable time stamps are provided by FPT_STM.1. Record in the audit log the precise time when the auditable events occur.

The necessary actions to fulfill O.AUDIT.LOGGED are (1), (2), (3), and (4). Therefore, O.AUDIT.LOGGED is fulfilled by accomplishing FAU_GEN.1, FAU_GEN.2, FAU_STG.1, FAU_STG.4, FAU_SAR.1, and FAU_SAR.2 considered as the necessary security functional requirements for these actions.

6.3.3 Dependency analysis

For the TOE security functional requirements, Table 25 shows the results of dependency analysis in this ST.

Table 25 : The Dependency Analysis Results of TOE Security Functional Requirements

TOE Security Functional Requirement	Required Dependency	Dependency satisfied in ST	Dependency not satisfied in ST
FAU_GEN.1	FPT_STM.1	FPT_STM.1	N/A
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1	N/A
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	N/A
FAU_STG.4	FAU_STG.1	FAU_STG.1	N/A
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	N/A
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	N/A
FDP_ACC.1(a)	FDP_ACF.1(a)	FDP_ACF.1(a)	N/A
FDP_ACC.1(b)	FDP_ACF.1(b)	FDP_ACF.1(b)	N/A
FDP_ACF.1(a)	FDP_ACC.1(a) FMT_MSA.3(a)	FDP_ACC.1(a) FMT_MSA.3(a)	N/A
FDP_ACF.1(b)	FDP_ACC.1(b) FMT_MSA.3(b)	FDP_ACC.1(b) FMT_MSA.3(b)	N/A
FDP_RIP.1	N/A	N/A	N/A
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	N/A
FIA_ATD.1	N/A	N/A	N/A
FIA_SOS.1	N/A	N/A	N/A
FIA_UAU.1	FIA_UID.1	FIA_UID.1	N/A
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	N/A
FIA_UID.1	N/A	N/A	N/A
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	N/A
FPT_FDI_EXP.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1	N/A
FMT_MSA.1(a)	[FDP_ACC.1(a) or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1(a) FMT_SMR.1 FMT_SMF.1	N/A
FMT_MSA.1(b)	[FDP_ACC.1(b) or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1(b) FMT_SMR.1 FMT_SMF.1	N/A
FMT_MSA.3(a)	FMT_MSA.1(a)	FMT_MSA.1(a)	N/A

	FMT_SMR.1	FMT_SMR.1	
FMT_MSA.3(b)	FMT_MSA.1(b) FMT_SMR.1	FMT_MSA.1(b) FMT_SMR.1	N/A
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	N/A
FMT_SMF.1	N/A	N/A	N/A
FMT_SMR.1	FIA_UID.1	FIA_UID.1	N/A
FPT_STM.1	N/A	N/A	N/A
FPT_TST.1	N/A	N/A	N/A
FTA_SSL.3	N/A	N/A	N/A
FTP_ITC.1	N/A	N/A	N/A

As shown in the above table, all required dependencies are satisfied.

6.3.4 Security assurance requirements rationale

This TOE is MFP software which is a commercial product. It is not assumed that attackers have the capability of more than intermediate level in this TOE, while the MFP is assumed to be used in general offices.

And the evaluation of TOE design (ADV_TDS.2) is sufficient to show the correctness of commercial products. Additionally, the attack to avoid or alter the TOE requires the high capability. This is not intended for the evaluation of this time, i.e., for general needs, it is sufficient to handle the attack from the attacker who has the basic capability (AVA_VAN.2).

Meanwhile, it is needed to keep the secrets of the relevant information for making the attack more difficult, and to ensure that the development environment is secure. That is, development security (ALC_DVS.1) is important.

In order to continue the TOE and maintain secure, it is important to appropriately correct the flaws found after starting the maintenance in accordance with the flaw reporting procedures (ALC_FLR.2). Therefore, for considering the evaluation period and costs, it is appropriate that the Evaluation Assurance Level of this TOE is EAL3+ALC_FLR.2.

7 TOE Summary Specification

In this chapter, the functional requirements stated in Clause 6.1 are described for each functional requirement on the methods and mechanisms which the TOE satisfies.

FAU_GEN.1 (Audit data generation)

The TOE generates audit log shown in Table 26 and adds the log to the audit log file for the auditable events shown in Table 26. Common audit data shown in Table 26 is information items which generate all auditable events, and the individual audit data shows the information items which records the necessary additional information for auditing when generating the auditable events.

Table 26 : Auditable Events and Audit Data

Auditable event	Audit log	
	Common audit data	Individual audit data
Starting audit function	- Date and time of event - Type of event - Subject identity information - The outcome of the event	-
Ending audit function		-
Storing, printing, downloading, and deleting user document		-
Success and failure of login operation		-
Recording Table 22 Administrative Item		-
Settings of Year-Month-Day-Hour-Minute		-
Session termination by auto logout		-
Failure of SSL cryptographic communications		Communication directions (IN/OUT) and the target device IP address

-: No Individual Audit Data

*The events for starting and ending audit functions substitute the events of the TOE start-up.

FAU_GEN.2 (User identity association)

The TOE adds user identification information (login user name) which causes the occurrence of each auditable event to audit log.

FAU_SAR.1 (Audit review)

The TOE allows MFP administrators who succeed in identification and authentication only to read audit logs in text form. Reading audit logs is provided by Web function in the TOE.

FAU_SAR.2 (Restricted audit review)

The TOE allows MFP administrators who succeed in identification and authentication only to read and delete audit logs. Reading audit logs is provided by Web function in the TOE.

FAU_STG.1 (Protected audit trail storage)

The TOE provides only MFP administrators who succeed in identification and authentication with the function to read and delete audit logs. For users except for MFP administrator, the TOE does not provide the function to access the audit logs.

FAU_STG.4 (Prevention of audit data loss)

The TOE overwrites the latest audit log to the oldest one if there is no generating area to add audit log to audit log file.

FDP_ACC.1 (a) (Subset access control)

The TOE controls deleting user document by MFP administrator process, and controls deleting, printing, and downloading the user document by normal user and it controls that supervisor does not operate the user document. And the TOE controls deleting user job by MFP administrator process and deleting normal user's user job by normal user process.

FDP_ACC.1 (b) (Subset access control)

The TOE controls the performance of copy function, printer function, scanner function, and document server function by normal user process.

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

The TOE specifies the rules among operations allowed to the accessible user role and each user role for user documents and user jobs as shown in Table 10, Table 11, and Table 12. According to the specification, the TOE provides the appropriate operations for each user who access to user documents and user jobs.

The TOE associates as security attributes MFP administrator process with login user name of MFP administrator, supervisor process with login user name of supervisor, and normal user process with login user name of normal user. And the TOE associates as security attributes user documents with the list of available document users, and user jobs with login user name of the user who creates a new user job.

The TOE set as security attributes the list of available document users in the storing user documents (printer user document, scanner user document) when storing the user documents (printer user document, scanner user document) by normal user process.

For access to user documents (printer user document, scanner user document) by normal user process, if checking and matching the login user name of normal user associated with normal user process and the login user name of normal user in the list of available document users associated with user documents, the access control is implemented to allow, for the normal user process, the operations of deleting and printing the printer user documents, or the operations of deleting and downloading the scanner user documents.

The TOE associates login user name of users who create a new user job as security attributes of user job.

For access to user job by normal user process, the TOE implements the access control to allow the operation of deleting user job for the normal user process if checking and matching the login user name of normal user associated with normal user process and the login user name of user job creator associated with user job.

For MFP administrator process, the access control is implemented to allow the operations of deleting all created user jobs and all stored user documents.

For supervisor process, the access control is implemented to deny the operations for all created user jobs and all stored user documents.

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

The TOE specifies the rules among operations allowed to the accessible user role and each user role for copy function, printer function, scanner function, and document server function as shown in Table 13 and Table 14. According to the specification, the TOE provides the appropriate operations for each user who access to copy function, printer function, scanner function, and document server function.

The TOE associates as security attributes normal user process with login user name of normal user and the available function list (list of functions in which normal user authorises the access rights).

The TOE implements the access control to allow the function performance for the normal user process only if the function which normal user process attempts to access is in the list of the available functions associated with the normal user process, and only if the target function exists in the available function list when accessing to copy function, printer function, scanner function, and document server function by the normal user process.

FDP_RIP.1 (Subset residual information protection)

The TOE provides Overwrite function to ensure there is no residual information by overwriting the residual data in user documents, temporarily documents and fragments which are deleted in HDD.

FIA_AFL.1 (Authentication failure handling)

The TOE counts the failure time of user authentication for each login user name of user. In case of successful user authentication, the TOE resets to ‘ZERO’ the failure time of user authentication to the login user name of user who authenticates successfully.

If the failure time of user authentication reaches to the allowance time of entering login password set in advance by MFP administrator, and in case of the consecutive authentication failure, lock out the login user name of the user.

The allowance time of entering login password is a value which MFP administrator set from 1 to 5.

The TOE releases the lockout of users who satisfy one of the following conditions:

(1) Release by the period of lockout time

Users lockout is released after a period of lockout time has elapsed for each locked out user. The lockout time is the time (60 minutes) set by MFP administrator.

(2) Release by Unlocking administrator

The unlocking administrators who are determined for each user role release the lockout. Table 27 shows the unlocking administrators of each user role.

Table 27 : Unlocking Administrators for Each User Role

User role(Lockedout User)	Unlocking administrator
Normal user	MFP administrator
Supervisor	MFP administrator
MFP administrator	Supervisor

(3) Release by turning ON / OFF the TOE power

If administrators (MFP administrator and supervisor) lock out, release the lockout of administrators when restarting up by turning ON / OFF the TOE power.

FIA_ATD.1 (User attribute definition)

The TOE associates as security attributes and maintains login user name of normal user for normal user, login user name of supervisor for supervisor, and login user name of MFP administrator for MFP administrator.

FIA_SOS.1 (Verification of secrets)

The TOE provides a function to register and change login passwords of normal user, MFP administrator, and supervisor. This function uses the characters described below (1). The TOE checks the login password to register and change, and if that meets the following conditions of (2) and (3), the TOE registers the login password. If not meeting those conditions, the TOE does not register the login password but displays the error message.

(1) Available characters and types:

Alphabetic upper case characters:[A-Z] (26 letters)
Alphabetic lower case characters:[a-z] (26 letters)
Numbers: [0-9] (10 letters)
Symbols: SP(space)! ” # $ % & ‘ ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~ (33 letters)

(2) Registerable number of characters:

For Normal User

Minimal number of characters for password set by MFP administrator is more than (8 to 32 digits), less than 128 digits.

For MFP Administrator and Supervisor

Minimal number of characters for password set by MFP administrator is more than (8 to 32 digits), less than 32 digits.

(3) Rules: Login password must be created by the combination of character types based on password complexity set by MFP administrator. MFP administrator set Level 1 and 2 to password complexity.

FIA_UAU.1 (Timing of authentication)

The TOE displays to require entering login user name and login password of user in Operation panel in case of no logged-in user from Operation panel, and it displays to require entering login user name and login password of user to the Web browser in case of any access to Web function of the TOE from client PCs. For both cases, the TOE authenticates login user name and login password of users entered by users.

When receiving requests for storing user documents as printer function from client PCs, the TOE authenticates login user name and login password of user which are sent from client PCs, prior to the function to store as user document. The users and the authentication methods that the Identification and Authentication Function identifies are shown in Table 28.

Table 28 : The Function that TOE Provides and Identifying Users and Authentication Methods

Identifying user	Authentication method
Normal User	Ensures that login user name and login password of normal user entered from Operation panel, Web browser in client PCs and Printer driver are identical to the login user name and password of normal user registered in the TOE.
Administrator	Ensures that login user name and login password of normal user entered from Operation panel, Web browser in client PCs are identical to the login user name and password of normal user registered in the TOE.

FIA_UAU.7 (Protected authentication feedback)

The TOE displays dummy characters in the authenticating feedback area for login password which users enter from Operation panel.

FIA_UID.1 (Timing of identification)

The TOE displays to require entering login user name and login password of users in Operation panel in case of no logged-in user from Operation panel, and it displays to require entering login user name and login password of users to the Web browser in case of any access to Web function of the TOE from client PCs which has no login users. For both cases, the TOE identifies login user names of users entered by users.

When receiving requests for storing user documents as printer function from client PCs, the TOE identifies login user name of user which are sent from client PCs, prior to the function to store as user document.

FIA_USB.1 (User-subject binding)

For users who succeed in identification and authentication, the TOE combines normal user process for normal user, supervisor process for supervisor, and MFP administrator process for MFP administrator. Moreover, the TOE associates as security attributes login user names of normal user for normal user process, supervisor for supervisor process, and MFP administrator for MFP administrator process, and reflects the applicable operation authority for each user role.

Additionally, the TOE permits creating up to 4 (maximum) new MFP administrators and deleting MFP administrators. The TOE does not permit deleting MFP administrators the result would be no MFP administrators with that role.

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

The TOE provides a function to allow user roles to operate for security attributes as described in Table 18.

The TOE provides MFP administrator with the function to allow the following operations for login user names of normal user and MFP administrator, and the list of available document users:

- Query, Modify, New Create, and Delete login user name of normal user
- Newly create login user name of MFP administrator
- Query and Modify login user name of MFP administrators themselves
- Query and Modify the list of available document users

The TOE provides supervisor with the function to permit the following operations for login user names of supervisor and MFP administrator:

- Query and Modify login user name of supervisor
- Query login user name of MFP administrator

The TOE provides normal user with the function to permit the following operations for login user name of normal user and the list of available document users:

- Query login user name of normal users themselves
- Query and Modify the list of available document users for user documents which normal users themselves stored.

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

The TOE provides a function to allow user roles to operate for security attributes as described in Table 19. The TOE provides MFP administrator with the function to allow the following operations for login user name of normal user and the list of available functions for normal user:

- Query, Modify, Newly create, and Delete login user name of normal user
- Query and Modify the list of available functions for normal user

The TOE provides normal user with the function to allow the following operations for login user name of normal user and the list of available functions for normal user:

- Query login user name of normal user themselves
- Query the list of available functions for normal user themselves

FMT_MSA.3 (a) (Static attribute initialisation)

The TOE associates the list of available document users as security attributes for the stored user documents when normal user stores user documents. The list of available document users is the authorised user to access to the stored user documents, and for the default values in the list of available document users, set a login user name of normal user who stores user documents.

The TOE associates a new user job as security attributes with login user name of normal user when normal user creates the new user job.

FMT_MSA.3 (b) (Static attribute initialisation)

The TOE associates the list of available functions as security attributes with normal user process when normal user perform copy function, printer function, scanner function, and document server function.

The list of available functions is a list of the authorised functions (copy function, printer function, scanner function, and document server function) to be performed for normal user, set those authorised functions. The default values in the list of available functions are allowed to perform all functions (copy function, printer function, scanner function, and document server function). When registering normal user, MFP administrator set the authorised functions to be performed for normal user.

FMT_MTD.1 (Management of TSF data)

The TOE provides a function to allow user roles to operate for TSF information (TSF data) as described and listed in Table 21.

The TOE provides supervisor with the function to allow the following operations:

- Modify login password of supervisor
- Modify login password of MFP administrator
- Query the settings of Year-Month-Day-Hour-Minute
- Query the setting of Service Mode Lock Function

The TOE provides MFP administrator with the function to allow the following operations:

- Newly create and Modify login password of normal user
- Newly create login password of MFP administrator
- Modify login password of MFP administrator themselves
- Query the allowance time of entering login password
- Query the timer setting of lockout release
- Query the time of lockout
- Query and Modify the settings of Year-Month-Day-Hour-Minute
- Query and Delete audit log
- Query the setting of Service Mode Lock Function

The TOE provides normal user with the function to allow the following operations:

- Modify login password of normal user themselves
- Query the settings of Year-Month-Day-Hour-Minute
- Query the setting of Service Mode Lock Function

FMT_SMF.1 (Specification of Management Functions)

The TOE provides security management functions shown in Table 22.

- Management of MFP administrators
- Management of login password of normal user
- Management of login password of MFP administrator
- Management of login password of supervisor
- Management of login user name of normal user
- Management of login user name of MFP administrator
- Management of login user name of supervisor
- Management of the available document user list for user documents
- Management of the settings of Year-Month-Day-Hour-Minute

FMT_SMR.1 (Security roles)

The TOE combines and maintains the process of user roles associated with users for users who succeed in identification and authentication. For registering users, the TOE assigns the user roles of normal user, supervisor, and MFP administrator.

Additionally, the TOE maintains the security roles by limiting the operation to login user name and login password of user to the specified user.

The following operations are limited to MFP administrators:

- Newly create and Delete login user name of normal user
- Newly create login user name of MFP administrator
- Newly create login password of normal user
- Newly create login password of MFP administrator

The following operation is limited to MFP administrators themselves:

- Modify login user name of MFP administrator

The following operations are limited to normal users themselves and MFP administrators:

- Query login user name of normal user
- Modify login password of normal user

The following operations are limited to MFP administrators themselves and supervisor:

- Query login user name of MFP administrator
- Modify login password of MFP administrator

The following operations are limited to supervisor:

- Query and Modify login user name of supervisor
- Modify login password of supervisor

FPT_STM.1 (Reliable time stamps)

The TOE acquires the date (Year-Month-Day) / time (Hour-Minute-Second) to generate in audit log from the system clock of the TOE.

FPT_TST.1 (TSF testing)

The TOE shall run a suite of self tests during initial start-up after turning on the power, and shall verify the integrity of executable codes in MFP control software and of audit log data file. In case of unusual operations by verifying the integrity of executable codes in the MFP control software, the TOE displays an error message on Operation panel and stops the performance with the TOE unavailable for normal user. In case of unusual operations by verifying the integrity of audit log data file, the TOE displays an error message on Operation panel and stops the performance with the TOE unavailable for normal user. If both of the above verification finds no unusual operations, normal users will be able to use the TOE.

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

The TSF surely identifies and authenticates the input information from Operation panel or LAN interfaces, and then the TOE performs the process to store user document into document server or changes each device setting or as user document. Therefore, the TOE does not provide the function to forward the input information via LAN interfaces without these processes.

FTA_SSL.3 (TSF-initiated termination)

The TOE provides a function to force users to auto logout after a period of the auto logout time (180 seconds) which an authorised machine administrator set in advance from the last time of Operation panel after login from Operation panel.

The TOE provides a function to force users to auto logout after a period of the fixed auto logout time (30 minutes) from the last time of Web browser after login from Web browser.

This TOE includes an interface from Printer driver and provides a function to force users to auto logout, immediately after receiving the print information from the printer driver.

FTP_ITC.1 (Inter-TSF trusted channel)

The TOE provides SSL cryptographic communications as trusted channels communication for protecting communications between the TOE and client PCs in the operation via Web browser of client PCs start-up which is the trusted IT product, and in the printing operation of client PC start-up which is the trusted IT product. No trusted channels communications of TSF initiation exist.