
Pro C5200/C5210 (RICOH/Savin/Lanier)

Security Target

Author : RICOH COMPANY, LTD.

Date : 2017-10-05

Version : 1.00

Portions of Pro C5200/C5210 (RICOH/Savin/Lanier) Security Target are reprinted with written permission from IEEE, 445 Hoes Lane, Piscataway, New Jersey 08855, from U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std 2600.2™-2009), Copyright © 2010 IEEE. All rights reserved.

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

Revision History

| Version | Date | Author | Detail |
|---------|------------|---------------------|----------------------|
| 1.00 | 2017-10-05 | RICOH COMPANY, LTD. | Publication version. |

Table of Contents

| | | |
|----------|--|-----------|
| 1 | <i>ST Introduction</i> | 7 |
| 1.1 | ST Reference | 7 |
| 1.2 | TOE Reference | 7 |
| 1.3 | TOE Overview | 7 |
| 1.3.1 | TOE Type | 7 |
| 1.3.2 | TOE Usage | 7 |
| 1.3.3 | Major Security Features of TOE | 9 |
| 1.4 | TOE Description | 9 |
| 1.4.1 | Physical Boundary of TOE | 10 |
| 1.4.2 | Guidance Documents | 12 |
| 1.4.3 | Definition of Users | 15 |
| 1.4.3.1. | Direct User | 16 |
| 1.4.3.2. | Indirect User | 16 |
| 1.4.4 | Logical Boundary of TOE | 17 |
| 1.4.4.1. | Basic Functions | 17 |
| 1.4.4.2. | Security Functions | 19 |
| 1.4.5 | Protected Assets | 21 |
| 1.4.5.1. | User Data | 21 |
| 1.4.5.2. | TSF Data | 21 |
| 1.4.5.3. | Functions | 22 |
| 1.5 | Glossary | 22 |
| 1.5.1 | Glossary for This ST | 22 |
| 2 | <i>Conformance Claim</i> | 25 |
| 2.1 | CC Conformance Claim | 25 |
| 2.2 | PP Claims | 25 |
| 2.3 | Package Claims | 25 |
| 2.4 | Conformance Claim Rationale | 26 |
| 2.4.1 | Consistency Claim with TOE Type in PP | 26 |
| 2.4.2 | Consistency Claim with Security Problems and Security Objectives in PP | 26 |
| 2.4.3 | Consistency Claim with Security Requirements in PP | 27 |
| 3 | <i>Security Problem Definitions</i> | 29 |

| | | |
|------------|---|------------------|
| 3.1 | Threats | 29 |
| 3.2 | Organisational Security Policies..... | 30 |
| 3.3 | Assumptions..... | 30 |
| 4 | <i>Security Objectives.....</i> | <i>32</i> |
| 4.1 | Security Objectives for TOE..... | 32 |
| 4.2 | Security Objectives of Operational Environment..... | 33 |
| 4.2.1 | IT Environment..... | 33 |
| 4.2.2 | Non-IT Environment..... | 34 |
| 4.3 | Security Objectives Rationale | 35 |
| 4.3.1 | Correspondence Table of Security Objectives | 35 |
| 4.3.2 | Security Objectives Descriptions | 36 |
| 5 | <i>Extended Components Definition.....</i> | <i>40</i> |
| 5.1 | Restricted forwarding of data to external interfaces (FPT_FDI_EXP) | 40 |
| 6 | <i>Security Requirements.....</i> | <i>42</i> |
| 6.1 | Security Functional Requirements | 42 |
| 6.1.1 | Class FAU: Security audit | 42 |
| 6.1.2 | Class FCS: Cryptographic support | 45 |
| 6.1.3 | Class FDP: User data protection | 46 |
| 6.1.4 | Class FIA: Identification and authentication | 50 |
| 6.1.5 | Class FMT: Security management..... | 53 |
| 6.1.6 | Class FPT: Protection of the TSF..... | 58 |
| 6.1.7 | Class FTA: TOE access | 58 |
| 6.1.8 | Class FTP: Trusted path/channels..... | 58 |
| 6.2 | Security Assurance Requirements..... | 59 |
| 6.3 | Security Requirements Rationale..... | 60 |
| 6.3.1 | Tracing | 60 |
| 6.3.2 | Justification of Traceability..... | 61 |
| 6.3.3 | Dependency Analysis | 67 |
| 6.3.4 | Security Assurance Requirements Rationale..... | 69 |
| 7 | <i>TOE Summary Specification.....</i> | <i>70</i> |
| 7.1 | Audit Function | 70 |
| 7.2 | Identification and Authentication Function | 72 |

| | | |
|-----|---|----|
| 7.3 | Document Access Control Function | 74 |
| 7.4 | Use-of-Feature Restriction Function | 75 |
| 7.5 | Network Protection Function..... | 76 |
| 7.6 | Residual Data Overwrite Function..... | 76 |
| 7.7 | Stored Data Protection Function | 77 |
| 7.8 | Security Management Function | 77 |
| 7.9 | Software Verification Function | 81 |

List of Figures

| | |
|--|----|
| Figure 1 : Example of TOE Environment | 8 |
| Figure 2 : Hardware Configuration of the TOE | 10 |
| Figure 3 : Logical Scope of the TOE | 17 |

List of Tables

| | |
|---|----|
| Table 1 : Guidance for English Version 1..... | 13 |
| Table 2 : Guidance for English Version 2..... | 14 |
| Table 3 : Guidance for English Version 3..... | 15 |
| Table 4 : Definition of Users | 16 |
| Table 5 : List of Administrative Roles | 16 |
| Table 6 : Definition of User Data | 21 |
| Table 7 : Definition of TSF Data..... | 21 |
| Table 8 : Specific Terms Related to This ST | 22 |
| Table 9 : Rationale for Security Objectives..... | 35 |
| Table 10 : List of Auditable Events..... | 43 |
| Table 11 : List of Cryptographic Key Generation | 45 |
| Table 12 : List of Cryptographic Operation | 46 |
| Table 13 : List of Subjects, Objects, and Operations among Subjects and Objects (a) | 46 |
| Table 14 : List of Subjects, Objects, and Operations among Subjects and Objects (b)..... | 47 |
| Table 15 : Subjects, Objects and Security Attributes (a) | 47 |
| Table 16 : Rules to Control Operations on Document Data and User Jobs (a) | 47 |
| Table 17 : Additional Rules to Control Operations on Document Data and User Jobs (a)..... | 48 |
| Table 18 : Subjects, Objects and Security Attributes (b)..... | 49 |
| Table 19 : Rule to Control Operations on MFP Applications (b) | 49 |
| Table 20 : List of Authentication Events | 50 |
| Table 21 : List of Actions for Authentication Failure..... | 50 |
| Table 22 : List of Security Attributes for Each User That Shall Be Maintained | 51 |
| Table 23 : Rules for Initial Association of Attributes | 52 |
| Table 24 : User Roles for Security Attributes (a) | 53 |
| Table 25 : User Roles for Security Attributes (b) | 54 |
| Table 26 : Authorised Identified Roles Allowed to Override Default Values..... | 54 |
| Table 27 : List of TSF Data | 55 |
| Table 28 : List of Specification of Management Functions..... | 56 |
| Table 29 : TOE Security Assurance Requirements (EAL2+ALC_FLR.2)..... | 59 |
| Table 30 : Relationship between Security Objectives and Functional Requirements | 60 |
| Table 31 : Results of Dependency Analysis of TOE Security Functional Requirements | 67 |
| Table 32 : List of Audit Events..... | 70 |
| Table 33 : List of Audit Log Items | 71 |
| Table 34 : Unlocking Administrators for Each User Role..... | 73 |
| Table 35 : Stored Documents Access Control Rules for Normal Users | 75 |

| | |
|---|----|
| Table 36 : Encrypted Communications Provided by the TOE | 76 |
| Table 37 : List of Cryptographic Operations for Stored Data Protection | 77 |
| Table 38 : Management of TSF Data | 78 |
| Table 39 : List of Static Initialisation for Security Attributes of Document Access Control SFP | 80 |

1 ST Introduction

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

1.1 ST Reference

The following are the identification information of this ST.

Title : Pro C5200/C5210 (RICOH/Savin/Lanier) Security Target
Version : 1.00
Date : 2017-10-05
Author : RICOH COMPANY, LTD.

1.2 TOE Reference

The identification information of the TOE is shown below.

TOE Names : Pro C5200/C5210 (RICOH/Savin/Lanier)
Version : E-1.01
TOE Type : Digital multifunction product (hereafter "MFP")
Target MFP : MFP equipped with Auto Document Feeder (ADF) (one-pass duplex scanning ADF).

- Pro C5200S, Pro C5210S

Make clear to the sales representative that you purchase the MFP as CC-certified product.

1.3 TOE Overview

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

1.3.1 TOE Type

This TOE is an MFP, which is an IT device that inputs, stores, and outputs documents.

1.3.2 TOE Usage

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

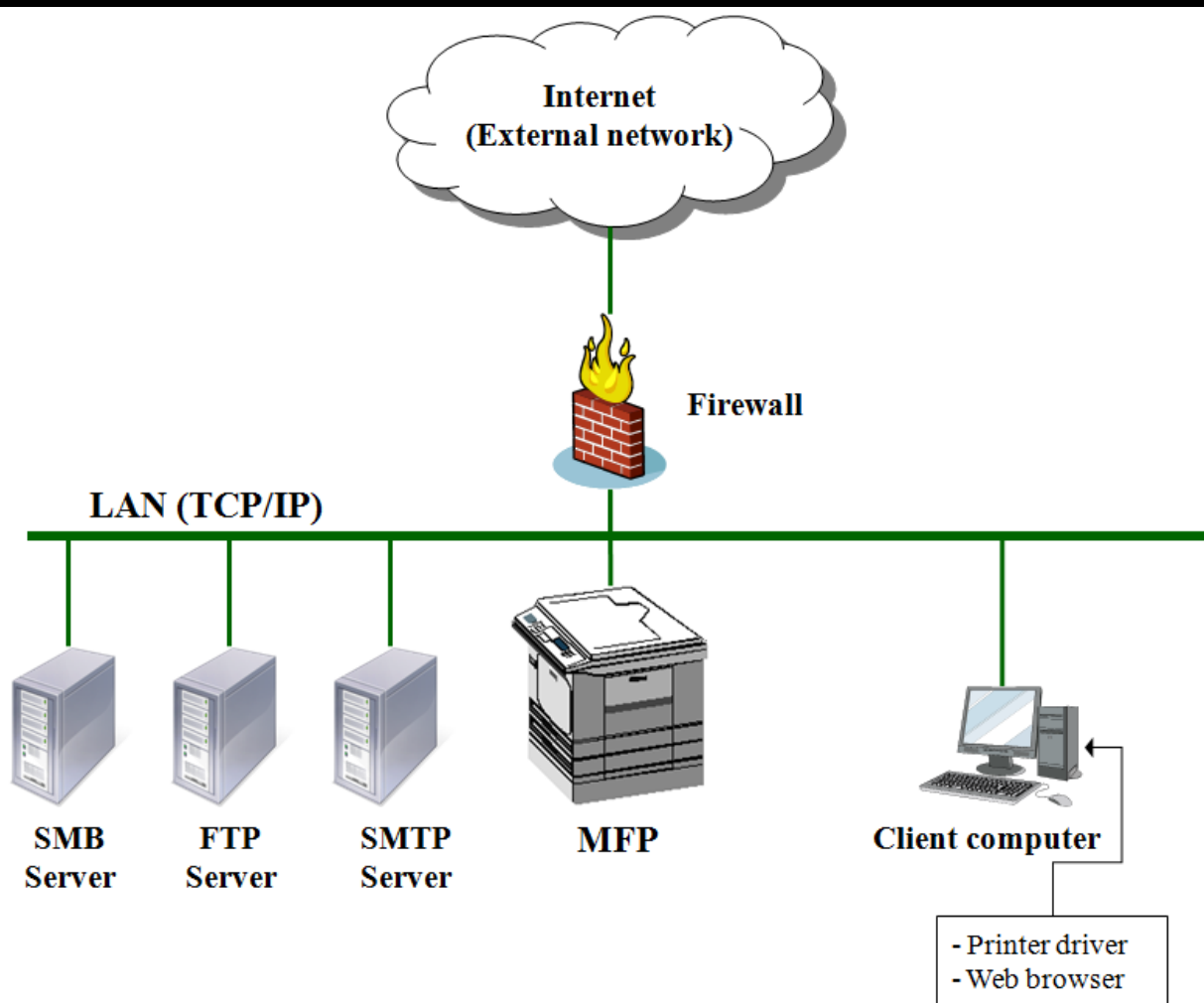


Figure 1 : Example of TOE Environment

The TOE is used by connecting to the local area network (hereafter "LAN"), as shown in Figure 1. Users can operate the TOE from the Operation Panel of the TOE or through LAN communications. Below, explanations are provided for the MFP, which is the TOE itself, and hardware and software other than the TOE.

MFP

A machinery that is defined as the TOE. The MFP is connected to the office LAN, and users can perform the following operations from the Operation Panel of the MFP:

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

LAN

Network used in the TOE environment.

Client computer

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

- Various settings for the MFP using a Web browser installed on the client computer,
- Operation of stored documents using a Web browser installed on the client computer,
- Storage and/or printing of documents using the printer driver installed on the client computer.

Firewall

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

FTP Server

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

SMB Server

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

SMTP Server

A server used by the TOE for e-mail transmission.

1.3.3 Major Security Features of TOE

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

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

1.4 TOE Description

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

1.4.1 Physical Boundary of TOE

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

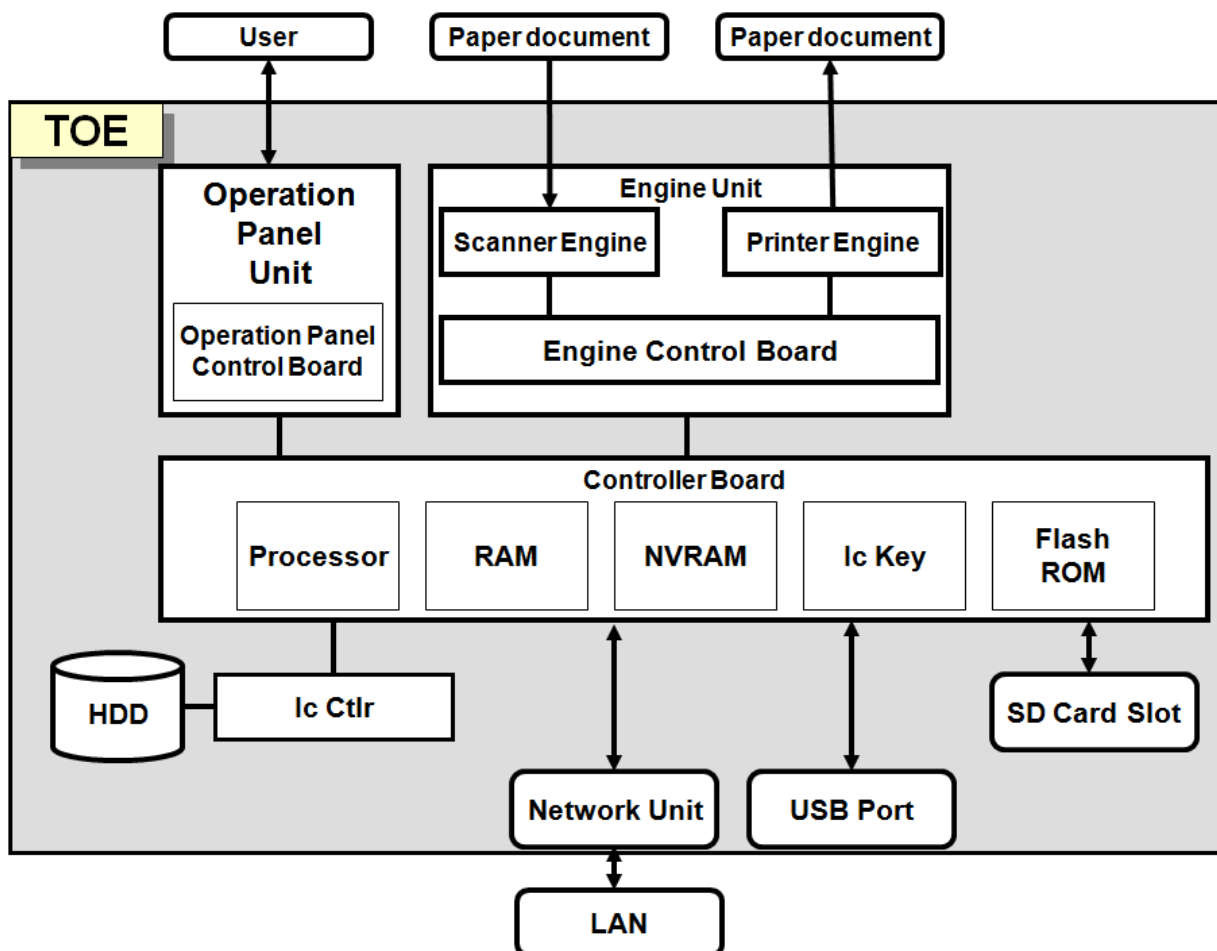


Figure 2 : Hardware Configuration of the TOE

Controller Board

The Controller Board is a device that contains Processors, RAM, NVRAM, Ic Key, and FlashROM. The Controller Board sends and receives information to and from the units and devices that constitute the MFP, and this information is used to control the MFP. The information to control the MFP is processed by the MFP Control Software on the Controller Board. The following describes the components of the Controller Board:

- Processor
A semiconductor chip that performs basic arithmetic processing for MFP operations.
- RAM
A volatile memory medium which is used as a working area for image processing such as

compressing/decompressing the image data. It can also be used to temporarily read and write internal information.

- NVRAM
A non-volatile memory medium in which TSF data for configuring MFP operations is stored.
- Ic Key
A security chip that has the functions of random number generation, cryptographic key generation and digital signature. It has the memory medium inside, and the signature root key is installed before the TOE is shipped.
- FlashROM
A non-volatile memory medium in which the MFP Control Software that constitutes the TOE is installed.

Operation Panel Unit (hereafter "Operation Panel")

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

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

Engine Unit

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

HDD

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

Ic Ctlr

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

Network Unit

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

USB Port

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

SD Card Slot

There are SD Card Slots for customer engineer and for users.

The SD Card Slot for customer engineer is used when the customer engineer installs the TOE. A cover is placed on the SD Card Slot during the TOE operation so that an SD Card cannot be inserted into or removed from the slot.

The SD Card Slot for users is used by users to print documents in the SD Card. The slot is set to disabled at the installation.

1.4.2 Guidance Documents

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

[English Version 1]

Table 1 : Guidance for English Version 1

| TOE Components | Guidance Documents for Product |
|----------------|---|
| MFP | <ul style="list-style-type: none"> - Read This First D260-7003 - SOFTWARE LICENSE AGREEMENT D241-7237 - Notes for Using This Machine Safely D195-7543A - Notes for Users D241-7084 - NOTICE TO USERS D241-7178 - User Guide D260-7087 - Operating Instructions Driver Installation Guide D257-7068 - About Open Source Software License D257-7054 - Operating Instructions Guide to Paper D260-7088 - About This Machine D260-7090 - Copy/Document Server D260-7091 - Print D260-7092 - Scan D260-7093 - Troubleshooting D260-7094 - Connecting the Machine/System Settings D260-7095 - Security Guide D260-7098 - PostScript 3 D260-7097 - Paper Settings D260-7096 - Extended Feature Settings D260-7099 - Notes for Administrators: Using This Machine in a Network Environment Compliant with IEEE Std 2600.2™-2009 D260-7069 - Notes on Security Functions D181-2583 - Help 83NHDGENZ1.00 v211 |

[English Version 2]

Table 2 : Guidance for English Version 2

| TOE Components | Guidance Documents for Product |
|----------------|---|
| MFP | <ul style="list-style-type: none"> - Read This First D260-7002 - Notes for Users D241-7068 - SOFTWARE LICENSE AGREEMENT D241-7237 - Notes for Using This Machine Safely D195-7543A - NOTICE TO USERS D241-7178 - Notes for Users D257-7081 - User Guide D260-7087 - Operating Instructions Driver Installation Guide D257-7068 - About Open Source Software License D257-7054 - Operating Instructions Guide to Paper D260-7088 - About This Machine D260-7090 - Copy/Document Server D260-7091 - Print D260-7092 - Scan D260-7093 - Troubleshooting D260-7094 - Connecting the Machine/System Settings D260-7095 - Security Guide D260-7098 - PostScript 3 D260-7097 - Paper Settings D260-7096 - Extended Feature Settings D260-7099 - Notes for Administrators: Using This Machine in a Network Environment Compliant with IEEE Std 2600.2™-2009 D260-7069 - Notes on Security Functions D181-2583 - Help 83NHDGENZ1.00 v211 |

[English Version 3]

Table 3 : Guidance for English Version 3

| TOE Components | Guidance Documents for Product |
|----------------|--|
| MFP | <ul style="list-style-type: none"> - Read This First D260-7004 - SOFTWARE LICENSE AGREEMENT D241-7237 - Notes for Using This Machine Safely D223-7236 - NOTICE TO USERS D241-7178 - Notes for Users D241-7087 - User Guide D260-7087 - Operating Instructions Driver Installation Guide D257-7068 - About Open Source Software License D257-7054 - Operating Instructions Guide to Paper D260-7088 - About This Machine D260-7090 - Copy/Document Server D260-7091 - Print D260-7092 - Scan D260-7093 - Troubleshooting D260-7094 - Connecting the Machine/System Settings D260-7095 - Security Guide D260-7098 - PostScript 3 D260-7097 - Paper Settings D260-7096 - Extended Feature Settings D260-7099 - Notes for Administrators: Using This Machine in a Network Environment Compliant with IEEE Std 2600.2™-2009 D260-7069 - Notes on Security Functions D181-2583 - Help 83NHDGENZ1.00 v211 |

1.4.3 Definition of Users

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

1.4.3.1. Direct User

The "user" referred to in this ST indicates a direct user. This direct user consists of normal users and administrators. The following table (Table 4) shows the definitions of these direct users.

Table 4 : Definition of Users

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

The administrator means the user registered for TOE management. According to its roles, the administrator can be classified as the supervisor and the MFP administrator. Up to four MFP administrators can be registered and selectively authorised to perform user management, machine management, network management, and file management. Therefore, the different roles of the management privilege can be allocated to multiple MFP administrators individually. The "MFP administrator" in this ST refers to the MFP administrator who has all management privileges (Table 5).

Table 5 : List of Administrative Roles

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

1.4.3.2. Indirect User

Responsible manager of MFP

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

Customer engineer

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

1.4.4 Logical Boundary of TOE

The Basic Functions and Security Functions are described as follows:

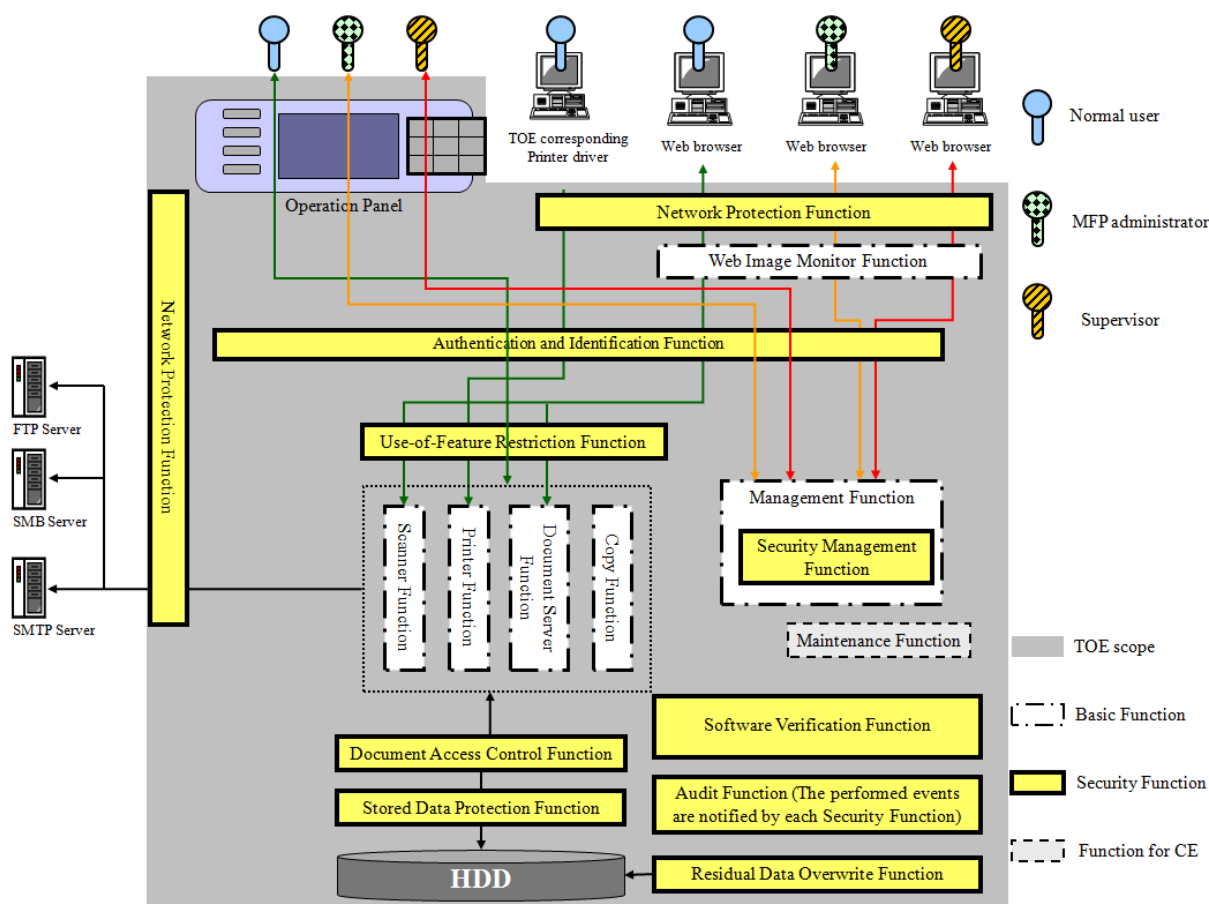


Figure 3 : Logical Scope of the TOE

1.4.4.1. Basic Functions

The overview of the Basic Functions is described as follows:

Copy Function

The Copy Function is to scan paper documents and copy scanned image data from the Operation Panel. Magnification and other editorial jobs can be applied to the copy image. It can also be stored on the HDD as a Document Server document.

Printer Function

The Printer Function is to print or store the documents received from the printer driver installed on the client computer. It also allows users to print and delete the documents stored in the TOE from the Operation Panel or the client computer.

- Receiving documents from the printer driver installed on the client computer.

The TOE receives documents from the printer driver installed on the client computer. Printing methods for documents is selected by users from the printer driver. The printing methods include direct print, Document Server storage, locked print, stored print, hold print, and sample print.

For direct print, documents received by the TOE will be printed. The documents will not be stored in the TOE.

For Document Server storage, the received documents will be stored on the HDD as Document Server documents.

For locked print, stored print, hold print, and sample print, the received documents will be stored on the HDD as printer documents. A dedicated password, which is used for locked print, is not subject to this evaluation.

- Operating from the Operation Panel

The TOE can print or delete printer documents according to the operations by users from the Operation Panel.

- Operating from the client computer

The TOE can print or delete printer documents according to the operations by users from the client computer.

- Deleting printer documents by the TOE

The deletion of printer documents by the TOE differs depending on printing methods. If locked print, hold print, or sample print is specified, the TOE deletes printer documents when printing is complete. If stored print is specified, the TOE does not delete printer documents even when printing is complete.

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

Scanner Function

The Scanner Function is for users to scan paper documents by operating from the Operation Panel. The users can send and then save those scanned documents to SMB server, FTP server, and the client computer. The images of the scanned paper documents can be stored in the TOE to be transmitted or deleted afterwards.

Methods to transmit documents include folder transmission, e-mail transmission of attachments, and e-mail transmission of the URL.

Folder transmission can be applied only to the destination folders in a server that the MFP administrator pre-registers in the TOE and with which secure communication can be ensured. E-mail transmission of attachments and e-mail transmission of the URL are possible only with the mail server and e-mail addresses that the MFP administrator pre-registers in the TOE and with which secure communication can be ensured. Users, who receive e-mails sent by e-mail transmission of the URL, can download scanner documents to the client computer.

Document Server Function

The Document Server Function is to operate documents stored in the TOE by using the Operation Panel and the client computer.

From the Operation Panel, users can store, duplicate, print, edit and delete Document Server documents.

From the client computer, users can print and delete Document Server documents. Also, users can send scanner documents to folders, send them by e-mail as attachments, download, and delete them.

Management Function

The Management Function is to control the MFP's overall behaviour. The management function can be operated by using the Operation Panel or the client computer.

Maintenance Function

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

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

Web Image Monitor Function

The Web Image Monitor Function (hereafter "WIM") is for the TOE user to remotely control the TOE from the client computer. The Operation Panel screen of the connected MFP can be displayed by the MFP administrator.

To use this function, the TOE user needs to install the designated Web browser on the client computer following the guidance documents and connect the client computer to the TOE via the LAN.

1.4.4.2. Security Functions

The Security Functions are described as follows:

Audit Function

The Audit Function is to generate the audit log of TOE use and security-relevant events (hereafter, "audit events"). Also, this function provides the recorded audit log in a legible fashion for users to audit. This function can be used only by the MFP administrator to view and delete the recorded audit log. To view the audit log, WIM will be used, and to delete the audit log, WIM or the Operation Panel will be used.

Identification and Authentication Function

The Identification and Authentication Function is to verify persons before they use the TOE. The persons are allowed to use the TOE only when confirmed as the authorised user.

Users can use the TOE from the Operation Panel or via the network. By the network, users can use the TOE from a Web browser and printer driver.

A person who attempts to use the TOE from the Operation Panel or a Web browser will be required to enter

his or her login user name and login password so that he or she can be verified as a normal user, MFP administrator, or supervisor.

A person who attempts to use the Printer Function from the printer driver will be required to enter his or her login user name and login password received from the printer driver, so that he or she can be verified as a normal user.

This function includes protection functions for the authentication feedback area, where dummy characters are displayed if a login password is entered using the Operation Panel. In addition, this function can be used to register passwords that fulfil the requirements of the Minimum Character No. (i.e. minimum password length) and obligatory character types the MFP administrator specifies, so that the lockout function can be enabled and login password quality can be protected.

Document Access Control Function

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

Use-of-Feature Restriction Function

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

Network Protection Function

The Network Protection Function is to prevent information leakage through wiretapping on the LAN and detect data tampering. When using WIM from the client computer, the protection function can be enabled by specifying the URL where encrypted communication is available. If the Printer Function is used, the protection function can be enabled using the printer driver to specify encrypted communication. If the folder transmission function of Scanner Function is used, the protection function can be enabled through encrypted communication. If the e-mail transmission function of Scanner Function is used, the protection function can be enabled through encrypted communication with communication requirements that are specified for each e-mail address.

Residual Data Overwrite Function

The Residual Data Overwrite Function is to overwrite specific patterns on the HDD and disable the reusing of the residual data included in deleted documents, temporary documents and their fragments on the HDD.

Stored Data Protection Function

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

Security Management Function

The Security Management Function is to control operations for TSF data in accordance with user role privileges or user privileges allocated to normal users, MFP administrator, and supervisor.

Software Verification Function

The Software Verification Function is to verify the integrity of the executable code of the MFP Control Software, and to ensure that they can be trusted.

1.4.5 Protected Assets

Assets to be protected by the TOE are user data, TSF data, and functions.

1.4.5.1. User Data

The user data is classified into two types: document data and function data. Table 6 defines user data according to these data types.

Table 6 : Definition of User Data

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

1.4.5.2. TSF Data

The TSF data is classified into two types: protected data and confidential data. Table 7 defines TSF data according to these data types.

Table 7 : Definition of TSF Data

| Type | Description |
|----------------|---|
| Protected data | This data must be protected from changes by unauthorised persons. No security threat will occur even this data is exposed to the public. In this ST, "protected data", listed below, is referred to as "TSF protected data". Login user name, Number of Attempts before Lockout, settings for Lockout Release Timer, lockout time, date settings (year/month/day), time settings, Minimum Character No., Password Complexity Setting, Operation Panel auto logout time, WIM auto logout time, S/MIME user information, destination folder, document user list, available function list, user authentication method, IPsec setting information, and Device Certificate. |

| Type | Description |
|-------------------|---|
| Confidential data | This data must be protected from changes by unauthorised persons and reading by users without viewing permissions. In this ST, "confidential data", listed below, is referred to as "TSF confidential data". Login password, audit log, and HDD cryptographic key. |

1.4.5.3. Functions

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

1.5 Glossary

1.5.1 Glossary for This ST

For clear understanding of this ST, Table 8 provides the definitions of specific terms.

Table 8 : Specific Terms Related to This ST

| Terms | Definitions |
|----------------------------------|--|
| MFP Control Software | A software component installed in the TOE. This component is stored in FlashROM. |
| Login user name | An identifier assigned to each normal user, MFP administrator, and supervisor. The TOE identifies users by this identifier. |
| Login password | A password associated with each login user name. |
| Lockout | A type of behaviour to deny login of particular users. |
| Auto Logout function | A function for automatic user logout if no access is attempted from the Operation Panel or the client computer before the predetermined time elapses. Also called Auto Logout. |
| Operation Panel auto logout time | Auto logout time for the Operation Panel. |
| WIM auto logout time | Auto logout time for WIM. |
| Minimum Character No. | The minimum number of registrable password digits. |
| Password Complexity Setting | The minimum combination of the characters and symbols that can be used as registrable passwords. There are four types of characters: uppercase and lower case alphabets, digits and symbols. There are Level 1 and Level 2 Password Complexity Settings. Level 1 requires a password to be a combination of two or more types of characters and symbols specified above. Level 2 requires a password to be a combination of three or more types of characters and symbols specified above. |

| Terms | Definitions |
|---------------------------|---|
| HDD | An abbreviation of hard disk drive. In this document, unless otherwise specified, "HDD" indicates the HDD installed on the TOE. |
| User job | A sequence of operations of each TOE function (Copy Function, Document Server Function, Scanner Function, and Printer Function) from beginning to end. A user job may be suspended or cancelled by users during operation. If a user job is cancelled, the job will be terminated. |
| Documents | General term for paper documents and electronic documents used in the TOE. |
| Document data attributes | Attributes of document data, such as +PRT, +SCN, +CPY, and +DSR. |
| +PRT | One of the document data attributes. Documents printed from the client computer, or documents stored in the TOE by locked print, hold print, and sample print using the client computer. |
| +SCN | One of the document data attributes. Documents sent to IT devices by e-mail or sent to folders, or downloaded on the client computer from the MFP. For these operations the Scanner Function is used. |
| +CPY | One of the document data attributes. Copies of original documents made by using Printer Function. |
| +DSR | One of the document data attributes. Documents saved in the TOE by using Copy Function, Scanner Function, and Document Server Function. Documents saved in the TOE after being printed with Document Server printing or stored print from the client computer. |
| Document user list | One of the security attributes of document data. A list of the login user names of the normal users whose access to documents is authorised, and it can be set for each document data. This list does not include the login user names of MFP administrators whose access to the document data is possible for administration. |
| Stored documents | Documents stored in the TOE so that they can be used with Document Server Function, Printer Function, and Scanner Function. |
| Stored document type | Classification of stored documents according to their purpose of use. This includes Document Server documents, printer documents, and scanner documents. |
| Document Server documents | One of the stored document types. Documents stored in the TOE when Document Server storage is selected as the printing method for Copy Function, Document Server Function, and Printer Function. |
| Printer documents | One of the stored document types. Documents stored in the TOE when any one of locked print, hold printing, and sample print is selected as the printing method for Printer Function. |
| Scanner documents | One of the stored document types. Documents stored in the TOE using Scanner Function. |
| MFP application | A general term for each function the TOE provides: Copy Function, Document Server Function, Scanner Function, and Printer Function. |
| Available function list | A list of the functions (Copy Function, Printer Function, Scanner Function, and Document Server Function) that normal users are authorised to access. This list is assigned as an attribute of each normal user. |

| Terms | Definitions |
|---|---|
| Operation Panel | A panel that consists of a touch screen LCD and key switches. The Operation Panel is used by users to operate the TOE. |
| Folder transmission | A function that sends documents from the MFP via networks to a shared folder in an SMB Server by using SMB protocol or that sends documents to a shared folder in an FTP Server by using FTP protocol. The following documents can be delivered to folders: scanned documents using Scanner Function, and scanned and stored documents using Scanner Function. IPsec protects the communication for realising this function. |
| Destination folder | Destination information for the "folder transmission" function. The destination folder includes the path information to the destination server, the folder in the server, and identification and authentication information for user access. The destination folder is registered and managed by the MFP administrator. |
| E-mail transmission | A function to send e-mails from the MFP to the client computer via the SMTP Server. |
| E-mail transmission of attachments | A function to send documents scanned by the Scanner Function as e-mail. S/MIME protects the communication for realising this function. |
| E-mail transmission of the URL | A function to send the URL of scanner documents stored in the MFP by e-mail. |
| S/MIME user information | Information required for e-mail transmission using S/MIME. Also, this information consists of e-mail address, user certificate, and encryption setting (S/MIME setting). Uniquely provided for each e-mail address, the S/MIME user information is registered and managed by the MFP administrator. |
| IPsec setting information | Information that determines the action of IPsec of the TOE. |
| Auto Document Feeder (ADF) (one-pass duplex scanning ADF) | A device that feeds the originals set on the device one by one to the exposure glass. When scanning both sides of the original, both sides are scanned simultaneously. |

2 Conformance Claim

This section describes Conformance Claim.

2.1 CC Conformance Claim

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

- CC version for which this ST and TOE claim conformance

Part 1:

Introduction and general model September 2012 Version 3.1 Revision 4 (Japanese translation ver.1.0) CCMB-2012-09-001

Part 2:

Security functional components September 2012 Version 3.1 Revision 4 (Japanese translation ver.1.0) CCMB-2012-09-002

Part 3:

Security assurance components September 2012 Version 3.1 Revision 4 (Japanese translation ver.1.0) CCMB-2012-09-003

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

2.2 PP Claims

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

PP Name/Identification : U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std 2600.2™-2009)

Version : 1.0

Notes: This PP conforms to "IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600-2008, Operational Environment B", published in Common Criteria Portal, and also satisfies "CCEVS Policy Letter #20".

2.3 Package Claims

The SAR package which this ST and TOE conform to is EAL2+ALC_FLR.2.

The selected SFR Packages from the PP are:

2600.2-PRT conformant

2600.2-SCN conformant

2600.2-CPY conformant

2600.2-DSR conformant

2600.2-SMI conformant

2.4 Conformance Claim Rationale

2.4.1 Consistency Claim with TOE Type in PP

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

The type of this TOE is the MFP. The MFP has the devices the HCDs have, and equips the Copy Function, Scanner Function, Printer Function, and Document Server Function, including the additional equipment. Therefore, this TOE type is consistent with the TOE type in the PP.

2.4.2 Consistency Claim with Security Problems and Security Objectives in PP

Defining all security problems in the PP, P.STORAGE_ENCRYPTION was augmented to the security problem definitions in chapter 3. Defining all security objectives in the PP, O.STORAGE.ENCRYPTED was augmented to the security objectives in chapter 4. Described below are the rationale for these augmented security problems and security objectives that conform to the PP.

Although the PP is written in English, the security problem definitions in chapter 3 and security objectives in chapter 4 are translated from English into Japanese. If the literal translation of the PP was thought to be difficult for readers to understand the PP in Japanese, the translation was made comprehensible. This, however, does not mean that its description deviates from the requirements of the PP conformance. Also, the description is neither increased nor decreased.

Augmentation of P.STORAGE_ENCRYPTION and O.STORAGE.ENCRYPTED

P.STORAGE_ENCRYPTION and O.STORAGE.ENCRYPTED encrypt data on HDD and satisfy both other organisational security policies in the PP and security objectives of the TOE. Therefore, P.STORAGE_ENCRYPTION and O.STORAGE.ENCRYPTED were augmented but still conform to the PP.

Augmentation of threat scope of T.DOC.DIS and T.DOC.ALT

The definition of a user allowed to view or modify D.DOC is the same in this TOE and the PP. However, the PP defines the scope in which the leakage and tampering of D.DOC may occur as inside the TOE. While on the other hand, the TOE defines it as inside the TOE and TOE's communication path, which means that the TOE incorporates the PP.

Therefore, T.DOC.DIS and T.DOC.ALT conform to the PP.

Augmentation of threat scope of T.FUNC.ALT

The definition of a user allowed to modify D.FUNC is the same in this TOE and the PP. However, the PP defines the scope in which the threat of tampering D.FUNC may occur as inside the TOE. While on the other hand, the TOE defines it as inside the TOE and TOE's communication path, which means that the TOE incorporates the PP.

Therefore, T.FUNC.ALT conforms to the PP.

For those points mentioned above, the security problems and security objectives in this ST are consistent with those in the PP.

2.4.3 Consistency Claim with Security Requirements in PP

The SFRs for this TOE consist of the Common Security Functional Requirements, 2600.2-PRT, 2600.2-SCN, 2600.2-CPY, 2600.2-DSR, and 2600.2-SMI.

The Common Security Functional Requirements are the indispensable SFR specified by the PP. 2600.2-PRT, 2600.2-SCN, 2600.2-CPY, 2600.2-DSR, and 2600.2-SMI are selected from the SFR Package specified by the PP.

2600.2-NVS is not selected because this TOE does not have any non-volatile memory medium that is detachable.

Although the security requirements of this ST were partly augmented and instantiated over the security requirements of the PP, they are still consistent with the PP. Described below are the parts augmented and instantiated with the reasons for their consistency with the PP.

Augmentation of FAU_STG.1, FAU_STG.4, FAU_SAR.1, and FAU_SAR.2

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

Augmentation of FIA_AFL.1, FIA_UAU.7, and FIA_SOS.1

For the Identification and Authentication Function of the TOE, FIA_AFL.1, FIA_UAU.7, and FIA_SOS.1 are augmented according to PP APPLICATION NOTE38.

Augmentation of FCS_CKM.1 and FCS_COP.1

This TOE claims O.STORAGE.ENCRYPTED as the security objectives for the data protection applied to non-volatile memory media that are neither allowed to be attached nor removed by the administrator. To fulfil this claim, additional changes were augmented to the functional requirements FCS_CKM.1 and FCS_COP.1 and to the functional requirements interdependent with FCS_CKM.1 and FCS_COP.1; however, these changes still satisfy the functional requirements demanded in the PP.

Augmentation of restricted forwarding of data to external interface (FPT_FDI_EXP)

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

Consistency Rationale of FDP_ACF.1(a)

While FDP_ACF.1.1(a) and FDP_ACF.1.2(a) in the PP require the access control SFP to the document data that is defined for each SFR package in the PP, this ST requires the access control SFP to the document data that is defined for each document data attribute, which is the security attribute for objects. This is not a deviation from the PP but an instantiation of the PP.

Although FDP_ACF.1.3(a) in the PP has no additional rules on access control of document data and user jobs, this ST allows the MFP administrator to delete document data and user jobs.

The TOE allows the MFP administrator to delete document data and user jobs on behalf of normal users who are privileged to delete them in case normal users cannot execute such privileges for some reasons. This does not deviate from the access control SFP defined in the PP.

Although FDP_ACF.1.4(a) in the PP has no additional rules on access control of document data and user jobs, this ST rejects supervisor to operate document data and user jobs.

Supervisor is not identified in the PP and are the special users for this TOE.

This indicates that the PP does not allow users to operate the TOE, unless they are identified as the users of document data and user jobs.

Therefore, FDP_ACF.1(a) in this ST satisfies FDP_ACF.1(a) in the PP.

Additional Rules on FDP_ACF.1.3(b)

While FDP_ACF.1.3(b) in the PP allows users with administrator privileges to operate the TOE functions, this ST does not allow the MFP administrator to operate the TOE functions.

The TOE allows the MFP administrator to delete document data and user jobs (document access control SFP, FDP_ACC.1(a) and FDP_ACF.1(a)), and as a result, the TSF restrictively allows the MFP administrator to access the TOE functions. Therefore, the requirements described in FDP_ACF.1.3(b) in the PP are satisfied at the same time.

Therefore, FDP_ACF.1.3(b) in this ST satisfies FDP_ACF.1.3(b) in the PP.

FTP_ITC.1.3 including D.DOC and D.FUNC

Although the PP does not define threat of leakage and tampering of D.DOC and D.FUNC in the communication path, FTP_ITC.1.3 in this ST states that D.DOC and D.FUNC communicate via the trusted channel. This suggests that the TOE protects D.DOC and D.FUNC in wider scope than the PP does. FTP_ITC.1.3 in this ST satisfies the PP.

3 Security Problem Definitions

This section describes Threats, Organisational Security Policies and Assumptions.

3.1 Threats

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

| | |
|-------------------|---|
| T.DOC.DIS | Document disclosure Documents under the TOE management may be disclosed to persons without a login user name, or to persons with a login user name but without an access permission to the document. |
| T.DOC.ALT | Document alteration Documents under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the document. |
| T.FUNC.ALT | User job alteration User jobs under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the user job. |
| T.PROT.ALT | Alteration of TSF protected data TSF Protected Data under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the TSF Protected Data. |
| T.CONF.DIS | Disclosure of TSF confidential data TSF Confidential Data under the TOE management may be disclosed to persons without a login user name, or to persons with a login user name but without an access permission to the TSF Confidential Data. |
| T.CONF.ALT | Alteration of TSF confidential data TSF Confidential Data under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the TSF Confidential Data. |

3.2 Organisational Security Policies

The following organisational security policies are taken:

P.USER.AUTHORIZATION User identification and authentication

Only users with operation permission of the TOE shall be authorised to use the TOE.

P.SOFTWARE.VERIFICATION Software verification

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

P.AUDIT.LOGGING Management of audit log records

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

P.INTERFACE.MANAGEMENT Management of external interfaces

To prevent unauthorised use of the external interfaces of the TOE, operation of those interfaces shall be controlled by the TOE and its IT environment.

P.STORAGE.ENCRYPTION Encryption of storage devices

The data stored on the HDD inside the TOE shall be encrypted.

3.3 Assumptions

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

A.ACCESS.MANAGED Access management

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

A.USER.TRAINING User training

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

A.ADMIN.TRAINING Administrator training

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

A.ADMIN.TRUST

Trusted administrator

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

4 Security Objectives

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

4.1 Security Objectives for TOE

This section describes the security objectives for the TOE.

- O.DOC.NO_DIS** **Protection of document disclosure**
- The TOE shall protect documents from unauthorised disclosure by persons without a login user name, or by persons with a login user name but without an access permission to the document.
- O.DOC.NO_ALT** **Protection of document alteration**
- The TOE shall protect documents from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the document.
- O.FUNC.NO_ALT** **Protection of user job alteration**
- The TOE shall protect user jobs from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the job.
- O.PROT.NO_ALT** **Protection of TSF protected data alteration**
- The TOE shall protect TSF Protected Data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the TSF Protected Data.
- O.CONF.NO_DIS** **Protection of TSF confidential data disclosure**
- The TOE shall protect TSF Confidential Data from unauthorised disclosure by persons without a login user name, or by persons with a login user name but without an access permission to the TSF Confidential Data.
- O.CONF.NO_ALT** **Protection of TSF confidential data alteration**
- The TOE shall protect TSF Confidential Data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the TSF Confidential Data.

O.USER.AUTHORIZED User identification and authentication

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

O.INTERFACE.MANAGED Management of external interfaces by TOE

The TOE shall manage the operation of external interfaces in accordance with the security policies.

O.SOFTWARE.VERIFIED Software verification

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

O.AUDIT.LOGGED Management of audit log records

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

O.STORAGE.ENCRYPTED Encryption of storage devices

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

4.2 Security Objectives of Operational Environment

This section describes the security objectives of the operational environment.

4.2.1 IT Environment

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

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

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

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

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

The IT environment shall take a countermeasure for the prevention of unmanaged access to TOE external interfaces.

4.2.2 Non-IT Environment

OE.PHYSICAL.MANAGED Physical management

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

OE.USER.AUTHORIZED Assignment of user authority

The responsible manager of MFP shall give users the authority to use the TOE in accordance with the security policies and procedures of their organisation.

OE.USER.TRAINED User training

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

OE.ADMIN.TRAINED Administrator training

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

OE.ADMIN.TRUSTED Trusted administrator

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

OE.AUDIT.REVIEWED Log audit

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

4.3 Security Objectives Rationale

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

4.3.1 Correspondence Table of Security Objectives

Table 9 describes the correspondence between the assumptions, threats and organisational security policies, and each security objective.

Table 9 : Rationale for Security Objectives

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

4.3.2 Security Objectives Descriptions

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

T.DOC.DIS

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

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

T.DOC.DIS is countered by these objectives.

T.DOC.ALT

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

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

T.DOC.ALT is countered by these objectives.

T.FUNC.ALT

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

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

T.FUNC.ALT is countered by these objectives.

T.PROT.ALT

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

By OE.USER.AUTHORIZED, the responsible manager of MFP gives the authority to use the TOE to users who follow the security policies and procedures of their organisation. By O.USER.AUTHORIZED, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE. By O.PROT.NO_ALT, the TOE protects the TSF protected

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

T.PROT.ALT is countered by these objectives.

T.CONF.DIS

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

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

T.CONF.DIS is countered by these objectives.

T.CONF.ALT

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

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

T.CONF.ALT is countered by these objectives.

P.USER.AUTHORIZATION

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

By OE.USER.AUTHORIZED, the responsible manager of MFP gives the authority to use the TOE to users who follow the security policies and procedures of their organisation. By O.USER.AUTHORIZED, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE.

P.USER.AUTHORIZATION is enforced by these objectives.

P.SOFTWARE.VERIFICATION

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

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

P.SOFTWARE.VERIFICATION is enforced by this objective.

P.AUDIT.LOGGING

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

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

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

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

P.AUDIT.LOGGING is enforced by these objectives.

P.INTERFACE.MANAGEMENT

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

By O.INTERFACE.MANAGED, the TOE manages the operation of the external interfaces in accordance with the security policies. By OE.INTERFACE.MANAGED, the TOE constructs the IT environment that prevents unmanaged access to TOE external interfaces.

P.INTERFACE.MANAGEMENT is enforced by these objectives.

P.STORAGE.ENCRYPTION

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

By O.STORAGE.ENCRYPTED, the TOE shall encrypt the data to be written on the HDD, and written on the HDD shall be those encrypted data.

P.STORAGE.ENCRYPTION is enforced by this objective.

A.ACCESS.MANAGED

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

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

A.ACCESS.MANAGED is upheld by this objective.

A.ADMIN.TRAINING

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

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

A.ADMIN.TRAINING is upheld by this objective.

A.ADMIN.TRUST

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

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

A.ADMIN.TRUST is upheld by this objective.

A.USER.TRAINING

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

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

OE.USER.TRAINED is upheld by this objective.

5 Extended Components Definition

This section describes Extended Components Definition.

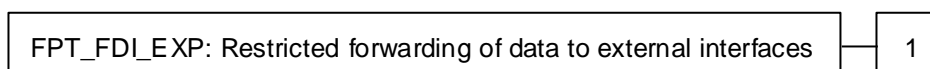
5.1 Restricted forwarding of data to external interfaces (FPT_FDI_EXP)

Family behaviour

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

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

Component levelling:



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

Management: FPT_FDI_EXP.1

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

- a) Definition of the role(s) that are allowed to perform the management activities
- b) Management of the conditions under which direct forwarding can be allowed by an administrative role
- c) Revocation of such an allowance

Audit: FPT_FDI_EXP.1

There are no auditable events foreseen.

Rationale:

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

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

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

The Common Criteria defines attribute-based control of user data flow in its FDP class. However, in this ST, the authors needed to express the control of both user data and TSF data flow using administrative control instead of attribute-based control. It is considered inappropriate to use FDP_IFF and FDP_IFC by applying refinement for this purpose. Therefore, the authors decided to define an extended component to address this functionality.

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

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to: No other components

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

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on **[assignment: list of external interfaces]** from being forwarded without further processing by the TSF to **[assignment: list of external interfaces]**.

6 Security Requirements

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

6.1 Security Functional Requirements

This section describes the TOE security functional requirements for fulfilling the security objectives defined in section 4.1. The security functional requirements are quoted from the requirement defined in the CC Part2. The security functional requirements that are not defined in CC Part2 are quoted from the extended security functional requirements defined in the PP.

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

6.1.1 Class FAU: Security audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

- a) Start-up and shutdown of the audit functions;
- b) All auditable events for the **[selection: not specified]** level of audit; and
- c) **[assignment: auditable events of the TOE shown in Table 10]**.

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

- a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[assignment: types of job for FDP_ACF.1(a), all login user names that attempted the user identification for FIA_UID.1, communication direction of communication by WIM, communication IP address of the communication used for WIM and folder transmission, recipient's e-mail address used for e-mail transmission of attachments, lockout operation type, Locked out User, and Locked out User who is to be released]**.

Table 10 shows the action (CC rules) recommended by the CC as auditable for each functional requirement and the corresponding auditable events of the TOE.

Table 10 : List of Auditable Events

| Functional Requirements | Actions Which Should Be Auditable | Auditable Events |
|--------------------------------|---|---|
| FDP_ACF.1(a) | <p>a) Minimal: Successful requests to perform an operation on an object covered by the SFP.</p> <p>b) Basic: All requests to perform an operation on an object covered by the SFP.</p> <p>c) Detailed: The specific security attributes used in making an access check.</p> | <p>Original:</p> <ul style="list-style-type: none"> - Start and end operation of creating (storing) document data. - Complete operation of creating (duplicating) document data successfully. - Start and end operation of printing document data. - Start and end operation of downloading document data. - Start and end operation of sending document data as attachments by e-mail. - Start and end operation of sending document data to folder. - Complete operation of editing document data. - Start and end operation of deleting document data. <p>Those described above, "creating, printing, downloading, sending attachments by e-mail, sending to folder, and deleting", are the job types of additional information that are required by the PP.</p> |
| FDP_ACF.1(b) | <p>a) Minimal: Successful requests to perform an operation on an object covered by the SFP.</p> <p>b) Basic: All requests to perform an operation on an object covered by the SFP.</p> <p>c) Detailed: The specific security attributes used in making an access check.</p> | Original: Not recorded. |
| FIA_AFL.1 | <p>a) Minimal: the reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).</p> | a) Minimal: Starting and releasing lockout |
| FIA_UAU.1 | <p>a) Minimal: Unsuccessful use of the authentication mechanism;</p> <p>b) Basic: All use of the authentication mechanism;</p> <p>c) Detailed: All TSF mediated actions performed before authentication of the user.</p> | b) Basic: Success and failure of login operation |

| Functional Requirements | Actions Which Should Be Auditable | Auditable Events |
|-------------------------|--|---|
| FIA_UID.1 | a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided; b) Basic: All use of the user identification mechanism, including the user identity provided. | b) Basic: Success and failure of login operation. Also includes the user identification that is required by the PP as the additional information. |
| FMT_SMF.1 | a) Minimal: Use of the management functions. | a) Minimal: Record of management items in Table 28. |
| 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 communication with trusted channel. |

FAU_GEN.2 User identity association

Hierarchical to: No other components.

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

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

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

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

FAU_STG.4 Prevention of audit data loss

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

Dependencies: FAU_STG.1 Protected audit trail storage

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

FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

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

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

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

6.1.2 Class FCS: Cryptographic support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: **cryptographic key generation algorithm in Table 11**] and specified cryptographic key sizes [assignment: **cryptographic key sizes in Table 11**] that meet the following: [assignment: **standards in Table 11**].

Table 11 : List of Cryptographic Key Generation

| Key Type | Standard | Cryptographic Key Generation Algorithm | Cryptographic Key Size |
|-----------------------|-----------------|---|-------------------------------|
| HDD cryptographic key | NIST SP 800-90A | HMAC_DRBG(SHA256) | 256 bits |

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or

- FCS_CKM.1 Cryptographic key generation]
 FCS_CKM.4 Cryptographic key destruction
- FCS_COP.1.1 The TSF shall perform [assignment: cryptographic operations shown in Table 12] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm shown in Table 12] and cryptographic key sizes [assignment: cryptographic key sizes shown in Table 12] that meet the following: [assignment: standards shown in Table 12].

Table 12 : List of Cryptographic Operation

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

6.1.3 Class FDP: User data protection

FDP_ACC.1(a) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(a) The TSF shall enforce the [assignment: document access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects in Table 13].

Table 13 : List of Subjects, Objects, and Operations among Subjects and Objects (a)

| | |
|------------|--|
| Subjects | - Normal user process - MFP administrator process - Supervisor process |
| Objects | - Document data - User jobs |
| Operations | - Read - Modify - Delete |

FDP_ACC.1(b) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(b) The TSF shall enforce the [assignment: TOE function access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects in Table 14].

Table 14 : List of Subjects, Objects, and Operations among Subjects and Objects (b)

| | |
|-----------|---|
| Subjects | - Normal user process - Supervisor process |
| Object | - MFP application |
| Operation | - 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: document access control SFP] to objects based on the following: [assignment: subjects or objects, and their corresponding security attributes shown in Table 15].

Table 15 : Subjects, Objects and Security Attributes (a)

| Category | Subjects or Objects | Security Attributes |
|----------|---------------------------|---|
| Subject | Normal user process | - Login user name of normal user - User role |
| Subject | MFP administrator process | - User role |
| Subject | Supervisor process | - User role |
| Object | Document data | - Document data attribute - Document user list |
| Object | User job | - Login user name of normal user |

FDP_ACF.1.2(a) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules to control operations among subjects and objects shown in Table 16].

Table 16 : Rules to Control Operations on Document Data and User Jobs (a)

| Objects | Document Data Attributes | Operations | Subjects | Rules to control Operations |
|---------------|--------------------------|------------|---------------------|---|
| Document data | +PRT | Delete | Normal user process | Not allowed. However, it is allowed for normal user process that created the document data. |
| Document data | +PRT | Read | Normal user process | Not allowed. However, it is allowed for normal user process that created the document data. |

| Objects | Document Data Attributes | Operations | Subjects | Rules to control Operations |
|---------------|---------------------------------------|------------|---------------------|---|
| Document data | +SCN | Delete | Normal user process | Not allowed. However, it is allowed for normal user process that created the document data. |
| Document data | +SCN | Read | Normal user process | Not allowed. However, it is allowed for normal user process that created the document data. |
| Document data | +CPY | Delete | Normal user process | Not allowed. However, it is allowed for normal user process that created the document data. |
| Document data | +CPY | Read | Normal user process | Not allowed. However, it is allowed for normal user process that created the document data. |
| Document data | +DSR | Delete | Normal user process | Not allowed. However, it is allowed for normal user process with login user name of normal user registered on document user list for document data. |
| Document data | +DSR | Read | Normal user process | Not allowed. However, it is allowed for normal user process with login user name of normal user registered on document user list for document data. |
| Document data | +DSR | Modify | Normal user process | Not allowed. However, it is allowed for normal user process with login user name of normal user registered on document user list for document data. |
| User jobs | No setting of document data attribute | Delete | Normal user process | Not allowed. However, it is allowed for normal user process with login user name of normal user, which is the security attribute of user jobs. |

FDP_ACF.1.3(a) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules to control operations among subjects and objects shown in Table 17]**.

Table 17 : Additional Rules to Control Operations on Document Data and User Jobs (a)

| Objects | Document Data Attributes | Operations | Subjects | Rules to control Operations |
|---------------|--------------------------|------------|---------------------------|-----------------------------|
| Document data | +PRT | Delete | MFP administrator process | Allows. |
| Document data | +DSR | Delete | MFP administrator process | Allows. |

| | | | | |
|-----------|---------------------------------------|--------|---------------------------|---------|
| User jobs | No setting of document data attribute | Delete | MFP administrator process | Allows. |
|-----------|---------------------------------------|--------|---------------------------|---------|

FDP_ACF.1.4(a) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[assignment: deny the operations on the document data and user jobs in case of supervisor process]**.

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

Hierarchical to: No other components.

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

FDP_ACF.1.1(b) The TSF shall enforce the **[assignment: TOE function access control SFP]** to objects based on the following: **[assignment: subjects or objects, and their corresponding security attributes shown in Table 18]**.

Table 18 : Subjects, Objects and Security Attributes (b)

| Category | Subjects or Objects | Security Attributes |
|----------|---------------------|--|
| Subject | Normal user process | - Login user name of normal user - Available function list - User role |
| | Supervisor process | - User role |
| Object | MFP application | - Function type |

FDP_ACF.1.2(b) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[assignment: rule to control operations among objects and subjects shown in Table 19]**.

Table 19 : Rule to Control Operations on MFP Applications (b)

| Object | Operation | Subject | Rule to control Operations |
|-----------------|-----------|---------------------|--|
| MFP application | Execute | Normal user process | Allows executing MFP application which MFP administrator allowed in available function list 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 are permitted]**.

FDP_ACF.1.4(b) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[assignment: deny an operation on MFP application in case of supervisor process]**.

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.1.4 Class FIA: Identification and authentication**FIA_AFL.1 Authentication failure handling**

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [selection: an administrator configurable positive integer within [assignment: 1 to 5]] unsuccessful authentication attempts occur related to [assignment: the authentication events shown in Table 20].

Table 20 : List of Authentication Events

| Authentication Events |
|--|
| User authentication using the Operation Panel |
| User authentication using WIM from the client computer |
| User authentication when printing from the client computer |

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: met], the TSF shall [assignment: perform actions shown in Table 21].

Table 21 : List of Actions for Authentication Failure

| Unsuccessfully Authenticated Users | Actions for Authentication Failure |
|------------------------------------|---|
| Normal user | The lockout for the normal user is released by the lockout time set by the MFP administrator, or release operation by the MFP administrator. |
| Supervisor | The lockout for a supervisor is released by the lockout time set by the MFP administrator, release operation by the MFP administrator, or elapse of a given time after the TOE's restart. |
| MFP administrator | The lockout for the MFP administrator is released by the lockout time set by the MFP administrator, release operation by a supervisor, or elapse of a given time after the TOE's restart. |

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: **[assignment: the security attributes listed in Table 22 for each user in Table 22].**

Table 22 : List of Security Attributes for Each User That Shall Be Maintained

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

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

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

(1) Usable character and types:

Upper-case letters: [A-Z] (26 letters)

Lower-case letters: [a-z] (26 letters)

Numbers: [0-9] (ten digits)

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

(2) Registrable password length:

For normal users:

No fewer than the minimum character number specified by MFP administrator (8-32 characters) and no more than 128 characters.

For MFP administrators and a supervisor:

No fewer than the minimum character number specified by MFP administrator (8-32 characters) and no more than 32 characters.

(3) Rule:

Passwords that are composed of a combination of characters based on the password complexity setting specified by the MFP administrator can be registered. The MFP administrator specifies either Level 1 or Level 2 for password complexity setting.

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow **[assignment: the viewing of the list of user jobs, WIM Help, system status, counter and information of inquiries]** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only **[assignment: displaying dummy letters as authentication feedback on the Operation Panel]** to the user while the authentication is in progress.

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow **[assignment: the viewing of the list of user jobs, WIM Help, system status, counter and information of inquiries]** 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 other TSF-mediated actions on behalf of that user.

FIA_USB.1 User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **[assignment: login user name of normal user, login user name of MFP administrator, available function list, and user role]**.

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 23]**.

Table 23 : Rules for Initial Association of Attributes

| Users | Subjects | User Security Attributes |
|-------------------|---------------------------|--|
| Normal user | Normal user process | - Login user name of normal user - User role - Available function list |
| Supervisor | Supervisor process | - User role |
| MFP administrator | MFP administrator process | - Login user name of MFP administrator - User role |

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **[assignment: none]**.

6.1.5 Class FMT: Security management

FMT_MSA.1(a) Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1(a) The TSF shall enforce the **[assignment: document access control SFP]** to restrict the ability to **[selection: query, modify, delete, [assignment: newly create]]** the security attributes **[assignment: security attributes in Table 24]** to **[assignment: the user roles with operation permission in Table 24]**.

Table 24 : User Roles for Security Attributes (a)

| Security Attributes | Operations | User Roles with Operation Permission |
|--|-------------------------------------|---|
| Login user name of normal user | Query, modify, delete, newly create | MFP administrator |
| | Query | Normal user who owns the applicable login user name |
| Login user name of supervisor | Query, modify | Supervisor |
| Login user name of MFP administrator | Newly create | MFP administrator |
| | Query, modify | MFP administrator who owns the applicable login user name |
| | Query | Supervisor |
| Document data attribute | No operation permitted | None |
| Document user list [when document data attributes are (+PRT), (+SCN), and (+CPY)] | No operation permitted | None |
| Document user list [when document data attribute is (+DSR)] | Query, modify | MFP administrator, applicable normal user who created the document data |

FMT_MSA.1(b) Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1(b)The TSF shall enforce the [assignment: TOE function access control SFP] to restrict the ability to [selection: query, modify, delete, [assignment: newly create]] the security attributes [assignment: security attributes in Table 25] to [assignment: the user roles with operation permission in Table 25].

Table 25 : User Roles for Security Attributes (b)

| Security Attributes | Operations | User Roles with operation permission |
|--------------------------------|-------------------------------------|---|
| Login user name of normal user | Query, modify, delete, newly create | MFP administrator |
| | Query | Normal user who owns the applicable login user name |
| Available function list | Query, modify | MFP administrator |
| | Query | Applicable normal user |
| Function type | No operation permitted | None |
| User role | No operation permitted | None |

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: document access control SFP] to provide [selection: restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(a)The TSF shall allow the [assignment: authorised identified roles shown in Table 26] to specify alternative initial values to override the default values when an object or information is created.

Table 26 : Authorised Identified Roles Allowed to Override Default Values

| Objects | Security Attributes | Authorised Identified Roles |
|-----------------------------------|-------------------------|--------------------------------|
| Document data | Document data attribute | No authorised identified roles |
| Document data [when document data | Document user list | MFP administrator |

| Objects | Security Attributes | Authorised Identified Roles |
|---|--------------------------------|--------------------------------|
| attribute is (+DSR)] | | |
| Document data [when document data attributes are (+PRT), (+SCN), and (+CPY)] | Document user list | No authorised identified roles |
| User job | Login user name of normal user | No authorised identified roles |

FMT_MSA.3(b) Static attribute initialisation

Hierarchical to: No other components.

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

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

FMT_MSA.3.2(b)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.

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

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

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: query, modify, delete, [assignment: newly create]] the [assignment: list of TSF data in Table 27] to [assignment: the user roles in Table 27].

Table 27 : List of TSF Data

| TSF Data | Operations | User Roles |
|-------------------------------------|----------------------|---|
| Login password of normal user | Newly create, modify | MFP administrator |
| | Modify | Normal user who owns the login password |
| Login password of supervisor | Modify | Supervisor |
| Login password of MFP administrator | Modify | Supervisor |
| | Newly create | MFP administrator |
| | Modify | MFP administrator who owns the login password |
| Number of Attempts before Lockout | Query, modify | MFP administrator |
| Setting for Lockout Release Timer | Query, modify | MFP administrator |

| TSF Data | Operations | User Roles |
|--|-------------------------------------|-------------------------|
| Lockout time | Query, modify | MFP administrator |
| Date setting (year, month, day), time setting (hour, minute) | Query, modify | MFP administrator |
| | Query | Supervisor, normal user |
| Minimum character number | Query, modify | MFP administrator |
| Password complexity setting | Query, modify | MFP administrator |
| Operation Panel auto logout time | Query, modify | MFP administrator |
| WIM auto logout time | Query, modify | MFP administrator |
| Audit logs | Query, delete | MFP administrator |
| HDD cryptographic key | Newly create | MFP administrator |
| S/MIME user information | Newly create, modify, query, delete | MFP administrator |
| | Query | Normal user |
| Destination information for folder transmission | Newly create, modify, query, delete | MFP administrator |
| | Query | Normal user |
| User authentication method | Query | MFP administrator |
| IPsec setting information | Query, modify | MFP administrator |
| Device Certificate | Modify | MFP administrator |

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **[assignment: management functions shown in Table 28]**.

Table 28 : List of Specification of Management Functions

| Management Functions |
|--|
| New creation, query, modification, and deletion of the login user name of normal user by MFP administrator |
| Query of own login user name by normal user |
| Query and modification of login user name of supervisor by supervisor |
| New creation of login user name of MFP administrator by MFP administrator |
| Query and modification of own login user name by MFP administrator |
| Query of login user name of MFP administrator by supervisor |
| New creation and modification of login password of normal user by MFP administrator |
| Modification of own login password by normal user |

| Management Functions |
|--|
| Modification of login password of supervisor by supervisor |
| Modification of login password of MFP administrator by supervisor |
| New creation of login password of MFP administrator by MFP administrator |
| Modification of own login password by MFP administrator |
| Query and modification of minimum character number by MFP administrator |
| Query and modification of Password Complexity by MFP administrator |
| Query and modification of Operation Panel auto logout time by MFP administrator |
| Query and modification of WIM auto logout time by MFP administrator |
| Query and modification of Number of Attempts before Lockout by MFP administrator |
| Query and modification of Lockout Release Timer Setting by MFP administrator |
| Query and modification of lockout time by MFP administrator |
| Query and modification of document user list by MFP administrator |
| Query and modification of document user list by the normal user who created the document |
| Query and modification of available function list by MFP administrator |
| Query of own available function list by normal user |
| Query and modification of default values of the document user list by MFP administrator |
| Query and modification of date and time by MFP administrator |
| Query of date and time by supervisor |
| Query of date and time by normal user |
| Query and deletion of audit logs by MFP administrator |
| New creation of HDD encryption key by MFP administrator |
| New creation, query, modification and deletion of S/MIME user information by MFP administrator |
| Query of S/MIME user information by normal user |
| New creation, query, modification and deletion of destination information for folder transmission by MFP administrator |
| Query of destination information for folder transmission by normal user |
| Query of user authentication method by MFP administrator |
| Query and modification of IPsec setting information by MFP administrator |
| Modification of Device Certificate by MFP administrator |

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [**assignment: normal user, supervisor, and MFP administrator**].

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

6.1.6 Class FPT: Protection of the TSF

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

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

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to: No other components.

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

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

6.1.7 Class FTA: TOE access

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [**assignment: lapse of Operation Panel auto logout time, lapse of WIM auto logout time, and completion of document data reception from the printer driver**].

6.1.8 Class FTP: Trusted path/channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

- FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
- FTP_ITC.1.2 The TSF shall permit [selection: the TSF, another trusted IT product] to initiate communication via the trusted channel.
- FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: communication via the LAN of document data, function data, protected data, and confidential data].

6.2 Security Assurance Requirements

The evaluation assurance level of this TOE is EAL2+ALC_FLR.2. Table 29 lists the assurance components of the TOE. ALC_FLR.2 was added to the set of components defined in evaluation assurance level 2 (EAL2).

Table 29 : TOE Security Assurance Requirements (EAL2+ALC_FLR.2)

| Assurance Classes | Assurance Components | |
|------------------------------------|----------------------|---|
| ADV: Development | ADV_ARC.1 | Security architecture description |
| | ADV_FSP.2 | Security-enforcing functional specification |
| | ADV_TDS.1 | Basic design |
| AGD: Guidance documents | AGD_OPE.1 | Operational user guidance |
| | AGD_PRE.1 | Preparative procedures |
| ALC: Life-cycle support | ALC_CMC.2 | Use of a CM system |
| | ALC_CMS.2 | Parts of the TOE CM coverage |
| | ALC_DEL.1 | Delivery procedures |
| | 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.1 | Evidence of coverage |
| | ATE_FUN.1 | Functional testing |
| | ATE_IND.2 | Independent testing - sample |
| AVA: Vulnerability assessment | AVA_VAN.2 | Vulnerability analysis |

6.3 Security Requirements Rationale

This section describes the rationale for security requirements.

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

6.3.1 Tracing

Table 30 shows the relationship between the TOE security functional requirements and TOE security objectives. Table 30 shows that each TOE security functional requirement fulfils at least one TOE security objective.

Table 30 : Relationship between Security Objectives and Functional Requirements

| | O.DOC.NO_DIS | O.DOC.NO_ALT | O.FUNC.NO_ALT | O.PROT.NO_ALT | O.CONF.NO_DIS | O.CONF.NO_ALT | O.USER.AUTHORIZED | O.INTERFACE.MANAGED | O.SOFTWARE.VERIFIED | O.AUDIT.LOGGED | O.STORAGE.ENCRYPTED |
|--------------|--------------|--------------|---------------|---------------|---------------|---------------|-------------------|---------------------|---------------------|----------------|---------------------|
| FAU_GEN.1 | | | | | | | | | | X | |
| FAU_GEN.2 | | | | | | | | | | X | |
| FAU_STG.1 | | | | | | | | | | X | |
| FAU_STG.4 | | | | | | | | | | X | |
| FAU_SAR.1 | | | | | | | | | | X | |
| FAU_SAR.2 | | | | | | | | | | X | |
| FCS_CKM.1 | | | | | | | | | | | X |
| FCS_COP.1 | | | | | | | | | | | X |
| FDP_ACC.1(a) | X | X | X | | | | | | | | |
| FDP_ACC.1(b) | | | | | | | X | | | | |
| FDP_ACF.1(a) | X | X | X | | | | | | | | |
| FDP_ACF.1(b) | | | | | | | X | | | | |
| FDP_RIP.1 | X | X | | | | | | | | | |
| FIA_AFL.1 | | | | | | | X | | | | |
| FIA_ATD.1 | | | | | | | X | | | | |
| FIA_SOS.1 | | | | | | | X | | | | |
| FIA_UAU.1 | | | | | | | X | X | | | |

| | O.DOC.NO_DIS | O.DOC.NO_ALT | O.FUNC.NO_ALT | O.PROT.NO_ALT | O.CONF.NO_DIS | O.CONF.NO_ALT | O.USER.AUTHORIZED | O.INTERFACE.MANAGED | O.SOFTWARE.VERIFIED | O.AUDIT.LOGGED | O.STORAGE.ENCRYPTED |
|---------------|--------------|--------------|---------------|---------------|---------------|---------------|-------------------|---------------------|---------------------|----------------|---------------------|
| FIA_UAU.7 | | | | | | | X | | | | |
| FIA_UID.1 | | | | | | | X | X | | | |
| FIA_USB.1 | | | | | | | X | | | | |
| FPT_FDI_EXP.1 | | | | | | | | X | | | |
| FMT_MSA.1(a) | X | X | X | | | | | | | | |
| FMT_MSA.1(b) | | | | | | | X | | | | |
| FMT_MSA.3(a) | X | X | X | | | | | | | | |
| FMT_MSA.3(b) | | | | | | | X | | | | |
| FMT_MTD.1 | | | | X | X | X | | | | | X |
| FMT_SMF.1 | | | | X | X | X | | | | | X |
| FMT_SMR.1 | | | | X | X | X | | | | | X |
| FPT_STM.1 | | | | | | | | | | X | |
| FPT_TST.1 | | | | | | | | X | | | |
| FTA_SSL.3 | | | | | | | X | X | | | |
| FTP_ITC.1 | X | X | X | X | X | X | | | | | |

6.3.2 Justification of Traceability

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

O.DOC.NO_DIS Protection of document disclosure

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

- (1) Specify and implement the access control to the document data.

FDP_ACC.1(a) and FDP_ACF.1(a) only allow the following persons to view document data according to the document data attributes: the normal user who generated the document data or the normal user who is registered on the document user list of the document data. The MFP administrator and supervisor are not allowed to view document data.

-
- (2) Prevent reading the deleted documents, temporary documents and their fragments.
Deleted documents, temporary documents and their fragments are prevented from being read by FDP_RIP.1.
 - (3) Use trusted channels for sending or receiving document data.
The document data sent and received by the TOE via the LAN are protected by FTP_ITC.1.
 - (4) Management of the security attributes.
FMT_MSA.1(a) specifies the available operations (newly create, query, modify and delete) on the login user name, and available operations (query and modify) on the document user list, and a specified user is thus restricted to perform each operation.
FMT_MSA.3(a) surely sets the restrictive value to the security attributes of document data (object) when document data are generated.
- By satisfying FDP_ACC.1(a), FDP_ACF.1(a), FDP_RIP.1, FTP_ITC.1, FMT_MSA.1(a) and FMT_MSA.3(a), which are the security functional requirements for these countermeasures, O.DOC.NO_DIS is fulfilled.

O.DOC.NO_ALT Protection of document alteration

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

- (1) Specify and implement the access control to document data.
FDP_ACC.1(a) and FDP_ACF.1(a) allow the following persons to modify and delete document data according to the document data attributes: the normal user who generated the document data or the normal user who is registered in the document user list of the document data. The MFP administrator is allowed to delete document data, but is not allowed to modify document data. The supervisor is not allowed to modify and delete document data.
- (2) Prevent deleting the deleted documents, temporary documents and their fragments.
Deleted documents, temporary documents and their fragments are prevented from being used by FDP_RIP.1.
- (3) Use trusted channels for sending or receiving document data.
The document data sent and received by the TOE via the LAN interface are protected by FTP_ITC.1.
- (4) Management of the security attributes.
FMT_MSA.1(a) specifies the available operations (newly create, query, modify and delete) on the login user name, and available operations (query and modify) on the document user list, and a specified user is thus restricted to perform each operation.
FMT_MSA.3(a) surely sets the restrictive value to the security attributes of document data (object) when the document data are generated.

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

O.FUNC.NO_ALT Protection of user job alteration

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

- (1) Specify and implement the access control to user jobs.
FDP_ACC.1(a) and FDP_ACF.1(a) allow the MFP administrator to delete user jobs, and the normal user with the permission to delete the applicable user job. The supervisor is not allowed to delete user jobs. Deletion is the only modification operation on this TOE's user jobs.
- (2) Use trusted channels for sending or receiving user jobs.
The user jobs sent and received by the TOE via the LAN are protected by FTP_ITC.1.
- (3) Management of the security attributes.
FMT_MSA.1(a) restricts each available operation (newly create, query, modify and delete) for the login user name to specified users only.
FMT_MSA.3(a) sets the restrictive value to the security attributes of user jobs (object) when the user jobs are generated.

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

O.PROT.NO_ALT Protection of TSF protected data alteration

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

- (1) Management of the TSF protected data.
By FMT_MTD.1, only the MFP administrator is allowed to manage the minimum character number, password complexity setting, Number of Attempts before Lockout, settings for Lockout Release Timer, lockout time, date, time, S/MIME user information, destination folder, IPsec setting information, Device Certificate, Operation Panel auto logout time, WIM auto logout time, and user authentication method.
- (2) Specification of the Management Function.
FMT_SMF.1 performs the required Management Functions for Security Function.
- (3) Specification of the roles.
FMT_SMR.1 maintains the users who have the privileges.
- (4) Use trusted channels for sending or receiving the TSF protected data.
The TSF protected data sent and received by the TOE via the LAN are protected by FTP_ITC.1.

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

O.CONF.NO_DIS Protection of TSF confidential data disclosure

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

-
- (1) Management of the TSF confidential data.

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

- (2) Specification of the Management Function.

FMT_SMF.1 performs the required Management Functions for Security Function.

- (3) Specification of the roles.

FMT_SMR.1 maintains the users who have the privileges.

- (4) Use trusted channels for sending or receiving TSF confidential data.

The TSF confidential data sent and received by the TOE via the LAN are protected by FTP_ITC.1.

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

O.CONF.NO_ALT Protection of TSF confidential data alteration

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

- (1) Management of the TSF confidential data.

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

- (2) Specification of the Management Function.

FMT_SMF.1 performs the required Management Functions for Security Function.

- (3) Specification of the roles.

FMT_SMR.1 maintains the users who have the privileges.

- (4) Use trusted channels for sending or receiving TSF confidential data.

The TSF confidential data sent and received by the TOE via the LAN are protected by FTP_ITC.1.

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

O.USER.AUTHORIZED User identification and authentication

O.USER.AUTHORIZED is the security objective to restrict users in accordance with the security policies so that only valid users can use the TOE functions. As for normal users, the MFP administrator, and a supervisor, who all access the TOE from the Operation Panel or from the client PC over a network, the security policies of the authentication failure handling and verification of secrets need to be augmented. To fulfil this security objective, it is required to implement the following countermeasures.

-
- (1) Identify and authenticate the users prior to the TOE use.
FIA_UID.1 and FIA_UAU.1 identify and authenticate the persons who attempt to use the TOE from the Operation Panel or client computer on the network.
 - (2) Allow the successfully identified and authenticated user to use the TOE.
FIA_ATD.1 and FIA_USB.1 manage the access procedures to the protected assets of the users who are defined in advance, and associate the users who are successfully identified and authenticated with the access procedures.
FDP_ACC.1(b) and FDP_ACF.1(b) allow the applicable normal user to use the MFP application according to the operation permission granted to the successfully identified and authenticated normal user.
 - (3) Complicate decoding of login password.
FIA_UAU.7 displays dummy letters as authentication feedback on the Operation Panel and prevents the login password from disclosure.
FIA_SOS.1 accepts only passwords that satisfy the minimum character number and password character combination specified by the MFP administrator, and makes it difficult to guess the password.
FIA_AFL.1 does not allow the user who is unsuccessfully authenticated for certain times to access to the TOE for certain period.
 - (4) Terminate login automatically.
FTA_SSL.3 automatically logs out of the Operation Panel or the client computer at the state of being logged in. It also logs out the status of document data reception after the completion of document data reception from the printer driver.
 - (5) Management of the security attributes.
According to FMT_MSA.1(b), the login user name and available function list of normal user are managed by the MFP administrator, and users are not allowed to operate the function type.
FMT_MSA.3(b) sets the restrictive default value to the function type.
By satisfying FDP_ACC.1(b), FDP_ACF.1(b), FIA_UID.1, FIA_UAU.1, FIA_ATD.1, FIA_USB.1, FIA_UAU.7, FIA_AFL.1, FIA_SOS.1, FTA_SSL.3, FMT_MSA.1(b) and FMT_MSA.3(b), which are the security functional requirements for these countermeasures, O.USER.AUTHORIZED is fulfilled.
The function for 2600.2-SMI (F.SMI), selected SFR Package from the PP, is used in conjunction with the function whose access control is enforced by FDP_ACC.1(b) and FDP_ACF.1(b). Therefore, the access control for F.SMI is included with the access control by FDP_ACC.1(b) and FDP_ACF.1(b) and fulfilled.

O.INTERFACE.MANAGED Management of external interfaces by TOE

O.INTERFACE.MANAGED is the security objective to ensure that the TOE manages the operation of external interface according to the security policy. To fulfil this security objective, it is required to implement the following countermeasures.

- (1) Identify and authenticate the users prior to use the Operation Panel and LAN interface.
FIA_UID.1 identifies the persons who attempt to use the TOE from the Operation Panel or client computer on the network, and FIA_UAU.1 authenticates the identified users.
- (2) Automatically terminate the connection to the Operation Panel and LAN interface.
FTA_SSL.3 terminates the session after no operation is performed from the Operation Panel or LAN interface for certain period.

-
- (3) Restricted forwarding of data to external interfaces.

FPT_FDI_EXP.1 prevents the data received from the Operation Panel and LAN interface from being transmitted from the LAN without further processing by the TSF.

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

O.SOFTWARE.VERIFIED Software verification

O.SOFTWARE.VERIFIED is the security objective to ensure that the TOE provides procedures to self-verify executable code in the TSF. To fulfil this security objective, it is required to implement the following countermeasures.

- (1) Self-check

FPT_TST.1 checks if the MFP Control Software is verified software at the start-up.

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

O.AUDIT.LOGGED Management of audit log records

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

- (1) Record the audit log.

FAU_GEN.1 and FAU_GEN.2 record the events, which should be auditable, with the identification information of the occurrence factor.

- (2) Protect the audit log.

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

- (3) Provide Audit Function.

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

- (4) Reliable occurrence time of the event

FPT_STM.1 provides a trusted time stamp, and a reliable record of the times when events occurred are recorded in the audit log.

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

O.STORAGE.ENCRYPTED Encryption of storage devices

O.STORAGE.ENCRYPTED is the security objective to ensure the data to be written into the HDD is encrypted. To fulfil this security objective, it is required to implement the following countermeasures.

- (1) Generate appropriate cryptographic keys.

FCS_CKM.1 generates the cryptographic key for encryption.

- (2) Perform cryptographic operation.
FCS_COP.1 encrypts the data to be stored in the HDD, and decrypts the data to be read from the HDD.
- (3) Manage the TSF data.
FMT_MTD.1 allows the MFP administrator to manage the cryptographic keys.
- (4) Specification of Management Function.
FMT_SMF.1 performs the required Management Functions for Security Function.
- (5) Specification of the roles.
FMT_SMR.1 maintains the users who have the privileges.

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

6.3.3 Dependency Analysis

Table 31 shows the result of dependency analysis in this ST for the TOE security functional requirements.

Table 31 : Results of Dependency Analysis of TOE Security Functional Requirements

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

| TOE Security Functional Requirements | Claimed Dependencies | Dependencies Satisfied in ST | Dependencies Not Satisfied in ST |
|--------------------------------------|--|--|----------------------------------|
| FIA_AFL.1 | FIA_UAU.1 | FIA_UAU.1 | None |
| FIA_ATD.1 | None | None | None |
| FIA_SOS.1 | None | None | None |
| FIA_UAU.1 | FIA_UID.1 | FIA_UID.1 | None |
| FIA_UAU.7 | FIA_UAU.1 | FIA_UAU.1 | None |
| FIA_UID.1 | None | None | None |
| FIA_USB.1 | FIA_ATD.1 | FIA_ATD.1 | None |
| FPT_FDI_EXP.1 | FMT_SMF.1 FMT_SMR.1 | FMT_SMF.1 FMT_SMR.1 | None |
| FMT_MSA.1(a) | [FDP_ACC.1(a) or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1 | FDP_ACC.1(a) FMT_SMR.1 FMT_SMF.1 | None |
| FMT_MSA.1(b) | [FDP_ACC.1(b) or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1 | FDP_ACC.1(b) FMT_SMR.1 FMT_SMF.1 | None |
| FMT_MSA.3(a) | FMT_MSA.1(a) FMT_SMR.1 | FMT_MSA.1(a) FMT_SMR.1 | None |
| FMT_MSA.3(b) | FMT_MSA.1(b) FMT_SMR.1 | FMT_MSA.1(b) FMT_SMR.1 | None |
| FMT_MTD.1 | FMT_SMR.1 FMT_SMF.1 | FMT_SMR.1 FMT_SMF.1 | None |
| FMT_SMF.1 | None | None | None |
| FMT_SMR.1 | FIA_UID.1 | FIA_UID.1 | None |
| FPT_STM.1 | None | None | None |
| FPT_TST.1 | None | None | None |
| FTA_SSL.3 | None | None | None |
| FTP_ITC.1 | None | None | None |

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

Rationale for Removing Dependencies on FCS_CKM.4

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

6.3.4 Security Assurance Requirements Rationale

This TOE is the MFP, which is a commercially available product. The MFP is assumed that it will be used in a general office and this TOE does not assume the attackers with Enhanced-Basic or higher level of attack potential.

The evaluation of the TOE design (ADV_TDS.1) is adequate to show the validity of commercially available products. A high attack potential is required for the attacks that circumvent or tamper with the TSF, which is not covered in this evaluation. Dealing with attacks performed by an attacker possessing Basic attack potential (AVA_VAN.2) is therefore adequate for general needs.

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

Based on the terms and costs of the evaluation, the evaluation assurance level of EAL2+ALC_FLR.2 is appropriate for this TOE.

7 TOE Summary Specification

This section describes the TOE summary specification for each security function. The security functions are described for each corresponding security functional requirement.

7.1 Audit Function

The Audit Function is to generate the audit log of TOE use and security-relevant events (hereafter, "audit events"). This function provides the recorded audit log in a legible fashion for users to audit (audit log review). The recorded audit log can be viewed and deleted only by the MFP administrator.

FAU_GEN.1 and FAU_GEN.2

The TOE records the audit log items, shown in Table 33, on the HDD in the TOE when audit events shown in Table 32 occur.

Audit log items include basic log items and expanded log items. Basic log items are recorded whenever audit logs are recorded, and expanded log items are recorded only when audit events occur and the audit log items shown in Table 33 are recorded.

FPT_STM.1

The date (year/month/day) and time (hour/minute/second) the TOE records for the audit log are derived from the system clock of the TOE.

FAU_SAR.1, FAU_SAR.2, and FAU_STG.1

The TOE displays the operation menu for audit logs to be read on WIM screen only when it is accessed by the MFP administrator. The TOE provides the audit logs in a text format when the MFP administrator instructs the TOE to read the audit logs.

FAU_STG.4

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

Table 32 : List of Audit Events

| Audit Events |
|---|
| Start-up of the Audit Function |
| Shutdown of the Audit Function |
| Success and failure of login operations |
| Starting and releasing Lockout |
| Table 28 Record of Management Function |
| Date settings (year/month/day), time settings (hour/minute) |

| Audit Events |
|--|
| Termination of session by auto logout |
| Failure of WIM communication |
| Folder transmission |
| E-mail transmission of attachments |
| Printing via networks |
| Creating (storing) document data |
| Successful completion of creating (duplicating) document data |
| Reading document data (print, download, e-mail transmission of attachments, and folder transmission) |
| Completion of modifying (editing) document data |
| Deleting document data |

Table 33 : List of Audit Log Items

| | Audit Log Items | Setting Values of Audit Log Items | Audit Events to record Audit Logs |
|--------------------|---------------------------------------|---|---|
| Basic Log Items | Starting date/time of an event | Values of the TOE system clock at an event occurrence | - All auditable events shown in Table 32 |
| | Ending date/time of an event | Values of the TOE system clock at an event termination | |
| | Event types | Audit event identity | |
| | Subject identity | User or TOE identity for an audit event caused by the user or TOE | |
| | Outcome (*1) | Audit event outcome (success or failure) | |
| Expanded Log Items | Communication directions | Communication directions (IN/OUT) | - WIM communication |
| | Communicating IP address | Communicating IP address | - WIM communication - Folder transmission - Printing via networks |
| | Communicating e-mail address | Communicating e-mail address for e-mail transmission of attachments | - E-mail transmission of attachments |
| | Lockout operation type | Information to identify starting Lockout and releasing Lockout | - Starting and releasing Lockout |
| | Locked out User | Login user name of a user who is locked out | - Starting and releasing Lockout |
| | Locked out User who is to be released | Login user name of a user who is released from Lockout | - Starting and releasing Lockout |

(*1): If an audit event is "Failure of WIM communication", the failure will be recorded as a result.

7.2 Identification and Authentication Function

The Identification and Authentication Function is to verify whether persons who intend to use the TOE are authorised users (MFP administrator, supervisor, and normal users) by referring to the identification and authentication information obtained from the users, so that only persons who are confirmed as authorised users are allowed to use the TOE. Verification methods for normal users include those by Basic Authentication and External Authentication.

FIA_UAU.1 and FIA_UID.1

The TOE identifies and authenticates a user by checking the login user name and login password entered by the user. However, regarding the viewing of user job lists, WIM Help, system status, the counter and information of inquiries, the TOE identification and authentication is not required for the use of the TOE.

When a user uses the Operation Panel, or uses WIM from the client computer, the screen for the user to enter his or her login user name and login password is displayed, and this screen will be displayed until the entry of the login user name and login password is complete.

When the TOE is used from the printer driver, the TOE receives the login user name and login password entered from each driver by a user.

When the entered login user name is the login user name of a normal user, MFP administrator, or supervisor, the TOE checks if the entered login password match with the one pre-registered in the TOE.

FIA_USB.1, FIA_ATD.1, and FMT_SMR.1

If a user is identified and authenticated as a result of checking FIA_UAU.1 and FIA_UID.1, the use of the TOE by the user is allowed as the identified user role (normal user, MFP administrator, or supervisor). The user role assigned to the user at login will be maintained until the user logs out. If user identification and authentication fails, use of the TOE is denied.

FTA_SSL.3

If a user has been logged on to the TOE from the Operation Panel, a Web browser, and printer driver, the user will be logged out of the TOE when the conditions shown below are met.

In case of the Operation Panel, the user is logged out of the TOE when the time that elapses since his or her final operation on the Operation Panel reaches Operation Panel auto logout time (10 to 999 seconds).

In case of a Web browser, the user is logged out of the TOE when the time that elapses since his or her final operation on a Web browser reaches WIM auto logout time (3 to 60 minutes).

In case of printer driver, the user is logged out of the TOE immediately after receiving the print data from the printer driver.

FIA_UAU.7

Regarding login passwords entered by a person who intends to use the TOE from the Operation Panel or by a person who intends to use WIM from the client computer, the TOE does not display the entered login password but it displays a sequence of dummy characters whose length is the same as that of the entered password.

FIA_AFL.1

The TOE counts the number of identification and authentication attempts that consecutively result in failure using the login user name of a normal user, MFP administrator, or supervisor. The TOE locks out the login user name if the number of consecutive login failures exceeds the number of attempts before lockout.

If a user name is locked out, the user with that user name is not allowed to log in unless any of the following conditions is fulfilled.

- The lockout time set by the MFP administrator elapses.
- An "unlocking administrator" shown in Table 34 and specified for each user role releases the lockout.
- In case of the MFP administrator and supervisor, sixty seconds elapse since the MFP becomes executable after its power is turned off and then on.

Table 34 : Unlocking Administrators for Each User Role

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

FIA_SOS.1

Login passwords for users can be registered only if these passwords meet the following conditions:

(1) Usable characters and types:

Upper-case letters: [A-Z] (26 letters)

Lower-case letters: [a-z] (26 letters)

Numbers: [0-9] (ten digits)

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

(2) Registrable password length:

- For normal users

No less than the minimum character number for password (8-32 characters) specified by the MFP administrator and no more than 128 characters.

- For MFP administrators and a supervisor

No less than the minimum character number for password (8-32 characters) specified by the MFP administrator and no more than 32 characters.

(3) Combination of character types:

The number of combined character types specified by the MFP administrators (two types or more, or three types or more).

FPT_FDI_EXP.1

The TOE inputs information after the TSF reliably identifies and authenticates the input information from the Operation Panel or the client computer via LAN interface. Therefore, the input information cannot be forwarded unless the TSF is not involved in information identification and authentication.

7.3 Document Access Control Function

The Document Access Control Function is to allow authorised TOE users to operate document data and user jobs in accordance with the provided user role privilege or user privilege.

FDP_ACC.1(a) and FDP_ACF.1(a)

The TOE controls user operations for document data and user jobs in accordance with (1) access control rule on document data and (2) access control rule on user jobs.

(1) Access control rule on document data

The TOE provides users with the interface for stored documents to be printed, downloaded to the client computers, sent by e-mail as attachments, sent to folders, duplicated, edited, and deleted. The interface enables users to delete all the stored documents. Duplication is the function to newly create and store the document data identical to Document Server documents. Editing is the function to insert a Document Server document into any page of another Document Server document and to delete any page of a Document Server document.

Users authorised to operate stored documents are MFP administrator and normal users. The supervisor is not allowed to operate stored documents.

When the MFP administrator or a normal user logs on to the TOE from the Operation Panel or to WIM from the client computer, the TOE displays a list of the stored documents whose operations are authorised and the menu for the authorised operations (printing, downloading to the client computers, sending by e-mail as attachments, sending to folders, duplicating, editing, deleting, and deleting all files). When the MFP administrator logs on to the TOE from the Operation Panel or to WIM from the client computer, the TOE displays a list of all the stored documents and the operation menu for deletion and deletion of all files. The MFP administrator can select and delete a document from the list of the stored documents or all documents.

Document user lists are set for stored documents. The login user names of normal users who are allowed to operate the stored documents are registered with the document user lists. A document user list is set for each stored document and it includes normal users who have been granted permission to operate the stored document. When a normal user logs on to the TOE from the Operation Panel or to WIM from the client computer, the TOE displays a list of the stored documents whose document user lists include the logged-in normal user, and an operation menu according to the rules shown in Table 35. The privileges that allow users to edit the document user list are shown in "7.8 Security Management Function".

Also, the TOE allows only the user job owner to view and delete the document data handled as a user job while Copy Function, Printer Function, Scanner Function, or Document Server Function is being used.

While no interface to change job owners is provided, an interface to cancel user jobs is provided. If a user job is cancelled, any document the cancelled job operates will be deleted.

Table 35 : Stored Documents Access Control Rules for Normal Users

| I/F to be Used | Available Functions for Users | Types of Stored Documents displayed in the List | Operations displayed on the Menu |
|-----------------|-------------------------------|---|--|
| Operation Panel | Document Server Function | Document Server documents | Print Duplicate Edit Delete |
| Operation Panel | Printer Function | Printer documents | Print Delete |
| Operation Panel | Scanner Function | Scanner documents | E-mail transmission of attachments Folder transmission Delete |
| Web browser | Document Server Function | Document Server documents | Print Delete |
| Web browser | Document Server Function | Scanner documents | E-mail transmission of attachments Folder transmission Download Delete (E-mail transmission of attachments and folder transmission are authorised for normal users who are privileged to use Scanner Function) |
| Web browser | Printer Function | Printer documents | Print Delete |

* The privileges to use available functions are shown in "7.4 Use-of-Feature Restriction Function".

(2) Access control rule on user jobs

The TOE displays on the Operation Panel a menu to cancel a user job only if the user who logs in from the Operation Panel is a user job owner or MFP administrator and a cancellation of a user job is attempted by the owner or MFP administrator. Other users are not allowed to operate user jobs.

When a user job is cancelled, any documents operated by the cancelled job will be deleted.

However, if the document data operated by the cancelled user job is a stored document, the data will not be deleted and remain stored in the TOE.

7.4 Use-of-Feature Restriction Function

The Use-of-Feature Restriction Function is to authorise TOE users to use Copy Function, Printer Function, Scanner Function, and Document Server Function in accordance with the roles of the identified and authenticated TOE users and user privileges set for each user.

FDP_ACC.1(b) and FDP_ACF.1(b)

The TOE verifies the role for an authorised TOE user who attempts to start operating Copy Function, Printer Function, Scanner Function, and Document Server Function.

If the role is that of normal user, the user can operate only functions that are included in the available function list set for each normal user.

If the role is that of supervisor, using any functions is not allowed.

7.5 Network Protection Function

The Network Protection Function is to provide network monitoring to prevent information leakage when LAN is used and to detect data tampering.

FTP_ITC.1

The encrypted communications provided by the TOE differ depending on communicating devices. Table 36 shows the encrypted communications provided by the TOE.

Table 36 : Encrypted Communications Provided by the TOE

| Communicating Devices | Encrypted communications provided by the TOE | |
|-----------------------|--|---|
| | Protocols | Cryptographic Algorithms |
| Client computer | TLS1.0, TLS1.1, TLS1.2 | AES(128bits, 256bits) |
| FTP server | IPsec | AES(128bits, 192bits, 256bits), 3DES(168bits) |
| SMB server | IPsec | AES(128bits, 192bits, 256bits), 3DES(168bits) |
| SMTP server | S/MIME | AES(128bits, 256bits) |

7.6 Residual Data Overwrite Function

The Residual Data Overwrite Function is to overwrite specific patterns on the HDD and disable the reusing of the residual data included in the deleted documents, temporary documents and their fragments on the HDD.

FDP_RIP.1

Methods to delete the HDD area through overwriting include sequential overwriting and batch overwriting. For sequential overwriting, the TOE constantly monitors the information on a residual data area, and overwrites the area if any existing residual data is discovered. If the user deletes document data, the TOE applies the method specified by the MFP administrator and overwrites the area on the HDD where the digital image data of the document data is stored. Also, when a user job is complete, the TOE applies the method specified by the MFP administrator and overwrites the area on the HDD where temporary documents that are

created while a user job is executed or the fragments of those temporary documents are stored. Sequential overwriting methods include NSA, DoD, and random number methods.

For batch overwriting, the TOE collectively overwrites the HDD with the method specified by the MFP administrator. Batch overwriting methods include NSA, DoD, random number, BSI/VSITR, and Secure Erase methods.

NSA method overwrites twice by random numbers and once by Null(0). The DoD method overwrites once by a certain value, once by its complement, and further by random numbers to be verified afterwards. Random number method overwrites for three to nine times by random numbers. The MFP administrator specifies the number of times to overwrite when the TOE is installed. The BSI/VSITR method overwrites data by 00, FF, 00, FF, 00, FF, AA in this order. The Secure Erase method overwrites data using the ATA command "secure erase".

Since the Residual Data Overwrite Function is used in combination with Stored Data Protection Function in this ST, all values that overwrite the HDD using sequential overwriting will be encrypted.

7.7 Stored Data Protection Function

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

FCS_CKM.1 and FCS_COP.1

The TOE encrypts data before writing it on the HDD, and decrypts the encrypted data after reading it from the HDD. This process is applied to all data written on and read from the HDD. Detailed cryptographic operations are shown in Table 37.

Table 37 : List of Cryptographic Operations for Stored Data Protection

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

Following operations by the MFP administrator, the TOE generates a cryptographic key. If a login user is the MFP administrator, the screen to generate an HDD cryptographic key is provided from the Operation Panel.

If the MFP administrator gives instructions to generate an HDD cryptographic key from the Operation Panel, the TOE uses a genuine random number generator and generates random numbers that conform to the standard NIST SP 800-90A.

7.8 Security Management Function

The Security Management Function consists of functions to 1) control operations for TSF data, 2) maintain user roles assigned to normal users, MFP administrator, or supervisor to operate the Security Management

Function, and 3) set appropriate default values to security attributes, all of which accord with user role privileges or user privileges that are assigned to normal users, MFP administrator, or supervisor.

FMT_MSA.1(a), FMT_MSA.1(b), FMT_MSA.3(a), FMT_MTD.1, FMT_SMF.1 and FMT_SMR.1

The TOE allows operations for TSF data according to the rules described in Table 38.

Table 38 : Management of TSF Data

| TSF Data | Operation Interface | Operations | Users |
|--|-----------------------------------|--|---|
| Login user names of normal users | Operation Panel, Web browser | Newly create, query, modify, delete | MFP administrator |
| | | Query | Applicable normal user |
| Login user name of supervisor | Operation Panel, Web browser | Query, modify | Supervisor |
| Login user name of MFP administrator | Operation Panel, Web browser | Newly create | MFP administrator |
| | | Query, modify | Applicable MFP administrator |
| | | Query | Supervisor |
| Document data attributes | No operation interfaces available | No operations allowed | None |
| Document user list Stored document types are Document Server document, scanner document, and printer document (with stored print) | Operation Panel, Web browser | Query, modify | MFP administrator, applicable normal user who stored the document |
| Default values of the document user list | Operation Panel, Web browser | Query, modify | MFP administrator |
| Available function list | Operation Panel, Web browser | Query, modify | MFP administrator |
| | Web browser | Query | Applicable normal user |
| Function types | No operation interfaces available | No operations allowed | None |
| User roles | No operation interfaces available | No operations allowed | None |
| Login passwords of normal users | Operation Panel, Web browser | Newly create, modify | MFP administrator |
| | | Modify | Applicable normal user |

| TSF Data | Operation Interface | Operations | Users |
|--------------------------------------|---------------------------------|--|------------------------------|
| Login password of supervisor | Operation Panel, Web browser | Modify | Supervisor |
| Login password of MFP administrator | Operation Panel, Web browser | Modify | Supervisor |
| | | Newly create | MFP administrator |
| | | Modify | Applicable MFP administrator |
| Number of Attempts before Lockout | Operation Panel, Web browser | Query, modify | MFP administrator |
| Settings for Lockout Release Timer | Web browser | Query, modify | MFP administrator |
| Lockout time | Web browser | Query, modify | MFP administrator |
| Date settings (year/month/day) | Operation Panel, Web browser | Query, modify | MFP administrator |
| | | Query | Supervisor, normal user |
| Time | Operation Panel, Web browser | Query, modify | MFP administrator |
| | | Query | Supervisor, normal user |
| Minimum character number of password | Operation Panel | Query, modify | MFP administrator |
| Password complexity setting | Operation Panel | Query, modify | MFP administrator |
| Operation Panel auto logout time | Operation Panel | Query, modify | MFP administrator |
| WIM auto logout time | Web browser | Query, modify | MFP administrator |
| Audit log | Web browser | Query, delete | MFP administrator |
| | Operation Panel | Delete | MFP administrator |
| HDD cryptographic key | Operation Panel | Newly create | MFP administrator |
| S/MIME user information | Operation Panel, Web browser | Newly create, modify, query, delete | MFP administrator |
| | | Query | Normal user |
| Destination folder | Operation Panel, Web browser | Newly create, modify, query, delete | MFP administrator |

| TSF Data | Operation Interface | Operations | Users |
|----------------------------|---------------------------------|------------------|-------------------|
| | | Query | Normal user |
| User authentication method | Operation Panel, Web browser | Query | MFP administrator |
| IPsec setting information | Operation Panel, Web browser | Query, modify | MFP administrator |
| Device Certificate | Operation Panel, Web browser | Modify | MFP administrator |

FMT_MSA.3(a) and FMT_MSA.3(b)

The TOE sets default values for objects/subjects according to the rules described in Table 39 when those objects/subjects are generated.

Table 39 : List of Static Initialisation for Security Attributes of Document Access Control SFP

| Objects | Security attributes | Default values |
|---|--------------------------------|---|
| Document data | Document data attribute | +PRT: Documents printed from the client computer with direct print, locked print, hold print, and sample print. +SCN: Documents sent by e-mail as attachments or to folders from the MFP. +CPY: Documents copied using the MFP. +DSR: Documents stored in the TOE by using Copy Function, Scanner Function, and Document Server Function. Documents printed using Document Server printing or stored print from the client computer. |
| Document data (stored document types are Document Server document and scanner document) | Document user list | Default values of a document user list assigned to a normal user who created the document data. |
| Document data (stored document type is printer document) | Document user list | Login user name of a normal user who stored the document data. |
| User jobs | Login user name of normal user | Login user name of a normal user who newly creates a user job. |

| Objects | Security attributes | Default values |
|--|---------------------|--|
| Each MFP application (Copy Function, Printer Function, Scanner Function, and Document Server Function) | Function type | The values specified for each function type is as follows: For Copy Function, values to identify Copy Function. For Document Server Function, values to identify Document Server Function. For Printer Function, values to identify Printer Function. For Scanner Function, values to identify Scanner Function. |

7.9 Software Verification Function

The Software Verification Function is to verify the integrity of the executable code of the MFP Control Software, and confirm that these codes can be trusted.

FPT_TST.1

The TOE verifies software at the TOE start-up.

The TOE verifies the integrity of the MFP Control Software by using the hash of the MFP Control Software or by checking the certificate. If the hash does not match its original value or the certificate verification fails, the TOE displays the error message and becomes unavailable. If the hash matches its original value and the certificate is verified, the TOE becomes available. The TOE also verifies the integrity of the audit log data files.