Di3510 Series/Di3510f Series
Multi-Function Peripheral Security Kit
Security Target

This document is a translation of the security target written in Japanese which has been evaluated and certified. The Japan Certification Body has reviewed and checked it.

Version: 1.18

Issued on: June 4, 2004

Created by: KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

<Revision history>

Date	Ver.	Approved by	Checked by	Created by	Revision
07/31/2003	1.00	Ishida	Hashimoto	Nakayama	Creation of the original version.
08/28/2003	1.01	Ishida	Hashimoto	Nakayama	Reflected modifications in the specifications.
09/02/2003	1.02	Ishida	Hashimoto	Nakayama	Typos corrected.
09/05/2003	1.03	Ishida	Hashimoto	Nakayama	Typos corrected.
09/12/2003	1.04	Ishida	Hashimoto	Nakayama	Typos corrected.
10/06/2003	1.05	Ishida	Hashimoto	Nakayama	Typos corrected.
11/12/2003	1.06	Ishida	Hashimoto	Nakayama	Typos corrected.
11/28/2003	1.07	Ishida	Hashimoto	Nakayama	Corrections for the Observation Report (ASE001-01 to ASE012-01). Typos corrected.
12/12/2003	1.08	Ishida	Hashimoto	Nakayama	Reflected modifications in the specifications. Typos corrected.
12/17/2003	1.09	Ishida	Hashimoto	Nakayama	Typos corrected.
12/24/2003	1.10	Ishida	Hashimoto	Nakayama	Typos corrected.
01/08/2004	1.11	Ishida	Hashimoto	Nakayama	Corrections for the Observation Report (ASE013-01 to ASE014-01). Typos corrected.
01/16/2004	1.12	Ishida	Hashimoto	Nakayama	Corrections for the Observation Report (ASE015-01 to ASE019-01). Typos corrected.
02/13/2004	1.13	Ishida	Hashimoto	Nakayama	Corrections for the Observation Report (ASE020-01 to ASE022-01). Typos corrected.
02/26/2004	1.14	Ishida	Hashimoto	Nakayama	Corrections for the Observation Report (ASE023-01). Typos corrected.
04/02/2004	1.15	Ishida	Hashimoto	Nakayama	Corrections for the Observation Report (ASE024-01 to ASE026-01). Typos corrected.
04/13/2004	1.16	Ishida	Hashimoto	Nakayama	Correction along with a modification in the UI version.
05/24/2004	1.17	Ishida	Hashimoto	Nakayama	Corrections for the Observation Report (ASE027-01). Typos corrected.
06/04/2004	1.18	Ishida	Hashimoto	Nakayama	Corrections for the Observation Report (ASE028-01).

---- *(Table of Contents)* --

1. ST Introduction..6
1.1. ST Identification..6
1.2. TOE Identification..6
1.3. CC Conformance Claim..6
1.4. ST Overview..7
1.5. Terminologies..8
2. TOE Description..10
2.1. TOE Type..10
2.2. Environment for the usage of MFP..10
2.3. Roles of the TOE user..11
2.4. Operational environment of the TOE..12
2.4.1. Hardware environment of the TOE..12
2.4.2. Software environment of the TOE..12
2.5. Functions provided by the TOE..15
2.5.1. General User Functions..15
2.5.2. Administrator function..17
2.5.3. Service engineer function..18
2.6. Details of the security functions provided by the TOE..18
2.6.1. Security function for general user functions..18
2.6.2. Security functions for the administrator functions..20
2.6.3. Security functions for the service engineer function..20
3. TOE Security Environment..21
3.1. Assumptions..21
3.2. Threats..22
3.3. Organisational Security policies..22
4. Security Objectives..23
4.1. Security Objectives of the TOE..23
4.2. Security objectives for the environment..23
4.2.1. IT environment security objectives..23
4.2.2. Non-IT environment security objective..24
5. IT Security requirements..26
5.1. TOE security requirements..26
5.1.1. TOE security function requirements..26
5.1.1.1. User data protection..26
5.1.1.2. Identification and authentication..28
5.1.1.3. Security management..32
5.1.1.4. Protection of the TSF..39
5.1.2. Minimum Security Strength of Function..40
5.1.3. TOE Security Assurance Requirements..40
5.2. Security requirements for the IT environment..41
5.2.1. Security functional requirements for the IT environment..41
5.2.1.1. User data protection..41

5.2.1.2. Identification and Authentication 43
5.2.1.3. Security management 43
5.2.2. Security assurance requirements for the IT environment 43
6. TOE Summary Specification 44
6.1. TOE Security Functions 44
6.1.1. F.ADMIN (Administrator mode security function) 45
6.1.2. F.SECURE-PRINT (Secure print security function) 46
6.1.3. F.SERVICE (Service mode security function) 47
6.1.4. F.USER-BOX (User box security function) 48
6.2. TOE Security Strength of Function 48
6.3. Assurance measures 49
7. PP Claims 50
8. Rationale 51
8.1. Security objectives rationale 51
8.1.1. Necessity 51
8.1.2. Sufficiency for the assumptions 52
8.1.3. Sufficiency for the threats 54
8.1.4. Sufficiency of the organisational security policies 55
8.2. IT security requirements rationale 56
8.2.1. Rationale for IT security functional requirements 56
8.2.1.1. Necessity 56
8.2.1.2. Sufficiency 57
8.2.1.3. Mutual support 62
8.2.2. Rationale for Minimum Strength of Function 67
8.2.3. Rationale for IT security assurance requirements 67
8.3. Rationale for TOE Summary Specifications 68
8.3.1. Rationale for the TOE security functions 68
8.3.1.1. Necessity 68
8.3.1.2. Sufficiency 69
8.3.2. Rationale for TOE security strength of function 77
8.3.3. Mutually supported TOE security functions 77
8.3.4. Rationale for assurance measures 77
8.4. PP claims rationale 78

---- (Figure List) ---

Figure 1 An example of the expected environment for usage of the MFP 10
Figure 2 Hardware structure of the MFP 12
Figure 3 Structure of the MFP control software components 13
Figure 4 MFP control software components that relate to the TOE operation processes 15

---- (Table List) ---

Table 1 Operational list for user box 26
Table 2 List of security management functions 35
Table 3 TOE Security Assurance Requirements 40
Table 4 List of operations for the secure print job information data file 41
Table 5 Security function name and identifier for TOE 44
Table 6 Correspondence between TOE security function and TOE security function requirements 44
Table 7Correspondence between TOE assurance requirements and assurance measures 49
Table 8 Conformity of security objectives to the assumptions and threats 51
Table 9 Conformity of IT security functional requirements to the security objectives 56
Table 10 Mutual support correlations of IT security functional requirements 62
Table 11 Dependencies of the IT security functional requirements 64
Table 12 Conformity of the TOE security functions with the TOE security functional requirements 68

1. ST Introduction

1.1. ST Identification

- ST Title : Di3510 Series/Di3510f Series[1],
  Multi-Function Peripheral Security Kit, Security Target
- Version : 1.18
- CC version : 2.1
- Created on : June 4, 2004
- Created by : KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

1.2. TOE Identification

- TOE Name : Japan: Di3510 Series/Di3510f Series Multi-Function Peripheral Security Kit
  Overseas: Di3510 Series/Di3510f Series Multi-Function Peripheral Security Kit
- TOE Version : * TOE is comprised of the following two software components, “User Interface” and “Network Module,” and each has their own version.
  - ➢ User Interface: 4030-20G0-05-00
  - ➢ Network Module: 4030-A0G0-03-00
- TOE type : Software
- Created by : KONICA MINOLTA BUSINESS TECHONOLOGIES, INC.

1.3. CC Conformance Claim

The TOE, which is the subject of this ST, conforms to the following.

- Security function requirement
  Conformity to Part 2

- Security assurance requirement
  Conformity to Part 3

- Evaluation assurance level
  Conformity to EAL 3 (No additional assurance component)

- PP Reference
  This ST does not carry out a PP reference.

[1] “Di3510 Series” indicates the Multi-Function Peripherals (MFP) that are identified as Di1810, Di2010, Di2510, Di3010, and Di3510. “Di3510f Series” indicates the MFPs that are identified as Di1810f, Di2010f, Di2510f, Di3010f, and Di3510f. The fax function is an optional product for the “Di3510 Series,” whereas the “Di3510f Series” is the MFPs that have a built-in fax function.

• References

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model version 2.1 August 1999 CIMB-99-031
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033
- CCIMB Interpretations - 0210
- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model version 2.1 August 1999 CIMB-99-031 (January 2001 Translation Version 1.2, Information-technology Promotion Agency Japan , Security Center)
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032 (January 2001 Translation Version 1.2, Information-technology Promotion Agency Japan, Security Center)
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033 (January 2001 Translation Version 1.2, Information-technology Promotion Agency Japan, Security Center)
- CCIMB Interpretations - 0210(Translation Version)

1.4. ST Overview

The Multi-Function Peripheral (MFP) is an office IT device that is comprised by selecting and combining the functions of copying, printing, scanning and faxing. The target of evaluation (TOE) of this ST is the “Di3510 Series/Di3510f Series Multi-Function Peripheral Security Kit” that is comprised of the “User Interface,” which is a software component that carries out operational control processes from the operations panel of the MFP body, and the “Network Module,” which is a software component that carries out operational control processes from the client PC, from among the built-in control software in the Di3510 Series/Di3510f Series MFP for monochrome printing, which is provided by Konica Minolta Business Technologies, Inc., and the present ST explains the security functions that are realized by the TOE.

The Di3510 Series/Di3510f Series MFP is installed in a general office environment, and its variety of usage methods include copying, printing, scanning and fax transmissions and receptions of a document. A wide variety of documents with low to high confidentiality are handled. For the above, the security functions of the TOE provide a protective function for the exposure of document data with high confidentiality that is spooled in the MFP during the use of a specific function of the Di3510 Series/Di3510f Series MFP. The specific function is a secure print (Lock Job) function in which a password is set and sent to the MFP by a client PC, and when the password is entered from the MFP body operational panel and is matched, then the print data that was sent to the MFP and which is in a print pending condition will be printed, and the user box function controls the access to the user box that is set as the storage area for the scanned data.

This ST is a document that describes the necessity and sufficiency of the security function of the TOE provided for the secure print function and user box function.

1.5. Terminologies

In this section, terminologies that have a particular meaning in the present ST will be described.

Job

Operational unit for a series of functions in the MFP, such as the copying function, scanning function, printing function, faxing function, etc.

Secure Print

A form of printing when printing from a client PC. When a password is set by the printer driver on a client PC, and printing data is transmitted to MFP, the printing is not executed but rather is pending at the MFP. When a set password is entered at the MFP, the pending is cancelled and the printing is executed.

Secure Print Job Information Data

Print data received by the MFP for secure print. This ST handles this as a protective asset.

Job ID

A control number assigned to a series of every jobs at the MFP, including secure print.

Secure Print Password

A password set for secure print during secure printing. (A password entered for secure print that is in the print pending state). A four-digit number can be entered.

User Box

A directory set as a storage area at the MFP for scanned image data when the HDD is loaded. Individual users can set the name and password only from a client PC. The user box indicated as “Public” is shared, so a password cannot be set. A name change cannot be carried out either.

User Box Identifier

A name set to the user box.

User Box Data

Image data stored in the user box. This ST handles this as a protective asset.

User Box Password

A password set for the individual user box. 95 types of ASCII codes can be set.

Administrator Mode

Functions that are provided for authenticated administrators only.

Administrator Mode Password

Passwords set for the administrator mode. Eight-digit numbers can be set.

Service Mode

Functions that are provided for authenticated service engineers only.

Service Code

A password that is set for the service mode, maintenance mode and initialization mode. Eight-digit numbers and “*” and “#” can be used.

Access Check Function

A function for which the operation setting is controlled by the administrator. When this function is valid, the user box authentication function operates and a series of unsuccessful authentication attempts is detected for each of the authentication functions for the administrator function, secure print function and user box function, and depending on the number of unsuccessful authentications, it locks each authentication function.

Unauthorized access detection count value for a user box

A value that is counted and stored as the number of unsuccessful trials, when an authentication trial fails for the user box authentication function while the access check function is operating.

Unauthorized access detection count value for secure print

A value that is counted and stored as the number of unsuccessful trials, when an authentication trial fails for the secure print authentication function while the access check function is operating.

Unauthorized access detection count value for administrator mode

A value that is counted and stored as the number of unsuccessful trials, when an authentication trial fails for the administrator authentication function while the access check function is operating.

Unauthorized access detection count value for service engineer

A value that is counted and stored as the number of unsuccessful trials, when an authentication trial fails for the service engineer authentication function. Unlike other unauthorized access detection count values, it does not rely on the operational setting of the access check function.

Penalty reset function

A function that clears the unauthorized access detection count value for a user box and the unauthorized access detection count value for secure print to zero. When the authentication function for a user box and secure print are locked, execution of this function unlocks them.

2. TOE Description

2.1. TOE Type

The Di3510 Series/Di3510f Series Multi-Function Peripheral Security Kit that is the TOE is a software product that comprises a portion of the MFP control software that is loaded on the MFP. More specifically, it is comprised of the "User Interface" that executes operational control from the operations panel on the MFP body, and the "Network Module" that executes operational control from the client PC.

2.2. Environment for the usage of MFP

The expected general environment for usage is shown in Figure 1.

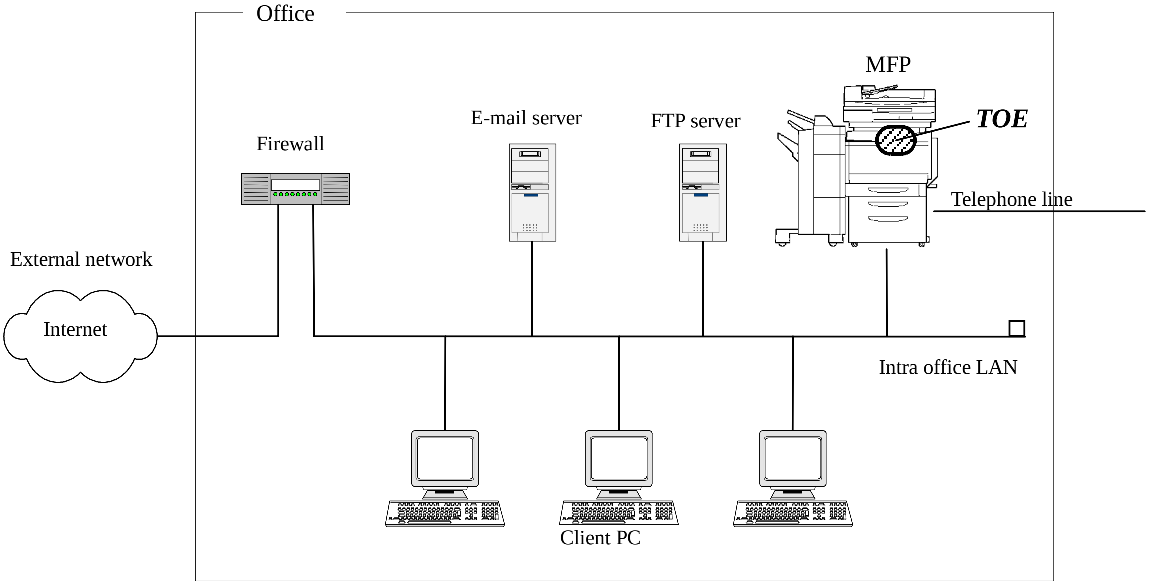

Figure 1 An example of the expected environment for usage of the MFP

As described in the above-mentioned figure, the MFP is installed in a general office. The office will have an operations management system that only allows personnel who are involved in the usage, operation and maintenance of the MFP to enter the room. An intra-office LAN exists as a network in the office. The MFP connects to the client PCs via the intra-office LAN, and has mutual data communication. When an e-mail server and FTP server are connected to the intra-office LAN, the MFP can carry out data communication by using these[2]. When the intra-office LAN connects to an external network, measures such as connecting via a firewall are taken, and an appropriate setup

[2] <Supplement: E-Mail server and FTP server>
Some office environments where the MFP is installed may not have an e-mail server or FTP server. Also, there may be cases in which there is no connection to an external network or telephone line. In these cases, functions that relate to e-mail, an FTP server or a FAX cannot be used; however, this does not affect the other MFP functions. The FTP server and mail server are not necessarily required for the use of the security function for the TOE, and neither is a connection to an external network or telephone line.

to block access requests to the MFP from the external network is carried out. In addition, the intra-office LAN provides a network environment where the communication data between the MFP and the client PC cannot be intercepted, by using a switching hub and office operation. The MFP is connected to the telephone line for fax transmission/reception and in order to communicate with the support center that carries out the maintenance and management of the MFP.

2.3. Roles of the TOE user

The roles of the user that relate to the use of the TOE are defined as follows.

- General user

  Personnel from the organization that use the MFP, who are allowed to enter the office where the MFP is installed. S/he can use the general user function that is stipulated in 2.5.1.

- Administrator

  Personnel from the organization that use the MFP, who are allowed to enter the office where the MFP is installed, as well as carry out the management of the operation. The administrator can use the general user function, for which details are stipulated in 2.5.1, as a general user, as well as the administrator function that is stipulated in 2.5.2.

- Service engineer

  Personnel who carry out management of the maintenance of the MFP, who are allowed to enter the office where the MFP is installed. S/he carries out machine maintenance (physical maintenance) of the printing engine, etc., of the MFP, and is also able to use the service engineer function that is provided as a management of the maintenance function to adjust each setting, etc. (See 2.5.3.) These personnel are not from the organization, so they are not involved in the operation of the MFP. These maintenance operations are carried out under the monitoring of an administrator and therefore there will be no unauthorized activities.

- Person in charge at the organization that uses the MFP

  A person in charge at the organization that manages the office where the MFP is installed. This person assigns an administrator who carries out the management of the operation of the MFP.

- Person in charge at the organization that manages the maintenance of the MFP

  A person in charge at the organization that carry out management of the maintenance of the MFP. This person assigns a service engineer who carries out the maintenance management of the MFP.

2.4. Operational environment of the TOE

2.4.1. Hardware environment of the TOE

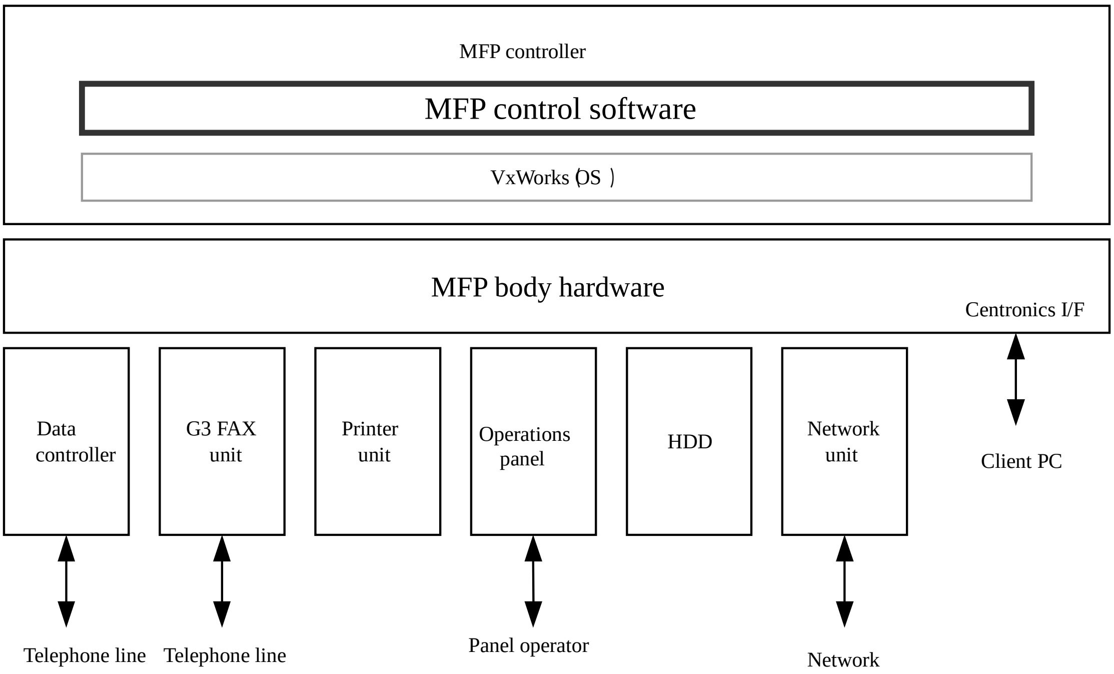

Figure 2 Hardware structure of the MFP

The hardware environment structure for the MFP is shown in the figure above. The MFP controller is installed in the MFP body hardware. The MFP body hardware is loaded with, in addition to the operations panel, a Centronics I/F, which is connected to the client PC, as standard. In addition, the MFP body hardware requires a printer unit, a G3 Fax unit, a data controller (hardware required for EP-NET), a hard disk (HDD), and a network unit, which is required when a printer unit is loaded.

2.4.2. Software environment of the TOE

The “User Interface” and the “Network Module” that are the TOE operate on the OS (VxWorks) that runs on the MFP controller in the MFP body as object code that is integrated with other MFP control software components. Figure 3 shows the structure of these MFP control software components. The physical area of the TOE is indicated in the dark color in the figure.

The operation overview of each software component including the TOE is described as follows.

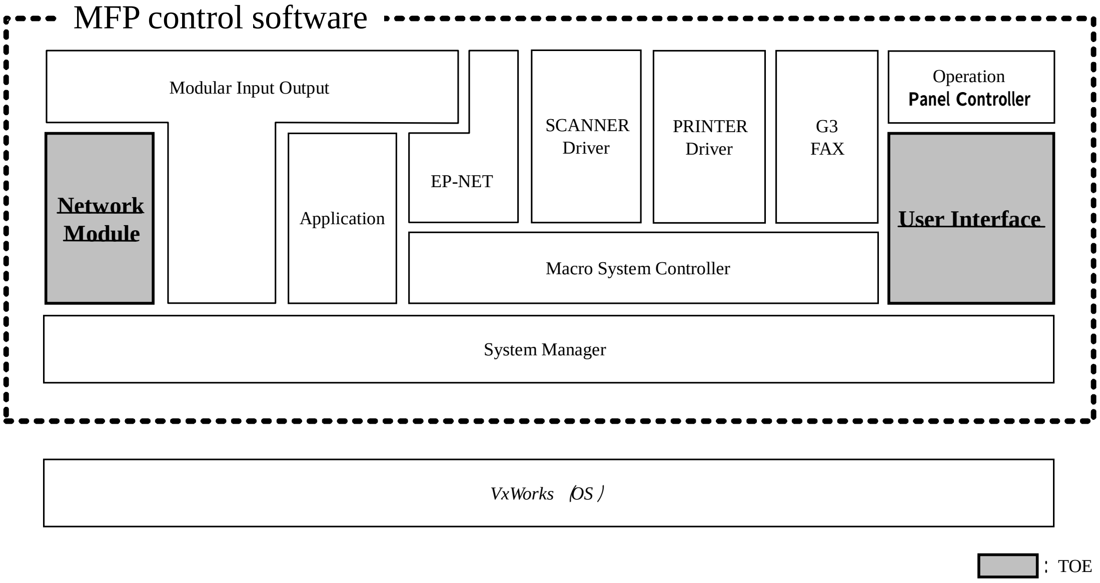

Figure 3 Structure of the MFP control software components

- *VxWorks (OS)*
  Basic software component required for the MFP control software to operate. An operating system. It provides services such as network functions, file system functions and multi-processing for the Di3510 series/Di3510f series MFP.

- System Manager
  A software component that registers and starts up jobs, and manages resources.

- Operations Panel Controller (abbr. OPE)
  A software component that controls hardware such as LCDs, LEDs and keys on the MFP body operations panel. The information entered from the MFP body operations panel is processed by this software component and is given to the "User Interface." Also, it receives the processing results from the "User Interface" and displays on the panel.

- **User Interface (abbr. UI)**
  A software component, which is the target of evaluation in this ST. It processes the information entered from the "Operations Panel Controller" and passes notification to the "System Manager," the "Macro System Controller," or the "Network Module" depending on the process. In addition, it processes messages from the "System Manager," the "Network Module," and the "Macro System Controller" and passes notification to the "Operations Panel Controller."

- Modular Input Output (abbr. MIO)
  A software component that converts the data received from a variety of external interfaces (network unit, Centronics I/F) to data that is handled by the "Application," the "Network Module," and the "System Manger." It realizes a WWW server function. In addition, it carries out a variety of network setting processes for the IP address, DNS server, etc.

- **Network Module (abbr. NM)**
  A software component that is a target of evaluation in this ST. By responding to operation requests from the client PC, it receives the data that the "Modular Input Output" received from the network with a designated protocol (HTTP, IPP, MIB), and processes and control the data. Depending on the process, it requests processing to "VxWorks," the "System Manger," the "Macro System Controller," or the "User Interface," and receives the data that is processed by "VxWorks," the "System Manger," the "Macro System Controller," or the "User Interface," and then requests processing to the "Modular Input Output."

- Macro Systems Controller (abbr. MSC)
  A software component that analyzes scanned image data and registers it as a job. It also controls the job sequence for copying, printing, scanning and faxing.

- Application
  An application software component that carries out e-mail transmission and reception (Internet fax transmission and reception), an FTP transmission and the receiving of print processing from a PC.

- SCANNER Driver
  A software component that controls the scanner device that carries out the scanning process during scanning.

- PRINTER Driver
  A software component that controls the printer device during printing (*It is different from the printer driver of the client PC.)

- G3 FAX
  A software component for a G3 standard fax transmission and reception.

- EP-NET
  A software component that receives access to a "remote maintenance function" from telephone lines (public lines) or the "Module Input Output," and carries out a remote maintenance function. The remote maintenance function is a function that receives a request for access from the support center via a telephone line. The support center collects information such as the number of MFP problems, a value that indicates the wear and tear on the expendable parts, and a printing counter value via a telephone line. In addition, it also has a function such that when a specific malfunction (significant malfunction) is generated in the MFP, it automatically accesses the support center and transmits the malfunction information for the MFP. An e-mail remote maintenance function that realizes the same function using e-mail is also available.

The "User Interface" and "Network Module" that are the TOE are in the relationship that is shown in the following figure with the other MFP control software components and the OS. The details of functions provided by the TOE indicated in the following figure will be described in the following section.

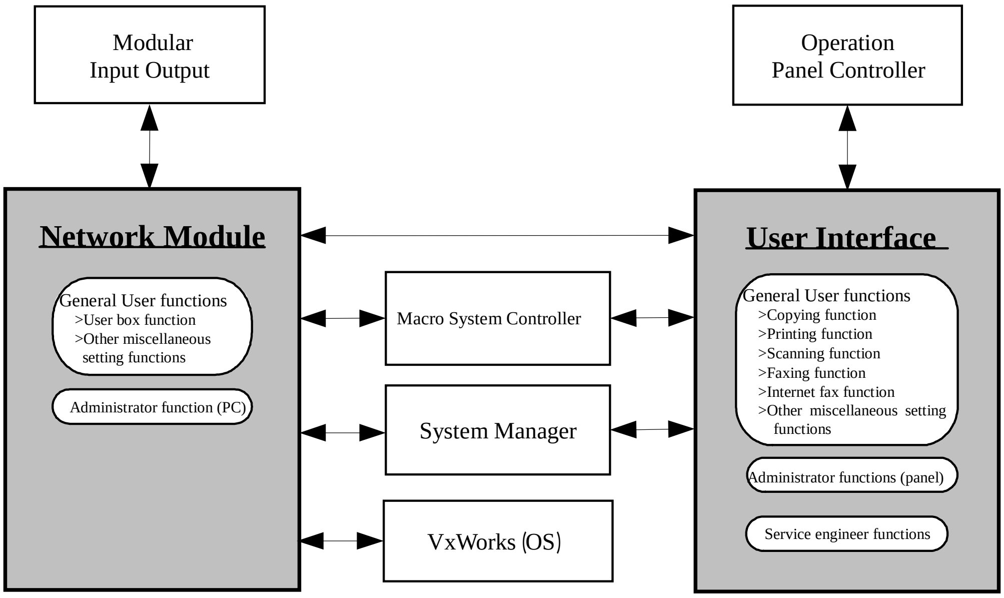

Figure 4 MFP control software components that relate to the TOE operation processes

2.5. Functions provided by the TOE

General users and the administrator use a variety of functions of the MFP with the built-in TOE from the client PC and the operations panel of the MFP body. A service engineer can use the functions for service engineers from the operations panel of the MFP body. **General User Functions** that a general user and administrator operate, a variety of functions in the administrator mode that can be operated only by administrators (**Administrator Functions (Panel), Administrator Functions (PC))** and a variety of functions for service engineers (**Service Engineer Functions**) are described as follows.

2.5.1. General User Functions

General users can use the copying function, the printing function, the scanning function and the faxing function, which are the main functions of the MFP. The TOE takes a partial role in the controlling processes of these main functions. The general functions handled by the general users as well as the processes run by the TOE for each function are described as follows.

(1) Copying function

A function that executes the scanning and printing of spooled image data as is by the MFP body operations panel. During this copying function, the TOE receives the execution, and indicates with a display the process in progress and receives the cancellation process.

(2) Printing function

When print data is transmitted to the MFP using the printer driver of the client PC, the MFP prints the received print data. The printing function includes the following printing method.

1) Normal print
A print function that prints the received print data via the MFP memory as is.

2) Reprint
A print function that allows re-printing or re-printing with different settings such as a print finishing so that when a "reprint" is selected by the client PC, the print data is stored in memory after the printing of the print data is completed. There is no specific access limit during the print execution operation.

3) Secure print (Lock Job)
When a document with high confidentiality is printed, "Lock Job" is selected from the printer driver of the client PC, the password is set and the print data is sent to the MFP. A job ID is given by the "System Manager" to the print data received by the MFP and registered as secure print job information data. The TOE verifies the password entered from the operations panel of the MFP body with the password of the secure print job information data and when they match, then notification is made to the "System Manager" for the cancellation of print pending for the secure print job identified by the job ID, in order to execute the printing. The secure print job information data that completed printing will be automatically deleted.

4) HDD Store print
A function that stores the print job information data in the HDD of the MFP. Printing can be done by operating the operations panel of the MFP body. There is no particular access limit for the operation of print execution.

For the above-mentioned multiple print functions, the TOE executes display processing that indicates the print data is being received, executes display processing that indicates that printing is in progress, and executes the cancellation process for each of the print functions that are being displayed. During secure printing, it receives and verifies the password while in the print pending state.

(3) Scanning function

A function that executes scanning from the operations panel of the MFP body and stores the image as data. There are several data transmission methods for the scanned image data such as e-mail and FTP, and they are used by connecting with the scanning. The image data can be stored in the user box of the HDD that is built in the MFP at the time of scanning without sending it outside MFP. For the scanning function, the TOE carries out the reception of execution, displays an indication of what is currently being executed and receives the cancellation of scanning.

(4) Faxing function

A function that transmits and receives fax data via a telephone line that is designated for a fax. In addition to the regular fax data transmission and reception function, it is compatible with fax functions that use the F code. For this fax function, the TOE receives an execution for the fax transmission, displays an indication for the transmission process, and executes the cancellation process for the fax transmission.

(5) Internet fax function

A function that receives and prints Internet faxes (e-mail with a standard attached image format). Also, it is a function that converts the scanned image data in the MFP to an attachment in an Internet Fax standard image compression format and sends an e-mail. For an Internet fax transmission, the TOE receives the transmission execution, displays an indication for the transmission process and executes a cancellation process for the transmission.

(6) User box function

Using the web-browser of the client PC, it creates a user box where the scanned image data will be stored (new setting for the name, and password) and provides the following operations for the user box* where the image data (hereinafter referred to as the user box data) is stored using the web-browser of the client PC.

- Downloading the user box data to the client PC
- Deletion of user box data
- Deletion of user box
- Change in settings for the user box (name change, password change)

** There is a default user box that is named "public." "Public" is a shared storage area for general users and operations such as a password setting, a name change or a box deletion cannot be carried out.*

(7) Other miscellaneous setting functions

In addition to the above-mentioned (1) to (6), there are a multiplicity of functions that carry out a variety of settings such as for Paper Select, Image Quality Select, and Zoom, etc., during printing which are operated from the operations panel of the MFP body, as functions for the general user. Furthermore, multiple functions, which carry out the viewing of the system status (device structure and outline) of the MFP, the viewing of the job status, the transmission method for the scanning function, and the setting of destination, etc., are available as functions that can be operated using a web-browser from the client PC.

2.5.2. Administrator function

The TOE provides a management function (administrator function) that supervises the general user functions with the administrator mode that is available only for the administrator. The following are descriptions for two categories: the administrator functions (panel) that is management function that can be executed from the operations panel of the MFP body, and the administrator functions (PC) that is management function that can be executed from a client PC.

(1) Administrator functions (panel)

- Function to change the administrator mode password
- Function for setting the operational status of the access check function
- Penalty reset function (A function that clears the unauthorized access detection count value for secure printing and for a user box to zero.)
- A variety of setting functions for the administrator (bulk deletion of secure print jobs, automatic cancellation settings for user box data, a variety of settings for a network, settings for limiting the number of copies, settings for date and time, etc.)

(2) Administrator functions (PC)

- Deletion of user box data
- Deletion of user box
- Change in settings for a user box (name change, password change)
- A variety of setting functions for the administrator (setting of the storage period for user box data, a variety of settings for a network, settings for limiting the number of copies, settings for date and time, etc.)

2.5.3. Service engineer function

The TOE provides a management function (service engineer function) for general user functions and administrator functions in service mode, maintenance mode and initialization mode that can only be operated by a service engineer from the operations panel of the MFP body. The present functions are described as follows.

(1) Service mode

- ROM version display function
- Initialization function for administrator mode password
- Function to change the service code
- A variety of setting functions for service engineers (operation setting function for each setting function provided for general users, settings for the counter for the number of pages to be printed, operational checks for each function, a sensor check, settings for an HDD installation, the HDD format, etc.)

(2) Maintenance mode

- A variety of setting functions for a service engineer (display adjustment for the operations panel of the MFP body, etc.)

(3) Initialization mode

- A variety of setting functions for the service engineer (language setting, etc.)

2.6. Details of the security functions provided by the TOE

In this section, the functions that are related to assets to be protected will be described in particular from among the functions of the TOE described in the previous section.

2.6.1. Security function for general user functions

With the general user functions, when using the printing function, the secure print function is valid during the printing of a document with high confidentiality. The exposure prevention function for secure print job information data is positioned as a security function. Also, to access the user box where the scanned image data is stored, a password that is set for the user box is required and this function, which controls access, is positioned as a security function to maintain the confidentiality of the user box data.

Details of the functions positioned as security functions from among the general user functions are described as follows.

- Identification and authentication that allows access by a general user to a secure print job
  A function that identifies and authenticates that a general user is a valid user for secure print job information data when the secure print job information data is printed. After failing three times at authentication it locks the authentication function for the concerned secure print job information data and access is denied.

- Function to create a user box
  A function by which a general user specifies a name and creates a user box.

- Identification and authentication that allows access to a user box by a general user and an access control function
  A function that identifies and authenticates that a general user is an authorized user of a user box when accessing the user box. After failing three times at authentication, it locks the authentication function for the concerned user box and access is denied.
  When authentication is successful, the downloading of all the user box data in the user box is permitted. (The user box named as "Public" is not subject to the present security function.)

- User box control function for general users whose access is authenticated
  A function by which a general user, who is a valid user of the user box, can change the settings (name, password) of the user box.

For the secure printing function, secure print job information data that is spooled and stored in the MFP is considered temporary data that is stored to maintain security during the printing of a confidential document. In other words, this data is not intended to be stored in the MFP for a long period of time, and therefore, a secure approach is not necessary for the deleting operation. When it is accidentally deleted, in principle, the original data exists in the client PC, and therefore it is not necessary to consider the lack of availability.

The user box function is a function to be used in order to handle printing material as electronic data at the client PC, and user box data is temporary data that is stored until it is loaded by the client PC. Therefore, as with the secure printing function, user box data is not intended to be stored in the MFP for a long period of time, and therefore, a secure approach is not necessary for the deleting operation. When it is accidentally deleted, in principle, the printing material that is the source of the user box data still exists, and therefore, it is not necessary to consider the lack of availability.

And thus, it is not necessary to set an appropriate protection function for the deletion function for secure print job information data and user box data.

2.6.2. Security functions for the administrator functions

There are management functions that involve assets to be protected from among the administrator functions. The access to this administrator function including the management function is limited to those authenticated by the administrator mode password, by using a password that could only be known by the administrator. The identification and authentication functions and the management functions that are related to the protected assets which can be operated after authentication are security functions. The details are described as follows.

➢ Identification and authentication function that allows access to the administrator mode
A function that identifies and authorizes the administrator when accessing the administrator mode using the operations panel of the MFP body or using a web-browser on the client PC. Failing three times locks the authentication function and access is denied.

➢ Security-related functions for administrator mode
The following functions allowing operation from the operations panel of the MFP body in administrator mode.

- Function to change the administrator mode password
- Function for setting the operation status of the access check function
- Penalty reset function

The following function, which can be operated from the client PC in administrator mode.

- Function to change the setting of the user box (name change, password change)

2.6.3. Security functions for the service engineer function

Some of the service engineer functions for the service mode are management functions that involve assets to be protected. The access to the service mode, including these management functions, is limited to those authenticated by the service code, by using a password that could only be known by the service engineer, along with undisclosed secret information that could only be known by the service engineer. The identification and authentication functions and the management functions that are related to the protected assets which can be operated after authentication are security functions. The details are described as follows.

➢ Identification and authentication function that allows access to the service mode
A function that identifies and authorizes the service engineer when accessing the service mode. Failing three times locks the authentication function and access is denied.

➢ Security-related functions for service engineer mode
The following functions allowing operation in service mode.

- Initialization function for the administrator mode password.
- Function to change the service code.

3. TOE Security Environment

This chapter will describe the assumptions, threats, and organisational security policies.

3.1. Assumptions

The present section identifies and describes the assumptions for the environment for using the TOE.

A.ACCESS-CHECK (Operation setting conditions for the access check function)
The user of the MFP uses the MFP under the condition of a setting in which the access check function always runs.

A.ADMIN (Personnel conditions to be an administrator)
The administrator, in the role given to them, shall not carry out a malicious act during the series of permitted operations given to them.

A.AUTH (Operation conditions for passwords)
Each password used for using the TOE shall be managed so that it will not be divulged by the owner of the password.

A.HDD (Protection conditions for the HDD)
The HDD shall not be taken out, unless the administrator permits the service engineer to take it out.

A.NETWORK (Network connection conditions for MFP)

- The organization that uses the MFP shall construct a network environment for an intra-office LAN where the MFP will be installed, which will not be intercepted.
- When the intra-office LAN where the MFP with the TOE will be installed is connected to an external network, access from the external network to the MFP is not allowed.

A.PHYSICAL (Installation conditions for the MFP)
The MFP where the TOE is loaded will be installed in a place where it is physically protected and where only the general users, administrator and service engineer are permitted to enter.

A.SERVICE (Personnel conditions to be a service engineer)
The service engineer, in the role given to them, shall not carry out a malicious act during the series of permitted operations during the installation of the TOE and the maintenance of the MFP.

A.SESSION (Session control conditions)

- General users shall always terminate the session after using the box function whenever leaving the place.
- The administrator shall always terminate the session after using the administrator function.
- The service engineer shall always terminate the session after using the service engineer function.

3.2. Threats

In this section, threats that are expected during the use of the TOE and the environment for using the TOE are identified and described.

T.ACCESS-SECURE-PRINT (Unauthorized operation of the secure print job information data)

Unauthorized exposure of secure print job information data when a malicious general user accesses the secure print job information data from the operations panel of the MFP body and prints the secure print job information data by pretending to be an authorized user.

T.ACCESS-USER-BOX (Unauthorized operation of the user box data)

Unauthorized exposure of user box data when a malicious general user accesses the created user box from the client PC and downloads the user box data of a user box by pretending to be an authorized user.

3.3. Organisational Security policies

P.BEHAVIOR-ACCESS-CHECK (Operation setting function for the access check function)

The access check function can be terminated to maintain compatibility with the existing model for operation purposes under a secure environment.

4. Security Objectives

In this chapter, in relation to the assumption, the threat and the organisational security policy identified in Chapter 3, the required security objectives policy for the TOE and the environment for the usage of the TOE is described by being divided into the categories of the security objectives of the TOE and the security objectives for the environment, as follows.

4.1. Security Objectives for the TOE

In this section, the security objectives for the TOE is identified and described.

O.ACCESS-ADMIN (management function operated by an administrator)
The TOE permits execution of the operation of administrator functions for the administrator only.

O.ACCESS-USER-BOX (user box access control)
The TOE permits the download operation of the user box data for a general user who is a valid user only.

O.ACCESS-SERVICE (management function operated by a service engineer)
The TOE permits execution of operation of the service engineer functions for the service engineer only.

O.I&A-ADMIN (identification and authentication of an administrator)
The TOE identifies and authenticates whether the user who accesses the administrator function from the client PC or the operations panel of the MFP body is an administrator.

O.I&A-SERVICE (identification and authentication of a service engineer)
The TOE identifies and authenticates whether the user who accesses the service engineer function from the operations panel of the MFP body is a service engineer.

O.I&A-USER (identification and authentication of a general user)
The TOE identifies and authorizes whether the user who accesses the secure print job information data or user box data is a general user who is a valid user.

4.2. Security objectives for the environment

In this section, the security objectives for the environment, in the environment of the usage of the TOE, is identified and described being divided into the IT environment security objectives and the non-IT environment security objectives.

4.2.1. IT environment security objectives

OE.ACCESS-SECURE-PRINT (secure print job access control)
The System Manager permits the print operation of secure print job information data for the general user who is a valid user only.

OE.SECURE-PRINT-QUALITY (quality scale for secure print job password)
The printer driver of the client PC adds a password, of which the strength is assured, to the print data that is sent to the MFP as a secure print.

4.2.2. Non-IT environment security objective

OE-N.ACCESS-CHECK (operation of the access check function)

The administrator shall always use the TOE with the access check function turned on.

OE-N.ADMIN (reliable administrator)

The person in charge in the organization who uses the MFP shall assign a person who can faithfully execute the given role during the operation of the MFP with the TOE as an administrator.

OE-N.AUTH (proper management and usage of password)

- The person in charge in the organization who uses the MFP shall have the administrator execute the following operations.
  - Administrator shall not use an administrator mode password that can be easily guessed.
  - Administrator shall keep the administrator mode password confidential.
  - Administrator shall appropriately change the administrator mode password.
  - Administrator shall always carry out the modification operation when the administrator mode password is initialized.
- The administrator shall have general users execute the following operations.
  - General users shall keep the secure print password and user box password confidential.
  - General users shall not use a secure print password and user box password that can be easily guessed.
  - General users shall appropriately change the user box password.
- The person in charge in the organization who manages the maintenance of the MFP shall have the service engineer execute the following operations.
  - Service engineer shall not use a service code that can be easily guessed.
  - Service engineer shall keep the service code confidential.
  - Service engineer shall appropriately change the service code.

OE-N.MAINTENANCE (maintenance and management of the MFP)

- The administrator shall not permit a person other than the service engineer to carry out the maintenance operation.
- The administrator shall prevent unauthorized removal of the HDD by having the operation management, in which the service engineer carries out the maintenance operation, be carried out in the presence of the administrator.

OE-N.NETWORK (network environment in which the MFP is connected)

- The administrator shall install devices that realize a network environment for the office LAN where the MFP with the TOE is installed that cannot be intercepted, and execute an appropriate setting that does not allow interception.
- The administrator shall install devices that block access to the MFP with the TOE from an external network, and execute an appropriate setting to block access.

OE-N.PHYSICAL (environment for the MFP installation)

The administrator shall install the MFP with the TOE in a physically protected office, and execute operation management where only the general users, administrator, and service engineer can enter the office.

OE-N.SERVICE (reliable service engineer)

The person in charge of the organization that carries out the maintenance management of the MFP shall assign a person who will faithfully carry out the given role for the installation of the TOE and the maintenance of the MFP with the TOE as a service engineer.

OE-N.STRUCTURE (HDD installation structure of the MFP)

The HDD used in the MFP with the TOE shall have an installation structure such that it cannot be removed by persons other than a service engineer.

OE-N.SESSION (termination of the session after use)

- The administrator shall have general users always terminate the session after use of the box function.
- The administrator shall always terminate the session after use of the administrator function.
- The service engineer shall always terminate the session after use of the service engineer function.

5. IT Security requirements

In this chapter, the TOE security requirements and IT environment security requirements are described.

5.1. TOE security requirements

5.1.1. TOE security function requirements

The security function requirements required for the TOE are described. Those regulated in CC Part 2 shall be directly used for all the functional requirements components , and the same labels shall be used as well. In the following description, when items are indicated in "italic" and "bold" it means that they are assigned or selected. When indicated in "italic" and "bold" and "underline" it means that they are refined. A number in the parentheses after a label means that the functional requirement is used repeatedly. The label in the parentheses "( )" in the dependent section indicates a label for the security functional requirements used in this ST. When it is a dependency that is not required to be used in this ST, it is described as "N/A" in the same parentheses.

5.1.1.1. User data protection

FDP_ACC.1	Subset access control

FDP_ACC.1.1

The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].

[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]:

Listed in "Table 1 Operational List for User Box"

[assignment: *access control SFP*]

User box access control

Hierarchical to: No other components

Dependencies: FDP_ACF.1 (FDP_ACF.1)

Table 1 Operational list for user box

Subject	Object	Operational list
Operational processes for the user box	***User box***	***• Read user box data in the user box*** ***• Creation***

FDP_ACF.1	Security attribute based access control

FDP_ACF.1.1

The TSF shall enforce the [assignment: access control SFP] to objects based on [assignment: security attributes, named groups of security attributes].

[assignment: *security attributes, named groups of security attributes*]:

User box identifier

[assignment: *access control SFP*]:

User box access control

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]:

- ***During the process of operating the user box having a "user box identifier" selected by a general user, the read operation of the user box data in the user box is permitted only for the user box having an identical "user box identifier" as above.***
- ***During the process of operating the user box having a "user box identifier" entered by a general user, if there is no user box having an identical "user box identifier," the creation of a user box having the "user box identifier" entered by the general user as the object attributes is permitted.***
- ***During the process of operating the user box having a "user box identifier" entered by a general user, if there is a user box having an identical "user box identifier," the creation of a user box having the "user box identifier" entered by the general user as the object attributes is denied.***

FDP_ACF.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules :[assignment: rules, based on security attributes, *that explicitly authorise access of subjects to objects*].

[assignment: rules, based on security attributes, *that explicitly authorize access of subjects to objects*]:

None

FDP_ACF.1.4[2]

The TSF shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes, *that explicitly deny access of subjects to objects*].

[assignment: rules, based on security attributes, *that explicitly deny access of subjects to objects*]:

None

Hierarchical to: No other components

Dependencies: FDP_ACC.1 (FDP_ACC.1), FMT_MSA.3 (FMT_MSA.3)

5.1.1.2. Identification and authentication

FIA_AFL.1[1] Authentication failure handling

FIA_AFL.1.1[1]

The TSF shall detect when [assignment*: number*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

[assignment: *list of authentication events*]:

Authentication of administrator

[assignment: *number*]:

3

FIA_AFL.1.2[1]

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].

[assignment: *list of actions*]:

Lock the authentication function of the administrator

<Operation for recovering the normal condition>

No function for resetting the lock is available.

Hierarchical to: No other components

Dependencies: FIA_UAU.1 (FIA_UAU.2[3])

FIA_AFL.1[2] Authentication failure handling

FIA_AFL.1.1[2]

The TSF shall detect when [assignment*: number*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

[assignment: *list of authentication events*]:

Authentication of a general user who is a valid user of the secure print job.

[assignment: *number*]:

3

FIA_AFL.1.2[2]

When the denied number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment : *list of actions*].

[assignment: *list of actions*]:

Unless the following operation to recover the normal condition is carried out, the authentication function is locked for the general user who is a valid user of the secure print job.

<Operation for recovering the normal condition>

Carry out the penalty reset function for the secure print job.

Hierarchical to: No other components

Dependencies: FIA_UAU.1 (FIA_UAU.2[1])

FIA_AFL.1[3] Authentication failure handling

FIA_AFL.1.1[3]

The TSF shall detect when [assignment*: number*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

[assignment: *list of authentication events*]:

Authentication of a general user who is a valid user of the user box.

[assignment: *number*]:

3

FIA_AFL.1.2[3]

When the denied of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].

[assignment: *list of actions*]:

Unless the following operation to recover the normal condition is carried out, the authentication function is locked for the general user who is a valid user of the user box.

<Operation for recovering the normal condition>

Carry out the penalty reset function for the user box.

Hierarchical to: No other components

Dependencies: FIA_UAU.1 (FIA_UAU.2[2])

FIA_AFL.1[4] Authentication failure handling

FIA_AFL.1.1[4]

The TSF shall detect when [assignment*: number*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

[assignment: *list of authentication events*]:

Authentication of a service engineer.

[assignment: *number*]:

3

FIA_AFL.1.2[4]

When the denied number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].

[assignment: *list of actions*]:

Lock the authentication function of the service engineer.

<Operation for recovering the normal condition>

No function for resetting the lock is available.

Hierarchical to: No other components

Dependencies: FIA_UAU.1 (FIA_UAU.2[4])

FIA_SOS.1[1] Verification of secrets

FIA_SOS.1.1[1]

The TSF shall provide a mechanism to verify that the ***user box password*** meets [assignment: a *defined quality metric*].

[assignment: a *defined quality metric*]:

Minimum 4 digits, maximum 64 digits ASCII code 0x20 to 0x7E (95 types in English one-byte characters and one byte symbols).

Hierarchical to: No other components

Dependencies: No dependencies

FIA_SOS.1[2] Verification of secrets

FIA_SOS.1.1[2]

The TSF shall provide a mechanism to verify that the ***administrator mode password*** meets [assignment: a *defined quality metric*].

[assignment: a *defined quality metric*]:

Exact 8-digit number (0 to 9).

Hierarchical to: No other components

Dependencies: No dependencies

FIA_SOS.1[3]	Verification of secrets

FIA_SOS.1.1[3]

The TSF shall provide a mechanism to verify that the ***service code*** meets [assignment: a *defined quality metric*].

[assignment: a *defined quality metric*]:

Exact 8-digit number (0 to 9) or "*" or "#."

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UAU.2[1]	User authentication before any action

FIA_UAU.2.1[1]

The TSF shall require each ***general user who is a valid user of a secure print job*** to authenticate itself before allowing any other TSF-mediated actions on behalf of that ***general user who is a valid user of the secure print job***.

Hierarchical to: FIA_UAU.1

Dependencies: FIA_UID.1 (FIA_UID.2[1])

FIA_UAU.2[2]	User authentication before any action

FIA_UAU.2.1[2]

The TSF shall require each ***general user who is a valid user of a user box*** to authenticate itself before allowing any other TSF-mediated actions on behalf of that ***general user who is a valid user of a user box***.

Hierarchical to: FIA_UAU.1

Dependencies: FIA_UID.1 (FIA_UID.2[2])

FIA_UAU.2[3]	User authentication before any action

FIA_UAU.2.1[3]

The TSF shall require an ***administrator*** to authenticate itself before allowing any other TSF-mediated actions on behalf of that ***administrator***.

Hierarchical to: FIA_UAU.1

Dependencies: FIA_UID.1 (FIA_UID.2[3])

FIA_UAU.2[4]	User authentication before any action

FIA_UAU.2.1

The TSF shall require each ***service engineer*** to authenticate itself before allowing any other TSF-mediated actions on behalf of that ***service engineer***.

Hierarchical to: No other components

Dependencies: FIA_UID.1 (FIA_UID.2[4])

FIA_UAU.6	Re-authenticating

FIA_UAU.6.1

The TSF shall re-authenticate the user under the conditions [assignment: *list of conditions under which re-authentication is required*].

[assignment: *list of conditions under which re-authentication is required*]

- ***Change administrator mode password.***
- ***Change service code.***

Hierarchical to: No other components
Dependencies: No dependencies

FIA_UAU.7	Protected authentication feedback

FIA_UAU.7.1

The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.

[assignment: *list of feedback*]:

Display "*" for each character of character data entered as an administrator mode password, service code, user box password or secure print password.

Hierarchical to: No other components
Dependencies: FIA_UAU.1 (FIA_UAU.2[1], FIA_UAU.2[2], FIA_UAU.2[3], FIA_UAU.2[4])

FIA_UID.2[1]	User identification before any action

FIA_UID.2.1[1]

The TSF shall require a ***general user who is a valid user of a secure print job*** to identify itself before allowing any other TSF-mediated actions on behalf of that ***general user who is a valid user of the secure print job***.

Hierarchical to: FIA_UID.1
Dependencies: No dependencies

FIA_UID.2[2]	User identification before any action

FIA_UID.2.1[2]

The TSF shall require a ***general user who is a valid user of a user box*** to identify itself before allowing any other TSF-mediated actions on behalf of that ***general user who is a valid user of a user box***.

Hierarchical to: FIA_UID.1
Dependencies: No dependencies

FIA_UID.2[3]	User identification before any action

FIA_UID.2.1[3]

The TSF shall require an ***administrator*** to identify itself before allowing any other TSF-mediated actions on behalf of that ***administrator***.

Hierarchical to: FIA_UID.1
Dependencies: No dependencies

FIA_UID.2[4]	User identification before any action

FIA_UID.2.1[4]

The TSF shall require a ***service engineer*** to identify itself before allowing any other TSF-mediated actions on behalf of that ***service engineer***.

Hierarchical to: FIA_UID.1
Dependencies: No dependencies

5.1.1.3. Security management

FMT_MOF.1	Management of security functions behaviour

FMT_MOF.1.1

The TSF shall restrict the ability to [selection: determine the behaviour of, disable, enable, modify the behaviour of] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*].

[assignment: *list of functions*]:

Access check function

[selection: determine the behaviour of, disable, enable, modify the behaviour of]

Enable, disable

[assignment: *the authorised identified roles*]:

Administrator

Hierarchical to: No other components
Dependencies: FMT_SMF.1 (FMT_SMF.1), FMT_SMR.1 (FMT_SMR.1[2])

FMT_MSA.1	Management of security attributes

FMT_MSA.1.1

The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to restrict the ability to [selection: change_default, query, modify, delete, *[assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

[assignment: *list of security attributes*]:

User box identifier

[selection: change_default, query, modify, delete, *[assignment: other operations]*] :

Modify

[assignment: *the authorised identified roles*]

General user who is a valid user of the user box, administrator

[assignment: *access control SFP, information flow control SFP*]

User box access control

Hierarchical to: No other components
Dependencies: FDP_ACC.1 or FDP_IFC.1 (FDP_ACC.1), FMT_SMF.1 (FMT_SMF.1),
FMT_SMR.1 (FMT_SMR.1[1], FMT_SMR.1[2])

FMT_MSA.3	Static attribute initialisation

FMT_MSA.3.1

The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection: restrictive, permissive, other property] default values for security attributes that are used to enforce the SFP.

[selection: restrictive, permissive, other property]:

Permissive

[assignment: *access control SFP, information flow control SFP*]:

User box access control

FMT_MSA.3.2

The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.

[assignment: *the authorised identified roles*]:

General user who creates the user box

Hierarchical to: No other components
Dependencies: FMT_MSA.1 (FMT_MSA.1), FMT_SMR.1 (FMT_SMR.1[4])

FMT_MTD.1[1] Management of TSF data

FMT_MTD.1.1[1]

The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, *[assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].

[assignment: *list of TSF data*]:

Administrator mode password

[selection: change_default, query, modify, delete, clear, *[assignment: other operations]*]:

Modify

[assignment: *the authorised identified roles*]:

Administrator

Hierarchical to: No other components
Dependencies: FMT_SMF.1 (FMT_SMF.1), FMT_SMR.1 (FMT_SMR.1[2])

FMT_MTD.1[2] Management of TSF data

FMT_MTD.1.1[2]

The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, *[assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].

[assignment: *list of TSF data*]:

User box password

[selection: change_default, query, modify, delete, clear, *[assignment: other operations]*]:

Modify

[assignment: *the authorised identified roles*]:

General user who is a valid user of the user box, administrator

Hierarchical to: No other components
Dependencies: FMT_SMF.1 (FMT_SMF.1), FMT_SMR.1 (FMT_SMR.1[1], FMT_SMR.1[2])

FMT_MTD.1[3] Management of TSF data

FMT_MTD.1.1[3]

The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, *[assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].

[assignment: *list of TSF data*]:

Service code

[selection: change_default, query, modify, delete, clear, *[assignment: other operations]*]:

Modify

[assignment: *the authorised identified roles*]:

Service engineer

Hierarchical to: No other components
Dependencies: FMT_SMF.1 (FMT_SMF.1), FMT_SMR.1 (FMT_SMR.1[3])

FMT_MTD.1[4] Management of TSF data

FMT_MTD.1.1[4]

The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, *[assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].

[assignment: *list of TSF data*]:

Administrator mode password

[selection: change_default, query, modify, delete, clear, *[assignment: other operations]*]:

[assignment: other operations]: initialization (operation to return to the default)

[assignment: *the authorised identified roles*]:

Service engineer

Hierarchical to: No other components
Dependencies: FMT_SMF.1 (FMT_SMF.1), FMT_SMR.1 (FMT_SMR.1[3])

FMT_MTD.1[5] Management of TSF data

FMT_MTD.1.1[5]

The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, *[assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].

[assignment: *list of TSF data*]:

- ***Unauthorized access detection count value for user box***
- ***Unauthorized access detection count value for secure print***

[selection: change_default, query, modify, delete, clear, *[assignment: other operations]*]:

Clear

[assignment: *the authorised identified roles*]:

Administrator

Hierarchical to: No other components
Dependencies: FMT_SMF.1 (FMT_SMF.1), FMT_SMR.1 (FMT_SMR.1[2])

FMT_SMF.1 Specification of management functions

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: [assignment: *list of security management functions provided by the TSF*].

[assignment: *list of security management functions provided by the TSF*]:

Listed in the applicable section of "Table 2 List of Security Management Functions"

Hierarchical to: No other components
Dependencies: No dependencies

Table 2 List of security management functions

N/A: Not Applicable

Functional requirement components	Management items listed in CC Part 2	Application
FDP_ACC.1	There are no management activities foreseen for this component.	N/A
FDP_ACF.1	The following actions could be considered for the management functions in FMT: a) Managing the attributes used to make explicit access or denial based decisions.	There is no management function that is applicable for the management items on the left; however, the following security management functions are specified as related items for the requirement. ***• Creation function of user box identifier*** ***• Modification function of user box identifier (operated by the general user who is a valid user of the user box)*** ***• Modification function of user box identifier (operated by the administrator)***
FIA_AFL.1[1]	The following actions could be considered for the management functions in FMT: a) Management of the threshold for unsuccessful authentication attempts: b) Management of actions to be taken in the event of an authentication failure.	There is no management function that is applicable for the management items on the left; however, the following security management functions are specified as related items for the requirement. ***• Operation setting function for the access check function***
FIA_AFL.1[2]	The following actions could be considered for the management functions in FMT: a) Management of the threshold for unsuccessful authentication attempts: b) Management of actions to be taken in the event of an authentication failure.	There is no management function that is applicable for the management items on the left; however, the following security management functions are specified as related items for the requirement. ***• Operation setting function for the access check function*** ***• Penalty reset function that eliminates the count value for detection of unauthorized access for a secure print***
FIA_AFL.1[3]	The following actions could be considered for the management functions in FMT: a) Management of the threshold for unsuccessful authentication attempts b) Management of actions to be taken in the event of an authentication failure.	There is no management function that is applicable for the management items on the left; however, the following security management functions are specified as related items for the requirement. ***• Operation setting function for the access check function*** ***• Penalty reset function that eliminates the count value for detection of unauthorized access for a user box***

Functional requirement components	Management items listed in CC Part 2	Application
FIA_AFL.1[4]	The following actions could be considered for the management functions in FMT: a) Management of the threshold for unsuccessful authentication attempts; b) Management of actions to be taken in the event of an authentication failure.	There is no management function that is applicable for the management items on the left.
FIA_SOS.1[1]	The following actions could be considered for the management functions in FMT: a) the management of the metric used to verify the secrets.	There is no management function that is applicable for the management items on the left.
FIA_SOS.1[2]	The following actions could be considered for the management functions in FMT: a) the management of the metric used to verify the secrets.	There is no management function that is applicable for the management items on the left.
FIA_SOS.1[3]	The following actions could be considered for the management functions in FMT: a) the management of the metric used to verify the secrets.	There is no management function that is applicable for the management items on the left.
FIA_UAU.2[1]	The following actions could be considered for the management functions in FMT: Management of the authentication data by an administrator; Management of the authentication data by the user associated with this data.	There is no management function that is applicable for the management items on the left.
FIA_UAU.2[2]	The following actions could be considered for management functions in FMT: Management of the authentication data by the administrator; Management of the authentication data by the user associated with this data.	***● Modification function for the user box password (operated by the general user who is a valid user of the user box)*** ***● Modification function for the user box password (operated by the administrator)*** --- Unlike the above, the following is not a management function that is applicable for the management items on the left; however, the following security management functions are specified as related items for the requirement. ***● Operation setting function for the access check function***
FIA_UAU.2[3]	The following actions could be considered for the management functions in FMT: Management of the authentication data by an administrator. Management of the authentication data by the associated user: Managing the list of actions that can be taken before the user is authenticated.	***● Modification function for the administrator mode password*** ***● Initialization function for the administrator mode password***
FIA_UAU.2[4]	The following actions could be considered for the management functions in FMT: Management of the authentication data by an administrator; Management of the authentication data by the user associated with this data.	***● Modification function for the service code***

Functional requirement components	Management items listed in CC Part 2	Application
FIA_UAU.6	The following actions could be considered for the management functions in FMT. If an authorised administrator could request re-authentication, the management includes a re-authentication request.	There is no management function that is applicable for the management items on the left.
FIA_UAU.7	There are no management activities foreseen.	N/A
FIA_UID.2[1]	The following actions could be considered for the management functions in FMT: a) the management of the user identities.	There is no management function that is applicable for the management items on the left.
FIA_UID.2[2]	The following actions could be considered for the management functions in FMT: a) the management of the user identities.	***• Creation function of user box identifier*** ***• Modification function of user box identifier (operated by the general user who is a valid user of the user box)*** ***• Modification function of user box identifier (operated by the administrator)***
FIA_UID.2[3]	The following actions could be considered for the management functions in FMT: a) the management of the user identities.	There is no management function that is applicable for the management items on the left.
FIA_UID.2[4]	The following actions could be considered for the management functions in FMT: a) the management of the user identities.	There is no management function that is applicable for the management items on the left.
FMT_MOF.1	The following actions could be considered for the management functions in FMT Management: a) Managing the group of roles that can interact with the functions in TSF.	There is no management function that is applicable for the management items on the left.
FMT_MSA.1	The following actions could be considered for the management functions in FMT Management: a) Managing the group of roles that can interact with the security attributes.	There is no management function that is applicable for the management items on the left.
FMT_MSA.3	The following actions could be considered for the management functions in FMT Management: a) Managing the group of roles that can specify initial values. b) Managing the permissive or restrictive setting of default values for given access control SFP.	There is no management function that is applicable for the management items on the left.
MFT_MTD.1[1]	The following actions could be considered for the management functions in FMT Management: a) Managing the group of roles that can interact with the TSF data.	There is no management function that is applicable for the management items on the left.
FMT_MTD.1[2]	The following actions could be considered for the management functions in FMT Management: a) Managing the group of roles that can interact with the TSF data.	There is no management function that is applicable for the management items on the left.

Functional requirement components	Management items listed in CC Part 2	Application
FMT_MTD.1[3]	The following actions could be considered for the management functions in FMT Management: a) Managing the group of roles that can interact with the TSF data.	There is no management function that is applicable for the management items on the left.
FMT_MTD.1[4]	The following actions could be considered for the management functions in FMT Management: a) Managing the group of roles that can interact with the TSF data.	There is no management function that is applicable for the management items on the left.
FMT_MTD.1[5]	The following actions could be considered for the management functions in FMT Management: a) Managing the group of roles that can interact with the TSF data.	There is no management function that is applicable for the management items on the left.
FMT_SMF.1	There are no management activities foreseen for this component.	N/A
FMT_SMR.1[1]	The following actions could be considered for the management functions in FMT Management: a) Managing the group of users that are part of a role.	There is no management function that is applicable for the management items on the left.
FMT_SMR.1[2]	The following actions could be considered for the management functions in FMT Management: a) Managing the group of users that are part of a role.	There is no management function that is applicable for the management items on the left.
FMT_SMR.1[3]	The following actions could be considered for the management functions in FMT Management: a) Managing the group of users that are part of a role.	There is no management function that is applicable for the management items on the left.
FMT_SMR.1[4]	The following actions could be considered for the management functions in FMT Management: a) Managing the group of users that are part of a role.	There is no management function that is applicable for the management items on the left.
FPT_RVM.1	There are no management activities foreseen.	N/A
FPT_SEP.1	There are no management activities foreseen.	N/A

FMT_SMR.1[1] Security roles

FMT_SMR.1.1[1]

The TSF shall maintain the roles [assignment: *the authorised identified roles*].

[assignment: *the authorised identified roles*]:

General user who is a valid user of the user box

FMT_SMR.1.2[1]

The TSF shall be able to associate users with roles.

Hierarchical to: No other components
Dependencies: FIA_UID.1 (FIA_UID.1[2])

FMT_SMR.1[2]	Security roles

FMT_SMR.1.1[2]
The TSF shall maintain the roles [assignment: *the authorised identified roles*].
[assignment: *the authorised identified roles*]:
Administrator
FMT_SMR.1.2[2]
The TSF shall be able to associate users with roles.
Hierarchical to: No other components
Dependencies: FIA_UID.1 (FIA_UID.2[3])

FMT_SMR.1[3]	Security roles

FMT_SMR.1.1[3]
The TSF shall maintain the roles [assignment: *the authorised identified roles*].
[assignment: *the authorised identified roles*]:
Service engineer
FMT_SMR.1.2[3]
The TSF shall be able to associate users with roles.
Hierarchical to: No other components
Dependencies: FIA_UID.1 (FIA_UID.2[4])

FMT_SMR.1[4]	Security roles

FMT_SMR.1.1[4]
The TSF shall maintain the roles [assignment: *the authorised identified roles*].
[assignment: *the authorised identified roles*]:
General user who creates the user box

FMT_SMR.1.2[4]
The TSF shall be able to associate users with roles.
Hierarchical to: No other components
Dependencies: FIA_UID.1 (N/A)

5.1.1.4. Protection of the TSF

FPT_RVM.1	Non-bypassability of the TSP

FMT_RVM.1.1
The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
Hierarchical to: No other components
Dependencies: No dependencies

FPT_SEP.1	TSF domain separation

FPT_SEP.1.1

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subject.

FPT_SEP.1.2

The TSF shall enforce separation between the security domains of subjects in the TSC.

Hierarchical to: No other components
Dependencies: No dependencies

5.1.2. Minimum Security Strength of Function

The minimum strength of function level of the TOE is

SOF-Basic. The required TOE security functions that use a probabilistic/permutational mechanism are, FIA_UAU.2[1], FIA_UAU.2[2], FIA_UAU.2[3], FIA_UAU.2[4], FIA_UAU.6, FIA_SOS.1[1], FIA_SOS.1[2], and FIA_SOS.1[3].

5.1.3. TOE Security Assurance Requirements

The TOE is a commercial office product that is used in a general office environment, and therefore a TOE security assurance requirement that is required for EAL3 conformance, which is a sufficient level as an assurance for commercial office products, is applied. The following table summarizes the applied TOE security assurance requirements.

Table 3 TOE Security Assurance Requirements

TOE Security Assurance Requirements		Component
Class ACM: Configuration management	CM capabilities	ACM_CAP.3
	CM scope	ACM_SCP.1
Class ADO: Delivery and operation	Delivery	ADO_DEL.1
	Installation, generation and start-up	ADO_IGS.1
Class ADV: Development	Function specification	ADV_FSP.1
	High-level design	ADV_HLD.2
	Representation correspondence	ADV_RCR.1
Class AGD: Guidance documents	Administrator guidance	AGD_ADM.1
	User guidance	AGD_USR.1
Class ALC: Life cycle support	Development security	ALC_DVS.1
Class ATE: Tests	Coverage	ATE_COV.2
	Depth	ATE_DPT.1
	Functional tests	ATE_FUN.1
	Independent testing	ATE_IND.2
Class AVA: Vulnerability assessment	Misuse	AVA_MSU.1
	Strength of TOE security functions	AVA_SOF.1
	Vulnerability analysis	AVA_VLA.1

5.2. Security requirements for the IT environment

The security function requirements required for the IT environment are described. Those regulated in CC Part 2 shall be directly used for all the functional requirements components, and the same labels shall be used as well. In the following description, when items are indicated in "italic" and "bold" it means that they are assigned or selected. When indicated in "italic" and "bold" and an "underline" it means that they are refined. An identifier "E" in the parentheses, after the label, is used in order to explicitly show this function requirement is a security requirement for the IT environment. The label in the parentheses "( )" in the dependency section indicates a label for the security function requirements used in this ST. When it is a dependency that is not required to be used in this ST, it is described as "N/A" in the same parentheses.

5.2.1. Security functional requirements for the IT environment

5.2.1.1. User data protection

FDP_ACC.1[E] Subset access control

FDP_ACC.1.1[E]

System Manager shall enforce the [assignment: *access control SFP*] on [assignment: list of *subjects, objects and operations among subjects and objects covered by the SFP*].

[assignment: *list of subjects, objects and operations among subjects and objects covered by the SFP*]:

"Table 4 List of operations for the secure print job information data file"

[assignment: *access control SFP*]:

Secure print job access control

Hierarchical to: No other components
Dependencies: FDP_ACF.1 (FDP_ACF.1[E])

Table 4 List of operations for the secure print job information data file

Subject	Object	Operation
Process that operates secure print job	***Secure print job information data file***	● ***Print*** ● ***Registration***

FDP_ACF.1[E] Security attribute based on access control

FDP_ACF.1.1[E]

System Manager shall enforce the [assignment: *access control SFP*] to objects based on [assignment: *security attributes, named groups of security attributes*].

[assignment: *security attributes, named groups of security attributes*]:

Job ID

[assignment: *access control SFP*]:

Secure print job access control

FDP_ACF.1.2[E]

System Manager shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

[assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]:

- ***The process that executes the secure print job having the "job ID" of the secure print job selected by a general user is permitted a print operation only for the secure print job information data file with a matched "job ID."***
- ***During the process that executes the secure print job, when a registration request for a secure print job is received, a "job ID" that is newly assigned is created, and the secure print job information data with the above-mentioned " job ID" as the object attribution are registered.***

FDP_ACF.1.3[E]

System Manager shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

[assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]:

None

FDP_ACF.1.4[E]

System Manager shall explicitly deny the access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]:

None

Hierarchical to: No other components

Dependencies: FDP_ACC.1 (FDP_ACC.1[E]), FMT_MSA.3 (FMT_MSA.3[E])

5.2.1.2. Identification and Authentication

FIA_SOS.1[E] Verification of secrets

FIA_SOS.1.1[E]

Printer driver of the client PC shall provide a mechanism to verify that the ***secure print password meets*** [assignment: *defined quality metric*].

[assignment: *defined quality metric*]:

4-digit number (0 to 9)

Hierarchical to: No other components

Dependencies: No dependencies

5.2.1.3. Security management

FMT_MSA.3[E] Static attribute initialisation

FMT_MSA.3.1[E]

System Manager shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection: *restrictive, permissive, other property*] default values for a ***job ID*** that is used to enforce the SFP.

[selection: *restrictive, permissive, other property*]:

Other characteristics (a value that can be uniquely identified for categorizing the secure print job from other jobs)

[assignment: *access control SFP, information flow control SFP*]:

Secure print job access control

FMT_MSA.3.2[E]

System Manager shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.

[assignment: *the authorised identified roles*]:

None

Hierarchical to: No other components

Dependencies: FMT_MSA.1 (N/A), FMT_SMR.1 (N/A)

5.2.2. Security assurance requirements for the IT environment

Security assurance requirements for the IT environment are not regulated.

6. TOE Summary Specification

6.1. TOE Security Functions

The security functions of the TOE satisfy, as shown in Tables 5 and 6 below, all the TOE security function requirements described in the previous chapter.

Table 5 Security function name and identifier for TOE

Identifier	TOE security function
F.ADMIN	Administrator mode security function
F.SECURE-PRINT	Secure print security function
F.SERVICE	Service mode security function
F.USER-BOX	User box security function

Table 6 Correspondence between TOE security function and TOE security function requirements

TOE Security Function TOE Security functional requirement	F.ADMIN	F.SECURE-PRINT	F.SERVICE	F.USER-BOX
FDP_ACC.1				●
FDP_ACF.1				●
FIA_AFL.1[1]	●			
FIA_AFL.1[2]		●		
FIA_AFL.1[3]				●
FIA_AFL.1[4]			●	
FIA_SOS.1[1]	●			●
FIA_SOS.1[2]	●			
FIA_SOS.1[3]			●	
FIA_UAU.2[1]		●		
FIA_UAU.2[2]				●
FIA_UAU.2[3]	●			
FIA_UAU.2[4]			●	
FIA_UAU.6	●		●	
FIA_UAU.7	●	●	●	●
FIA_UID.2[1]		●		
FIA_UID.2[2]				●

TOE Security Function TOE Security functional requirement	F.ADMIN	F.SECURE-PRINT	F.SERVICE	F.USER-BOX
FIA_UID.2[3]	●			
FIA_UID.2[4]			●	
FMT_MOF.1	●			
FMT_MSA.1	●			●
FMT_MSA.3				●
FMT_MTD.1[1]	●			
FMT_MTD.1[2]	●			●
FMT_MTD.1[3]			●	
FMT_MTD.1[4]			●	
FMT_MTD.1[5]	●			
FMT_SMF.1	●		●	●
FMT_SMR.1[1]				●
FMT_SMR.1[2]	●			
FMT_SMR.1[3]			●	
FMT_SMR.1[4]				●
FPT_RVM.1	●	●	●	●
FPT_SEP.1	●	●	●	●

6.1.1. F.ADMIN (Administrator mode security function)

F.ADMIN is a series of security functions for the administration mode that are accessed from the operations panel on the MFP body or the client PC, such as the administrator identification and authentication functions, the security management function that changes the administrator mode password, the user box password, and the user box identifier, the operation setting function for the access check function, the penalty reset function, etc.

<Identification and authentication function during access to the administrator mode>

- Identifies the accessing user as an administrator by requesting access to the administrator mode.
- Provides an administrator mode password authentication mechanism that authenticates the accessing user as the administrator using the 8-digit number administrator mode password in response to the access request to the administrator mode.
- Returns "*" for each character as feedback for the entered administrator mode password.
- Failing at authentication three times makes it determine that an unauthorized access is being carried out and this authentication function is locked.

<Security management functions in administrator mode that are accessed from the client PC>

- If authentication of the administrator has been carried out for the accessi of the administrator mode from the client PC, the access and operation of the security management function that changes the user box identifier and the user box password for any user box are permitted.

- For changing a user box password, when an entry of a newly set user box password, and a re-entry to prevent an entry error are received, and when both match, the password is replaced for the user box password of the concerned user box.
- Checks that the user box password is 4 to 64 digits and ASCII codes 0x20 to 0x7E (a total of 95 types of English one-byte characters and one byte symbols).

<Security management function in the administrator mode that is accessed from the operations panel of the MFP body>

- When the authentication of an administrator is made for access to the administrator mode from the operations panel on the MFP body, access and operation of (1) the administrator mode password change function, (2) the operation setting function for the access check function and (3) the penalty reset function are permitted.

  (1) Administrator mode password change function,

  ➢ Provides an administrator mode password authentication mechanism that re-authenticates that it is the administrator with the administrator mode password.
  ➢ Returns "*" for each character as feedback for the entry of an administrator mode password during re-authentication.
  ➢ When the entry of a newly set user box password, and the re-entry to prevent entry errors are received, and when both match, the password is replaced as the administrator mode password.
  ➢ Checks that the newly set administrator mode password is an 8-digit number.
  ➢ Counts the count value for the detected number of unauthorized accesses to the administrator mode by the erroneous entries of the administrator mode password that are entered for re-authentication. Failing three times cancels the access permission to the administrator mode and locks the authentication function that accesses administrator mode.

  (2) Operation setting function for the access check function

  ➢ Turn on the access check function by selecting/executing "enable."
  ➢ Turn off the access check function by selecting/executing "disable."

  (3) Penalty reset function

  ➢ Releases the lock on the authentication function that authenticates a general user who is a valid user of a secure print job by clearing the count value to zero for detected unauthorized accesses to secure print for each secure print job.
  ➢ Releases the lock on the authentication function that authenticates a general user who is a valid user of a user box, by clearing the count value to zero for detected unauthorized accesses to the user box for user boxes.

6.1.2. F.SECURE-PRINT (Secure print security function)

F.SECURE-PRINT is a function that identifies and authenticates if a user of secure print job information data is valid for access to the secure print job information data from the operations panel of the MFP body.

<Identification and authentication function to print the secure print job>

- When a secure print job is selected, it provides a secure print password authentication mechanism that authenticates that the person who accesses the selected secure print job information data is a general user who is a valid user of the secure print job, using a 4-digit secure print password.

- Returns “*” for each character as feedback for the entry of the secure print password.
- When the authentication fails three times, it determines that an unauthorized access is being carried out and it locks the authentication function for accessing the secure print job information data. This locked status is released by executing the penalty reset function for the secure print job provided by F.ADMIN.

After it is identified and authenticated, it notifies the “System Manager,” which is a TOE external entity (software component for the IT environment), that the ID and authentication for the secure print job information data were valid. (* printing of the secure print job information data is executed by the “System Manager.”)

6.1.3. F.SERVICE (Service mode security function)

F. SERVICE is a series of security functions for service mode that are accessed from the operations panel of the MFP body, such as the service engineer identification and authentication function, the modification function for the service code, and the initialization function for the administrator mode password.

<Identification and authentication function for access to the service mode>

- Identifies the accessing user as a service engineer by requesting access to the service mode (executes an operations procedure for the service mode that is not disclosed to anyone other than to service engineers).
- When it receives an operations procedure for the service mode, it provides a service code authentication mechanism that authenticates that the accessing user to the service mode is the service engineer by using a password comprised of 8 digits of numbers, “#” or “*” (service code).
- Returns “*” for each character as feedback for the service code entry.
- When the authentication fails three times, it determines that an unauthorized access is being carried out and it locks the authentication function for access to the service mode.

<Security management function for service mode>

- When the person accessing the service mode is authenticated as the service engineer, it permits the access and operation of the security management function for the service mode.

(1) Modification function of the service code

- ➢ The modification function for the service code provides a service code authentication mechanism that re-authenticates the service engineer, after an additional operation procedure, which is not disclosed, is entered in the service mode.
- ➢ Returns “*” for each character as feedback for the service code entry during the re-authentication.
- ➢ Receives the service code entry for a new setting, and the re-entry to prevent an error, and when both are identical, it replaces the service code with the password.
- ➢ Checks that the newly set service code is comprised of 8 digits of numbers, “#” or “*.”
- ➢ When the service code that was entered for this re-authentication is wrong, it cancels the access permission to the service mode, and increments the count value of detected unauthorized access for the service engineer.

(2) Initialization function for the administrator mode password

- ➢ When the initialization function for the administrator mode password is executed, it sets the administrator mode password to default at the setup.

6.1.4. F.USER-BOX (User box security function)

F.USER-BOX is a security function that identifies and authenticates that a general user's access to a user box from a client PC is a valid use of the user box data, controls the access to the user box, creates a user box, and manages the setting of the user box.

<User box creation function>

- A user box creation function is provided to general users.
- When the user box creation function starts up, a process that operates the user box starts up.
- When a user box identifier entered by a general user through the process to operate the user box has not been set to another user box, a user box with the user box identifier entered by the general user as the attribute is created. (If it already exists, it is denied.)

<Identification and authentication function for accessing a user box>

- When a user box to be accessed is selected, it provides a user box password authentication mechanism that authenticates that the user, who is attempting access, is the general user who is the valid user of the user box with a user box password that is comprised of 4 to 64 digits of ASCII code 0x20 to 0x7E (95 types of English one-byte characters and one byte symbols)
- Returns "*" as feedback for the user box password entry.
- When the authentication trial fails 3 times, it locks the authentication function for accessing the target user box. This locked state is released by executing the penalty reset function for the user box provided by F.ADMIN.

<User box access control function after identification and authentication>

- When a general user is authenticated as a general user who is a valid user of the user box, based on the user box access control function, for the process that operates the user box, the "read the user box data in the user box" operation for a user box with a "user box identifier" that is identical to the subject attributes is permitted

<User box setting management function>

- Provides a function to modify the settings of a user box (modification of the user box identifier, modification of the user box password) for the concerned user box to the identified and authenticated valid user of the user box.
- During the modification of the user box password, the entry of a new user box password to be set and the re-entry to prevent erroneous entries are received, and when both are identical, the user box password is modified.
- Checks whether the newly set user box password is comprised of 4 to 64 digits of ASCII code 0x20 to 0x7E (95 types of English one-byte characters and one byte symbols).
- When the authentication trials fail 3 times, it locks the authentication function for the general user who is a valid user of the user box. This locked state is released by executing the penalty reset function for the user box provided by F.ADMIN.

6.2. TOE Security Strength of Function

The TOE security functions that have probabilistic/permutational mechanisms are (1) the administrator mode password authentication mechanism by F. ADMIN, (2) the secure print password authentication mechanism by F.SECURE-PRINT, (3) the user box password authentication mechanism by F.USER-BOX and (4) the service code authentication mechanism provided by F.SERVICE. The strength of each of the functions satisfies the SOF-Basic.

6.3. Assurance measures

The following table shows the assurance measures to meet the component of the TOE security assurance requirements for EAL3 that are stipulated in Table 7.

Table 7Correspondence between TOE assurance requirements and assurance measures

TOE security assurance requirement		Component	Assurance measures
Class ACM: Configuration management	CM capabilities	ACM_CAP.3	• Configuration management plan • Configuration list • CM record
	CM scope	ACM_SCP.1	
Class ADO: Delivery and operation	Delivery	ADO_DEL.1	Delivery instructions
	Installation, generation and start-up	ADO_IGS.1	• Set-up instructions (*Japanese: for domestic use) • Set-up instructions/SET UP INSTRUCTIONS (*Japanese/English bilingual: for abroad) • Installation checklist (*Japanese) • Installation checklist (*English) • Additional information/additional information (*Japanese/English bilingual)
Class ADO: Development	Functional specification	ADV_FSP.1	Security function specifications
	High-level design	ADV_HLD.2	Security high level design specifications
	Representation correspondence	ADV_RCR.1	Representation correpondence analysis report
Guidance document	Administrator guidance	AGD_ADM.1	• User's manual, security kit (*Japanese) Di1810f/Di2510f/Di3010f/Di3510f Di1810/Di2510/Di3010/Di3510 • User manual Security Kit (*English) Di2010f/Di2510f/Di3010f/Di3510f Di2010/Di2510/Di3010/Di3510 • User Manual PageScope Light (*Japanese) • User Manual PageScope Light (*English) • Service Manual Security Kit (*Japanese) Di1810f/Di2510f/Di3010f/Di3510f Di1810/Di2510/Di3010/Di3510 • Service Manual Security Kit (*English) Di2010f/Di2510f/Di3010f/Di3510f Di2010/Di2510/Di3010/Di3510
	User guidance	AGD_USR.1	
Class ALC: Life cycle support	Development security	ALC_DVS.1	Development security instructions
Class ATE: Tests	Coverage	ATE_COV.1	Coverage analysis report
	Depth	ATE_DPT.1	Depth analysis report
	Functional tests	ATE_FUN.1	Test specification and results report
	Independent testing	ATE_IND.2	MFP control software including TOE
Class AVA: Vulnerability assessment	Misuse	AVA_MSU.1	Reflected in the guidance documents
	Strength of TOE security functions	AVA_SOF.1	Strength of Function analysis report
	Vulnerability analysis	AVA_VLA.1	Vulnerability analysis report

7. PP Claims

There is no conformance to a PP in this ST.

8. Rationale

The justification of the contents regulated in this ST is described.

8.1. Security objectives rationale

8.1.1. Necessity

The correspondence between the assumptions, threats and security objectives are shown in the following table. It shows that the security objectives corresponds to at least one assumption or threat.

Table 8 Conformity of security objectives to the assumptions and threats

Assumption/threat Security objectives	A.ACCESS-CHECK	A.ADMIN	A.AUTH	A.HDD	A.NETWORK	A.PHYSICAL	A.SERVICE	A.SESSION	T.ACCESS-SECURE-PRINT	T.ACCESS-USER-BOX	P.BEHAVIOR-ACCESS-CHECK
O.ACCESS-ADMIN									●	●	●
O.ACCESS-USE-BOX										●	
O.ACCESS-SERVICE									●	●	
O.I&A-ADMIN									●	●	●
O.I&A-SERVICE									●	●	
O.I&A-USER									●	●	
OE.ACCESS-SECURE-PRINT									●		
OE.SECURE-PRINT-QUALITY									●		
OE-N.ACCESS-CHECK	●										
OE-N.ADMIN		●									
OE-N.AUTH			●								
OE-N.MAINTENANCE				●							
OE-N.NETWORK					●						
OE-N.PHYSICAL						●					
OE-N.SERVICE							●				
OE-N.STRUCTURE				●							
OE-N.SESSION								●			

8.1.2. Sufficiency for the assumptions

The security objectives for the assumptions are described as follows.

- **A.ACCESS-CHECK (Operation setting conditions for access check function)**
  This condition assumes that the access check function always operates.
  OE-N.ACCESS-CHECK assumes that the administrator turns on the access check function during the use of the MFP with the TOE, and this assures the operation of the access check function.
  And therefore, this condition is realized.

- **A.ADMIN (Roles and condition of the administrator)**
  This condition assumes that the administrator is not malicious.
  With OE-N.ADMIN, the organization that uses the MFP assigns a person who is reliable in the organization that uses the MFP, so the reliability of the administrator is assured.
  And therefore, this condition is realized.

- **A.AUTH (Operational condition regarding password)**
  This condition assumes that each password (secure print password, user box password, administrator mode password, and service code) used for the use of the TOE is not divulged by the user of the password.
  OE-N.AUTH regulates that the person in charge of the organization that uses the MFP enforces compliance, with the operation regulation for the administrator password, to the administrator.
  This security objective regulates that the administrator enforces compliance with the operation rule, regarding the secure print password and user box password, to general users.
  In addition, this security objective regulates that the person in charge of the organization that manages the maintenance of the MFP enforces compliance of the operation rule regarding the service code to the service engineer.
  Therefore, the handling of each password that is used for the use of the TOE is explicitly regulated by the operation rule, and so it is assured that the divulging of a password during the operation should not occur. And therefore, this condition is realized.

- **A.HDD (Protective condition of HDD)**
  This condition assumes that in principle, the HDD installed in the MFP is not taken out, and even if it is unusually taken out by a service engineer, it cannot be taken out unless it is permitted by the administrator.
  The highest risk for an HDD to be taken out is assumed to exist during the maintenance operation of the MFP. OE-N.MAINTENANCE regulates that the organization that uses the MFP does not permit the carrying out of the maintenance operation of the MFP by someone other than the service engineer, and in addition, the maintenance operation of the MFP is carried out in the presence of the administrator so that even the service engineer cannot take out the HDD without getting the permission of the administrator and therefore, it is assured operationally that the HDD is not taken out unlawfully.
  In addition, OE-N.STRUCTURE, assumes that structurally, the HDD cannot be taken out by anyone other than the service engineer, and it physically assures that the HDD will not be taken out.
  This matter is handled operationally and physically, and therefore, this condition is realized.

- **A.NETWORK (network connection conditions for the MFP)**
  This condition assumes that there are no wiretapping activities for the intra-office LAN and no access by an unspecified person from an external network, because of a variety of conditions on the network environment connected to the MFP.
  OE-N.NETWORK regulates measures such as the installation of devices such as a switching hub and encoding between the MFP and client PC, and executes an appropriate environmental setting that does not allow wiretapping, in order to realize a network environment that does not allow wiretapping of the intra-office LAN. It also regulates the installation of devices that block access from external networks to the MFP, and executes an appropriate setting to block external access.
  And therefore, this condition is realized.
  A network environment that does not allow wiretapping can be realized specifically using the following methods, etc.
  (1) Structure the intra-office LAN using switching hubs only and use an intra-office LAN environment based on the operation policy of an office that prohibits wiretapping activities.
  (2) Connect the MFP to the intra-office LAN via a specific device and execute a setting by which all the communication data between the device and client PCs on the intra-office LAN are encoded by, for example, IPsec.

- **A.PHYSICAL (installation conditions for the MFP)**
  This condition assumes that the place where the MFP with the TOE is installed is a physically protected place where only the general users, administrator and service engineer are allowed to enter.
  OE-N.PHYSICAL regulates that the installation of the MFP with the TOE is in an office that is physically protected. In addition, this security objective regulates the execution of an operation management that limits entry to the office to only general users, an administrator and a service engineer, and this assures the physical protection of the TOE.
  And therefore, this condition is realized.

- **A.SERVICE (roles and conditions of service engineer)**
  This condition assumes that the service engineer is not malicious.
  With OE-N.SERVICE, the organization that manages the maintenance of the MFP assigns a reliable person, from the organization that manages the maintenance of the MFP, as the service engineer, so that the reliability of the service engineer is assured.
  And therefore, this condition is realized.

- **A.SESSION (management method for sessions)**
  This condition assumes that a session is always terminated, after the use of each function by each user is completed, as a session management method.
  OE-N.SESSION regulates that the administrator has general users always terminate the session after the use of box function by each user is completed, and the administrator him/herself terminates the session after the use of the administrator function is completed and it is assured that a threat by impersonation will not occur.
  Furthermore, it regulates that the service engineer terminates the session after the use of service engineer function is completed, and it is assured that a threat by impersonation will not occur.
  And therefore this condition is realized.

8.1.3. Sufficiency for the threats

The security objectives against threats are described as follows.

- **T.ACCESS-SECURE-PRINT (Unauthorized operation of the secure print job information data)**
This threat assumes the possibility that secure print job information data is accessed from the operations panel of the MFP body, and the secure print job information data is unlawfully printed. To counter this, verification is carried out that the accessing user is a valid user and access and operation by persons other than authorized valid users is limited.

  As a security objective to counter this threat, O.I&A-USER regulates the identification and authentication of whether the user who is accessing the secure print job information data is a general user who is a valid user of the secure print job. In addition, OE.ACCESS-SECURE-PRINT regulates that only a general user who is identified and authenticated as a valid user is permitted to execute the print operation for secure print job information data, which is the target of the access.
With this authentication function, in order to maintain the strength of function , a certain length of password is required. OE.SECURE-PRINT-QUALITY regulates such that only data, which satisfies the quality metric that is regulated as a secure print password that is configured for a secure print for the printer driver that is installed in the client PC, is received.

  In addition, an operation setting function for the access check function that detects unauthorized access during the authentication function of a general user, who is a valid user of a secure print job, and a penalty reset function that releases the lock status of the authentication function, are provided in administrator mode. O.I&A-ADMIN regulates the identification and authentication of whether the user who is accessing the administrator mode is definitely the administrator, and in addition, O.ACCESS-ADMIN regulates it so that only the administrator is allowed to operate the administrator function. Through the above, we are protected from unauthorized access to the security management function related to the secure print job information data in the administrator mode.

  Furthermore, as countermeasures against service mode, which has a managing function to initialize the administrator mode password, O.I&A-SERVICE regulates the identification and authentication of whether the user who is accessing the service mode is definitely the service engineer, and O.ACCESS-SERVICE regulates so that only the service engineer is allowed to operate the security related functions in service mode.

  And therefore fulfillment of these security objectives can sufficiently counterthis threat.

- **T.ACCESS-USER-BOX (Unauthorized operation to user box data)**
This threat assumes the possibility that the user box data is accessed from the client PC and the user box data is unlawfully downloaded. To counter this, an accessing user should be verified as a valid user and access and operation by anyone other than a person who is authorized as a valid user should be limited.

  As a security objective to counter this threat, O.I&A-USER regulates the identification and authorization of whether the person who is accessing the user box is a general user who is a valid user of the user box. In addition, O.ACCESS-USER-BOX regulates the permission for the download operation of the user box data from the user box, which is the target of access, to only be by the identified and authenticated general user who is a valid user.

In addition, the operation setting function for the access check function that detects unauthorized access during the authentication function of a general user who is a valid user of the user box, and the penalty reset function that releases the locked state of the concerned authentication function, and the setting management function of the user box are provided in the administrator mode. O.I&A-ADMIN regulates the identification and authentication of whether a person who is accessing the administrator mode is definitely the administrator. Furthermore, O.ACCESS-ADMIN regulates so that only the administrator is allowed to operate the administrator function. By doing so, it is protected from unauthorized access to the security management function for the user box data in the administrator mode.

Moreover, as a countermeasure against the service mode having a management function that initializes the administrator mode password, O.I&A-SERVICE regulates the identification and authentication of whether the person who is accessing the service mode is definitely the service engineer. O.ACCESS-SERVICE regulates so that only the service engineer is allowed to operate security-related functions in the service mode.

Therefore, by satisfying these security objectives , it is possible to sufficiently counter these threats.

8.1.4. Sufficiency of the organisational security policies

The security objective that includes the measures for the organisational security policy is described as follows.

- **P.BEHAVIOR-ACCESS-CHECK (operation setting function of the access check function)**
  The organisational security policy stipulates that it is possible to terminate the access check function in order to realize operability with compatibility with the past, in the case it is used in a secure environment. In order to realize this, an operation setting function for the access check function shall be provided. The access check function has the great effect to strength of function, and therefore the management of the function shall be limited to those who can be trusted.

  The security objective that realizes the organisational security policy is regulated by O.I&A-ADMIN for the identification and authentication of whether the person accessing the administrator mode is definitely the administrator. In addition, O.ACCESS-ADMIN regulates so that only the administrator is allowed to operate the administrator function. (The operation setting function of the access check function is provided as one of the administrator functions.)

  And therefore, by fulfilling these two security objectives, it sufficiently realizes the organisational security policy.

8.2. IT security requirements rationale

8.2.1. Rationale for IT security functional requirements

8.2.1.1. Necessity

The correspondence between the security objectives and the IT security functional requirements are shown in the following table. It shows that the IT security functions correspond to at least one security objective.

Table 9 Conformity of IT security functional requirements to the security objectives

Security Objective Security Functional Requirement	O.ACESS-ADMIN	O.ACCESS-USER-BOX	O.ACCESS-SERVICE	O.I&A-ADMIN	O.I&A-SERVICE	O.I&A-USER	OE.ACCESS-SECURE-PRINT	OE.SECURE-PRINT-QUALITY
FDP_ACC.1		●						
FDP_ACF.1		●						
FIA_AFL.1[1]	●			●				
FIA_AFL.1[2]						●		
FIA_AFL.1[3]						●		
FIA_AFL.1[4]			●		●			
FIA_SOS.1[1]	●					●		
FIA_SOS.1[2]	●							
FIA_SOS.1[3]			●					
FIA_UAU.2[1]						●		
FIA_UAU.2[2]						●		
FIA_UAU.2[3]				●				
FIA_UAU.2[4]					●			
FIA_UAU.6	●		●					
FIA_UAU.7	●		●	●	●	●		
FIA_UID.2[1]						●		
FIA_UID.2[2]						●		
FIA_UID.2[3]				●				
FIA_UID.2[4]					●			
FMT_MOF.1	●							
FMT_MSA.1	●	●				●		

Security Objective Security Functional Requirement	O.ACESS-ADMIN	O.ACCESS-USER-BOX	O.ACCESS-SERVICE	O.I&A-ADMIN	O.I&A-SERVICE	O.I&A-USER	OE.ACCESS-SECURE-PRINT	OE.SECURE-PRINT-QUALITY
FMT_MSA.3		●				●		
FMT_MTD.1[1]	●							
FMT_MTD.1[2]	●					●		
FMT_MTD.1[3]			●					
FMT_MTD.1[4]			●					
FMT_MTD.1[5]	●							
FMT_SMF.1	●	●	●			●		
FMT_SMR.1[1]		●				●		
FMT_SMR.1[2]	●							
FMT_SMR.1[3]			●					
FMT_SMR.1[4]		●				●		
FPT_RVM.1*	*	*	*	*	*	*		
FPT_SEP.1*	*	*	*	*	*	*		
FDP_ACC.1[E]							●	
FDP_ACF.1[E]							●	
FIA_SOS.1[E]								●
FMT_MSA.3[E]							●	

* FPT_RVM.1 and FPT_SEP.1 are the requirements that do not directly relate to the security objectives ; however, they are applied as requirements that support the functional requirements that are applied by the related security objectives that are indicated with "*" in the above-mentioned table. This relationship of support (mutual support) will be described in detail in a later section.

8.2.1.2. Sufficiency

The IT security functional requirements for the security objectives are described as follows.

- **O.ACCESS-ADMIN (Management function operated by the administrator)**
  The security objective regulates access to the management functions provided in the administrator mode, and the subject that operates each security management function shall be regulated. For this, the following functional requirements are applied.
  The operation setting management of the Access check function is limited to only the administrator by FMT_MOF.1.

  The operation of the changing of the administrator mode password is limited to the administrator by FMT_MTD.1[1], MFT_SMF.1. The administrator password that is set is verified by FIA_SOS.1[2] is an 8-digit number. The operation of changing the administrator mode password is an important operation in security management, and therefore, FIA_UAU.6 re-authenticates that it is an administrator upon use. At this time, FIA_UAU.7 returns “*” for each character as feedback for the entered administrator mode password. In addition, the number of unsuccessful attempts at this re-authentication is also counted by FIA_AFL.1[1] as unauthorized access to the authentication of an administrator, and therefore the operation to change the administrator mode password is even more strictly protected.

The count value for detected unauthorized access to the user box and the count value for detected unauthorized access to a secure print is limited by FMT_MTD.1[5] and FMT_SMF.1 so that only the administrator carries out the clear operation.

FMT_MTD.1[2], and MFT_SMF.1 allow, in addition to the general user who is a valid user of the user box, the administrator to change the user box password. The set user box password is verified as being 4 to 64 one-byte characters and one-byte symbols by FIA_SOS.1[1].

FMT_MSA.1 and FMT_SMF.1 allow, in addition to the general user who is a valid user of the user box, the administrator to change the user box identifier.

The role that is allowed by FMT_SMR.1[2] to operate the above-mentioned security management function is the administrator.

By combining this multiplicity of functional requirements, this security objective is realized.

- **O.ACCESS-USER-BOX (user box access control)**
  This security objective regulates the download operation of the user box data by a general user. A regulation that controls the creation of a user box and access to the user box by general users is necessary. For this, the following functional requirements are employed for this.

  In accordance with FDP_ACC.1 and FDP_ACF.1, which define the access control policy to the user box, during the process of user box operation, if there is no user box with the same name as the entered “user box identifier” in existence, access control is carried out so that an operation to create a user box with the name as its attribute is permitted. (If a user box with the same name as the entered “user box identifier” exists, the operation of creation is denied.)
  In addition, with the same functional requirement, access control that permits an operation, to “read the user box data in the user box” for the user box having the “user box identifier,” which matches the selected “user box identifier selected by the general user” and kept by the operated process by the user box, is executed.
  In principle, this security objective is satisfied by the above-mentioned FDP-ACC.1 and FDP_ACF.1. The following functional requirements that are described are the functional requirements related to the user box access control.

FMT_MSA.3 gives a blank (null), which is a permitted value, as the default value of the user box identifier that is used as a security attributes. This value can be set to an appropriate default value by only the general user who creates the user box.
The role is given by FMT_SMR.1[4] to the general users who create the user box, in order to set the blank of the above-described user box identifier to an appropriate default.

FMT_MSA.1 and FMT_SMF.1 allow general users who are valid users of the user box to change the user box identifier.
The role is given by FMT_SMR.1[1] to the general users who are valid users of the user box so that they are allowed to operate the above-described security management function.

In addition to the above-mentioned functional requirements that regulate access control, the functional requirements that are equivalent to the management of the access control are combined and therefore, this security objective is realized.

- **O.ACCESS-SERVICE (management function operated by the service engineer)**
  This security objective regulates the access to the management function for the service engineer that is provided under the service mode. Additionally, the subject that allows operation of each security management function shall be regulated. For this, the following functional requirements are applied.

  FMT_MTD.1[3] and FMT_SMT.1 limit the changing of the service code so that only the service engineer can change the setting. The set service code is limited by FIA_SOS.1[3] to 8 digits of numbers and "#" and "*." The changing of the service code is an important operation for the security management and therefore, FIA_UAU.6 re-authenticates that the person is a service engineer upon use. At that time, FIA_UAU.7 returns "*" for each character entered as feedback for the entered service code. In addition, the number of unsuccessful attempts at this re-authentication is also counted by FIA_AFL.1[4] as unauthorized access to the authentication of a service engineer, and therefore the operation to change the administrator mode password is even more strictly protected.

  The operation to initialize the administrator mode password is limited to the service engineer only by FMT_MTD.1[4] and MFT_SMF.1.

  The role is given by FMT_SMR.1[3] to the service engineer so that they can operate the above-mentioned security management function.

  By combining this multiplicity of functional requirements, this security objective is realized.

- **O.I&A-ADMIN (identification and authentication of the administrator)**
  This security objective regulates the authentication of whether the person who is accessing the administrator mode is definitely the administrator, and appropriate conditions upon authentication are required. The following functional requirements are applied.

  The user who accesses the administrator mode is identified and authenticated as the administrator by FIA_UID.2[3] and FIA_UAU.2[3]. During the authentication, FIA_UAU.7 returns "*" for each character entered as feedback for the entered administrator mode password.
  During accessing of the administrator mode, if the administrator authentication is unsuccessful three times, FIA_AFL.1[1] determines it as an unauthorized access, and it locks the access to the authentication function from thereon, and therefore it is strictly protected.

By combining this multiplicity of functional requirements, this security objective is realized.

- **O.I&A-SERVICE (identification and authentication of the service engineer)**
  This security objective regulates the authentication of whether the person who is accessing the service mode is definitely the service engineer, and appropriate conditions upon authentication are required. For this, the following functional requirements are applied.

  The user who accesses the service mode is identified and authenticated as the service engineer by FIA_UID.2[4] and FIA_UAU.2[4]. During the authentication, FIA_UAU.7 returns "*" for each character entered as feedback for the entered service code.
  During accessing of the service mode, if the service engineer authentication is unsuccessful three times, FIA_AFL.1[4] determines it as an unauthorized access, and it locks the access to the authentication function from thereon, and therefore it is strictly protected.

  By combining this multiplicity of functional requirements, this security objective is realized.

- **O.I&A-USER (identification and authentication of the general users)**
  This security objective regulates the identification and authentication of whether the user who is accessing a secure print job is a general user who is a valid user of the secure print job. In addition, it also regulates the identification and authentication of whether the user who is downloading the user box data is a general user who is a valid user of the user box, and therefore, appropriate conditions for the identification and authentication are required. For this, the following functional requirements are applied.

<Identification and authentication of the general user for accessing a secure print job>

FIA_UID.2[1] and FIA_UAU.2[1] identify and authenticate whether a general user is the valid user of the secure print job. (The authentication strength of the secure print password used during this authentication is assured by OE.SECURE-PRINT-QUALITY. See the description in a later section.)

During the authentication of a general user who is the valid user of the secure print job, FIA-UAU.7 returns "*" for each character entered as feedback for the entered secure print password.

If authentication for the secure print job fails 3 times, FIA_AFL.1[2] determines that it is unauthorized access and the authentication function for the general user who is the valid user of the secure print job is locked from thereon. The lock can be released by FMT_MTD.1[5] that is related to O.ACCESS-ADMIN.

<Identification and authentication of the general user for accessing the user box data>

FIA_UID.2[2] and FIA_UAU.2[2] identify and authenticate whether a person accessing the user box is the general user who is a valid user of the user box.

The above-mentioned, during each authentication according to FIA_UAU.2[2], FIA_UAU.7 returns "*" for each character entered as feedback for the entered user box password.

If any authentication fails 3 times, FIA_AFL.1[3] determines that it is an unauthorized access and the authentication function for the general user who is the valid user of the user box is locked from thereon.
The lock can be released by FMT_MTD.1[5] that is related to O.ACCESS-ADMIN.

FMT_MSA.3 gives a blank (null), which is a permitted value, as the default value of the user box identifier that is used to identify the general user who is a valid user of the user box. This value can be set to an appropriate default value by only the general user who creates the user box.
The role is given by FMT_SMR.1[4] to the general users who create the user box, in order to set the blank of the above-described user box identifier to an appropriate default.

FMT_MSA.1 and FMT_SMF.1 allow general users who are valid users of the user box, as well as the administrator to change the user box identifier.

FMT_MTD.1[2] and FMT_SMF.1 allow general users who are valid users of the user box, as well as the administrator to change the user box password. FIA_SOS.1[1] verifies that the set user box password is 4 to 64 digits of English one-byte characters and one-byte symbols.

The role is given by FMT_SMR.1[1] to the valid users of the user box, in order to operate the above-mentioned security management function.

By combining this multiplicity of functional requirements, this security objective is realized.

- **OE.ACCESS-SECURE-PRINT (secure print job access control)**
  This security objective regulates such that the System Manager, which is an IT environment, limits the print operation of the secure print job information data. An access control that is executed during the printing of a secure print job is required. For this, the following functional requirements are applied.

  When a request to register a secure print job is received, in accordance with FDP_ACC.1[E] and FDP_ACF.1[E], a “newly assigned job ID” is created by the process that operates the secure print job by the system manager, and an access control that registers the secure print job information data file with the above as an attribute is carried out. The default value of the job ID that is used as the security attributes is isolated from other jobs by FMT_MSA.3[E], and a value that can be uniquely identified is assigned.
  During the printing, in accordance with FDP_ACC.1[E] and FDP_ACF.1[E], “A job ID for the secure print job selected by a general user” is given to the process that operates the secure print job by the system manager, and an access control that prints the secure print job information data having the matched “job ID” is executed.

  This security objective is realized by combining these multiplicities of functional requirements.

- **OE.SECURE-PRINT-QUALITY (quality metric of the secure print password)**
  This security objective regulates the addition of a password with an assured strength to the secure print job information data when spooling the secure print to the MFP where the TOE is loaded, at the printer driver of the client PC that is an IT environment.

For this, in accordance with FIA_SOS.1[E], the printer driver of the client PC verifies whether the set secure print password is a 4-digit number. Therefore when the secure print is spooled to the MFP, a 4-digit password is always assigned.
This security objective is realized by this functional requirement.

8.2.1.3. Mutual support

(1) Complementarity
The IT Security functional requirements for effectively operating other security functional requirements without having a direct corresponding relationship with the security objectives are shown in the following table.

Table 10 Mutual support correlations of IT security functional requirements

N/A:Not Applicable

IT Security Functional Requirement	Functional requirements component that operates other security functional requirements validly			
	(1) Bypass Prevention	(2) Interference/destruction prevention	(3) Deactivation prevention	(4) Disabling detection
FDP_ACC.1	N/A	FPT_SEP.1	N/A	N/A
FDP_ACF.1	N/A	FPT_SEP.1	N/A	N/A
FIA_AFL.1[1]	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1	N/A
FIA_AFL.1[2]	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1	N/A
FIA_AFL.1[3]	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1	N/A
FIA_AFL.1[4]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_SOS.1[1]	N/A	FPT_SEP.1	N/A	N/A
FIA_SOS.1[2]	N/A	FPT_SEP.1	N/A	N/A
FIA_SOS.1[3]	N/A	FPT_SEP.1	N/A	N/A
FIA_UAU.2[1]	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1	N/A
FIA_UAU.2[2]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UAU.2[3]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UAU.2[4]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UAU.6	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UAU.7	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UID.2[1]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UID.2[2]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UID.2[3]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UID.2[4]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FMT_MOF.1	N/A	FPT_SEP.1	N/A	N/A
FMT_MSA.1	N/A	FPT_SEP.1	N/A	N/A
FMT_MSA.3	N/A	FPT_SEP.1	N/A	N/A
FMT_MTD.1[1]	N/A	FPT_SEP.1	N/A	N/A
FMT_MTD.1[2]	N/A	FPT_SEP.1	N/A	N/A
FMT_MTD.1[3]	N/A	FPT_SEP.1	N/A	N/A
FMT_MTD.1[4]	N/A	FPT_SEP.1	N/A	N/A
FMT_MTD.1[5]	N/A	FPT_SEP.1	N/A	N/A
FMT_SMF.1	N/A	FPT_SEP.1	N/A	N/A
FMT_SMR.1[1]	N/A	FPT_SEP.1	N/A	N/A
FMT_SMR.1[2]	N/A	FPT_SEP.1	N/A	N/A
FMT_SMR.1[3]	N/A	FPT_SEP.1	N/A	N/A
FMT_SMR.1[4]	N/A	FPT_SEP.1	N/A	N/A
FPT_RVM.1	N/A	FPT_SEP.1	N/A	N/A
FPT_SEP.1	N/A	N/A	N/A	N/A
FDP_ACC.1[E]	N/A	N/A	N/A	N/A
FDP_ACF.1[E]	N/A	N/A	N/A	N/A
FIA_SOS.1[E]	N/A	N/A	N/A	N/A

IT Security Functiona; Requirement	Functional requirements component that operates other security functional requirements validly			
	(1) Bypass Prevention	(2) Interference/destruction prevention	(3) Deactivation prevention	(4) Disabling detection
FMT_MSA.3[E]	N/A	N/A	N/A	N/A

1) Bypass prevention

TSP execution functions are as follows.

1. An identification and authentication function for accessing a secure print job, which is a function that should be executed before permitting the operation advancement of the access control function for the secure print job (Executed by FIA_UID.2[1], FIA_UAU.2[1], FIA_UAU.7, and FIA_AFL.1[2])
2. An authentication function for a general user who is a valid user of the user box, which is a function that should be executed before permitting the operation advancement of the access control function for the user box data and the setting management of the user box (change in user box password and user box identifier) operated by a general user. (Executed by FIA_UID.2[2], FIA_UAU.2[2], FIA_UAU.7 and FIA_AFL.1[3].)
3. An identification and authentication for the administrator, which is a function that should be executed before permitting the operation advancement of the security management function in the administrator mode. (Executed by FIA_UID.2[3], FIA_UAU.2[3], FIA_UAU.7 and FIA_AFL.1[1].)
4. An administrator re authentication function, which is a function that should be executed before permitting the operation advancement of the function to change the administrator mode password, from among the security management functions in the administrator mode. (Executed by FIA_UAU.2[3], FIA_UAU.6, FIA_UAU.7, and FIA_AFL.1[1].)
5. A function that identifies and authenticates the service engineer, which is a function that should be executed before permitting the operation advancement of the security management function in the service mode. (Executed by FIA_UID.2[4], FIA_UAU.2[4], FIA_UAU.7, and FIA_AFL.1[4].)
6. A service engineer re authentication function, which is a function that should be executed before permitting the operation advancement of the function to change the service code, from among the security management functions in the service mode. (Executed by FIA_UAU.2[4], FIA_UAU.6, FIA_UAU.7 and FIA_AFL.1[4].)

As described above, the TSP execution function is supported such that everything is always called by FPT_RVM.1 and successes.

2) Interference and destruction prevention

To realize FPT_SEP.1, the TOE maintains the following.

- Security domain in the individual user box
- Security domain in administrator mode
- Security domain in service mode

Therefore, there is support such that there is no interference or tampering by an unreliable subject of the security domain that is the protected asset scope of the TOE and the operation scope of the TSF.

3) Deactivation prevention

FMT_MOF.1 limits the management of the detection/lock during the detection of an unsuccessful authentication (FIA_AFL.1[1], FIA_AFL.1[2], FIA_AFL.1[3]) and operation of the authentication for accessing a user box (FIA_UAU.2[2]) to the administrator only and FMT_MOF.1 provides a protection against an attack that attempts to deactivate these operations.

4) Disabling detection
Because of the security functional requirements that have already been employed by taking bypass prevention and interference and destruction prevention into account, even though security that relates to disabling detection is not considered, it has a structure that adequately satisfies the required security objective. Therefore, security functional requirements to detect an attack that disables the security function are not applied.

(2) Dependencies of the IT security functional requirements
The dependencies of the IT security functional requirements components are shown in the following table. When a dependency regulated in CC Part 2 is not satisfied, the reason is provided in the section for the “dependencies Relation in this ST.”

Table 11 Dependencies of the IT security functional requirements

Functional requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1, FMT_MSA.3
FIA_AFL.1[1]	FIA_UAU.1	FIA_UAU.2[3] <Supplement> FIA_UAU.2 is hierarchical component to FIA_UAU.1 and therefore, the dependencies are satisfied.
FIA_AFL.1[2]	FIA_UAU.1	FIA_UAU.2[1] <Supplement> FIA_UAU.2 is hierarchical component to FIA_UAU.1 and therefore, the dependencies are satisfied.
FIA_AFL.1[3]	FIA_UAU.1	FIA_UAU.2[2] <Supplement> FIA_UAU.2 is hierarchical component to FIA_UAU.1 and therefore, the dependencies are satisfied.
FIA_AFL.1[4]	FIA_UAU.1	FIA_UAU.2[4] <Supplement> FIA_UAU.2 is hierarchical component to FIA_UAU.1 and therefore, the dependencies are satisfied.
FIA_SOS.1[1]	None	None
FIA_SOS.1[2]	None	None
FIA_SOS.1[3]	None	None

Functional requirements Component for this ST	Dependencies on CC Part 2	Dependencies in this ST
FIA_UAU.2[1]	FIA_UID.1	FIA_UID.2[1] <Supplement> FIA_UID.2 is hierarchical component to FIA_UID.1 and therefore, the dependencies are satisfied.
FIA_UAU.2[2]	FIA_UID.1	FIA_UID.2[2] <Supplement> FIA_UID.2 is hierarchical component to FIA_UID.1 and therefore, the dependencies are satisfied.
FIA_UAU.2[3]	FIA_UID.1	FIA_UID.2[3] <Supplement> FIA_UID.2 is hierarchical component to FIA_UID.1 and therefore, the dependencies are satisfied.
FIA_UAU.2[4]	FIA_UID.1	FIA_UID.2[4] <Supplement> FIA_UID.2 is hierarchical component to FIA_UID.1 and therefore, the dependencies are satisfied.
FIA_UAU.6	None	None
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2[1], FIA_UAU.2[2], FIA_UAU.2[3], FIA_UAU.2[4]
FIA_UID.2[1]	None	None
FIA_UID.2[2]	None	None
FIA_UID.2[3]	None	None
FIA_UID.2[4]	None	None
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[2]
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	FDP_ACC.1, FMT_SMF.1, FMT_SMR.1[1], FMT_SMR.1[2]
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1, FMT_SMR.1[4]
FMT_MTD.1[1]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[2]
FMT_MTD.1[2]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[1], FMT_SMR.1[2]
FMT_MTD.1[3]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[3]
FMT_MTD.1[4]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[3]
FMT_MTD.1[5]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[2]
FMT_SMF.1	None	None

Functional requirements Component for this ST	Dependencies on CC Part 2	Dependencies in this ST
FMT_SMR.1[1]	FIA_UID.1	FIA_UID.2[2] <Supplement> FIA_UID.2 is hierarchical component to FIA_UID.1 and therefore, the dependencies are satisfied.
FMT_SMR.1[2]	FIA_UID.1	FIA_UID.2[3] <Supplement> FIA_UID.2 is hierarchical component to FIA_UID.1 and therefore, the dependencies are satisfied.
FMT_SMR.1[3]	FIA_UID.1	FIA_UID.2[4] <Supplement> FIA_UID.2 is hierarchical component to FIA_UID.1 and therefore, the dependencies are satisfied.
FMT_SMR.1[4]	FIA_UID.1	None <Reason why it does not satisfy FIA_UID.1> Creation of the user box is allowed for an arbitrary general user and therefore there is no need to identify the user that is related to this role.
FPT_RVM.1	None	None
FPT_SEP.1	None	None
FDP_ACC.1[E]	FDP_ACF.1	FDP_ACF.1[E]
FDP_ACF.1[E]	FDP_ACC.1 FMT_MSA.3	FDP_ACF.1[E], FMT_MSA.3[E]
FIA_SOS.1[E]	None	None
FMT_MSA.3[E]	FMT_MSA.1 FMT_SMR.1	None <Reason why it does not satisfy (1) FMT_MSA.1 and (2) FMT_SMR.1> (1) The job ID is an identifier that is assigned to distinguish between jobs and therefore, there is no need to allow an operation to change or delete the default. In addition, the job ID is not confidential, and therefore, there is no need to limit users who make an inquiry. (2) The job ID is an identifier that is assigned to distinguish between jobs and therefore, there is no need to change it to an alternative default value. Thus, there is no need to regulate the role designated based on the above.

As described above, sets of IT security requirements have a structure that mutually support each other as a whole, as shown in the dependencies in (1) complementarity and (2) IT security functional requirements.

8.2.2. Rationale for Minimum Strength of Function

The MFP that is loaded with this TOE is installed in a general office environment where an entry to the office is controlled, and is connected to an intra-office LAN with appropriately controlled connections with external networks. Therefore, there is no possibility that it is directly attacked by unspecified people via the Internet. As long as it has a strength level that can counter the threat by general users who are users of the TOE and a person in the office as an agent, it is acceptable, as explicitly described in section 3.2. Therefore, this TOE regulates security objectives by assuming an unskilled attacker and thus, the selection of the SOF-Basic as the minimum strength of function is reasonable.

8.2.3. Rationale for IT security assurance requirements

This TOE is installed and used in an environment where adequate security is maintained in terms of the physical, personnel, and connectivity. Nonetheless, adequate effectiveness in the environment where the TOE is used shall be assured. As a general commercial office product, the execution of tests based on function specifications and high level design, and analysis of the strength of function and a search for vulnerabilities are required. In addition, it is desirable that it has a development environment control, a configuration management for the TOE and a secure distribution procedure. And therefore, the selection of EAL3, which provides an adequate assurance level is reasonable.

8.3. Rationale for TOE Summary Specifications

8.3.1. Rationale for the TOE security functions

8.3.1.1. Necessity

The conformity of the TOE security functions and the TOE security functional requirements are shown in the following table. It shows that the TOE security functions correspond to at least one TOE security functional requirement.

Table 12 Conformity of the TOE security functions with the TOE security functional requirements

TOE Security function TOE Security Functional Requirement	F.ADMIN	F.SECURE-PRINT	F.SERVICE	F.USER-BOX
FDP_ACC.1				●
FDP_ACF.1				●
FIA_AFL.1[1]	●			
FIA_AFL.1[2]		●		
FIA_AFL.1[3]				●
FIA_AFL.1[4]			●	
FIA_SOS.1[1]	●			●
FIA_SOS.1[2]	●			
FIA_SOS.1[3]			●	
FIA_UAU.2[1]		●		
FIA_UAU.2[2]				●
FIA_UAU.2[3]	●			
FIA_UAU.2[4]			●	
FIA_UAU.6	●		●	
FIA_UAU.7	●	●	●	●
FIA_UID.2[1]		●		
FIA_UID.2[2]				●
FIA_UID.2[3]	●			
FIA_UID.2[4]			●	
FMT_MOF.1	●			
FMT_MSA.1	●			●
FMT_MSA.3				●
FMT_MTD.1[1]	●			
FMT_MTD.1[2]	●			●

TOE Security function TOE Security Functional Requirement	F.ADMIN	F.SECURE-PRINT	F.SERVICE	F.USER-BOX
FMT_MTD.1[3]			●	
FMT_MTD.1[4]			●	
FMT_MTD.1[5]	●			
FMT_SMF.1	●		●	●
FMT_SMR.1[1]				●
FMT_SMR.1[2]	●			
FMT_SMR.1[3]			●	
FMT_SMR.1[4]				●
FPT_RVM.1	●	●	●	●
FPT_SEP.1	●	●	●	●

8.3.1.2. Sufficiency

The TOE security functions for the TOE security functional requirements are described.

- FDP_ACC.1
  FDP_ACC.1 regulates the relationship between the controlled subject to the object: the user box and the operation.
  F.USER-BOX executes the operation: “user box access control” that controls the “creation” and the “reading of the user box data in the user box” to the object: “user box” of the subject: “process that operates the user box.”
  Therefore, this functional requirement is satisfied.

- FDP_ACF.1
  FDP_ACF.1 regulates the regulation of the controlled subject: “a process that operates the user box,” object: “user box,” and operation: “reading of the user box data in the user box” and “creation.”
  F.USER-BOX executes the user box access control that is comprised of the following three regulations.
  - ➢ The process that operates the user box having a selected “user box identifier” is permitted the operation of reading the user box data in the user box to the user box having an identical “user box identifier” as above.
  - ➢ The process that operates the user box having the entered “user box identifier” is permitted the operation of creating a user box having the entered “user box identifier” as an object attributes when there is no user box having a “user box identifier” that is identical to the above.

- ➢ The process that operates the user box having the entered "user box identifier" executes the denied control of the operation of creating a user box having an entered "user box identifier" as an object attributes, when there is a user box having a "user box identifier" that is identical to the above.

Therefore, this functional requirement is satisfied.

- FIA_AFL.1[1]

FIA_AFL.1[1] regulates the detection of unauthorized access, when a certain number of unsuccessful authentication attempts for the authentication event related to the administrator mode occurs, and the execution of some action after the detection of the unauthorized access. F.ADMIN locks the authentication function when three unsuccessful attempts are detected during the authentication to access administrator mode, or a re-authentication for the function to change the administrator mode password. (In the case of re-authentication for the function to change the administrator mode password, access to administrator mode is denied and then the authentication function to access administrator mode is locked.) There is no function to reset this lock.

Therefore, this functional requirement is satisfied.

- FIA_AFL.1[2]

FIA_AFL.1[2] regulates the detection of unauthorized access when a certain number of unsuccessful authentication attempts for the authentication event related to the secure print job information data occurs, and a method of recovery to the normal state after some action is executed when an unauthorized access is detected.

F. SECURE-PRINT locks the authentication function when three unsuccessful attempts are detected during the authentication to access secure print job information data. This locked state is reset by executing the penalty reset function provided by F. ADMIN.

Therefore, this functional requirement is satisfied.

- FIA_AFL1[3]

FIA_AFL1[3] regulates the detection of unauthorized access when a certain number of unsuccessful authentication attempts occurs for the authentication event related to the user box data, and a method of recovery to the normal state after some action is executed when an unauthorized access is detected.

F.USER-BOX locks the authentication function when three unsuccessful attempts are detected during the authentication to access a user box. This locked state is reset by executing the penalty reset function provided by F. ADMIN.

Therefore, this functional requirement is satisfied.

- FIA_AFL1[4]

FIA_AFL1[4] regulates the detection of unauthorized access when a certain number of unsuccessful authentication attempts for the authentication event related to the authentication of a service engineer occurs as well as the execution of some action after the detection of the unauthorized action.

F.SERVICE locks the authentication function when three unsuccessful attempts are detected during the authentication to access service mode, or the re-authentication for the function to change the service code. (In the case of re-authentication for the function to change the service code, access to the service is denied and then the authentication function to access service mode is locked.) There is no function to reset this lock.

Therefore, this functional requirement is satisfied.

- FIA_SOS.1[1]
  FIA_SOS.1[1] regulates the quality metric of the user box password, which is a minimum of 4 digits and a maximum of 64 digits of one-byte English characters or one-byte symbols.
  F.USER-BOX checks whether 4- to 64-digit ASCII code 0x20 to 0x7E (one-byte English characters or one-byte symbols, 95 types) is set as the quality metric of the user box password for the function to change the user box password.
  F.ADMIN checks whether 4- to 64-digit ASCII code 0x20 to 0x7E (one-byte English characters or one-byte symbols, 95 types) is set as the quality metric of the user box password for the function to change the user box password.
  Therefore, this functional requirement is satisfied.

- FIA_SOS.1[2]
  FIA_SOS.1[2] regulates the quality metric of the administrator mode password, which is an 8-digit number.
  F.ADMIN checks whether an 8-digit number is set as the quality metric for the administrator mode password.
  Therefore, this functional requirement is satisfied.

- FIA_SOS.1[3]
  FIA_SOS.1[3] regulates the quality metric of the service code, which is 8 digits of numbers, "*" or "#."
  F.SERVICE checks whether 8 digits of numbers, "*" or "#" is set as the quality metric for the service code for the function to change the service code.
  Therefore, this functional requirement is satisfied.

- FIA_UAU.2[1]
  FIA_UAU.2[1] regulates the authentication of a general user who is a valid user of the secure print job, during the access of a general user to the secure print job information data.
  F. SECURE-PRINT authenticates a general user who is a valid user of a secure print job through a secure print password during the access to the secure print job information, and permits execution of the operations that are available for the secure print job information data, for which the subject is only an authenticated general user who is the valid user of the secure print job.
  Therefore, this functional requirement is satisfied.

- FIA_UAU.2[2]
  FIA_UAU.2[2] regulates the authentication of a general user who is a valid user of the user box during the accessing by a general user to the user box.
  F. USER-BOX authenticates a general user who is a valid user of the user box through a user box password, and permits the execution of access to the user box, for which the subject is only the authenticated general user who is the valid user of the user box.
  Therefore, this functional requirement is satisfied.

- FIA_UAU.2[3]
  FIA_UAU.2[3] regulates the authentication of the administrator before using the administrator function.
  F. ADMIN authenticates the administrator during the accessing of administrator mode, and permits execution of the operations available only for the authenticated administrator in administrator mode. In addition, it authenticates (re-authenticates) the administrator before the execution of the function to change the administrator mode password, which is a security management function in the administrator mode.

Therefore, this functional requirement is satisfied.

- FIA_UAU.2[4]
  FIA_UAU.2[4] regulates the authentication of the service engineer before using the service engineer functions.
  F.SERVICE authenticates the service engineer during the accessing of service mode, and permits the execution of the operations available only to the service engineer in service mode. In addition, it authenticates (re-authenticates) the service engineer before the execution of the function to change the service code, which is a security management function in service mode.
  Therefore, this functional requirement is satisfied.

- FIA_UAU.6
  FIA_UAU.6 regulates an authentication event that requires re-authentication.
  F.ADMIN re-authenticates the administrator during the function to change the administrator mode password, which is an important function in terms of the security for the administrator who has already been permitted access to administrator mode, and it permits only a re-authenticated administrator to execute the function to change the administrator mode password.
  F.SERVICE re-authenticated the service engineer during the function to change the service code, which is an important function in terms of security for the service engineer who has already been permitted access to service mode, and it permits only a re-authenticated service engineer to execute the function to change the service code.
  Therefore, this functional requirement is satisfied.

- FIA_UAU.7
  FIA_UAU.7 regulates the return of “*” as feedback during authentication.
  F.SECURE-PRINT returns “*” for each character as feedback for the character entry (secure print password) for authentication during access to secure print job information data.
  F.USER-BOX returns “*” for each character as feedback for the character entry (user box password) for authentication during access to the user box.
  F.ADMIN returns “*” for each character as feedback for the character entry for the following cases.
  - Characters entered for the authentication function during accessing from the operations panel of the MFP body or the client PC in administrator mode.
  - Characters entered for the re-authentication function when changing the administrator mode password.

  F.SERVICE returns “*” for each character as feedback for the character entry for the following cases.
  - Characters entered for the authentication function that uses the service code during accessing to service mode.
  - Characters entered for the re-authentication function when changing the service code.

  Therefore, this functional requirement is satisfied.

- FIA_UID.2[1]
  FIA_UID.2[1] regulates the identification of the valid user of a secure print job during the accessing of the secure print job information data by a general user.
  F.SECURE-PRINT identifies a general user who is a valid user of the secure print job through the selection of a secure print job, which is the object to be operated by the general user, based on the name of the secure print job, during the accessing of the secure print job information data.
  Therefore, this functional requirement is satisfied.

- FIA_UID.2[2]
  FIA_UID.2[2] regulates the identification of a valid user of a user box during the access to the user box by a general user.
  F.USER-BOX identifies a general user who is a valid user of the user box through the selection of the user box that is set, during the accessing of the user box.
  Therefore, this functional requirement is satisfied.

- FIA_UID.2[3]
  FIA_UID.2[3] regulates the identification of a user as an administrator before they use the administrator functions.
  F.ADMIN identifies the user as an administrator by the access request of the user to the administrator mode.
  Therefore, this functional requirement is satisfied.

- FIA_UID.2[4]
  FIA_UID.2[4] regulates the identification of a user as a service engineer before they use the service engineer functions.

  F.SERVICE identifies the user as a service engineer by access request of the user to the service mode (execution of an operation procedure that is not public).
  Therefore, this functional requirement is satisfied.

- FMT_MOF.1
  FMT_MOF.1 regulates the behavior management of the access check function by the administrator.
  F.ADMIN provides a setting management function that enables and disables the access check function.
  Therefore, this functional requirement is satisfied.

- FMT_MSA.1
  FMT_MSA.1 regulates the limitation on the operation to change the user box identifier, which is a security attribute that is used for the user box access control, to “a general user who is the valid user of the user box” and the administrator.
  F.ADMIN provides a function to change the user box identifier operated by the administrator in administrator mode.
  F.USER-BOX provides a function to change the user box identifier operated by the general user who is the valid user, who is permitted to access the user box.
  Therefore, this functional requirement is satisfied through the operation of these two TOE security functions.

- FMT_MSA.3
  FMT_MSA.3 regulates the permitted default value during the creation of the user box identifier, which is the security attribution used during the user box access control. In addition, it regulates the limitation on the role of setting an initial value that replaces the default value to the general user who creates the user box.
  F.USER-BOX provides a blank (null) as a default value for the user box identifier, when the function to create a user box is started, and also provides a function to create a user box identifier that sets an alternative initial value to the blank for the general user who creates the user box.
  Therefore, this functional requirement is satisfied.

- FMT_MTD.1[1]
  FMT_MTD.1[1] regulates the role of changing the administrator mode password, which is TSF data.
  F.ADMIN provides a function to change the administrator mode password operated by the administrator in administrator mode.
  Therefore, this functional requirement is satisfied.

- FMT_MTD.1[2]
  FMT_MTD.1[2] regulates the role of changing the user box password, which is TSF data.
  F.ADMIN provides a function to change the user box password operated by the administrator in administrator mode.
  F.USER-BOX provides a function to change the user box password operated by a general user who is the valid user of the user box.
  Therefore, this functional requirement is satisfied by the operation of these two TOE security functions.

- FMT_MTD.1[3]
  FMT_MTD.1[3] regulates the role of changing the service code.
  F.SERVICE provides a function to change the service code operated by the service engineer in service mode.
  Therefore, this functional requirement is satisfied.

- FMT_MTD.1[4]
  FMT_MTD.1[4] regulates the role of initializing the administrator mode password.
  F.SERVICE provides a function to initialize the administrator mode password operated by the service engineer in service mode. When this function is executed, a default value during set up is set as the administrator mode password.
  Therefore, this functional requirement is satisfied.

- FMT_MTD.1[5]
  FMT_MTD.1[5] regulates the role of deleting the detected unauthorized access count value for a secure print, and the detected unauthorized access count value for the user box.
  F.ADMIN provides a penalty reset function operated by the administrator in administrator mode. This function clears the detected unauthorized access count value for the secure print, or the detected unauthorized access count value to zero.
  Therefore, this functional requirement is satisfied.

- FMT_SMF.1
  FMT_SMF.1 regulates the security management functions that are provided by the TOE.
  F.USER-BOX provides the following security management functions, operated by a general user who is the valid user of the user box, for the user box.
  - ➢ Function to change the user box identifier of the user box
  - ➢ Function to change the user box password for the user box

  In addition, F.USER-BOX provides the following security management functions for the general user who creates the user box, during the creation of a user box.
  - ➢ Function to create a user box identifier

F.ADMIN provides the following security management functions operated by the administrator in administrator mode.

- ➢ Operation setting function for the access check function
- ➢ Penalty reset function that clears the detected unauthorized access count value for a secure print to zero
- ➢ Penalty reset function that clears the detected unauthorized access count value for a user box to zero
- ➢ Function to change the administrator password.
- ➢ Function to change the user box identifier for any user box
- ➢ Function to change the user box password for any user box

F.SERVICE provides the following security management functions operated by the service engineer in service mode.

- ➢ Function to change the service code
- ➢ Initialization function for the administrator mode password.

Therefore, this functional requirement is satisfied.

- FMT_SMR.1[1]
  FMT_SMR.1[1] regulates the role as a “general user who is the valid user of the user box.”
  F.USER-BOX authorizes an identified and authenticated user as the “general user who is a valid user of the user box” for access to the user box. And therefore, this functional requirement is satisfied.

- FMT_SMR.1[2]
  FMT_SMR.1[2] regulates the role as an “administrator”
  F.ADMIN authorizes an authenticated user as the “administrator” for access to administrator mode.
  Therefore, this functional requirement is satisfied.

- FMT_SMR.1[3]
  FMT_SMR.1[3] regulates the role asa “service engineer”
  F.SERVICE authorizes an authenticated user as the “service engineer” for access to service mode.
  Therefore, this functional requirement is satisfied.

- FMT_SMR.1[4]
  FMT_SMR.1[4] regulates the role as a “general user who is the valid user of the user box.”
  F.USER-BOX authorizes a user who starts a function to create a user box as a “general user who is the valid user of the user box” for the creation of a user box.
  Therefore, this functional requirement is satisfied.

- FPT_RVM.1
  FPT_RVM.1 regulates support so that the TSP enforcement functions are always invoked before each security function within the TOE is allowed to proceed. F.ADMIN always executes a function that identifies and authenticates the user who is accessing administrator mode as the administrator before the security management function in administrator mode becomes available to operate. In addition, the function to change the administrator mode password provided by F.ADMIN executes a function to re-authenticate the administrator before its execution is permitted. These authentication functions are the TSP enforcement functions that are operated before each security function is allowed to proceed, and there is a system so that they are always executed.
  F.SECURE-PRINT always executes a function that identifies and authenticates a general user who is the valid user of the secure print job information data, which is the subject of the

printing, before a secure print job information data is allowed to print. This identification and authentication function is a TSP enforcement function that is operated before permission for the print operation by the operation of the secure print job access control function, and it has a system so that it is always executed.

F.SERVICE always executes a function that identifies and authenticates that the user who is accessing the service mode is the service engineer, before the security management function in the service mode becomes available to operate. In addition, the function to change the service code provided by F.SERVICE executes a function to re-authenticate the service engineer before the execution is permitted. These authentication functions are the TSP enforcement functions that are operated before each security function is allowed to proceed, and there is a system so that they are always executed.

F.USER-BOX executes a function that authenticates a general user who is the valid user of the user box, before the downloading function of the user box data, and a function to change the user box identifier and the user box password, which are security management functions operated by the general user are allowed to execute. The authentication function for access to the user box is a TSP enfocement function that is executed before each function is allowed to execute, and it has a system so that they are always executed.

Therefore, each of the TSP enforcement functions are always invoked before each function, wherein all of the identified TOE security functions are controlled, is allowed to proceed, and therefore, this functional requirement is satisfied.

- FPT_SEP.1

  FPT_SEP.1 regulates the maintenance of the security domains that protects it from interference and tampering by untrusted subjects, and regulates the separation between the security domains of subject.

  With F.ADMIN, the security domain after the authentication of the administrators is categorized in two ways, access from the panel and access from the client PC. Neither are interfered with by an untrusted subject.

  F.USER-BOX allows the receiving of access to the same user box by a multiplicity of users. Nonetheless, the security domains maintained by each of the authorized valid users are separated and therefore there is no interference

  F.SERVICE does not receive any access from another subject while in service mode, which is a security domain maintained after authentication by a service code.

  Therefore, each of the security domains are not interfered with and thus, this functional requirement is satisfied.

8.3.2. Rationale for TOE security strength of function

The TOE security functions having a probabilistic/permutational mechanism are (1) the administrator mode password authentication mechanism by F. ADMIN, (2) the secure print password authentication mechanism by F.SECURE-PRINT, (3) the service code authentication mechanism provided by F.SERVICE and (4) the user box password authentication mechanism by F.USER-BOX. Each authentication mechanism has a password space of (1) an 8-digit number, (2) a 4-digit number, (3) 8 digits of number or "#" or "*," and (4) 4 to 64 digit ASCII code 0x20 to 0x7E (95 types of characters), respectively, and operates along with the access check function. (Three unsuccessful authentication attempts lock the access. See Section 6.1 for details. Note, when the service code authentication mechanism detects three unsuccessful trials it locks the access regardless of the operation setting of the access check function.) Therefore, as claimed in Section 6.2, the strength of function of the mechanisms adequately satisfies the SOF-Basic, and it is consistent with the minimum strength of function: SOF-Basic that is claimed for the TOE security functional requirement for the security strength of function, stipulated in item 5.1.2.

8.3.3. Mutually supported TOE security functions

The TOE security functional requirements that are satisfied by a combination of IT security functions that are identified in the TOE summary specifications, are as shown in the text regarding the rationale in the section of 8.3.1.2.

8.3.4. Rationale for assurance measures

The required document for the evaluation assurance level EAL3 is covered by the reference document shown in the assurance measures described in Section 6.3. The TOE security assurance requirements are satisfied through development, test conduction, vulnerability analysis, the development environment control, configuration management, life cycle management, and delivery procedures in accordance with the document provided as the assurance measures, as well as the preparation of a proper guidance document.

8.4. PP claims rationale

There is no PP that is referenced by this ST.

~ LAST PAGE ~