



**KONICA MINOLTA**

***bizhub 751 / bizhub 601 / ineo 751 / ineo 601 /  
VarioLink 7522 / VarioLink 6022  
Control Software  
A0PN0Y0-0100-G00-15  
A0PN0Y0-1D00-G00-11  
Security Target***

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

Version : 1.07

Issued on : January 21, 2009

Created by : KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

<Revision History>

Date	Ver.	Division	Approved	Checked	Created	Revision
2008/03/20	1.00	Development Div. 11	Yamazaki	Kakutani	Ichiki	Initial Version.
2008/09/09	1.01	Development Div. 11	Yamazaki	Kakutani	Ichiki	Deal with typos corresponding to the same series machine.
2008/09/26	1.02	Development Div. 11	Yamazaki	Kakutani	Ichiki	Deal with typos.
2008/10/03	1.03	Development Div. 11	Yamazaki	Kakutani	Ichiki	Deal with expression for hardware configuration.
2008/10/24	1.04	Development Div. 11	Yamazaki	Kakutani	Ichiki	Deal with typos.
2008/12/04	1.05	Development Div. 11	Yamazaki	Ichiki	Yasukaga	Revision of TOE identification version.
2008/12/19	1.06	Development Div. 11	Yamazaki	Ichiki	Yasukaga	Amendment of machine name, Addition of the user's guide name (English) and Deal with typos.
2009/01/21	1.07	Development Div. 11	Yamazaki	Ichiki	Yasukaga	Deal with typos.

---- [ Contents ] -----

<b>1. ST Introduction</b>	<b>6</b>
1.1. ST Identification	6
1.2. TOE Identification	6
1.3. TOE Overview	6
1.3.1. TOE Type	6
1.3.2. Usage of TOE and main Security Functions	6
1.4. TOE Description	7
1.4.1. Role of the TOE User	7
1.4.2. Physical Range of TOE	8
1.4.3. Logical Range of TOE	11
<b>2. Conformance Claims</b>	<b>19</b>
2.1. CC Conformance Claim	19
2.2. PP Claim	19
2.3. Package Claim	19
2.4. Reference	19
<b>3. Security Problem Definition</b>	<b>20</b>
3.1. Protected Assets	20
3.2. Assumptions	21
3.3. Threats	21
3.4. Organizational Security Policies	23
<b>4. Security Objectives</b>	<b>24</b>
4.1. Security Objectives for the TOE	24
4.2. Security objectives for the operation environment	26
4.3. Security Objectives Rationale	28
4.3.1. Necessity	28
4.3.2. Sufficiency of Assumptions	29
4.3.3. Sufficiency of Threats	29
4.3.4. Sufficiency of Organizational Security Policies	33
<b>5. Extended Components Definition</b>	<b>35</b>
5.1. Extended Function Component	35
5.1.1. FAD_RIP.1 Definition	36
5.1.2. FIA_EID.1 Definition	36
5.1.3. FIT_CAP.1 Definition	37
<b>6. IT Security Requirements</b>	<b>39</b>
6.1. TOE Security Requirements	39
6.1.1. TOE Security Function Requirements	39
6.1.2. TOE Security Assurance Requirements	61
6.2. IT Security Requirements Rationale	61
6.2.1. Rationale for IT Security Functional Requirements	61
6.2.2. Rationale for IT Security Assurance Requirements	61
<b>7. TOE Summary Specification</b>	<b>61</b>
7.1. F.ADMIN (Administrator Function)	61
7.1.1. Administrator identification authentication function	61
7.1.2. Auto logoff function of administrator mode	61

7.1.3. Function offered in Administrator mode.....	61
7.2. F.ADMIN-SNMP (SNMP administrator function).....	61
7.2.1. Identification and authentication function by SNMP password.....	61
7.2.2. Management function using SNMP.....	61
7.3. F.SERVICE (Service mode function).....	61
7.3.1. Service engineer identification authentication function.....	61
7.3.2. Function offered in service mode.....	61
7.4. F.USER (User Function).....	61
7.4.1. User Identification and Authentication Function.....	61
7.4.2. Auto logoff function in user identification and authentication domain.....	61
7.4.3. Modification function of user password.....	61
7.5. F.BOX (User Box Function).....	61
7.5.1. Personal User Box Function.....	61
7.5.2. Public User Box Function.....	61
7.5.3. Group User Box Function.....	61
7.6. F.PRINT (Secure Print Function).....	61
7.6.1. Secure Print Function.....	61
7.7. F.OVERWRITE-ALL (All area overwrite deletion function).....	61
7.8. F.CRYPT (Encryption key generation function).....	61
7.9. F.VALIDATION-HDD (HDD verification function).....	61
7.10. F.VALIDATION-CF (CF verification function).....	61
7.11. F.RESET (Authentication Failure Frequency Reset Function).....	61
7.12. F.TRUSTED-PASS (Trust Channel Function).....	61
7.13. F.S/MIME (S/MIME Encryption Processing Function).....	61
7.14. F.SUPPORT-AUTH (External Server authentication operation support function).....	61
7.15. F.SUPPORT-CRYPTO (Crypton kit operation support function).....	61
7.16. F.SUPPORT-HDD (HDD lock operation support function).....	61
7.17. F.SUPPORT-CF (CF lock operation support function).....	61

---- [ List of Figures ] -----

Figure 1 An example of the expected environment for usage of the MFP .....	8
Figure 2 Hardware composition that relates to TOE .....	9

---- [ List of Tables ] -----

Table 1 Conformity of Security Objectives to assumptions and Threats .....	28
Table 2 Cryptographic Key Generation Relation of Standards-Algorithm-Key sizes .....	39
Table 3 Cryptographic Operation Relation of Algorithm-Keysizes-Cryptographic Operation .....	40
Table 4 User Box Access Control Operational List.....	41
Table 5 Secure Print File Access Control: Operational List.....	41
Table 6 Setting Management Access Control: Operational List .....	42
Table 7 TOE Security Assurance Requirements .....	61
Table 8 Conformity of IT Security Functional Requirements to Security Objectives .....	61
Table 9 Dependencies of IT Security Functional Requirements Components .....	61
Table 10 The list of the name and identifier of TOE Security function.....	61
Table 11 character and number of digits used for password .....	61
Table 12 A type of overwrite deletion of all area and the method of overwriting.....	61

## 1. ST Introduction

### 1.1. ST Identification

-ST Title : bizhub 751 / bizhub 601 / ineo 751 / ineo 601 / VarioLink 7522 / VarioLink 6022 Control Software  
A0PN0Y0-0100-G00-15 / A0PN0Y0-1D00-G00-11  
Security Target

-ST Version : 1.07

-CC Version : 3.1R2

-Created on : January 21, 2009

-Created by : KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.  
Masayuki Yasukaga

### 1.2. TOE Identification

-TOE Name : Japanese Name : bizhub 751 / bizhub 601 / ineo 751 / ineo 601 / VarioLink 7522 / VarioLink 6022 Zentai Control Software  
English Name : bizhub 751 / bizhub 601 / ineo 751 / ineo 601 / VarioLink 7522 / VarioLink 6022 Control Software

-TOE Version : A0PN0Y0-0100-G00-15 (System Controller)  
A0PN0Y0-1D00-G00-11 (BIOS Controller)

-TOE Type : Software

-Created by : KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

### 1.3. TOE Overview

This paragraph explains the usage of TOE, main Security Functions and Operation Environment of the TOE.

#### 1.3.1. TOE Type

The bizhub 751 / bizhub 601 / ineo 751 / ineo 601 / VarioLink 7522 / VarioLink 6022 Control Software that is the TOE is an embedded software product that controls the operation of whole MFP overall in the compact flash memory and flash memory on the MFP controller.

#### 1.3.2. Usage of TOE and main Security Functions

bizhub 751, bizhub 601, ineo 751, ineo 601, VarioLink 7522, VarioLink 6022 is Konica Minolta Business Technologies, Inc. digital MFP, in which this TOE is installed, comprised by selecting and combining copy, print, scan and FAX functions (Hereinafter referred to as "MFP"). TOE is the "bizhub 751 / bizhub 601 / ineo 751 / ineo 601 / VarioLink 7522 / VarioLink 6022 Control Software" that controls the entire operation of MFP, including the operation control processing and the image data management that are accepting from the panel of the main body of MFP or through the network.

TOE offers the protection from exposure of the highly confidential document stored in the MFP. Moreover, TOE can prevent the unauthorized access to the image data written in HDD for the danger of taking HDD that is the medium that stores the image data in MFP out illegally by using the HDD lock function loaded on the HDD. Besides, TOE has the deletion method to follow various overwrite deletion standards. It deletes all the data of HDD completely and it contributes to the prevention of the divulging information of the organization that uses MFP by using the method at the time of abandonment or the lease returns.

## 1.4. TOE Description

### 1.4.1. Role of the TOE User

The roles of the personnel that relate to the use of the MFP with the TOE are defined as follows.

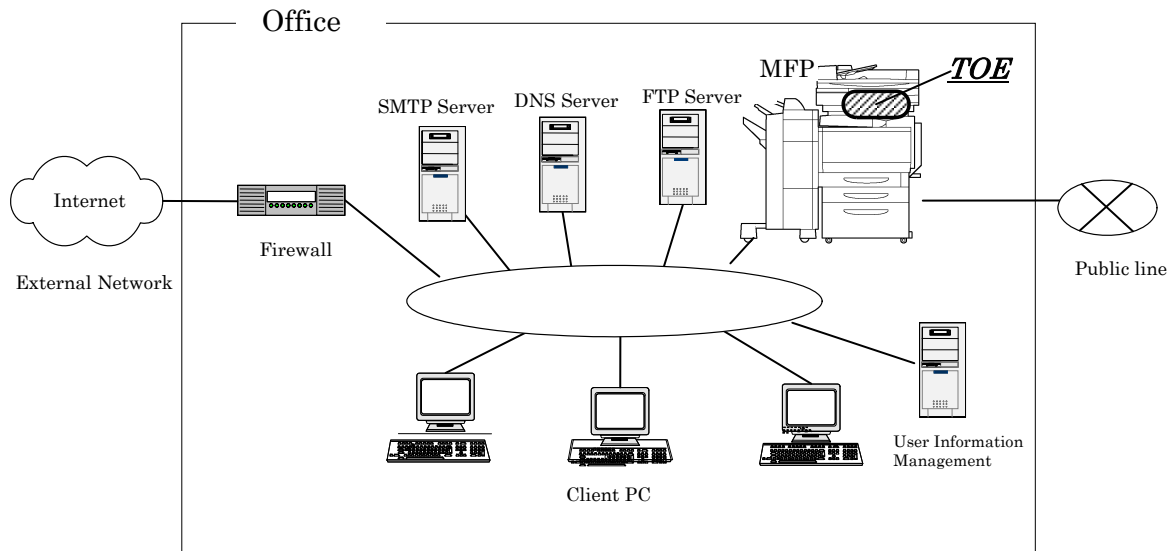
- User  
MFP's user who is registered into MFP. (In general, the employee in the office is assumed.)
- Administrator  
MFP's user who carries out the management of the operation of MFP. An administrator performs the operation management of MFP and the management of user. (In general, it is assumed that the person elected from the employees in the office plays this role.)
- Service Engineers  
A user who performs management of maintenance for the MFP. Service Engineer performs the repair and adjustment of MFP. (In general, the person in charge at the sales companies that performs the maintenance service of MFP and is in cooperation with Konica Minolta Business Technologies, Inc. is assumed.)
- 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 carries out management of the maintenance for the MFP. This person assigns service engineers who perform the maintenance management for the MFP.

Besides this, though not a user of TOE, a person who goes in and out the office are assumed as an accessible person to TOE.

## 1.4.2. Physical Range of TOE

### 1.4.2.1. Environment for the usage

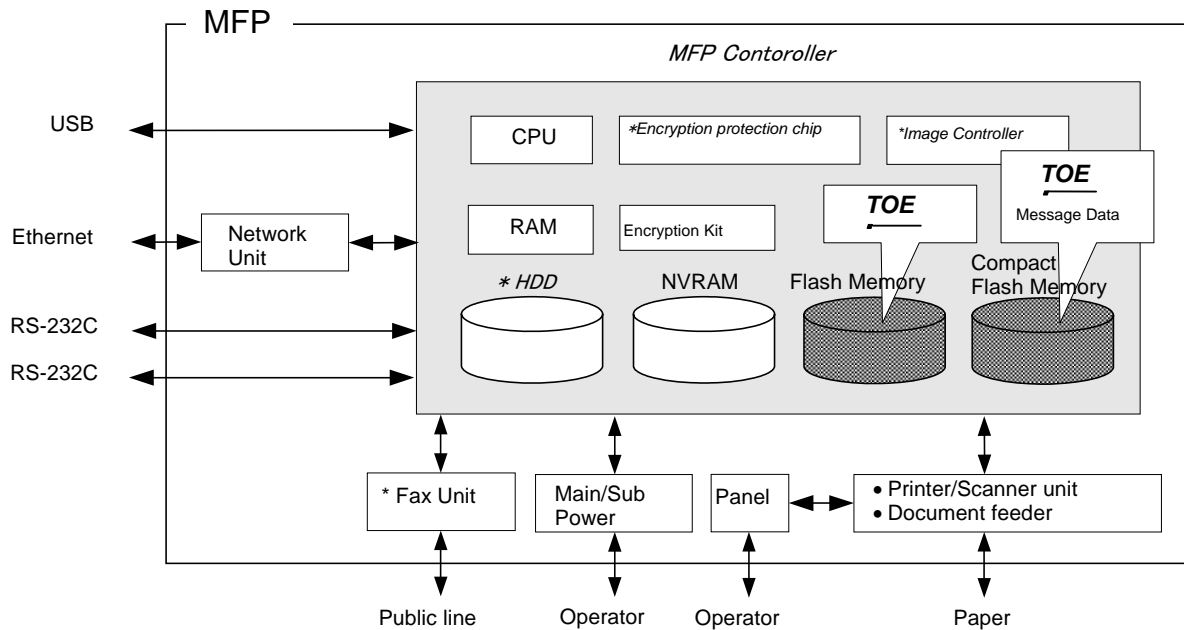
Figure 1 shows the expected general environment for the usage of MFP equipped with TOE. Moreover, the matters, assumed in the environment for the usage, show by a run of the item below



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

- The 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 the SMTP server or FTP server or WebDAV server are connected to the intra-office LAN, the MFP can carry out data communication with these. (Need the DNS Service when setting the Domain name of SMTP Server or FTP Server or WebDAV server)
- The case, which is unifying management of the user ID and the user password in the server, also assumes. In this case, TOE can control the access to the MFP by using the user registration information in the user information management server.
- When the intra-office LAN connects to an external network, measures such as connecting via a firewall are taken, and an appropriate setup to block access requests to the MFP from the external network is carried out.
- The intra-office LAN provides a network environment that cannot be intercepted by the office operation including using the switching hub and installing the wiretapping detector.
- The public line connected with MFP is used to communicate with the FAX and the remote support function.

### 1.4.2.2. Operation Environment



**Figure 2 Hardware composition that relates to TOE**

Figure 2 shows the structure of the hardware environment on the MFP that TOE needs for the operation. TOE exists as System Controller on the compact flash memory and as BIOS Controller on the flash memory on the MFP controller which builds in the body of the MFP and is loaded and run on the RAM when main power is switched ON.

The following explains about the unique hardware on the MFP controller, the hardware having the interface to the MFP controller, and the connection by using RS-232C, shown in Figure 2.

- Compact Flash memory (Hereafter, use "CF" as abbreviated name)

Storage medium that stores the object code of the System Controller of "MFP Control Software" that is the TOE. Additionally, it stores the message data of each country's language to display the response accessed through the panel and network.

This medium also stores various setting values which are needed for the operation of the MFP used for processing of TOE. As for security related data, various setting values are included except Administrator password, CE password, HDD lock password, encryption passphrase and CF lock password.

As a feature function, the security function (CF lock function) is installed, being possible to set the password and not being possible to read and write unless it agrees to the password. Furthermore, when the frequency of uniformity of it becomes unsuccessful in password collation, the function is also ready to lock the password collation function.

- Flash memory

Storage medium that stores the object code of the BIOS Controller of "MFP Control Software".

- HDD (\* Option)

Hard disk drive of 60GB in capacity. It is utilized besides the image data is stored as a file, temporarily image data with such as extension conversion, and as an area where the transmission address data kept.

As a feature function, the security function (HDD lock function) is installed, being possible to set the password and not being possible to read and write unless it agrees to the password. Furthermore, when the frequency of uniformity of it becomes unsuccessful in password collation, the function is also ready to lock the password collation function. It is not pre-installed in MFP as standard according to the circumstances in sales, but is an optional part., but it is an essential component under this ST assumption.

- NVRAM

Nonvolatile Memory. The memory medium that stores various setting values needed for the operation of the MFP used for processing of TOE.

- Encryption Kit or Encryption Protection Chip (\* Option)

The cryptographic function, which is mounted in the Encryption Kit, the hardware on the MFP Controller, is installed in order to encipher image data to be written in HDD or CF. Encryption Protection Chip sold as an optional part is necessary to work encryption function.

- Image Controller (\* Option parts)

The controller for image conversion process that be connected to MFP controller with Video bus. It is not pre-installed in MFP as standard according to the circumstances in sales, but is an optional part., but it is an essential component under this ST assumption.

- Panel

The exclusive control device for the operation of the MFP equipped with the touch panel of a liquid crystal monitor, ten-key, start key, stop key, screen switch key, etc.

- Main power supply, Sub power supply

The power switch for activating MFP

- Network Unit

The interface device to connect to the Ethernet. It supports 10BASE-T, 100BASE-TX and Gigabit Ethernet.

- Local Connecting Unit (\* Option)

A unit that connects the client PC with USB. It is available to use Print function through this interface.

- USB

The Port to print with local connection. It has interface connected directly to MFP controller to backup the setting values, to update the TOE in addition to use Print function.

- FAX Unit (\* Option parts)

A device that is used for the communication for sending and receiving FAX and for the remote

diagnosis function (described later) via public line. It is not pre-installed in MFP as standard according to the circumstances in sales, but is sold as an optional part.

- Scan Unit/ An automatic manuscript feeder  
The device that scans images and photos from a paper and converts them into the digital data.
- Printer Unit  
The device that actually prints the converted image data for printing when demanded to print by the MFP controller.
- RS-232C  
Two ports are available. The serial connection can be done through D-sub 9 pins. When troubled or needed, the maintenance function can be used through this interface. And it can utilize a remote diagnostic function (later description) to connect with the modem connected with the public circuit.

#### 1.4.2.3. Guidance

- bizhub 751/601 SERVICE MANUAL SECURITY FUNCTION (Japanese)
- bizhub 751/601 ineo 751/601 VarioLink 7522/6022 SERVICE MANUAL SECURITY FUNCTION (English)
- bizhub 751/601 User's Guide [Security Operations] (Japanese)
- bizhub 751/601 User's Guide [Security Operations] (English)
- ineo 751/601 User's Guide [Security Operations] (English)
- VarioLink 7522/6022 User's Guide [Security Operations] (English)

#### 1.4.3. Logical Range of TOE

A User uses a variety of functions of the TOE from the panel and a client PC via the network. The following explains typical functions, such as the basic function, the user box function to manage the image files stored, the user identification and authentication function, the administrator function manipulated by administrator, the service engineer function manipulated by service engineer, and the function operated in the background without user's awareness.

##### 1.4.3.1. Basic Function

In MFP, a series of function for the office work concerning the image such as copy, print, scan, and fax exists as a basic function, and TOE performs the core control in the operation of these functions. It converts the raw data acquired from the external device of the MFP controller into the image file, and registered in RAM and HDD. (After two or more conversion processing is done, the conversion is done as for the print image file from PC.) The image file which has been converted into data for the print or for the transmission, and is transmitted to the device outside of the MFP controller concerned.

Operations of copy, print, scan, and fax are managed by the unit of job, and can be changed the

operation order, can be modified the finishing if it's a printing job, and can be cancelled the operation, by the command from the panel.

The following is the functions related to the security in the basic function.

- **Secure Print Function**

When the Secure Print password is received with the printing data, the image data is stored as the standby status. And the print command and password input from the panel allows printing.

This function, in the printing operation by the client PC, removes the possibility that other users stole a glance at the printing of high-leveled confidential data and lost it into the other printings.

#### **1.4.3.2. User Box Function**

The directory named "user box" can be created as an area to store the image file in HDD. Three types of user box exist; the first is the personal user box which a user possesses, the second is the public user box which the registered user making a group within a certain number uses jointly and the third is the group box which the users belong to same account uses jointly. As for the personal user box, the operation is limited only for the user who owns it, the public user box performs access control by sharing a password set to the user box among users and group box, the operation is limited only for the user who the use of the account is permitted.

TOE processes the following required operation, against the user box or the image file in a user box for an operation requests that is transmitted from the panel or the network unit through a network from a client PC.

- Print, transmission, and download from client PC, of image file in a user box
  - The encryption of box file is possible in the E-mail that is one of the transmission methods.
- Deletion of the image file in the user box, and move and copy to other user boxes
- Storage period setting of image file in user box (Delete automatically after the period passes.)
- Change of user box name, change of the password, and deletion of user box, etc.
- Attribute setting of user box (classification change of a personal user box , a public user box and a group box)

#### **1.4.3.3. User Authentication Function**

TOE can limit the user who uses MFP. When accessing it through the panel or the network, TOE performs the identification and authentication that the user is permitted to use the MFP by applying the user password and user ID. When the identification and authentication succeeds, TOE permits the user the use of the basic function and the user box function, etc.

Several types of the following are supported in the method of the user authentication.

- (1) **Machine authentication**

A method to authenticate on MFP by registering a user ID and a user password into HDD on MFP controller.

(2) External server authentication

A method to authenticate with processing the authentication on MFP by using the user ID and the user password that are registered on the user information management server which is connected by the intra-office LAN without managing the user ID and user password on the MFP side. Though two or more methods named Active Directory<sup>1</sup>, NTLM<sup>2</sup>, and NDS are supported, the method of the external server authentication assumed in this ST is applied only the case with Active Directory.

#### 1.4.3.4. Account Authentication Function

TOE can manage the MFP users by grouping them into Account unit. The methods of Account Authentication are as follows.

(1) Method synchronized with User Authentication

The user is set Account ID which he belongs to beforehand, and the user is related to account ID of belonging account when user is certified.

(2) Method not synchronized with User Authentication

When the certification is done by the account password set to each account ID, the user is related to the concerned account ID.

#### 1.4.3.5. Administrator Function

TOE provides the functions such as the management of user boxes, management of user information at the time of MPF authentication and management of various settings of the network, image quality, etc in the administrator mode that only authenticated administrator can manipulate.

The following shows the function related to the security.

- The user registration management
  - Registration or change in user ID and user password, and deletion of a user.
  - Change the association of user with account ID
- The account registration management
  - Registration or change in account ID and account password.
- Management of user box settings
  - Registration or change in user box password, and management of user attributes
- Operation setting of automatic system reset
  - Setting of the function that logs out automatically when the setting time passed.
- Management of network setting
  - Connection setting of the intra-office LAN (setting of DNS server)
  - SMTP setting (setting of SMTP server utilized by E-mail transmission)
  - IP address, NetBIOS name and AppleTalk printer name etc.
- Backup or restore function of NVRAM, CF and HDD
  - It is performed through the network by using an application exclusive use for the

---

<sup>1</sup> A method of directory service that Windows Server 2000 (after it) offers to consolidate user information in network environment of Windows platform.

<sup>2</sup> Abbreviation of NT LAN Administrator. Authentic method used in directory service that Windows NT offers to consolidate user information in network environment of Windows platform.

management installed in the client PC.

- Complete overwrite deletion function of HDD
  - There is the data deletion method conformed to various military standards (ex. Military Standard of United States Department of Defense)
  - When it's started, in conformity with a set method, the overwrite deletion is executed for all area of HDD.
- Format function of HDD
  - A logical format is executable.
- Management of FAX setting
  - Setting of TSI<sup>3</sup> receiving
  - Setting of FAX output at PC-FAX receiving (Storing in Box or common Boxarea for all users are available.)
- FTP Serverfunction setting
  - Selecting On or OFF

The followings are the operation setting function related especially to the behavior of the security function.

- Method setting of a user authentication function
  - Select the machine authentication, the external server authentication, or the user authentication stop.
  - Combination with Account Authentication is set up. (Method synchronized with User Authentication, Method not synchronized with User Authentication)
- User: Setting of access by PUBLIC
  - Select the permission and prohibition of MFP utilization of the user who is not identified by user ID.
- Setting of a password policy function
  - Select ON or OFF for the function to check the several conditions of the password, such as the valid number of digits for the various passwords, etc.
- Setting of the authentication method of secure print and the prohibit function of authenticating operations.
  - There are the mode that the authentication operation prohibition function operates for the authentication of the secure print, and the mode not done.
  - The operation mode of the function that the failure authentication in each authentication function detects the failure synchronizes, too.
  - Selecting the above-mentioned operational mode
- Setting of the network setting modification function by SNMPv1 and v2.
  - Select the permission or the prohibition of the modification operation function of MIB by SNMPv1 and v2
- Operational Setting of Authentication Function when writing using SNMPv3
  - Select Authenticate or Not Authenticate Setting Level.
  - Select "only Authentication password" or "Authentication password + Privacy password" for Authentication operation
- Setting of HDD lock function

---

<sup>3</sup> Abbreviation of Transmting Subscriber Identification. The Same meaning of Identification of Subscriber's Termnal. TSI receiving is the function that can designate the Box to be stored for each Subscriber.

- Selecting ON or OFF.
- Register or change the HDD lock password when ON is selected.
- Setting of CF lock function
  - Selecting ON or OFF.
  - Register or change the CF lock password when ON is selected.
- Setting of encryption function (\* only when the encryption protection chip installed)
  - Selecting ON or OFF.
  - Register or change the Encryption passphrase when ON is selected.
- Setting of user box collective management function
  - Select the permission or the prohibition for the user box collective management function.
- Setting of the print capture function
  - A function to verify the print data received by MFP when print function breaks down.
  - Selecting ON or OFF for the above-mentioned function.
- Setting of network setting management reset function
  - A network setting management reset function resets a series of items in a factory default.
  - Selecting permission or prohibition for the above-mentioned function.
- Setting of Trusted Channel (SSL/TLS encryption communication) Function
  - Create or import SSL/TLS server certificate.
  - Setting of encryption method that is used for communication.
- Setting of Transmission address data
  - Setting of address or method that is used for box file transmission etc.
  - Import S/MIME certificate
  - Setting of encryption method that is used for data encryption.
- Setting of FTP server function
  - Selecting ON or OFF.
  - FTP service is the function to manage counter information such as the number of prints per user.
  - Each account and user information can also be managed with counter information.

#### 1.4.3.6. Service Engineer Function

TOE provides a management function of administrator and a maintenance function, such as adjusting the device for Scan/Print etc, within the service mode that only a service engineer can operate. The following shows the functions related to the security.

- Modification function of administrator password

The followings are the operation setting function related especially to the behavior of the security function.

- Authentication setting of the service engineer with the CE<sup>4</sup> password.
  - Select ON or OFF.
- Setting of remote diagnostic function (later description)
  - Able to select permission or prohibition.
- Setting of a TOE update function via Internet

---

<sup>4</sup>Abbreviation of Customer Service engineer

- Able to select permission or prohibition.
- Setting of maintenance function
  - Able to select permission or prohibition.
- The format function of HDD
  - A logical format and a physical format are executable.
- Installation setting of HDD
  - An explicit installation setting is necessary to use HDD as a data storage area.
- Initialization function
  - The various setting values that the user or the administrator has set and the data that the user has stored are deleted.

#### 1.4.3.7. Other Functions

TOE provides the functions that run background without awareness of the user and the updating function of TOE. The following explains the major functions.

(1) Encryption key generation function

When the encryption protection chip, an optional product, is installed in MFP controller, the encoding and decoding is processed to the reading and writing data in HDD. (TOE does not process the encryption and decryption itself.)

The operation setting of this function is performed by the administrator function. When it operates, TOE generates the encryption key by the encryption passphrase that was entered on the panel.

(2) Remote diagnostic function

Making use of several connected systems such as E-mail, and a modem connection through a FAX public line mouth or a RS-232C, in communication with support center of MFP produced by Konica Minolta business technologies, Inc., it manages the state condition of MFP and the machinery information such as frequency of printing. In addition, if necessary, appropriate service (shipment of an additional toner, the account claim, dispatch of the service engineer due to the failure diagnosis, etc.) is provided.

(3) Updating function of TOE

TOE facilitated with the function to update itself. As for the update means, there are a method that exists as one of items of remote diagnostic function, a method that downloads from FTP server through Ethernet (TOE update function via Internet), and a method that performs the connection of the memory medium such as USB memory.

(4) Encryption Communication function

TOE can encrypt the data transmitted from client PC to MFP, and the data received by download from MFP by using SSL/TLS.

The operation setting of this function is performed by the administrator function.

(5) S/MIME certificate automatic registration function

It is the function to register the certificate for S/MIME (conforms to ITU-T X.509) with each transmission address automatically. When a certificate is attached in received e-mail, MFP

recognizes user ID according to the information of e-mail header, and registers the certificate as certificate of the same user ID.

TOE uses effectively the security function of external entity as HDD and CF. The following explains the major functions related to the external entity.

(1) Utilization of HDD Lock Function

HDD as an external entity has the HDD lock function as measure against the illegal taking out, when the password is set.

The administrator function does the operation setting of this function. As for the starting operation of MFP, the access to HDD is permitted by the matching of the HDD lock password set to the HDD and the one set on the MFP. (Even if HDD is taken out, it is impossible to use it excluding the MFP that the concerned HDD installed.)

(2) Utilization of CF Lock Function

CF as an external entity has the CF lock function as measure against the illegal taking out, when the password is set.

The administrator function does the operation setting of this function. As for the starting operation of MFP, the access to CF is permitted by the matching of the CF lock password set to the CF and the one set on the MFP. (Even if CF is taken out, it is impossible to use it excluding the MFP that the concerned CF installed.)

#### 1.4.3.8. Enhanced Security Function

Various setting functions related to the behavior of the security function for the Administrator function and the Service engineer function can be set collectively to the secure values by the operation settings of the "Enhanced Security Function". Each value set is prohibited changing itself into the vulnerable one individually. As the function that does not have a setting function of the operation individually, there is the reset function of the network setting and the update function of TOE through the network, but the use of these functions is prohibited.

The following explains the series of the setting condition of being the enhanced security function active. In order to activate the enhanced security function, the prerequisite is required that an administrator password and a CE password should be set along with the password policy.

- Setting of user identification and authentication function
  - : Valid (Either the machine authentication, or the external server authentication are available)
- User : Setting of access of PUBLIC : Prohibit
- Setting of a service engineer authentication function
  - : Valid
- Setting of password policy function : Valid
- Setting of secure print authentication method
  - : Authentication operation prohibition function effective method
- Setting of Authentication Operation Prohibition function

- : It becomes in the state of the panel lock for five seconds at the time of the authentication failure in the panel.
  - And it becomes the account lock (Failure Frequency threshold : 1-3 times).
- Setting of User Box : Prohibit
- Setting of user box collective management function : Prohibit
- Setting of the network setting modification function with SNMPv1 and v2 : Prohibit
- Authentication Operation when writing using SNMPv3 : Valid
- Setting of HDD lock function : Valid
- Setting of CF lock function : Valid
- Setting of print capture function : Prohibit
- Remote diagnostic function : Prohibit
- Network setting management reset function : Prohibit
- TOE update function via Internet : Prohibit
- Setting function of transmission address data by user : Prohibit
- Operation setting of Trusted Channel function : Valid
- Administrator Authentication lock Time: Prohibit for 1-4 minutes
- CE Authentication Lock Time : Prohibit for 1-4 minutes
- Setting of FTP Server function : Prohibit
- Panel auto log-off time (System auto reset) : more than 1 minute

The following function becomes as follows at the timing of the operation settings of the "Enhanced Security Function", but contrary to above mentioned settings, this setting can be changed individually.

- Setting of maintenance function : Prohibit

## 2. Conformance Claims

### 2.1. CC Conformance Claim

This ST conforms to the following standards.

Common Criteria for Information Technology Security Evaluation

Part 1: Introduction and general model 2006/9 Version 3.1 Revision 1 (Translation v1.2)

Part 2: Security functional requirements 2007/9 Version 3.1 Revision 2 (Translation v2.0)

Part 3: Security assurance requirements 2007/9 Version 3.1 Revision 2 (Translation v2.0)

- Security function requirement : Part2 Extended
- Security assurance requirement : Part3 Conformant

### 2.2. PP Claim

There is no PP that is referenced by this ST.

### 2.3. Package Claim

This ST conforms Package : EAL3. There is no additional assurance component.

### 2.4. Reference

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model September 2006 Version 3.1 Revision 1 CCMB-2006-09-001
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2007 Version 3.1 Revision 2 CCMB-2007-09-002
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components September 2007 Version 3.1 Revision 2 CCMB-2007-09-003
- Common Criteria for Information Technology Security Evaluation Evaluation methodology September 2007 Version 3.1 Revision 2 CCMB-2007-09-004

### 3. Security Problem Definition

This chapter will describe the concept of protected assets, assumptions, threats, and organizational security policies.

#### 3.1. Protected Assets

Security concept of TOE is "the protection of data that can be disclosed against the intention of the user". As MFP is generally used, the following image file in available situation becomes the protected assets.

- Secured print file  
Image file registered by secured print.
- User Box file  
Image file stored in the personal user box, public user box and group user box.

As for a image file of a job kept as a wait state by activities of plural jobs, and a image file of a job kept that prints the remainder of copies becoming as a wait state for confirmation of the finish, and other than the image file dealt with the above-mentioned is not intended to be protected in the general use of MFP, so that it is not treated as the protected assets.

In the print of the secure print file and the transmission of the user box file, making in the preparation for the threat thought when illegal MFP or mail server is connected by any chance, or when operation setting of PC-FAX is changed even if without illegal MFP, the setting of MFP (IP address etc.) and operation setting of PC-FAX require not to be modified illegally. Therefore, the setting of MFP (IP address etc.) and operation setting of PC-FAX are considered as subsidiary protected assets.

On the other hand, when the stored data have physically been separated from the jurisdiction of a user, such as the use of MFP ended by the lease return or being disposed, or the case of an HDD or CF theft, a user has concerns about leak possibility of every remaining data. Therefore, in this case, the following data files become protected assets.

- Secure Print File
- User Box File
- On Memory Image File
  - Image file of job in the wait state
- Stored Image File
  - Stored image files other than secure print file and user box file
- HDD remaining Image File
  - The file which remains in the HDD data area that is not deleted only by general deletion operation (deletion of a file maintenance area)
- CF remaining Image File
  - The file which remains in the Compact Flash memory data area that is not deleted only by general deletion operation (deletion of a file maintenance area). The data leak possibility does not exist when HDD is preinstalled as standard. When HDD is not

preinstalled and image file happens to be in CF, this leakage possibility exists.

- File related to the Image
  - Temporary data file generated in print image file processing
- Transmission Address Data File
  - File including E-mail address and telephone numbers that become the destination to transmit an image.

## 3.2. Assumptions

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

### **A.ADMIN (Personnel conditions to be an administrator)**

Administrators, in the role given to them, will not carry out a malicious act during the series of permitted operations given to them.

### **A.SERVICE (Personnel conditions to be a service engineer)**

Service engineers, in the role given to them, will not carry out a malicious act during series of permitted operations given to them.

### **A.NETWORK (Network connection conditions for MFP)**

- The intra-office LAN where the MFP with the TOE will be installed is not 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.SECRET (Operational condition about secret information)**

Each password and encryption passphrase does not leak from each user in the use of TOE.

### **A.SETTING (Operational setting condition of Enhanced Security function)**

- MFP with the TOE is used after enabling the enhanced security function.

## 3.3. 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.DISCARD-MFP (Lease-return and disposal of MFP)**

When the leaser returned or the discarded MFP were collected, secure print file, a user box file, on memory image file, the stored image file, the HDD remaining image file, the CF remaining image file, the image-related file, the transmission address data file, and the set various passwords can leak by the person with malicious intent taking out and analyzing an HDD or CF or NVRAM in MFP.

### **T.BRING-OUT-STORAGE (An unauthorized carrying out of HDD)**

- A secure print file, a user box file, a on memory image file, a stored image file, a HDD

remaining image file, an image-related file, a transmission address data file, and the set-up various passwords can leak by a person or a user with malicious intent illegally taking out and analyzing an HDD in MFP.

- A person or a user with malicious intent illegally replaces an HDD in MFP. In the replaced HDD, new files of the secure print file, a user box file, on memory image file, a stored image file, a HDD remaining image file, an image related file, a transmission address data file and set various passwords are accumulated. A person or a user with malicious intent takes out and analyzes the replaced HDD and image files leak.

#### **T.ACCESS-PRIVATE-BOX (Unauthorized access to the personal user box which used a user function)**

Exposure of the user box file when a person or a user with malicious intent accesses the user box where other user owns, and downloads, prints and transmits the user box file (E-mail transmission, FTP transmission, fax transmission, SMB<sup>5</sup> transmission and WebDAV transmission).

#### **T.ACCESS-PUBLIC-BOX (Unauthorized access to public box which used a user function)**

Exposure of the user box file when a person or the user with malicious intent accesses the public user box which is not permitted to use, and downloads, prints, transmits (E-mail transmission, FTP transmission, FAX transmission, SMB transmission and WebDAV transmission) and removes and copies to the other user box the user box file.

#### **T.ACCESS-GROUP-BOX (Unauthorized access to the group user box which used a user function)**

Exposure of the user box file when a person or the user with malicious intent accesses the group user box which the account where a user does not belong to owns, and downloads, prints, transmits (E-mail transmission, FTP transmission, FAX transmission, SMB transmission and WebDAV transmission) and removes and copies to the other user box the user box file.

#### **T.ACCESS-SECURE-PRINT (Unauthorized access to the secure print file which used a user function)**

Exposure of the secure print file when a person or the user with malicious intent prints the secure print file which is not permitted to use.

#### **T.UNEXPECTED-TRANSMISSION (Transmission to unintended address)**

- Malicious person or user changes the network settings that is related to the transmission of a user box file. Even an addressee is set precisely, a user box file is transmitted (the E-mail transmission or the FTP transmission) to the entity which a user does not intend to, so that a user box file is exposed.  
<The network setting which is related to user box file transmission>
  - Setting related to the SMTP server
  - Setting related to the DNS server
- Malicious person or user changes the network setting which set in MFP to identify MFP itself where TOE installed, by setting to the value of the entity such as another illegal MFP from the value of MFP (NetBIOS name, AppleTalk printer name, IP address etc) that TOE is

---

<sup>5</sup>Abbreviation of Server Message Block. Protocol to realize the file sharing or printer sharing on Windows.

originally installed, so that secure print file is exposed.

- Malicious person or user changes the TSI receiving settings. A user box file is stored to the entity which a user does not intend to, so that a user box file is exposed.
- Malicious person or user changes the PC-FAX operation settings. By changing the setting of the storing for the public user box to store to common area for all users, a user box file is stored to the entity which a user does not intend to, so that a user box file is exposed.

\* This threat exists only in the case that the operation setting of PC-FAX is meant to work as the operation setting for box storing.

#### **T.ACCESS-SETTING (An unauthorized change of a function setting condition related to security)**

The possibility of leaking user box file and secure print file rises because malicious person or user changes the settings related to the enhanced security function.

#### **T.BACKUP-RESTORE (Unauthorized use of Backup function and restoration function)**

The user box file and the secure print file can leak by malicious person or user using the backup function and the restoration function illegally. Also highly confidential data such as password can be exposed and each setting values are falsified.

#### **T.BRING-OUT-CF (An unauthorized carrying out of Compact Flash Memory)**

The possibility of the following rises because a malicious person or a user with malicious intent illegally taking out and analyzing a CF in MFP.

- Leak of setting value (SNMP password).
- Operation by a falsified password (SNMP password, other operation setting values of various functions).
- Operation under falsified TOE.
- Leak of image information existed in the Compact Flash Memory through remaining CF image file.

### **3.4. Organizational Security Policies**

Recently, there are a lot of organizations that demand security of network in office.

Although a threat of wiretapping activities etc. in intra-office LAN is not assumed in this ST, TOE security environment that corresponds to the organization that demanded security measures in intra-office LAN is assumed.

Particularly, correspond to the secure communication of Protected Assets considering the confidentiality showed in the preceding.

The security policies applied in the organization that uses TOE are identified and described as follows.

#### **P.COMMUNICATION-DATA (secure communication of image file)**

Highly confidential image file (secure print file and user box file) which transmitted or received between IT equipment is communicated via trusted pass to the correct destination, or has to be encrypted in the case of the organization or the user expect to be protected.

## 4. Security Objectives

In this chapter, in relation to the assumptions, the threats, and the organizational security policy identified in Chapter 3, the required security objectives policy for the TOE and the environment for the usage of the TOE are described by being divided into the categories of the security objectives for 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.REGISTERED-USER (Utilization of registered user)**

TOE permits only the registered user to use the MFP installing TOE.

#### **O.PRIVATE-BOX (Personal user box access control)**

- TOE permits only a user to use the user function of the personal user box which this user owns.
- TOE permits only a user to use the user function of the use box file in the personal user box which this user owns.

#### **O.PUBLIC-BOX (Public user box access control)**

- TOE permits the registered user the reading operation of the public user box.
- TOE permits the user function of the public user box only to the user who is permitted the use of this public user box.
- TOE permits the user function of the user box file in the public user box only to the user who is permitted the use of this public user box.

#### **O.GROUP-BOX (Group user box access control)**

- TOE permits the user function of the group user box which this account owns only to the user who is permitted the use of this account.
- TOE permits the user function of the user box file in the group user box which this account owns only to the user who is permitted the use of this account.

#### **O.SECURE-PRINT (Secure print file access control)**

TOE permits the print of the secure print file only to the user who is permitted the use of this secure print file.

#### **O.CONFIG (Access limitation to management function)**

TOE permits only the administrator the operation of the following functions.

- The setting function related to the SMTP server
- The setting function related to the DNS server
- The setting function related to the address of MFP
- Backup function
- Restoration function
- The setting function of HDD Lock function

- The setting function of CF Lock function
  - The setting function of Encryption function
  - The setting function of Trusted Channel function setting data
  - The setting function of certification, transmission address data, etc used for S/MIME function.
  - The setting of TSI receiving
  - The setting of PC-FAX operation
- TOE permits the operation of the following functions only to the administrator and the service engineer.
- The function related to the setting of Enhanced Security function

#### **O.OVERWRITE-ALL (Complete overwrite deletion)**

TOE overwrites all data regions of HDD and CF in MFP by using the deletion data, and makes all the image data of restoration impossible. In addition, TOE offers a function to initialize a setting value such as the highly confidential password on NVRAM (Administrator Password, HDD Lock Password, Encryption Passphrase) and password on CF (SNMP Password) that is set by a user or an administrator.

#### **O.CRYPT-KEY (Encryption key generation)**

TOE generates the encryption key to encrypt and store the image file written in HDD in MFP.

#### **O.CHECK-HDD (Validity confirmation of HDD)**

TOE verifies that correct HDD is installed.

#### **O.CHECK-CF (Validity confirmation of CF)**

TOE verifies that correct CF is installed.

#### **O.TRUSTED-PASS (The use of Trusted Channel)**

TOE offers the function that communicates via Trusted Channel the following image file which is transmitted and received between MFP and client PC.

< Image file transmitted from MFP to client PC >

- User box file
- < Image file transmitted from client PC to MFP >
- Image file that will be stored as user box file
  - Image file that will be stored as secure print file

#### **O.CRYPTO-MAIL (The use of encrypted mail)**

TOE offers the function that encrypts and transmits the user box file transmitted from MFP to the correct destination with e-mail.

#### **O.AUTH-CAPABILITY (The support operation to utilize user identification and authentication function)**

TOE supports the necessary operation to utilize the user identification and authentication function by user information management server using ActiveDirectory.

#### **O.CRYPTO-CAPABILITY (The support operation to utilize cryption function)**

TOE supports the necessary operation to utilize the crypton function by crypton kit.

**O.LOCK-HDD-CAPABILITY (The support operation to utilize HDD lock function)**

TOE supports the necessary operation to utilize the HDD lock function by HDD.

**O.LOCK-CF-CAPABILITY (The support operation to utilize CF lock function)**

TOE supports the necessary operation to utilize the CF lock function by CF.

## 4.2. Security objectives for the operation environment

In this section, the security objectives for the environment, in the operation environment of the usage of the TOE, is described.

**OE.CRYPT (Utilization of Encryption function)**

The administrator buys a license of encryption protection chip to set encryption of image files stored in HDD under this TOE. Then the administrator sets encryption kit with service engineer to encrypt image files to be written in HDD inside MFP.

**OE.FEED-BACK (Utilization of application to show secure password)**

The administrator and user utilize the application of a browser etc., used by client PC to access MFP, that offers the appropriate feedback protected for input user password, user box password, account password, administrator password, secure print password and SNMP password.

**OE.LOCK-HDD (Utilization of HDD with HDD lock function)**

The service engineer and the administrator install HDD with HDD lock function in MFP and set to utilize the function.

**OE.LOCK-CF (Utilization of CF with CF lock function)**

The service engineer and the administrator install CF with CF lock function in MFP and set to utilize the function.

**OE.SERVER (Utilization of user information management server)**

The administrator sets to utilize user management by Active Directory in case of using external user information management server in stead of MFP for the management of user account.

**OE.SESSION (Termination of session after operation)**

The administrator has the user implement the following operation.

- After the operation of the secure print file, and the operation of user box and user box file end, the logoff operation is performed.

The administrator executes the following operation.

- After the operation of the various function in administrator mode ends, the logoff operation is performed

The service engineer executes the following operation.

- After the operation of the various function in service mode ends, the logoff operation is

performed.

#### **OE.ADMIN (A reliable administrator)**

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

#### **OE.SERVICE (The service engineer's guarantee)**

- The person in charge in the organization that carries out the maintenance management of the MFP educates a service engineer in order to faithfully carry out the given role for the installation of the TOE, the set up of TOE and the maintenance of the MFP with TOE.
- The administrator observes the maintenance work of MFP with TOE by a service engineer.

#### **OE.NETWORK (Network Environment in which the MFP is connected)**

- The person in charge in the organization who uses MFP carries out the tapping prevention measures by setting the cipher communications equipment and the tapping detection equipment to the LAN of the office where MFP with TOE is installed.
- The person in charge in the organization who uses MFP carries out the measures for the unauthorized access from the outside by setting up the equipment such as the firewall to intercept the access from an external network to MFP with TOE.

#### **OE.SECRET (Appropriate management of confidential information)**

The administrator has the user implement the following operation.

- Keep the user password and secure print password confidential.
- Keep the user box password and account password confidential between the user who commonly utilizes it.
- Should not set the value that can be guessed for the user password, secure print password and the user box password.
- The user password and the user box password should be properly changed.
- When the administrator changes the user password or the user box password, make the user to change them promptly.

The administrator executes the following operation.

- Should not set the value that can be guessed for the administrator password, the account password, SNMP password, the HDD lock password, the CF lock password and encryption passphrase.
- Keep the administrator password, account password, the SNMP password, the HDD lock password and the encryption passphrase confidential.
- The administrator password, the account password, the SNMP password, the HDD lock password, the CF lock password and the encryption Passphrase should be properly changed.

The service engineer executes the following operation.

- Should not set the value that can be guessed for the CE password.
- Keep the CE password confidential.
- The CE password should be properly changed.
- When the service engineer changes the administrator password, make the administrator to change it promptly.

#### **OE.SETTING-SECURITY (Operation setting of Enhanced Security function)**

The administrator makes the setting of the enhanced security function effective for the operation of TOE.

### 4.3. Security Objectives Rationale

#### 4.3.1. Necessity

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

**Table 1 Conformity of Security Objectives to assumptions and Threats**

Assumption/Treat	A.ADMIN	A.SERVICE	A.NETWORK	A.SECRET	A.SETTING	T.DISCARD-MFP	T.BRING-OUT-STORAGE	T.ACCESS-PRIVATE-BOX	T.ACCESS-PUBLIC-BOX	T.ACCESS-GROUP-BOX	T.ACCESS-SECURE-PRINT	T.UNEXPECTED-TRANSMISSION	T.ACCESS-SETTING	T.BACKUP-RESTORE	T.BRING-OUT-CF	P.COMMUNICATION-DATA
O.REGISTERED-USER								X	X	X	X					
O.PRIVATE-BOX								X								
O.PUBLIC-BOX									X							
O.GROUP-BOX										X						
O.SECURE-PRINT											X					
O.CONFIG												X	X	X		X
O.OVERWRITE-ALL						X										
O.CRYPT-KEY							X									
O.CHECK-HDD							X									
O.CHECK-CF															X	
O.TRUSTED-PASS																X
O.CRYPTO-MAIL																X
O.CRYPTO-CAPABILITY							X									
O.LOCK-HDD-CAPABILITY							X									
O.LOCK-CF-CAPABILITY															X	
O.AUTH-CAPABILITY								X	X	X	X					
OE.CRYPT							X									
OE.LOCK-HDD							X									
OE.LOCK-CF															X	
OE.FEED-BACK								X	X	X	X	X	X	X		X
OE-SERVER								X	X	X	X					
OE-SESSION								X	X	X	X	X	X	X		X
OE-ADMIN	X															
OE-SERVICE		X														
OE-NETWORK			X													
OE-SECRET				X												
OE-SETTING-SECURITY					X											

### 4.3.2. Sufficiency of Assumptions

The security objectives for the assumptions are described as follows.

- **A.ADMIN (Personnel Conditions to be an Administrator )**

This condition assumes that administrators are not malicious.

With OE.ADMIN, the organization that uses the MFP assigns personnel who are reliable in the organization that uses the MFP, so the reliability of the administrator is realized.

- **A.SERVICE (Personnel Conditions to be a Service Engineer)**

This condition assumes the service engineer are not malicious.

With OE.SERVICE, the organization that manages the maintenance of the MFP educates the service engineer. Also the administrator needs to observe the maintenance of the MFP, so that the reliability of service engineers is assured.

- **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.

OE.NETWORK regulates the wiretapping prevention by the installation of devices such as a wiretapping detection device and device to perform the encryption communication on the intra-office LAN. It also regulates the unauthorized access prevention from external by the installation of devices such as firewall in order to block access to the MFP from the external networks, so that this condition is realized.

- **A.SECRET (Operating condition concerning confidential information)**

This condition assumes each password and encryption passphrase using for the use of TOE should not be leaked by each user.

OE.SECRET regulates that the administrator makes the user to execute the operation rule concerning the secure print password, the user box password, user password and account password and that the administrator executes the operation rule concerning the administrator password, the HDD lock password, the CF lock password, SNMP password, encryption passphrase and account password. It also regulates that the service engineer executes the operation rule concerning the CE password, and that the service engineer makes the administrator to execute the operation rule concerning the administrator password, so that this condition is realized.

- **A.SETTING (Enhanced Security Function Operational Settings Condition)**

This condition assumes the enhanced security function operational settings condition is satisfied.

OE.SETTING-SECURITY regulates that this is used after the administrator activates the enhanced security function, so that this condition is realized.

### 4.3.3. Sufficiency of Threats

The security objectives against threats are described as follows.

- **T.DISCARD-MFP (Lease return and disposal of MFP)**

This threat assumes the possibility of leaking information from MFP collected from the user. O.OVERWRITE-ALL is that TOE offers the function to overwrite data for the deletion of all area of HDD and initializes the information of NVRAM and CF, so that the possibility of the threat is removed by executing this function before MFP is collected. Accordingly, this threat is countered sufficiently.

- **T.BRING-OUT-STORAGE (Unauthorized taking out of HDD)**

This threat assumes the possibility that the image data in HDD leaks by being stolen from the operational environment under MFP used or by installing the unauthorized HDD and taking away with the data accumulated in it.

For the above, the possibility of the threat is reduced because the HDD lock function is activated by O.LOCK-HDD-CAPABILITY operation supporting to use HDD lock function and by OE.LOCK-HDD operation activating the operation of HDD lock function set by the administrator and the service engineer. Moreover a series of countermeasure for HDD, the possibility of the threat is more reduced because O.CRYPT-KEY generates the encryption key for TOE to encrypt data to be written in HDD, and O.CRYPTO-CAPABILITY supports the operation of using encryption function, and OE.CRYPTO utilize the encryption function of encryption kit set by the administrator and the service engineer.

The danger of leaking exists by taking out the HDD and replacing another HDD without the HDD lock function, but the validity of HDD installed by TOE is verified by O.CHECK-HDD, data is not written in the HDD replaced secretly. The possibility of the threat is removed consequently. The possibility of the threat for the unauthorized access by the leak of the management information attached image file is removed because the operation conditions achieved through security enhanced function do not permit to select the condition of O.CRYPT-KEY and OE.CRYPT only.

Accordingly, this threat is countered sufficiently.

- **T.ACCESS-PRIVATE-BOX (Unauthorized access to personal user box using user function)**

This threat assumes the possibility that an unauthorized operation is done by using the user function for the personal user box which each user uses to store the image file.

O.REGISTERED-USER is assumed that only the user to whom TOE was registered is permitted to use MFP installed TOE, furthermore, the operation of a personal user box and the user box file in a personal user box is restricted only to the user who is the owner by O.PRIVATE-BOX, so that the possibility of the threat is reduced. When the user information management server is used, the possibility of the threat is reduced because the user identification and authentication function is operated through O.AUTH-CAPABILITY supporting the operation for the user identification and authentication function by the user information management server of Active Directory and through OE.SERVER setting to use the user management by the administrator.

OE.FEED-BACK uses the application regulating to return the protected feedback for the entered password in the user's authentication, and OE-N.SESSION also requires the log-off operation after the operation ends, so that O.REGISTERED-USER and O.PRIVATE-BOX are supported sufficiently.

Accordingly, this threat is countered sufficiently.

- **T.ACCESS-PUBLIC-BOX (Unauthorized access to public user box using user function)**

This threat assumes the possibility that an unauthorized operation is done by using the user function for the public user box which each user shares to store the image file.

O.REGISTERED-USER assumes that only the user to whom TOE was registered is permitted to use MFP installing TOE, furthermore, the operation of the public user box and the user box file in the public user box is restricted only to the user who is permitted by O.PUBLIC-BOX, so that the possibility of the threat is reduced. When the user information management server is used, the possibility of the threat is reduced because the user identification and authentication function is operated through O.AUTH-CAPABILITY supporting the operation for the user identification and authentication function by the user information management server of Active Directory and through OE.SERVER setting to use the user management by the administrator.

OE.FEED-BACK uses the application regulating to return the protected feedback for the entered password in the user's authentication and user box's authentication, and OE-N.SESSION requires the log-off operation after the operation ends, so that O.REGISTERED-USER and O.PUBLIC-BOX are supported sufficiently.

Accordingly, this threat is countered sufficiently.

- **T.ACCESS-GROUP-BOX (Unauthorized access to a group user box using user function)**

This threat assumes the possibility that an unauthorized operation is performed by using the user function for the group box that is a storage area of image file used by user who is permitted the use of the account, or the user box file in it.

O.REGISTERED-USER assumes that only the user to whom TOE was registered is permitted to use MFP installed TOE, furthermore, the operation of the group user box and user box file in the group user box is restricted only to the permitted user by O.GROUP-BOX, so that the possibility of the threat is removed. When the user information management server is used, the possibility of the threat is reduced because the user identification and authentication function is operated through O.AUTH-CAPABILITY supporting the operation for the user identification and authentication function by the user information management server of Active Directory and through OE.SERVER setting to use the user management by the administrator.

OE.FEED-BACK uses the application regulating to return the protected feedback for the entered password in the user's authentication and account's authentication, and OE-N.SESSION also requires the log-off operation after the operation ends, so that O.REGISTERED-USER and O.GROUP-BOX are supported sufficiently.

Accordingly, this threat is countered sufficiently.

- **T.ACCESS-SECURE-PRINT (Unauthorized access to a secure print file using user function)**

This threat assumes the possibility that an unauthorized operation is done to the secure print using user function.

O.REGISTERED-USER assumes that only the user to whom TOE was registered is permitted to use MFP installing TOE, furthermore, the operation of the secure print is limited only to the authorized user by O.SECURE-PRINT, so that the possibility of the threat is reduced. When the user information management server is used, the possibility of the threat is reduced because the user identification and authentication function is operated through O.AUTH-CAPABILITY supporting the operation for the user identification and

authentication function by the user information management server of Active Directory and through OE.SERVER setting to use the user management by the administrator.

OE.FEED-BACK uses the application regulating to return the protected feedback for the entered password in the user's authentication and access authentication to the secure print, and OE-N.SESSION requires the log-off operation after the operation ends, so that O.REGISTERED-USER and O.SECURE-PRINT are supported sufficiently.

Accordingly, this threat is countered sufficiently.

- **T.UNEXPECTED-TRANSMISSION (Transmission to unintended address)**

This threat assumes the possibility of sending the user box file to the address that isn't intended, when the network setting that relates to the transmission is illegally changed. This is concerned about a possibility that the user box file is transmitted to the specified server illegally without the change of the network environment constitution by the malicious person by, for instance, illegally being changed the address of the SMTP server that relays E-mail for the E-mail, or illegally being changed the address of the DNS server where the domain name is inquired when the address of the SMTP server is used for a search of the domain name. For FTP transmission, by being likely to use the mechanism of the search of the domain name is concerned about the similar possibility of the incident might be occurred by E-mailing.

Furthermore, when the network setting which is related to the address of MFP is modified illegally, it assumes the possibility to use the print function to the unauthorized entity from client PC by the user who believes as TOE. Especially, it becomes a problem if a secure print file which is required to be concealed from other users in the office is transmitted to the unauthorized entity.

The setting of PC-FAX operation and the setting of TSI reception assumes the possibility of unintended box file storing at FAX reception. On the other hand, O.CONFIG regulates that the role to operate the network setting relating to the transmission of TOE, the setting of PC-FAX operation and the setting of TSI reception are limited to the administrator, and so the possibility of this threat is removed.

OE.FEED-BACK uses the application regulating that the feedback protected is returned for the entered password by the administrator's authentication and OE-N.SESSION requires to logoff after the operation ends, so that O.CONFIG is supported sufficiently.

Accordingly, this threat is countered sufficiently.

- **T.ACCESS-SETTING (Unauthorized change of function setting condition related to security)**

This threat assumes the possibility of developing consequentially into the leakage of the user box file and the secure print file by having been changed the specific function setting which relates to security.

O.CONFIG regulates that only the administrator is permitted to perform the setting of the enhanced security function that controls all setting function related to a series of security, and so the possibility of the threat is removed.

OE.FEED-BACK uses the application regulating that the feedback protected is returned for the entered various passwords by the administrator's authentication, and OE-N.SESSION is also requested to logoff respectively after the operations of the administrator mode ends, so that O.CONFIG is supported sufficiently.

Accordingly, this threat is countered sufficiently.

- **T.BACKUP-RESTORE (Unauthorized use of back-up function and restoration function)**

This threat assumes a possibility that the user box file and the secure print file may leak since the back-up function or the restoration function being illegally used. Moreover, this assumes that because of a leak of confidential data such as the password, the various setting values are falsified and there is a similar possibility that the user box file or the secure print file may leak.

O.CONFIG regulates that the use of the back-up function and the restoration function is permitted only to the administrator, so that the possibility of the threat is removed.

OE.FEED-BACK uses the application regulating that the protected feedback is returned for the entered password by the administrator authentication and OE-N.SESSION is also requested the log-off operation after the operation ends, and so O.CONFIG is sufficiently supported.

Accordingly, this threat is countered sufficiently.

- **T.BRING-OUT-CF (Unauthorized taking out of CF)**

This threat assumes the possibility that the leak of the information data in CF by being taken away or the unauthorized operation by installing the CF with falsified information or TOE.

For the above, the possibility of the threat is reduced because the CF lock function is activated by O.LOCK-CF-CAPABILITY operation supporting to use CF lock function and by OE.LOCK-CF operation activating the operation of CF lock function set by the administrator and the service engineer.

The danger of vulnerable operation for setting values related security exists by taking out the CF and replacing another CF without the CF lock function or another CF disabled CF lock function, but the validity of CF installed by TOE is verified by O.CHECK-CF, the replaced CF does not work. The possibility of the threat is removed consequently.

Accordingly, this threat is countered sufficiently.

#### 4.3.4. Sufficiency of Organizational Security Policies

Security objective corresponding to organizational security policies is explained as follows.

- **P.COMMUNICATION-DATA (secure communication of image file)**

This organizational security policy prescribes carrying out processing via trusted pass to a correct destination or encrypting to ensure the confidentiality about the image file which flows on a network in the case of the organization or the user expect to be protected. As this corresponds as one's request, there is no need to provide secure communication function for all communication. At least one secure communication method between MFP and client PC needs to be provided when transmitting the secure print file or the user box file.

O.TRUSTED-PASS offers the Trusted Channel to a correct destination in the transmission and reception of an image such as from MFP to client PC or from client PC to MFP, for the user box file and the secure print file that is a confidential image, so that the organizational security policies is achieved.

Also, the security objective offers the transmission function to a correct destination by encrypting the user box file transmitted by e-mail from MFP to client PC by

O.CRYPTO-MAIL, so that the organizational security policies is achieved. Furthermore,

O.CONFIG restricts the Trusted Channel function setting data, the management of the user

box files' encryption by e-mail and the transmission address data to the administrator. And then, OE.FEED-BACK uses the application regulating that the protected feedback is returned for the entered password in the administrator's authentication, and OE.SESSION is also regulated to log off after the operations of the administrator mode ends, so that O.CONFIG is supported.

Accordingly, this organizational security policies is sufficiently to achieve.

## 5. Extended Components Definition

### 5.1. Extended Function Component

In this ST, three extended function components are defined. The necessity of each security function requirement and the reason of the labeling definition are described.

- **FAD\_RIP.1**

This is the security function requirement for the protection of the remaining information of user data and TSF data.

- Necessity of extension

The regulation for the protection of the TSF data remaining information is necessary. But the security function requirement to explain the protection of the remaining information exists only in FDP\_RIP.1 for the user data. There is no security function requirement to satisfy this requirement.

- Reason for applied class (FAD)

There is no requirement to explain both of the user data and the TSF data with no distinction. Therefore new Class was defined.

- Reason for applied family (RIP)

As this is the extension upto the TSF data by using the content explained by the relevant family of FDP class, the same label of this family was applied.

- **FIA\_EID.1**

This is the security function requirement for regulating the conditions at the access to external entity from TOE.

- Necessity of extension

This is the approval of the action involved by TOE itself to the external entity, not the action of access to TOE from the external entity. There is no security function requirement to satisfy this requirement.

- Reason for applied class (FIA)

As this regulates to distinguish the external entity, FIA class is optimal to summarize the various security function requirements for identification certification.

- Reason for applied family (EID)

This requirement is judged to be not relevant to the content extension of the existing family. Therefore new Family was defined.

- **FIT\_CAP.1**

This is the security function requirement for regulating the necessary ability for TOE to use effectively the security function of the external entity, IT environment.

- Necessity of extension

In case of TOE using the external security functions, the external security function to be surely secure is important, but TOE ability to provide is very important in order to use correctly the external security function. But there is no concept as this requirement in the security function requirements.

- Reason for applied class (FIT)

There is no such concept in CC part 2. Therefore new Class was defined.

- Reason for applied family (CAP)

As similar to class, there is no such concept in CC part 2. Therefore new Family was defined.

### 5.1.1. FAD\_RIP.1 Definition

- **Class name**

FAD: Protection of all data

Meaning of abbreviation: FAD (Functional requirement for All Data protection)

- **Class behaviour**

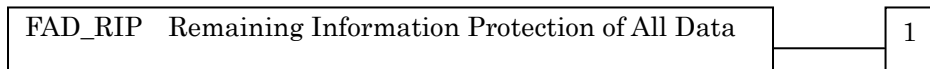
This class contains a family specifying the requirement related with the protection of the user data and the TSF data with no distinction. One family exists here.

- Remaining Information Protection of All Data (FAD\_RIP);

- **Family behaviour**

This family corresponds to the necessity never to access the deleted data or newly created object and TSF data which should not set as accessible. This family requires the protection for the information that was deleted or released logically but has a possibility to exist still in TOE.

- **Component leveling**



FAD\_RIP.1: "Remaining Information Protection of All Data after the explicit deletion operation" requires of TSF to assure that the subset of the defined object controlled by TSF cannot utilize every remaining information of every resource under the allocation of resource or the release of it.

<b>Audit</b> : FAD_RIP.1
The use of the user identification information with the explicit deletion operation
<b>Management</b> : FAD_RIP.1
No expected management activity

<b>FAD_RIP.1</b>	<b>Remaining Information Protection of All Data after the explicit deletion operation</b>
FAD_RIP.1.1	
	TSF shall ensure that the content of the information allocated to source before shall not be available after the explicit deletion operation against the object and TSF data.: [assignment: object list and TSF data list]
Hierarchical to	: No other components
Dependencies	: No dependencies

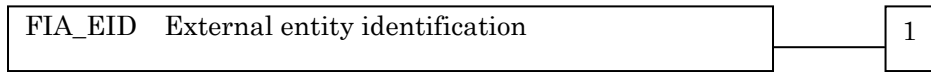
### 5.1.2. FIA\_EID.1 Definition

- **Family behaviour**

This family corresponds to the necessity to ensure that IT environment entity is not illegally

replaced when IT environment entity out of TOE provides the security functions. This family requires the verification of the authentication of IT environment entity.

● **Component leveling**



Meaning of abbreviation: EID (External entity IDentification)

FIA\_EID.1: "IT environment entity identification becoming an access object of TOE" requires the success of validity verification for IT environment entity before the action is involved in IT environment entity..

<b>Audit : FIA_EID.1</b>
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST. a) Minimal Unsuccessful use of IT environment entity identification mechanism including offered IT environment entity identification information b) Basic Use all of IT environment entity identification mechanism including offered IT environment entity identification information
<b>Management : FIA_EID.1</b>
The following actions could be considered for the management functions in FMT. a) management of IT environment entry identification information

<b>FIA_EID.1</b>	<b>Identification of IT environment becoming an access object from TOE</b>
FIA_EID.1.1	TSF shall demand to succeed in the IT environment entity's identification before the action is taken to IT environment entity by TOE.
FIA_EID.1.2	TSF shall stop the start of the action to IT environment entity by TOE if the IT environment entity's identification is failed.
Hierarchical to	: No other components
Dependencies	: No dependencies

5.1.3. FIT\_CAP.1 Definition

● **Class name**

FIT: Support for IT environment entity

Meaning of abbreviation: FIT (Functional requirement for IT environment support)

● **Class behaviour**

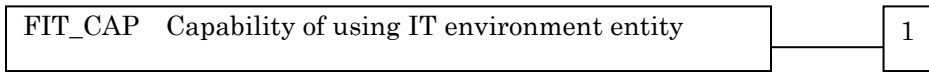
This class contains a family specifying the requirement related with the use of the security service provided by IT environment entity. One family exists here.

- Use of IT environment entity (FIT\_CAP);

● **Family behaviour**

This family corresponds to the capability definition for TOE at the use of security function of IT environment entity.

● **Component leveling**



Meaning of abbreviation: CAP (CAPability of using it environment)

FIT\_CAP.1: "Capability of using security seervice of IT environment entity" corresponds to the substantiation of capability needed to use the security function correctly provided by IT environment entity.

<b>Audit : FIT_CAP.1</b>
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST.
a) Minimal Failure of operation for IT environment entity
b) Basic Use all operation of IT environment entity (success, failure)
<b>Management : FIT_CAP.1</b>
The following actions could be considered for the management functions in FMT.
There is no management activity expected

<b>FIT_CAP.1</b>	<b>Capability of using security service of IT environment entity</b>
FIT_CAP.1.1	
TSF shall provide the necessary capability to use the service for [assignment: <i>security service provided by IT environment entity</i> ]. : [assignment: <i>necessary capability list for the operation of security service</i> ]	
Hierarchical to	: No other components
Dependencies	: No dependencies

## 6. IT Security Requirements

In this chapter, the TOE security requirements are described.

### <Definition of Label>

The security function requirements required for the TOE are described. Those regulated in CC Part 2 will be directly used for the functional requirements components, and the same labels will be used as well. The new additional requirement which is not described in CC part 2 is newly established and identified with the label that doesn't compete with CC part 2.

### < Method of specifying security function requirement "Operation" >

In the following description, when items are indicated in "italic" and "bold." it means that they are assigned or selected. When items are indicated in "italic" and "bold" with parenthesis right after the underlined original sentences, it means that the underlined sentences are refined. A number in the parentheses after a label means that the functional requirement is used repeatedly.

### <Method of clear indication of dependency>

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.

## 6.1. TOE Security Requirements

### 6.1.1. TOE Security Function Requirements

#### 6.1.1.1. Cryptographic Support

<b>FCS_CKM.1</b>		<b>Cryptographic key generation</b>
FCS_CKM.1.1		
The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: <i>cryptographic key generation algorithm</i> ] and specified cryptographic key sizes [assignment: <i>cryptographic key sizes</i> ] that meet the following: [assignment: <i>list of standards</i> ].		
[assignment: <i>list of standards</i> ] :		
<b><i>Listed in "Table2 Cryptographic key generation Relation of Standards-Algorithm-Key sizes"</i></b>		
[assignment: <i>cryptographic key generation algorithm</i> ] :		
<b><i>Listed in "Table2 Cryptographic key generation Relation of Standards-Algorithm-Key sizes"</i></b>		
[assignment: <i>cryptographic key sizes</i> ] :		
<b><i>Listed in "Table2 Cryptographic key generation Relation of Standards-Algorithm-Key sizes"</i></b>		
Hierarchical to	:	No other components
Dependencies	:	FCS_CKM.2 or FCS_COP.1 (FCS_COP.1 (only partial event)) , FCS_CKM.4 (N/A) ,

**Table 2 Cryptographic Key Generation Relation of Standards-Algorithm-Key sizes**

List of Standards	Cryptographic Key Generation Algorithm	Cryptographic Key sizes
<b><i>FIPS 186</i></b>	<b><i>Pseudorandom number Generation Algorithm</i></b>	<b><i>- 128 bit</i></b> <b><i>- 192 bit</i></b>

		- 168 bit - 256 bit
<b>KonicaMinolta Encryption specification standard</b>	<b>KonicaMinolta HDD Encryption Key Generation Algorithm (SHA-256)</b>	<b>256 bit</b>

<b>FCS_COP.1</b>	<b>Cryptographic operations</b>
------------------	---------------------------------

FCS_COP.1.1	
The TSF shall perform [assignment: <i>list of Cryptographic operations</i> ] in accordance with a specified cryptographic algorithm [assignment: <i>cryptographic algorithm</i> ] and cryptographic key sizes [assignment: <i>cryptographic key sizes</i> ] that meet the following: [assignment: <i>list of standards</i> ].	
[assignment: <i>list of standards</i> ] : <b>Listed in "Table3 Cryptographic operation Relation of Algorithm-Key sizes-Cryptographic operation"</b>	
[assignment: <i>cryptographic algorithm</i> ] : <b>Listed in "Table3 Cryptographic operation Relation of Algorithm-Key sizes-Cryptographic operation"</b>	
[assignment: <i>cryptographic key sizes</i> ] : <b>Listed in "Table3 Cryptographic operation Relation of Algorithm-Key sizes-Cryptographic operation"</b>	
[assignment: <i>list of cryptographic operation</i> ] : <b>Listed in "Table3 Cryptographic operation Relation of Algorithm-Key sizes-Cryptographic operation"</b>	
Hierarchical to	: No other components
Dependencies	: FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 (FCS_CKM.1 ( only a part of events)), FCS_CKM.4 (N/A)

**Table 3 Cryptographic Operation Relation of Algorithm-Keysizes-Cryptographic Operation**

List of standards	Cryptographic algorithm	Cryptographic key sizes	Contents of Cryptographic operation
<b>FIPS PUB 197</b>	<b>AES</b>	- 128 bit - 192 bit - 256 bit	<b>Encryption of S/MIME transmission data</b>
<b>SP800-67</b>	<b>3-Key-Triple-DES</b>	- 168 bit	<b>Encryption of S/MIME transmission data</b>
<b>FIPS 186-1</b>	<b>RSA</b>	- 1024 bit - 2048 bit - 3072 bit - 4096 bit	<b>Encryption of cryptographic key to encrypt S/MIME transmission data</b>

6.1.1.2. User data protection

<b>FDP_ACC.1[1]</b>	<b>Subset access control</b>
FDP_ACC.1.1[1]	
The TSF shall enforce the [assignment: <i>access control SFP</i> ] on [assignment: <i>list of subjects, objects, and operations among subjects and objects covered by the SFP</i> ].	
[assignment: <i>list of subjects, objects, and operations among subjects and objects covered by the SFP</i> ] : <b>Listed in "Table4 User box access control operational list "</b>	
[assignment: <i>access control SFP</i> ] : <b>User Box access control</b>	
Hierarchical to	: No other components
Dependencies	: FDP_ACF.1 (FDP_ACF.1[1])

**Table 4 User Box Access Control Operational List**

Subject	Object	Operational List
<i>A task to act for a user</i>	<i>User Box</i>	<i>-A List of user boxes</i>
	<i>User Box File</i>	<i>-Print -Transmission (E-mail transmission, FTP transmission, SMB transmission, FAX transmission and WebDAV transmission) -Download -Move to other user boxes -Copy to other user boxes -Backup</i>

<b>FDP_ACC.1[2]</b>	<b>Subset access control</b>
FDP_ACC.1.1[2]	
The TSF shall enforce the [assignment: <i>access control SFP</i> ] on [assignment: <i>list of subjects, objects, and operations among subjects and objects covered by the SFP</i> ].	
[assignment: <i>list of subjects, objects, and operations among subjects and objects covered by the SFP</i> ] : <b>Listed in "Table5 Secure print file access control operational list"</b>	
[assignment: <i>access control SFP</i> ] : <b>Secure print file access control</b>	
Hierarchical to	: No other components
Dependencies	: FDP_ACF.1 (FDP_ACF.1[2])

**Table 5 Secure Print File Access Control: Operational List**

Subject	Object	Operational list
<i>A task to act for a user</i>	<i>Secure Print File Access Control</i>	<i>-A List of Secure Print Files -Print -Back-Up</i>

<b>FDP_ACC.1[3]</b>	<b>Subset access control</b>
FDP_ACC.1.1[3]	
The TSF shall enforce the [assignment: <i>access control SFP</i> ] on [assignment: <i>list of subjects, objects, and operations among subjects and objects covered by the SFP</i> ].	
[assignment: <i>list of subjects, objects, and operations among subjects and objects covered by the SFP</i> ] : <b>Listed in "Table6 Setting management access control operational list"</b>	
[assignment: <i>access control SFP</i> ] : <b>Setting management access control</b>	

Hierarchical to	: No other components
Dependencies	: FDP_ACF.1 (FDP_ACF.1[3])

**Table 6 Setting Management Access Control: Operational List**

Subject	Object	Operational list
<i>A task to act for a user</i>	<ul style="list-style-type: none"> <li>-SMTP Server Group Object</li> <li>-DNS Server Group Object</li> <li>-MFP Address Group Object <sup>6</sup></li> <li>-PC-FAX operation setting Object</li> </ul>	<ul style="list-style-type: none"> <li>- Settings</li> <li>- Restore</li> </ul>

FDP_ACF.1[1]	Security attribute based access control
FDP_ACF.1.1[1]	
The TSF shall enforce the [assignment: <i>access control SFP</i> ] to objects based on the following: [assignment: <i>list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes</i> ].	
[assignment: <i>list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes</i> ] :	
<p><b>&lt;Subject&gt;</b>  <i>-A task to act for a user</i></p>	<p><b>&lt;Subject attributes&gt;</b>  → <i>-User Attribute (User ID)</i>  <i>-Account Name (Account ID)</i>  <i>-User Box Attribute (User Box ID)</i>  <i>-Administrator Attribute</i></p>
-----	
<p><b>&lt;Object&gt;</b>  <i>-User Box</i>  <i>-User Box File</i></p>	<p><b>&lt;Object attributes&gt;</b>  → <i>-User Attribute (User ID or Public or Account ID)</i>  → <i>-User Box Attribute (User Box ID)</i></p>
[assignment: <i>access control SFP</i> ] :	
<b><i>User Box access control</i></b>	
FDP_ACF.1.2[1]	
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: <i>rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects</i> ].	
[assignment: <i>rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects</i> ] :	
<p><b>&lt;Operation control to Personal user box&gt;</b>  <i>A task to act for a user is permitted to do the list display operation to the user box with the user attribute (user ID) of an object attribute corresponding to the user attribute (user ID) of the subject attribute.</i></p>	
<p><b>&lt;Operation control to Group user box&gt;</b>  <i>A task to act for a user is permitted to do the list display operation to the user box with the Account Name (account ID) of an object attribute corresponding to the Account Name (account ID) of the subject attribute.</i></p>	
<p><b>&lt;Operation control to Public user box&gt;</b>  <i>A task to act for the user who is related to the user attribute (user ID) is permitted to do the list display operation to the user box where "Public" is set to the user attributes of the object attribute.</i></p>	
<p><b>&lt;Operational control to User box file&gt;</b>  <i>A task to act for a user is permitted to print, transmit (E-mail transmission, FTP transmission, SMB transmission, FAX transmission and WebDAV transmission), download, move to other user boxes and copy to the other user boxes, to the user box file that have the matched the user box attribute (user box ID) of the object attribute with the user box attribute (user box ID) of the subject attribute.</i></p>	

<sup>6</sup>The MFP address group object is a series of data concerning the address of the main body of MFP such as IP address and the Appletalk printer name.

FDP_ACF.1.3[1]	
The TSF shall explicitly permit access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].	
[assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects] :	
<p><b><i>-A task to act for the user that has a administrator attribute is permitted to operate displaying of user box list.</i></b></p> <p><b><i>-A task to act for the user that has a administrator attribute is permitted to operate the back-up the user box file.</i></b></p>	
FDP_ACF.1.4[1]	
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] :	
<b><i>None</i></b>	
Hierarchical to	: No other components
Dependencies	: FDP_ACC.1 (FDP_ACC.1[1]), FMT_MSA.3 (FMT_MSA.3[1], FMT_MSA.3[3])

<b>FDP_ACF.1[2]</b>		<b>Security attribute based access control</b>	
FDP_ACF.1.1[2]			
The TSF shall enforce the [assignment: <i>access control SFP</i> ] to objects based on the following: [assignment: <i>list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes</i> ].			
[assignment: <i>list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes</i> ] :			
<b>&lt;Subject&gt;</b>		<b>&lt;Subject attributes&gt;</b>	
<b><i>-task substituted for a user</i></b>		<b>→ <i>-File attributes (Secure print internal control ID)</i></b>	
		<b><i>-User attributes (User ID)</i></b>	
		<b><i>-Administrator attributes</i></b>	
-----			
<b>&lt;Object&gt;</b>		<b>&lt;Object attributes&gt;</b>	
<b><i>-Secure print file</i></b>		<b>→ <i>-File attributes (Secure print internal control ID)</i></b>	
[assignment: <i>access control SFP</i> ] :			
<b><i>Secure print file access control</i></b>			
FDP_ACF.1.2[2]			
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: <i>rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects</i> ].			
[assignment: <i>rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects</i> ] :			
<p><b><i>-A task to act for a user who has a user attribute (user ID) is permitted to display of the list of all the secure print files.</i></b></p> <p><b><i>-A task to act for a user who has the file attribute (the secure print internal control ID) is permitted the print operation to the secure print file that has matched the file attribute (secure print internal control ID) with the file attribute (secure print internal control ID).</i></b></p>			
FDP_ACF.1.3[2]			
The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].			
[assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects] :			
<b><i>A task to act for a user who has a administrator attribute is permitted to back up secure print file.</i></b>			
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] :			
<b><i>None</i></b>			
Hierarchical to	: No other components		
Dependencies	: FDP_ACC.1 (FDP_ACC.1[2]), FMT_MSA.3 (FMT_MSA.3[2])		

FDP_ACF.1[3]	Security attribute based access control
FDP_ACF.1.1[3]	
The TSF shall enforce the [assignment: <i>access control SFP</i> ] to objects based on the following: [assignment: <i>list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes</i> ].	
[assignment: <i>list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes</i> ] :	
<p><b>&lt;Subject&gt;</b>  <i>-Task substituted for a user</i></p>	<p><b>&lt;Subject attributes&gt;</b>  <i>→ -Administrator attributes</i></p>
-----	
<p><b>&lt;Object&gt;</b>  <i>-SMTP server group object</i>  <i>-DNS server group object</i>  <i>-MFP address group object</i>  <i>-PC-FAX operation setting object</i>  <i>* No Object Attribute</i></p>	
[assignment: <i>access control SFP</i> ] :	
<b>Setting management access control</b>	
FDP_ACF.1.2[3]	
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: <i>rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects</i> ].	
[assignment: <i>rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects</i> ] :	
<b>-A task act for a user who has a administrator attribute is permitted to set the SMTP server group object, the DNS server group object the MFP address group object and the PC-FAX operation setting object, and to operate the restoration.</b>	
FDP_ACF.1.3[3]	
The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: <i>rules, based on security attributes, that explicitly authorize access of subjects to objects</i> ].	
[assignment: <i>rules, based on security attributes, that explicitly authorize access of subjects to objects</i> ] :	
<b>None</b>	
FDP_ACF.1.4[3]	
The TSF shall explicitly deny access of subjects to objects based on the [assignment: <i>rules, based on security attributes, that explicitly deny access of subjects to objects</i> ].	
[assignment: <i>rules, based on security attributes, that explicitly deny access of subjects to objects</i> ] :	
<b>None</b>	
Hierarchical to	: No other components
Dependencies	: FDP_ACC.1 (FDP_ACC.1[3]) , FMT_MSA.3 (N/A)

### 6.1.1.3. Identification and authentication

FIA_AFL.1[1]	Authentication failure handling
FIA_AFL.1.1[1]	
The TSF shall detect when [selection: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within [assignment: <i>range of acceptable values</i> ]] unsuccessful authentication attempts occur related to [assignment: <i>list of authentication events</i> ].	
[assignment: <i>list of authentication events</i> ] :	
<p><b>-Authentication for accessing the service mode</b>  <b>-Re-authentication for changing the CE password.</b></p>	

[selection: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within <i>[assignment: range of acceptable values]</i> ] <i>[assignment: range of acceptable values]</i> : an administrator configurable positive integer within 1~3	
FIA_AFL.1.2[1]	
When the defined number of unsuccessful authentication attempts has been [selection: <i>met, surpassed</i> ], the TSF shall [assignment: <i>list of actions</i> ].	
[selection: <i>met, surpassed</i> ] :	<b>Surpassed</b>
[assignment: <i>list of actions</i> ] :	<b>&lt;Action when it is detected&gt;</b> <ul style="list-style-type: none"> <li>• <i>Log off from the authentication status of the service mode if it is, and lock the authentication function which uses the CE password.</i></li> <li>• <i>If it's not under the authentication status, lock the authentication function which uses the CE password.</i></li> </ul> <b>&lt;Operation for recovering the normal condition&gt;</b> <ul style="list-style-type: none"> <li>- <i>Perform the lock release function of CE authentication by specific operation.</i></li> <li><i>(When CE authentication lock time passed from specific operation, the release process is performed.)</i></li> </ul>
Hierarchical to	: No other components
Dependencies	: FIA_UAU.1 (FIA_UAU.2[1])

<b>FIA_AFL.1[2]</b>	<b>Authentication failure handling</b>
---------------------	--

FIA_AFL.1.1[2]	
The TSF shall detect when [selection: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within <i>[assignment: range of acceptable values]</i> ] unsuccessful authentication attempts occur related to [assignment: <i>list of authentication events</i> ].	
[assignment: <i>list of authentication events</i> ] :	<ul style="list-style-type: none"> <li>- <i>Authentication for accessing the administrator mode</i></li> <li>- <i>Re-authentication for changing the administrator password</i></li> </ul>
[selection: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within <i>[assignment: range of acceptable values]</i> ] :	<i>[assignment: range of acceptable values]</i> : an administrator configurable positive integer within 1~3
FIA_AFL.1.2[2]	
When the defined number of unsuccessful authentication attempts has been [selection: <i>met, surpassed</i> ], the TSF shall [assignment: <i>list of actions</i> ].	
[selection: <i>met, surpassed</i> ] :	<b>Surpassed</b>
[assignment: <i>list of actions</i> ] :	<b>&lt;Action when it is detected&gt;</b> <ul style="list-style-type: none"> <li>• <i>Log off from the authentication status of the administrator mode if it is, and lock the authentication function which uses the administrator password.</i></li> <li>• <i>If it's not under the authentication status, lock the authentication function which uses the administrator password.</i></li> </ul> <b>&lt;Operation for recovering the normal condition&gt;</b> <ul style="list-style-type: none"> <li>- <i>Perform the lock release function offered within the service mode.</i></li> <li>- <i>Perform the boot process of the TOE. (Release process is performed after Administrator authentication lock time by the boot process.)</i></li> </ul>
Hierarchical to	: No other components
Dependencies	: FIA_UAU.1 (FIA_UAU.2[2])

<b>FIA_AFL.1[3]</b>	<b>Authentication failure handling</b>
---------------------	--

FIA_AFL.1.1[3]	
The TSF shall detect when [selection: <i>[assignment: positive integer number]</i> , an administrator	

<i>configurable positive integer within [assignment: range of acceptable values]</i> unsuccessful authentication attempts occur related to [assignment: <i>list of authentication events</i> ].	
[assignment: <i>list of authentication events</i> ] :	
<b>Authentication for accessing the MIB object through SNMP</b>	
[selection: <i>[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]</i> ] :	
<b>[assignment: range of acceptable values] : an administrator configurable positive integer within 1~3</b>	
FIA_AFL.1.2[3]	
When the defined number of unsuccessful authentication attempts has been [selection: <i>met, surpassed</i> ], the TSF shall [assignment: <i>list of actions</i> ].	
[selection: <i>met, surpassed</i> ] :	
<b>Surpassed</b>	
[assignment: <i>list of actions</i> ] :	
<b>&lt;Action when it is detected&gt;</b>	
<b>Deny the access to the MIB object and lock the authentication function to use SNMP password.</b>	
<b>&lt;Operation for recovering the normal condition&gt;</b>	
<b>-Perform the delete function of authentication failure frequency offered within the administrator mode.</b>	
Hierarchical to	: No other components
Dependencies	: FIA_UAU.1 (FIA_UAU.2[2])

<b>FIA_AFL.1[4]</b>	<b>Authentication failure handling</b>
---------------------	--

FIA_AFL.1.1[4]	
The TSF shall detect when [selection: <i>[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]</i> ] unsuccessful authentication attempts occur related to [assignment: <i>list of authentication events</i> ].	
[assignment: <i>list of authentication events</i> ] :	
<b>Authentication for accessing the TOE by user</b>	
[selection: <i>[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]</i> ] :	
<b>[assignment: range of acceptable values] : an administrator configurable positive integer within 1~3</b>	
FIA_AFL.1.2[4]	
When the defined number of unsuccessful authentication attempts has been [selection: <i>met, surpassed</i> ], the TSF shall [assignment: <i>list of actions</i> ].	
[selection: <i>met, surpassed</i> ] :	
<b>Surpassed</b>	
[assignment: <i>list of actions</i> ] :	
<b>&lt;Action when it is detected&gt;</b>	
<b>Log off from the authentication status of the user if it is, and lock the authentication function for the user.</b>	
<b>&lt;Operation for recovering the normal condition&gt;</b>	
<b>-Perform the delete function of authentication failure frequency offered within the administrator mode.</b>	
Hierarchical to	: No other components
Dependencies	: FIA_UAU.1 (FIA_UAU.2[3])

<b>FIA_AFL.1[5]</b>	<b>Authentication failure handling</b>
---------------------	--

FIA_AFL.1.1[5]	
The TSF shall detect when [selection: <i>[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]</i> ] unsuccessful authentication attempts occur related to [assignment: <i>list of authentication events</i> ].	
[assignment: <i>list of authentication events</i> ] :	
<b>Authentication for accessing the secure print file</b>	
[selection: <i>[assignment: positive integer number], an administrator configurable positive integer</i>	

<i>within [assignment: range of acceptable values] :</i>	
<b><i>[assignment: range of acceptable values] : an administrator configurable positive integer within 1~3</i></b>	
FIA_AFL.1.2[5]	
When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the TSF shall [assignment: list of actions].	
[selection: <i>met, surpassed</i> ] :	
<b><i>Surpassed</i></b>	
[assignment: list of actions] :	
<b>&lt;Action when it is detected&gt;</b>	
<b><i>Deny the access to the secure print file and lock the authentication function for the secure print file.</i></b>	
<b>&lt;Operation for recovering the normal condition&gt;</b>	
<b><i>-Perform the delete function of authentication failure frequency offered within the administrator mode.</i></b>	
<b><i>-Reboot the TOE.</i></b>	
Hierarchical to	: No other components
Dependencies	: FIA_UAU.1 (FIA_UAU.2[4])

<b>FIA_AFL.1[6]</b>	<b>Authentication failure handling</b>
---------------------	--

FIA_AFL.1.1[6]	
The TSF shall detect when [selection: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within [assignment: range of acceptable values]] unsuccessful authentication attempts occur related to [assignment: list of authentication events].	
[assignment: list of authentication events] :	
<b><i>Authentication for accessing the public user box</i></b>	
[selection: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within [assignment: range of acceptable values]] :	
<b><i>[assignment: range of acceptable values] : an administrator configurable positive integer within 1~3</i></b>	
FIA_AFL.1.2[6]	
When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the TSF shall [assignment: list of actions].	
[selection: <i>met, surpassed</i> ] :	
<b><i>Surpassed</i></b>	
[assignment: list of actions] :	
<b>&lt;Action when it is detected&gt;</b>	
<b><i>Log off from the authentication status of the user box if it is, and lock the authentication function for the concerned user box.</i></b>	
<b>&lt;Operation for recovering the normal condition&gt;</b>	
<b><i>-Perform the delete function of authentication failure frequency offered within the administrator mode.</i></b>	
Hierarchical to	: No other components
Dependencies	: FIA_UAU.1 (FIA_UAU.2[5])

<b>FIA_AFL.1[7]</b>	<b>Authentication failure handling</b>
---------------------	--

FIA_AFL.1.1[7]	
The TSF shall detect when [selection: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within [assignment: range of acceptable values]] unsuccessful authentication attempts occur related to [assignment: list of authentication events].	
[assignment: list of authentication events] :	
<b><i>-Account authentication: Account authentication when the belonging account of the user who accesses in the synchronized method is not registered.</i></b>	
<b><i>-Account authentication: Account authentication of the user who accesses in the method not synchronized.</i></b>	
[selection: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within [assignment: range of acceptable values]] :	

<i>[assignment: range of acceptable values] : an administrator configurable positive integer within 1~3</i>	
FIA_AFL.1.2[7]	
When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the TSF shall [assignment: list of actions].	
[selection: met, surpassed] :	
<b>Surpassed</b>	
[assignment: list of actions] :	
<b>&lt;Action when it is detected&gt;</b>	
<b>Lock the authentication function for the concerned account, and deny the access to the TOE by the user who permitted the use of the account.</b>	
<b>&lt;Operation for recovering the normal condition&gt;</b>	
<b>Perform the delete function of authentication failure frequency offered within the administrator mode.</b>	
Hierarchical to	: No other components
Dependencies	: FIA_UAU.1 (FIA_UAU.2[6])

<b>FIA_AFL.1[8] Authentication failure handling</b>	
FIA_AFL.1.1[8]	
The TSF shall detect when [selection: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within <i>[assignment: range of acceptable values]</i> ] unsuccessful authentication attempts occur related to [assignment: list of authentication events].	
[assignment: list of authentication events] :	
<ul style="list-style-type: none"> <li>- <b>Authentication when it accesses service mode</b></li> <li>- <b>Authentication when it accesses administrator mode from the panel</b></li> <li>- <b>User authentication when user accesses TOE from the panel</b></li> <li>- <b>Account authentication when user accesses TOE from the panel</b></li> <li>- <b>Authentication when it accesses secure print file</b></li> <li>- <b>Authentication when it accesses Public user box from the panel</b></li> </ul>	
[selection: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within <i>[assignment: range of acceptable values]</i> ] :	
<b><i>[assignment: positive integer number] : 1</i></b>	
FIA_AFL.1.2[8]	
When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the TSF shall [assignment: list of actions].	
[selection: met, surpassed] :	
<b>Surpassed</b>	
[assignment: list of actions] :	
<b>&lt;Action when it is detected&gt;</b>	
<b>Deny all access from the panel.</b>	
<b>&lt;Operation for recovering the normal condition&gt;</b>	
<b>Automatically release the lock after 5 seconds.</b>	
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_UAU.2[5], FIA_UAU.2[6])

<b>FIA_ATD.1 User attribute definition</b>	
FIA_ATD.1.1	
The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: list of security attributes].	
[assignment: list of security attributes] :	
<ul style="list-style-type: none"> <li>-<b>User attributes (User ID)</b></li> <li>-<b>User box attributes (User box ID)</b></li> <li>-<b>File attributes (Secure print internal control ID)</b></li> <li>-<b>Account name (Account ID)</b></li> </ul>	

<b>-Administrator Attribute</b>	
Hierarchical to	: No other components
Dependencies	: No dependencies

<b>FIA_SOS.1[1]</b>	<b>Verification of secrets</b>
FIA_SOS.1.1[1]	
The TSF shall provide a mechanism to verify that <u>secrets</u> ( <i>Administrator Password, CE Password</i> ) meet [assignment: <i>a defined quality metric</i> ].	
[assignment: <i>a defined quality metric</i> ]:	
<ul style="list-style-type: none"> <li>-<i>Number of digits: 8- digits</i></li> <li>-<i>Character type: possible to choose among more than 92 characters</i></li> <li>-<i>Rule</i> : <ul style="list-style-type: none"> <li>(1) <i>Do not compose by only the same character strings.</i></li> <li>(2) <i>Do not set the same password as the current setting after change.</i></li> </ul> </li> </ul>	
Hierarchical to	: No other components
Dependencies	: No dependencies

<b>FIA_SOS.1[2]</b>	<b>Verification of secrets</b>
FIA_SOS.1.1[2]	
The TSF shall provide a mechanism to verify that <u>secrets</u> ( <i>SNMP Password</i> ) meet [assignment: <i>a defined quality metric</i> ].	
[assignment: <i>a defined quality metric</i> ]:	
<ul style="list-style-type: none"> <li>-<i>Number of digits: 8- digits or more</i></li> <li>-<i>Character type: possible to choose among more than 93 characters</i></li> </ul>	
Hierarchical to	: No other components
Dependencies	: No dependencies

<b>FIA_SOS.1[3]</b>	<b>Verification of secrets</b>
FIA_SOS.1.1[3]	
The TSF shall provide a mechanism to verify that <u>secrets</u> ( <i>User Password</i> ) meet [assignment: <i>a defined quality metric</i> ].	
[assignment: <i>a defined quality metric</i> ]:	
<ul style="list-style-type: none"> <li>-<i>Number of digits: 8- digits or more</i></li> <li>-<i>Character type: possible to choose among more than 95 characters</i></li> <li>-<i>Rule</i> : <i>Do not composed by only the same character strings.</i></li> </ul>	
Hierarchical to	: No other components
Dependencies	: No dependencies

<b>FIA_SOS.1[4]</b>	<b>Verification of secrets</b>
FIA_SOS.1.1[4]	
The TSF shall provide a mechanism to verify that <u>secrets</u> ( <i>HDD Lock Password, CF Lock Password, Encryption passphrase</i> ) meet [assignment: <i>a defined quality metric</i> ].	
[assignment: <i>a defined quality metric</i> ]:	
<ul style="list-style-type: none"> <li>-<i>Number of digits: 20- digits</i></li> <li>-<i>Character type: possible to choose among more than 83 characters</i></li> <li>-<i>Rule</i> : <ul style="list-style-type: none"> <li>(1) <i>Do not compose by only the same character strings.</i></li> <li>(2) <i>Do not set the same password or passphrase as the current setting after change.</i></li> </ul> </li> </ul>	
Hierarchical to	: No other components
Dependencies	: No dependencies

<b>FIA_SOS.1[5]</b>		<b>Verification of secrets</b>	
FIA_SOS.1.1[5]			
The TSF shall provide a mechanism to verify that <u>secrets</u> ( <i>Secure Print Password, Box Password, Account Password</i> ) meet [assignment: <i>a defined quality metric</i> ].			
[assignment: <i>a defined quality metric</i> ] :			
- <i>Number of digits: 8- digits or more</i>			
- <i>Character type: possible to choose among more than 95 characters</i>			
- <i>Rule : Do not composed by only the same character strings.</i>			
Hierarchical to	:	No other components	
Dependencies	:	No dependencies	

<b>FIA_SOS.1[6]</b>		<b>Verification of secrets</b>	
FIA_SOS.1.1[6]			
The TSF shall provide a mechanism to verify that <u>secrets</u> ( <i>Session Information</i> ) meet [assignment: <i>a defined quality metric</i> ].			
[assignment: <i>a defined quality metric</i> ] :			
<i>10<sup>10</sup> and above</i>			
Hierarchical to	:	No other components	
Dependencies	:	No dependencies	

<b>FIA_SOS.2</b>		<b>TSF Generation of secrets</b>	
FIA_SOS.2.1			
The TSF shall provide a mechanism to generate secrets ( <i>Session information</i> ) that meet [assignment: <i>a defined quality metric</i> ].			
[assignment: <i>a defined quality metric</i> ] :			
<i>10<sup>10</sup> and above</i>			
FIA_SOS.2.2			
The TSF shall be able to enforce the use of TSF generated secrets for [assignment: <i>list of TSF functions</i> ].			
[assignment: <i>list of TSF functions</i> ] :			
- <i>Administrator authentication (Access through the network)</i>			
- <i>User authentication (Access through the network)</i>			
- <i>User box authentication (Access through the network)</i>			
Hierarchical to	:	No other components	
Dependencies	:	No dependencies	

<b>FIA_UAU.2[1]</b>		<b>User authentication before any action</b>	
FIA_UAU.2.1[1]			
The TSF shall require each <u>user</u> ( <i>Service Engineer</i> ) to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <i>Service Engineer</i> ).			
Hierarchical to	:	FIA_UAU.1	
Dependencies	:	FIA_UID.1 (FIA_UID.2[1])	

<b>FIA_UAU.2[2]</b>		<b>User authentication before any action</b>	
FIA_UAU.2.1[2]			
The TSF shall require each <u>user</u> ( <i>Administrator</i> ) to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <i>Administrator</i> ).			
Hierarchical to	:	FIA_UAU.1	
Dependencies	:	FIA_UID.1 (FIA_UID.2[2])	

<b>FIA_UAU.2[3]</b>	<b>User authentication before any action</b>
FIA_UAU.2.1[3]	
The TSF shall require each <u>user</u> ( <i>User</i> ) to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <i>User</i> ).	
Hierarchical to	: FIA_UAU.1
Dependencies	: FIA_UID.1 (FIA_UID.2[3])

<b>FIA_UAU.2[4]</b>	<b>User authentication before any action</b>
FIA_UAU.2.1[4]	
The TSF shall require each <u>user</u> ( <i>User who is permitted to use secure print file</i> ) to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <i>User who is permitted to use secure print file</i> ).	
Hierarchical to	: FIA_UAU.1
Dependencies	: FIA_UID.1 (FIA_UID.2[4])

<b>FIA_UAU.2[5]</b>	<b>User authentication before any action</b>
FIA_UAU.2.1[5]	
The TSF shall require each <u>user</u> ( <i>User who is permitted to use the public user box</i> ) to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <i>User who is permitted to use the public user box</i> ).	
Hierarchical to	: FIA_UAU.1
Dependencies	: FIA_UID.1 (FIA_UID.2[5])

<b>FIA_UAU.2[6]</b>	<b>User authentication before any action</b>
FIA_UAU.2.1[6]	
The TSF shall require each <u>user</u> ( <i>User who is permitted to use the account</i> ) to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <i>User who is permitted to use the account</i> ).	
Hierarchical to	: FIA_UAU.1
Dependencies	: FIA_UID.1 (FIA_UID.2[6])

<b>FIA_UAU.6</b>	<b>Re-authenticating</b>
FIA_UAU.6.1	
The TSF shall re-authenticate the use under the conditions [assignment: <i>list of conditions under which re-authentication is required</i> ].	
[assignment: <i>list of conditions under which re-authentication is required</i> ]	
<ul style="list-style-type: none"> <li>-When the administrator modifies the administrator password.</li> <li>-When the service engineer modifies the CE password.</li> <li>-When the administrator changes the HDD lock setting.</li> <li>-When the administrator changes the Encryption function setting.</li> <li>-When the administrator changes the CF lock setting.</li> </ul>	
Hierarchical to	: No other components
Dependencies	: No dependencies

<b>FIA_UAU.7</b>	<b>Protected authentication feedback</b>
------------------	--

FIA_UAU.7.1	
The TSF shall provide only [assignment: <i>list of feedback</i> ] to the user while the authentication is in progress.	
[assignment: <i>list of feedback</i> ] : <b>Display "*" every character data input.</b>	
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_UAU.2[5], FIA_UAU.2[6])

<b>FIA_UID.2[1]</b>	<b>User identification before any action</b>
---------------------	--

FIA_UID.2.1[1]	
The TSF shall require each <u>user</u> ( <i>Service Engineer</i> ) to identify itself before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <i>Service Engineer</i> ).	
Hierarchical to	: FIA_UID.1
Dependencies	: No dependencies

<b>FIA_UID.2[2]</b>	<b>User identification before any action</b>
---------------------	--

FIA_UID.2.1[2]	
The TSF shall require each <u>user</u> ( <i>Administrator</i> ) to identify itself before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <i>Administrator</i> ).	
Hierarchical to	: FIA_UID.1
Dependencies	: No dependencies

<b>FIA_UID.2[3]</b>	<b>User identification before any action</b>
---------------------	--

FIA_UID.2.1[3]	
The TSF shall require each <u>user</u> ( <i>User</i> ) to identify itself before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <i>User</i> ).	
Hierarchical to	: FIA_UID.1
Dependencies	: No dependencies

<b>FIA_UID.2[4]</b>	<b>User identification before any action</b>
---------------------	--

FIA_UID.2.1[4]	
The TSF shall require each <u>user</u> ( <i>User who is permitted to use secure print file</i> ) to be successfully identified before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <i>User who is permitted to use secure print file</i> ).	
Hierarchical to	: FIA_UID.1
Dependencies	: No dependencies

<b>FIA_UID.2[5]</b>	<b>User identification before any action</b>
---------------------	--

FIA_UID.2.1[5]	
The TSF shall require each <u>user</u> ( <i>User who is permitted to use the public user box</i> ) to be successfully identified before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <i>User who is permitted to use the public user box</i> ).	
Hierarchical to	: FIA_UID.1
Dependencies	: No dependencies

<b>FIA_UID.2[6]</b>	<b>User identification before any action</b>
---------------------	--

FIA_UID.2.1[6]	
The TSF shall require each <u>user</u> ( <i>User who is permitted to use the account</i> ) to be successfully identified before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <i>User who is permitted to use the account</i> ).	
Hierarchical to	: FIA_UID.1
Dependencies	: No dependencies

<b>FIA_UID.2[7]</b>	<b>User identification before any action</b>
---------------------	--

FIA_UID.2.1[7]	
The TSF shall require each <u>user</u> ( <i>External Server</i> ) to be successfully identified before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <i>External Server</i> ).	
Hierarchical to	: FIA_UID.1
Dependencies	: No dependencies

<b>FIA_USB.1</b>	<b>User-subject binding</b>
------------------	-----------------------------

FIA_USB.1.1	
The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment; <i>list of user security attributes</i> ].	
[assignment; <i>list of user security attributes</i> ]:	
<ul style="list-style-type: none"> <li>-<i>User attributes (User ID)</i></li> <li>-<i>User box attributes (User box ID)</i></li> <li>-<i>File attributes (Secure print internal control ID)</i></li> <li>-<i>Account name (Account ID)</i></li> <li>-<i>Administrator Attribute</i></li> </ul>	
FIA_USB.1.2	
The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: <i>rules for the initial association of attributes</i> ].	
[assignment: <i>rules for the initial association of attributes</i> ]:	
<p>&lt;<i>User box attribute</i>&gt;  <i>the user box ID of the concerned user box associates to the task acting on the behalf of users when authenticated with the access to the user box</i></p> <p>&lt;<i>Account Name</i>&gt;  <i>In the method not synchronized with User authentication, the account ID of the concerned account associates to the task acting on the behalf of users when authenticated with the access to the account.</i>  <i>In the method synchronized with User authentication, the account ID that is set to the concerned user associates to the task acting on the behalf of users when authenticated with the access to the user.</i></p> <p>&lt;<i>File attribute</i>&gt;  <i>The secure print internal control ID of the concerned secure print file associates to the task acting on the behalf of users when authenticated with the access to the secure print file.</i></p> <p>&lt;<i>User attribute</i>&gt;  <i>the user ID of the concerned user associates to the task acting on the behalf of users when authenticated with the access to the user</i></p> <p>&lt;<i>Administrator attribute</i>&gt;  <i>the Administrator ID associates to the task acting on the behalf of users when authenticated with the access to the Administrator</i></p>	
FIA_USB.1.3	
The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: <i>rules for the changing of attributes</i> ].	
[assignment: <i>rules for the changing of attributes</i> ].	
<b>None</b>	
Hierarchical to	: No other components
Dependencies	: FIA_ATD.1 (FIA_ATD.1)

#### 6.1.1.4. Security management

FMT_MOF.1[1] Management of security functions behavior	
FMT_MOF.1.1[1]	
The TSF shall restrict the ability to [selection: <i>determine the behavior of, disable, enable, modify the behavior of</i> ] the functions [assignment: <i>list of functions</i> ] to [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>list of functions</i> ] :	<ul style="list-style-type: none"> <li>-<b>Enhanced Security Setting</b></li> </ul>
[selection: <i>determine the behavior of, disable, enable, modify the behavior of</i> ] :	<b>disable</b>
[assignment: <i>the authorized identified roles</i> ] :	<ul style="list-style-type: none"> <li>-<b>Administrator</b></li> <li>-<b>Service Engineer</b></li> </ul>
Hierarchical to :	No other components
Dependencies :	FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[1], FMT_SMR.1[2])

FMT_MOF.1[2] Management of security functions behavior	
FMT_MOF.1.1[2]	
The TSF shall restrict the ability to [selection: <i>determine the behavior of, disable, enable, modify the behavior of</i> ] the functions [assignment: <i>list of functions</i> ] to [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>list of functions</i> ] :	<ul style="list-style-type: none"> <li>-<b>User Authentication Function</b></li> <li>-<b>S/MIME function</b></li> <li>-<b>SNMP password authentication function</b></li> </ul>
[selection: <i>determine the behavior of, disable, enable, modify the behavior of</i> ] :	<b>modify the behavior of</b>
[assignment: <i>the authorized identified roles</i> ] :	<b>Administrator</b>
Hierarchical to :	No other components
Dependencies :	FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2])

FMT_MOF.1[3] Management of security functions behavior	
FMT_MOF.1.1[3]	
The TSF shall restrict the ability to [selection: <i>determine the behavior of, disable, enable, modify the behavior of</i> ] the functions [assignment: <i>list of functions</i> ] to [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>list of functions</i> ] :	<ul style="list-style-type: none"> <li>-<b>Account Authentication Function</b></li> <li>-<b>Trusted Channel Function</b></li> </ul>
[selection: <i>determine the behavior of, disable, enable, modify the behavior of</i> ] :	<b>disable, modify the behavior of</b>
[assignment: <i>the authorized identified roles</i> ] :	<b>Administrator</b>
Hierarchical to :	No other components
Dependencies :	FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2])

FMT_MOF.1[4] Management of security functions behavior	
FMT_MOF.1.1[4]	
The TSF shall restrict the ability to [selection: <i>determine the behavior of, disable, enable, modify the behavior of</i> ] the functions [assignment: <i>list of functions</i> ] to [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>list of functions</i> ] :	

<b>Maintenance Function</b>	
[selection: <i>determine the behavior of, disable, enable, modify the behavior of</i> ]	:
<b>Enable</b>	
[assignment: <i>the authorized identified roles</i> ]	:
<b>Service engineer</b>	
Hierarchical to	: No other components
Dependencies	: FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[1])

<b>FMT_MSA.1[1] Management of security attributes</b>	
FMT_MSA.1.1[1]	
The TSF shall enforce the [assignment: <i>access control SFP, information flow control SFP</i> ] to restrict the ability to [selection: <i>change_default, query, modify, delete, [assignment: other operations]</i> ] the security attributes [assignment: <i>list of security attributes</i> ] to [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>list of security attributes</i> ] :	
<b>User attributes of the user box that is set user's own [user ID].</b>	
[selection: <i>change_default, query, modify, delete, [assignment: other operations]</i> ] :	
<b>Modify (modify to other user's [User ID], [account ID] or [public])</b>	
[assignment: <i>the authorized identified roles</i> ] :	
-User -Administrator	
[assignment: <i>access control SFP, information flow control SFP</i> ] :	
<b>User box access control</b>	
Hierarchical to	: No other components
Dependencies	: FDP_ACC.1 or FDP_IFC.1 (FDP_ACC.1[1]) , FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2]) , FMT_SMR.1[3]

<b>FMT_MSA.1[2] Management of security attributes</b>	
FMT_MSA.1.1[2]	
The TSF shall enforce the [assignment: <i>access control SFP, information flow control SFP</i> ] to restrict the ability to [selection: <i>change_default, query, modify, delete, [assignment: other operations]</i> ] the security attributes [assignment: <i>list of security attributes</i> ] to [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>list of security attributes</i> ] :	
<b>User attributes of user box that is set the [public].</b>	
[selection: <i>change_default, query, modify, delete, [assignment: other operations]</i> ] :	
<b>modify (modify to [User ID] or [account ID])</b>	
[assignment: <i>the authorized identified roles</i> ] :	
-User who is permitted to use that public user box -Administrator	
[assignment: <i>access control SFP, information flow control SFP</i> ] :	
<b>User box access control</b>	
Hierarchical to	: No other components
Dependencies	: FDP_ACC.1 or FDP_IFC.1 (FDP_ACC.1[1]) , FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2]) , FMT_SMR.1[4]

<b>FMT_MSA.1[3] Management of security attributes</b>	
FMT_MSA.1.1[3]	
The TSF shall enforce the [assignment: <i>access control SFP, information flow control SFP</i> ] to restrict the ability to [selection: <i>change_default, query, modify, delete, [assignment: other operations]</i> ] the security attributes [assignment: <i>list of security attributes</i> ] to [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>list of security attributes</i> ] :	
<b>User attributes of user box that is set the [Account ID].</b>	
[selection: <i>change_default, query, modify, delete, [assignment: other operations]</i> ] :	
<b>modify (modify to [user ID], [public] or other [account ID])</b>	

[assignment: <i>the authorized identified roles</i> ] :	
- <i>User who is permitted to use that account</i>	
- <i>Administrator</i>	
[assignment: <i>access control SFP, information flow control SFP</i> ] :	
<i>User box access control</i>	
Hierarchical to	: No other components
Dependencies	: FDP_ACC.1 or FDP_IFC.1 (FDP_ACC.1[1]) , FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2], FMT_SMR.1[6])

<b>FMT_MSA.3[1]</b>	<b>Static attribute initialization</b>
---------------------	--

FMT_MSA.3.1[1]	
The TSF shall enforce the [assignment: <i>access control SFP, information flow control SFP</i> ] to provide [selection, choose one of: <i>restrictive, permissive, [assignment: other property]</i> ] default values for <u>security attributes</u> ( <i>User attributes of the user box</i> ) that are used to enforce the SFP.	
[selection, choose one of: <i>restrictive, permissive, [assignment: other property]</i> ] :	
<i>[assignment: other property]</i> :	
<i>Responded the registered situation of the user box classified into the following cases.</i>	
<i>(1) [Public], when an user box is registered by the operation of user or administrator</i>	
<i>(2) [User ID] of the user who performed the relevant job, when an user box is registered automatically according to the operation of stored job specifying unregistered user box.</i>	
[assignment: <i>access control SFP, information flow control SFP</i> ] :	
<i>User box access control</i>	
FMT_MSA.3.2[1]	
The TSF shall allow the [assignment: <i>the authorized identified roles</i> ] to specify alternative initial values to override the default values when an object or information is created.	
[assignment: <i>the authorized identified roles</i> ]	
<i>Case (1) identified in [assignment: other property] of FMT_MSA.3.1 : User</i>	
<i>Case (2) identified in [assignment: other property] of FMT_MSA.3.1 : None</i>	
Hierarchical to	: No other components
Dependencies	: FMT_MSA.1 (FMT_MSA.1[1], FMT_MSA.1[2]) , FMT_SMR.1 (FMT_SMR.1[3])

<b>FMT_MSA.3[2]</b>	<b>Static attribute initialization</b>
---------------------	--

FMT_MSA.3.1[2]	
The TSF shall enforce the [assignment: <i>access control SFP, information flow control SFP</i> ] to provide [selection, choose one of: <i>restrictive, permissive, [assignment: other property]</i> ] default values for <u>security attributes</u> ( <i>Secure print internal control ID</i> ) that are used to enforce the SFP.	
[selection, choose one of: <i>restrictive, permissive, [assignment: other property]</i> ] :	
<i>[assignment: other property]</i> : <i>Identified uniquely</i>	
[assignment: <i>access control SFP, information flow control SFP</i> ] :	
<i>Secure print file access control</i>	
FMT_MSA.3.2[2]	
The TSF shall allow the [assignment: <i>the authorized identified roles</i> ] to specify alternative initial values to override the default values when an object or information is created.	
[assignment: <i>the authorized identified roles</i> ]	
<i>None</i>	
Hierarchical to	: No other components
Dependencies	: FMT_MSA.1 (N/A) , FMT_SMR.1 (N/A)

<b>FMT_MSA.3[3]</b>	<b>Static attribute initialization</b>
---------------------	--

FMT_MSA.3.1[3]	
The TSF shall enforce the [assignment: <i>access control SFP, information flow control SFP</i> ] to provide [selection, choose one of: <i>restrictive, permissive, [assignment: other property]</i> ] default values for	

<u>security attributes</u> ( <b>User box attributse of user box file</b> ) that are used to enforce the SFP.	
[selection, choose one of: <i>restrictive, permissive, [assignment: other property]</i> ]: <b>[assignment: other property]: Corresponds with the value of the user box attributes of the user box that selected as a target to store the user box file concerned.</b>	
[assignment: <i>access control SFP, information flow control SFP</i> ]: <b>User box access control</b>	
FMT_MSA.3.2[3]	
The TSF shall allow the [assignment: <i>the authorized identified roles</i> ] to specify alternative initial values to override the default values when an object or information is created.	
[assignment: <i>the authorized identified roles</i> ]: <b>None</b>	
Hierarchical to	: No other components
Dependencies	: FMT_MSA.1 (N/A) , FMT_SMR.1 (N/A)

<b>FMT_MTD.1[1] Management of TSF data</b>	
FMT_MTD.1.1[1]	
<b>(When the [machine authentication] is selected as the User authentication method)</b> The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear, [assignment: other operations]</i> ] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>list of TSF data</i> ]: <b>User password</b>	
[selection: <i>change_default, query, modify, delete, clear, [assignment: other operations]</i> ]: <b>[assignment: other operations] : Registration</b>	
[assignment: <i>the authorized identified roles</i> ]: <b>Administrator</b>	
Hierarchical to	: No other components
Dependencies	: FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2])

<b>FMT_MTD.1[2] Management of TSF data</b>	
FMT_MTD.1.1[2]	
<b>(When the [machine authentication] is selected as the User authentication method)</b> The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear, [assignment: other operations]</i> ] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>list of TSF data</i> ]: <b>User's own user password</b>	
[selection: <i>change_default, query, modify, delete, clear, [assignment: other operations]</i> ]: <b>modify</b>	
[assignment: <i>the authorized identified roles</i> ]: <b>-User</b> <b>-Administrator</b>	
Hierarchical to	: No other components
Dependencies	: FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2], FMT_SMR.1[3])

<b>FMT_MTD.1[3] Management of TSF data</b>	
FMT_MTD.1.1[3]	
The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear, [assignment: other operations]</i> ] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>list of TSF data</i> ]: <b>- User ID</b> <b>- Account ID</b> <b>- Account password</b> <b>- Secure print password</b>	

<ul style="list-style-type: none"> <li>- <i>Panel auto log-off time</i></li> <li>- <i>Threshold Number of authentication failure</i></li> <li>- <i>External server authentication setting data</i></li> <li>- <i>S/MIME certificate<sup>7</sup></i></li> <li>- <i>Transmission address data</i></li> <li>- <i>Belonging Account of User</i></li> <li>- <i>Administrator authentication lock time</i></li> <li>- <i>Encryption passphrase</i></li> <li>- <i>HDD lock password</i></li> <li>- <i>CF lock password</i></li> <li>- <i>SNMP password</i></li> <li>- <i>TSI receiving setting data</i></li> </ul>
[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] : <b><i>modify</i></b>
[assignment: <i>the authorized identified roles</i> ] : <b><i>Administrator</i></b>
Hierarchical to : No other components
Dependencies : FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2])

<b>FMT_MTD.1[4]</b>	<b>Management of TSF data</b>
FMT_MTD.1.1[4]	
The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>list of TSF data</i> ] : <b><i>User box password of the relevant user box</i></b>	
[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] : <b><i>modify</i></b>	
[assignment: <i>the authorized identified roles</i> ] : <b><i>-User who is permitted to use that public user box</i></b> <b><i>-Administrator</i></b>	
Hierarchical to : No other components	
Dependencies : FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2], FMT_SMR.1[4])	

<b>FMT_MTD.1[5]</b>	<b>Management of TSF data</b>
FMT_MTD.1.1[5]	
The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>list of TSF data</i> ] : <b><i>User box password</i></b>	
[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] : <b><i>[assignment: other operations] : Registration</i></b>	
[assignment: <i>the authorized identified roles</i> ] : <b><i>-User</i></b> <b><i>-Administrator</i></b>	
Hierarchical to : No other components	
Dependencies : FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2], FMT_SMR.1[3])	

<b>FMT_MTD.1[6]</b>	<b>Management of TSF data</b>
FMT_MTD.1.1[6]	
The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear</i> , [assignment:	

<sup>7</sup> It intends the operation of replacing a settable digital certificate for each user in stead of the modification of the value itself.

[other operations]] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>list of TSF data</i> ] :	
<b><i>Administrator password</i></b>	
[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] :	
<b><i>modify</i></b>	
[assignment: <i>the authorized identified roles</i> ] :	
<b><i>-Administrator</i></b>	
<b><i>-Service Engineer</i></b>	
Hierarchical to	: No other components
Dependencies	: FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[1], FMT_SMR.1[2])

<b>FMT_MTD.1[7]</b>	<b>Management of TSF data</b>
---------------------	-------------------------------

FMT_MTD.1.1[7]	
The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>list of TSF data</i> ] :	
<b><i>-SNMP password</i></b>	
<b><i>-User password</i></b>	
<b><i>-Account password</i></b>	
<b><i>-User box password</i></b>	
<b><i>-Secure print password</i></b>	
<b><i>-Encryption passphrase</i></b>	
[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] :	
<b><i>query</i></b>	
[assignment: <i>the authorized identified roles</i> ] :	
<b><i>Administrator</i></b>	
Hierarchical to	: No other components
Dependencies	: FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2])

<b>FMT_MTD.1[8]</b>	<b>Management of TSF data</b>
---------------------	-------------------------------

FMT_MTD.1.1[8]	
The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>list of TSF data</i> ] :	
<b><i>Secure print password</i></b>	
[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] :	
<b><i>[assignment: other operations] : Registration</i></b>	
[assignment: <i>the authorized identified roles</i> ] :	
<b><i>User</i></b>	
Hierarchical to	: No other components
Dependencies	: FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[3])

<b>FMT_MTD.1[9]</b>	<b>Management of TSF data</b>
---------------------	-------------------------------

FMT_MTD.1.1[9]	
The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>list of TSF data</i> ] :	
<b><i>-CE password</i></b>	
<b><i>-CE authentication lock time</i></b>	
[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] :	
<b><i>modify</i></b>	
[assignment: <i>the authorized identified roles</i> ] :	

<b><i>Service Engineer</i></b>	
Hierarchical to	: No other components
Dependencies	: FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[1])

<b>FMT_MTD.1[10] Management of TSF data</b>	
FMT_MTD.1.1[10]	
The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>list of TSF data</i> ] :	
<b><i>User ID</i></b>	
[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] :	
<b><i>[assignment: other operations] : Registration</i></b>	
[assignment: <i>the authorized identified roles</i> ] :	
<b><i>Administrator, External server</i></b>	
Hierarchical to	: No other components
Dependencies	: FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2], FMT_SMR.1[5])

<b>FMT_MTD.1[11] Management of TSF data</b>	
FMT_MTD.1.1[11]	
The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>list of TSF data</i> ] :	
- <b><i>Account ID</i></b>	
- <b><i>Account password</i></b>	
- <b><i>SMIME certificate</i></b>	
- <b><i>Transmission address data</i></b>	
- <b><i>Encryption passphrase</i></b>	
[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] :	
<b><i>[assignment: other operations] : Registration</i></b>	
[assignment: <i>the authorized identified roles</i> ] :	
<b><i>Administrator</i></b>	
Hierarchical to	: No other components
Dependencies	: FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2])

<b>FMT_MTD.1[12] Management of TSF data</b>	
FMT_MTD.1.1[12]	
The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>list of TSF data</i> ] :	
<b><i>Belonging Account of a user oneself</i></b>	
[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] :	
<b><i>[assignment: other operations] : Registration</i></b>	
[assignment: <i>the authorized identified roles</i> ]:	
<b><i>Administrator, the user who is permitted to use of the account<sup>8</sup></i></b>	
Hierarchical to	: No other components
Dependencies	: FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2], FMT_SMR.1[6])

<b>FMT_SMF.1 Specification of Management Functions</b>	
--	--

<sup>8</sup> A user who isn't related with an account name, and who was informed of the account password for the account ID from the administrator off-line.

**FMT\_SME.1.1**

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

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

- Stop Function of Enhanced security function by administrator*
- Operation Method Setting Function of User Authentication Function by administrator*
- Operation Method Setting Function of Account Authentication Function by administrator*
- Operation Setting Function of SNMP password authentication function by administrator*
- Setting function of authentication failure frequency threshold by administrator in the authentication operation prohibition function*
- Backup Function by administrator*<sup>9</sup>
- Restoration Function by administrator*<sup>10</sup>
- Registration function of account ID by administrator*
- Modification function of account ID by administrator*
- Registration function of account password by administrator*
- Modification function of account password by administrator*
- Panel Auto Log-off Time Setting Function by administrator*
- Modification function of administrator password by administrator*
- Modification function of SNMP password by administrator*
- Registration function of user box password by administrator*
- Modification function of user box password by administrator*
- User box registration function by administrator (However, only when the [public] is registered for user attribute.)*
- Modification function of user attribute of the user box by the administrator (However, only when the user attribute of previous setting is "user ID")*
- Registration function of user ID by administrator*
- Registration function of user password when method of user authentication by administrator is machine authentication*
- Modification function of user password when method of user authentication by administrator is machine authentication*
- Registration function of S/MIME certificate by administrator*
- Registration modification function of S/MIME certificate by administrator*
- Operation setting function of S/MIME function by administrator*
- Registration function of transmission address data by administrator*
- Modification function of transmission address data by administrator*
- Operation setting function of Trusted Channel function by administrator*
- Registration function of Belonging Account of user by administrator*
- Modification function of Belonging Account of user by administrator*
- Modification function of Administrator authentication lock time by administrator*
- Modification function of HDD Lock password by administrator*
- Modification function of CF Lock password by administrator*
- Modification function of Encryption passphrase by administrator*
- Operation setting function of Function to use encryption function realized by encryption kit by administrator*
- Modification function of TSI receiving setting data by administrator*
- Modification function of service engineer password by service engineer*
- Modification function of administrator password by service engineer*
- Stop function of Enhanced Security function by service engineer*
- Modification function of CE authentication lock time by service engineer*
- Operation function of Maintenance function by service engineer*
- Overwrite function for the default value of the user attribute of the user box by the user.*
- Modification function of user password when method of user authentication is machine authentication by user*
- Registration function of user box password by user*
- Modification function of user attribute of user box by user*

<sup>9</sup> A part of a backup function corresponds to the inquiry function of TSF data.

<sup>10</sup> A part of the restoration function corresponds to the modification function of the TSF data.

<ul style="list-style-type: none"> <li>-Registration function of Belonging Account of user oneself by user who is permitted the use of the account</li> <li>-User box registration function by user</li> <li>-Automatic Personal user box registration function by user box stored job that specifies unregistered box by user</li> <li>-Machine non-registered users' user ID automatic registration function with external server when user authentication method is external server authentication</li> <li>-Registration function of secure print password according to secure print file registration by user</li> <li>-Modification function of user attribute of user box by user who is permitted the use of public user box</li> <li>-Modification function of user box password of the user box by user who is permitted the use of public user box</li> <li>-Modification function of the concerned user box's user attribute by user who is permitted the use of the group box</li> </ul>	
Hierarchical to	: No other components
Dependencies	: No dependencies

<b>FMT_SMR.1[1] Security roles</b>	
FMT_SMR.1.1[1]	
The TSF shall maintain the roles [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>the authorized identified roles</i> ] : <b><i>Service Engineer</i></b>	
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.2[1])

<b>FMT_SMR.1[2] Security roles</b>	
FMT_SMR.1.1[2]	
The TSF shall maintain the roles [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>the authorized identified roles</i> ] : <b><i>Administrator</i></b>	
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[2])

<b>FMT_SMR.1[3] Security roles</b>	
FMT_SMR.1.1[3]	
The TSF shall maintain the roles [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>the authorized identified roles</i> ] : <b><i>User</i></b>	
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[3])

<b>FMT_SMR.1[4] Security roles</b>	
FMT_SMR.1.1[4]	
The TSF shall maintain the roles [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>the authorized identified roles</i> ] : <b><i>User who is authorized to use that public user box</i></b>	

FMT_SMR.1.2[4]	
The TSF shall be able to associate users with roles.	
Hierarchical to	: No other components
Dependencies	: FIA_UID.1 (FIA_UID.2[5])

<b>FMT_SMR.1[5]</b>	<b>Security roles</b>
---------------------	-----------------------

FMT_SMR.1.1[5]	
The TSF shall maintain the roles [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>the authorized identified roles</i> ] :	
<b><i>External server</i></b>	
FMT_SMR.1.2[5]	
The TSF shall be able to associate users with roles.	
Hierarchical to	: No other components
Dependencies	: FIA_UID.1 (FIA_UID.2[7])

<b>FMT_SMR.1[6]</b>	<b>Security roles</b>
---------------------	-----------------------

FMT_SMR.1.1[6]	
The TSF shall maintain the roles [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>the authorized identified roles</i> ] :	
<b><i>The user who is permitted to use of the account</i></b>	
FMT_SMR.1.2[6]	
The TSF shall be able to associate users with roles.	
Hierarchical to	: No other components
Dependencies	: FIA_UID.1 (FIA_UID.2[6])

6.1.1.5. TOE Access

<b>FTA_SSL.3</b>	<b>TSF-initiated termination</b>
------------------	----------------------------------

FTA_SSL.3.1	
The TSF shall terminate an interactive session after a [assignment: <i>time interval of user inactivity</i> ].	
[assignment: <i>time interval of user inactivity</i> ] :	
<b><i>Time decided from the final operation depending on the panel auto logoff time (1-9 minute/s) while a administrator or a user is operating on the panel</i></b>	
Hierarchical to	: No other components
Dependencies	: No dependencies

6.1.1.6. Trusted pass/channel

<b>FTP_ITC.1</b>	<b>Inter-TSF trusted channel</b>
------------------	----------------------------------

FTP_ITC.1.1	
The TSF shall provide a communication channel between itself and a other trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.	
FTP_ITC.1.2	
The TSF shall permit [selection : <i>the TSF, the other trusted IT product</i> ] to initiate communication via the trusted channel.	
[selection : <i>the TSF, the other trusted IT product</i> ]	
<b><i>The other trusted IT product</i></b>	
FTP_ITC.1.3	

The TSF shall initiate communication via the trusted channel for [assignment : <i>list of functions for which a trusted channel is required</i> ].	
[assignment : <i>list of functions for which a trusted channel is required</i> ] <ul style="list-style-type: none"> <li>-<i>Download of the user box file.</i></li> <li>-<i>Upload of the image file that will be stored as a user box file.</i></li> <li>-<i>Upload of the image file that will be the secure print file.</i></li> </ul>	
Hierarchical to	: No other components
Dependencies	: No dependencies

6.1.1.7. Extension: Remaining all information protection

<b>FAD_RIP.1</b>	<b>Protection of all remaining information after explicit deletion operation</b>
FAD_RIP.1.1	
TSF shall guarantee not to be able to use the content of any information before having been assigned to the resource on the explicit deleting operation to the following objects and the TSF data: [assignment: <i>list of object and list of TSF data</i> ].	
[assignment : <i>List of object and list of TSF data</i> ] : <ul style="list-style-type: none"> <li>&lt;<i>Objects</i>&gt; <ul style="list-style-type: none"> <li>-<i>User Box file</i></li> <li>-<i>Secure print file</i></li> <li>-<i>On memory image file</i></li> <li>-<i>Stored image file</i></li> <li>-<i>HDD remaining image file</i></li> <li>-<i>CF remaining image file</i></li> <li>-<i>Image-related file</i></li> <li>-<i>Transmission addressee data file</i></li> </ul> </li> <li>&lt;<i>TSF data</i>&gt; <ul style="list-style-type: none"> <li>-<i>HDD lock password</i></li> <li>-<i>CF lock password</i></li> <li>-<i>Encryption passphrase</i></li> <li>-<i>Administrator password</i></li> <li>-<i>SNMP password</i></li> <li>-<i>User ID</i></li> <li>-<i>User password</i></li> <li>-<i>User Box password</i></li> <li>-<i>Secure print password</i></li> <li>-<i>Account ID</i></li> <li>-<i>Account password</i></li> <li>-<i>S/MIME certificate</i></li> <li>-<i>Trusted Channel setting data</i></li> <li>-<i>Remaining TSF data</i><sup>11</sup></li> </ul> </li> </ul>	
Hierarchical to	: No other components
Dependencies	: No dependencies

6.1.1.8. Extension: Approval of access destination

<b>FIA_EID.1[1]</b>	<b>Identification of IT environment becoming an access object from TOE</b>
FIA_EID.1.1[1]	
TSF shall demand to succeed in the <u>IT environment entity's</u> ( <b>HDD</b> ) identification before the action is	

<sup>11</sup> TSF data remaining in the HDD data area, that cannot be deleted only by the deletion of the file management area.

taken to <u>IT environment entity's (HDD)</u> by TOE.	
FIA_NEW.1.2[1]	
TSF shall stop the start of the action to <u>IT environment entity's (HDD)</u> identification by TOE if the <u>IT environment entity's (HDD)</u> identification is failed.	
Hierarchical to	: No other components
Dependencies	: No dependencies

<b>FIA_EID.1[2]</b>	<b>Identification of IT environment becoming an access object from TOE</b>
FIA_EID.1.1[2]	
TSF shall demand to succeed in the <u>IT environment entity's (CF)</u> identification before the action is taken to <u>IT environment entity's (CF)</u> by TOE.	
FIA_NEW.1.2[2]	
TSF shall stop the start of the action to <u>IT environment entity's (CF)</u> identification by TOE if the <u>IT environment entity's (CF)</u> identification is failed.	
Hierarchical to	: No other components
Dependencies	: No dependencies

#### 6.1.1.9. Extension: Capability of using IT environment entity

<b>FIT_CAP.1[1]</b>	<b>Capability of using security service of IT environment entity</b>
FIT_CAP.1.1[1]	
TSF shall provide the necessary capability to use the service for [assignment: <i>security service provided by IT environment entity</i> ]. : [assignment: <i>necessary capability list for the operation of security service</i> ]	
[assignment: <i>security service provided by IT environment entity</i> ] :	
<b><i>User identification and authentication function of user information management server using ActiveDirectory</i></b>	
[assignment: <i>necessary capability list for the operation of security service</i> ] :	
- <b><i>Inquirey function of authentication information for the identification and authentication target user</i></b>	
- <b><i>Acquirement function of authentication information for the identification and authentication target user</i></b>	
Hierarchical to	: No other components
Dependencies	: No dependencies

<b>FIT_CAP.1[2]</b>	<b>Capability of using security service of IT environment entity</b>
FIT_CAP.1.1[2]	
TSF shall provide the necessary capability to use the service for [assignment: <i>security service provided by IT environment entity</i> ]. : [assignment: <i>necessary capability list for the operation of security service</i> ]	
[assignment: <i>security service provided by IT environment entity</i> ] :	
<b><i>Encryption function achieved by encryption kit</i></b>	
[assignment: <i>necessary capability list for the operation of security service</i> ] :	
<b><i>Support function of the the image files processing by encryption function</i></b>	
Hierarchical to	: No other components
Dependencies	: No dependencies

<b>FIT_CAP.1[3]</b>	<b>Capability of using security service of IT environment entity</b>
FIT_CAP.1.1[3]	
TSF shall provide the necessary capability to use the service for [assignment: <i>security service provided by IT environment entity</i> ]. : [assignment: <i>necessary capability list for the operation of security service</i> ]	
[assignment: <i>security service provided by IT environment entity</i> ] :	
<b><i>HDD lock function achieved by HDD</i></b>	

[assignment: <i>necessary capability list for the operation of security service</i> ] :	
<b>-Support function of modifying HDD lock password</b>	
<b>-Support function of releasing HDD lock function</b>	
Hierarchical to	: No other components
Dependencies	: No dependencies

<b>FIT_CAP.1[4] Capability of using security service of IT environment entity</b>	
FIT_CAP.1.1[4]	
TSF shall provide the necessary capability to use the service for [assignment: <i>security service provided by IT environment entity</i> ]. : [assignment: <i>necessary capability list for the operation of security service</i> ]	
[assignment: <i>security service provided by IT environment entity</i> ] :	
<b>CF lock function achieved by CF</b>	
[assignment: <i>necessary capability list for the operation of security service</i> ] :	
<b>-Support function of modifying CF lock password</b>	
<b>-Support function of releasing CF lock function</b>	
Hierarchical to	: No other components
Dependencies	: No dependencies

### 6.1.2. 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 7 TOE Security Assurance Requirements**

TOE Security Assurance Requirements		Component
Class ADV: Development	Security architecture description	ADV_ARC.1
	Functional specification with complete summary	ADV_FSP.3
	Architectural design	ADV_TDS.2
Class AGD: Guidance documents	Operational user guidance	AGD_OPE.1
	Preparative procedures	AGD_PRE.1
Class ALC: Life Cycle Support	Authorisation controls	ALC_CMC.3
	Implementation representation CM coverage	ALC_CMS.3
	Delivery procedures	ALC_DEL1
	Identification of security measures	ALC_DVS.1
	Developer defined life-cycle model	ALC_LCD.1
Class ASE: Security Target Evaluation	Conformance claims	ASE_CCL.1
	Extended components definition	ASE_ECD.1
	ST introduction	ASE_INT.1
	Security objectives	ASE_OBJ.2
	Derived security requirements	ASE_REQ.2
	Security problem definition	ASE_SPD.1
	TOE summary specification	ASE_TSS.1
Class ATE:	Analysis of coverage	ATE_COV.2

TOE Security Assurance Requirements		Component
Tests	Testing: basic design	ATE_DPT.1
	Functional testing	ATE_FUN.1
	Independent testing - sample	ATE_IND.2
Class AVA: Vulnerability Assessment	Vulnerability analysis	AVA_VLA.1

## 6.2. IT Security Requirements Rationale

### 6.2.1. Rationale for IT Security Functional Requirements

#### 6.2.1.1. 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 functional requirements correspond to at least one security objective.

**Table 8 Conformity of IT Security Functional Requirements to Security Objectives**

Security Objective	O.REGISTERED-USER	O.PRIVATE-BOX	O.PUBLIC-BOX	O.GROUP-BOX	O.SECURE-PRINT	O.CONFIG	O.OVERWRITE-ALL	O.CRYPT-KEY	O.CHECK-HDD	O.CHECK-CF	O.TRUSTED-PASS	O.CRYPTO-MAIL	O.AUTH-CAPABILITY	O.CRYPTO-CAPABILITY	O.LOCK-HDD-CAPABILITY	O.LOCK-CF-CAPABILITY	* set.admin	* set.service
<b>set.admin</b>	X	X	X	X	X	X												
<b>set.service</b>	X	X	X	X	X	X												
FCS_CKM.1								X				X						
FCS_COP.1												X						
FDP_ACC.1[1]		X	X	X		X												
FDP_ACC.1[2]					X	X												
FDP_ACC.1[3]						X												
FDP_ACF.1[1]		X	X	X		X												
FDP_ACF.1[2]					X	X												
FDP_ACF.1[3]						X												
FIA_AFL.1[1]																	X	X
FIA_AFL.1[2]																	X	
FIA_AFL.1[3]						X												
FIA_AFL.1[4]	X																	
FIA_AFL.1[5]					X													
FIA_AFL.1[6]			X															
FIA_AFL.1[7]				X														
FIA_AFL.1[8]	X		X	X	X												X	X
FIA_ATD.1		X	X	X	X	X												
FIA_SOS.1[1]																	X	X
FIA_SOS.1[2]						X												
FIA_SOS.1[3]	X																	

Security Objective Security Functional Requirements	O.REGISTERED-USER	O.PRIVATE-BOX	O.PUBLIC-BOX	O.GROUP-BOX	O.SECURE-PRINT	O.CONFIG	O.OVERWRITE-ALL	O.CRYPT-KEY	O.CHECK-HDD	O.CHECK-CF	O.TRUSTED-PASS	O.CRYPTO-MAIL	O.AUTH-CAPABILITY	O.CRYPTO-CAPABILITY	O.LOCK-HDD-CAPABILITY	O.LOCK-CF-CAPABILITY	* set-admin	* set-service
FIA_SOS.1[4]						X												
FIA_SOS.1[5]			X	X	X													
FIA_SOS.1[6]	X		X														X	
FIA_SOS.2	X		X														X	
FIA_UAU.2[1]																		X
FIA_UAU.2[2]						X											X	
FIA_UAU.2[3]	X																	
FIA_UAU.2[4]					X													
FIA_UAU.2[5]			X															
FIA_UAU.2[6]				X														
FIA_UAU.6						X											X	X
FIA_UAU.7	X		X	X	X												X	X
FIA_UID.2[1]																		X
FIA_UID.2[2]						X											X	
FIA_UID.2[3]	X																	
FIA_UID.2[4]					X													
FIA_UID.2[5]			X															
FIA_UID.2[6]				X														
FIA_UID.2[7]	X																	
FIA_USB.1		X	X	X	X	X												
FMT_MOF.1[1]						X												
FMT_MOF.1[2]	X					X												
FMT_MOF.1[3]				X		X												
FMT_MOF.1[4]						X												
FMT_MSA.1[1]		X				X												
FMT_MSA.1[2]			X			X												
FMT_MSA.1[3]				X		X												
FMT_MSA.3[1]		X	X															
FMT_MSA.3[2]					X													
FMT_MSA.3[3]		X	X	X														
FMT_MTD.1[1]	X																	
FMT_MTD.1[2]	X					X												
FMT_MTD.1[3]	X		X	X	X	X											X	X
FMT_MTD.1[4]			X			X												
FMT_MTD.1[5]			X															
FMT_MTD.1[6]																	X	
FMT_MTD.1[7]						X												
FMT_MTD.1[8]					X													
FMT_MTD.1[9]																		X
FMT_MTD.1[10]	X																	
FMT_MTD.1[11]				X		X												
FMT_MTD.1[12]				X														
FMT_SMF.1	X	X	X	X	X	X											X	X
FMT_SMR.1[1]						X											X	X

Security Objective	O.REGISTERED-USER	O.PRIVATE-BOX	O.PUBLIC-BOX	O.GROUP-BOX	O.SECURE-PRINT	O.CONFIG	O.OVERWRITE-ALL	O.CRYPT-KEY	O.CHECK-HDD	O.CHECK-CF	O.TRUSTED-PASS	O.CRYPTO-MAIL	O.AUTH-CAPABILITY	O.CRYPTO-CAPABILITY	O.LOCK-HDD-CAPABILITY	O.LOCK-CF-CAPABILITY	* set.admin	* set.service
FMT_SMR.1[2]	X	X	X	X	X	X											X	
FMT_SMR.1[3]	X	X			X													
FMT_SMR.1[4]			X															
FMT_SMR.1[5]	X																	
FMT_SMR.1[6]				X														
FTA_SSL.3	X																X	
FTP_ITC.1											X							
FAD_RIP.1							X											
FIA_EID.1[1]								X										
FIA_EID.1[2]									X									
FIT_CAP.1[1]												X						
FIT_CAP.1[2]													X					
FIT_CAP.1[3]														X				
FIT_CAP.1[4]															X			

Note) **set.admin** and **set.service** indicates the set of the requirements. And the security objectives assumed to have the correspondence and presented by "X" also correspond to a series of requirement set associated by \* set.admin and \* set.service shown in column.

### 6.2.1.2. Sufficiency

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

- **O.REGISTERED-USER (Usage of a registered user)**

This security objective limits the utilization of MFP installing TOE to only the registered user, and needs various requirements that related to the user identification and authentication.

<Necessary requirement for identification and authentication of the user>

It identifies and authenticates that the user who accesses is a registered user by FIA\_UID.2[3] and FIA\_UAU.2[3].

FIA\_UAU.7 returns "\*" for each entered character as feedback protected by the panel and supports the authentication.

In the case of the failure authentication from the panel, FIA\_AFL.1 [8] refuses all input acceptances from the panel for 5 seconds in every failure. When the authentication failure reaches 1-3 times, FIA\_AFL.1 [4] locks the authentication function for that user from then on. This lock status is released by the administrator's release operation.

FMT\_MOF.1[2] permits only the administrator the selection of the user authentication methods which are "Machine authentication" and "External server authentication". FMT\_MTD.1[3] permits only the administrator the setting (modification) of the threshold of the Authentication failure frequency which is the trial frequency of the failure authentication

in the user authentication.

FIA\_SOS.1[6] secures the quality verification of the session information used in the user authentication via the network, and FIA\_SOS.2 secures the quality of the session information which is generated and used.

<Necessary requirements for managing session of user who is identified and authenticated>

The duration of session of the user who is identified and authenticated contributes to reduce the chance of attacking associated with unnecessary session connection, by ending the session after the panel automatic logoff time elapses with FTA\_SSL.3. when it logs in from the panel. The change in the panel auto logoff time is limited to the administrator by FMT\_MTD.1[3].

<Necessary requirement for managing the identification and authentication information of the user>

When "the machine authentication" is chosen in a method of the user authentication by FMT\_MTD.1[1], the initial registration of a user password in the user's registration is permitted only by the administrator.

When "the machine authentication" has been selected in the method of the user authentication, the registration of the user ID in the user registration is permitted to the administrator by FMT\_MTD.1[10]. When the "external server authentication" (has been selected in the user authentication method, the user who is authenticated the identification is permitted from an external server and registered automatically by this requirement. (This corresponds to the user ID registration of the "external server".) At this registration, the external server accessing TOE is identified the external server registered by FIA\_UID.2[7]. This management behavior is maintained as the role of the external server by FMT\_SMR.1 [5]. In addition, the registration function of user ID is specified for the administration function by FMT\_SMF.1. The setting change operation of an external server is limited to only the administrator by FMT\_MTD.1[3].

The quality of the user password is verified by FIA\_SOS.1[3]. When "machine authentication" is selected in the method of the user authentication, a change of the user password is limited to the user itself and the administrator by FMT\_MTD.1[2].

<Necessary requirement to keep the administrator secure>

→ refer to set.admin

<Necessary requirement to keep the service engineer secure>

→ refer to set.service

<Role and management function for each management>

The role to do these managements is maintained as a administrator by FMT\_SMR.1[2] and a user by FMT\_SMR.1[3]. Moreover, these management functions are specified by FMT\_SMF.1.

This security objective is satisfied by the completion of these multiple functional requirements.

- **O.PRIVATE-BOX (personal user box access control)**

This security objective limits access to the personal user box and the user box file in the

personal user box to only the user who owns that user box, and needs various requirements that relate to the access control.

<User box access control (a personal user box)>

After the user has been identified and authorized, the user ID is related to the task of acting a use by FIA\_ATD.1 and FIA\_USB.1. By FDP\_ACC.1[1] and FDP\_ACF.1[1], the task of acting the user has a user ID, and is permitted to display the list of the user box with a corresponding user attribute. In addition, after the user box has been selected, when the user box ID is related to the task of acting a use by FIA\_ATD.1 and FIA\_USB.1, the operation such as a print, a download, transmissions, a movement, and a copy is permitted to the user box file that has a corresponding object attribute to user ID and user box ID of the subject attribute.

<Management of a personal user box>

FMT\_MSA.1[1] permits to the user and the administrator the change operation of the user attribute of the user box where the user ID is set.

As for the registration of the user box, public is appointed to the user attribute of the user box by FMT\_MSA.3[1], and it is permitted only to the user being able to give the initial value to change. In addition, when the job to store the non-registered user box into the user box appointed is executed due to the same requirement, a user ID of the user who executes a job concerned is appointed automatically.

<Necessary requirement to keep the administrator secure>

→ refer to set.admin

<Necessary requirement to keep the service engineer secure>

→ refer to set.service

<Role and controlling function for each management>

As the role of doing these managements, FMT\_SMR.1[2] maintains an administrator and FMT\_SMR.1[3] maintains a user permitted the use of the user box. FMT\_SMF.1 specifies these management functions.

This security objective is satisfied by the completion of these multiple functional requirements.

- **O.PUBLIC-BOX (a public user box access control)**

This security objective permits the inspection of the public user box to all users, and limits the setting of the public user box and the operation of the user box file in the public user box only to the user who permitted the utilization of that public user box. And it needs the various requirements that related to the access control.

<User box access control (a public user box)>

After the user has been identified and authorized, the user ID is related to the task of acting a use by FIA\_ATD.1 and FIA\_USB.1. FDP\_ACC.1[1] and FDP\_ACF.1[1] permits the list display operation to the user box where public is set to the user attribute to the task of acting the user

who has user ID.

It is required to be a user who is permitted the use of the user box to operate the user box file in the public user box. FIA\_UID.2[5] and FIA\_UAU.2[5] identifies and authenticates that it is a user who is permitted the use of the user box.

FIA\_UAU.7 returns "\*" for each entered character as feedback protected by the panel and supports the authentication.

In the case of the failure authentication from the panel, FIA\_AFL.1 [8] refuses all input acceptances from the panel for 5 seconds in every failure. When the authentication failure reaches 1-3 times, FIA\_AFL.1 [6] locks the authentication function for that user from then on. This lock status is released by the administrator's release operation.

FMT\_MTD.1[3] permits only to the administrator the setting of the threshold of the unauthorized access detection value that is the trial frequency of the failure authentication in the authentication of the user who is permitted the use of the user box.

When FIA\_ATD.1 and FIA\_USB.1 relates a user box ID to the task of acting use, FDP\_ACC.1[1] and FDP\_ACF.1[1] permit the user box file that has a corresponding object attribute to the user box ID of the subject attribute and is set public to the user attribute of user box, the operation such as a print, a download, transmissions, a movement, and a copy.

FIA\_SOS.1[6] secures the quality verification of the session information used in the user box authentication via the network, and FIA\_SOS.2 secures the quality of the session information which is generated and used.

<Management of a public user box>

FMT\_MSA.1[2] permits the user who is permitted the use of the user box to operate the change of the user attribute of use box which "Public" is set. FMT\_MTD.1[4] permits the change in the user box password only to the administrator and the user who is permitted to the use of the user box. FIA\_SOS.1[5] verifies the quality of the user box password.

As for the user box registration, FMT\_MSA.3[1] specifies the public to the user attribute of the user box, and permits only the user to be given the initial value to change it. Moreover, when the job that stores an unregistered user box in the box where is specified by this requirement is executed, the user ID of the user who executed a job concerned is automatically specified. FMT\_MTD.1[5] permits the registration of the user box password only to the user or the administrator. For the user box attribute of the user box file, the user box attribute value of the selected user box as storage is set by FMT\_MSA.3[3].

<Necessary requirement to keep the administrator secure>

→ refer to set.admin

<Necessary requirement to keep the service engineer secure>

→ refer to set.service

<Role and controlling function for each management>

As the role of doing these managements, FMT\_SMR.1[2] maintains an administrator and FMT\_SMR.1[4] maintains a user permitted the use of the user box. FMT\_SMF.1 specifies these management functions.

This security objective is satisfied by the completion of these multiple functional

requirements.

- **O.GROUP-BOX (Group user box access control)**

This security objective permits the browser of the group box only to the user who is permitted the use of the account, and limits the operation of the user function of the box file in the group user box, set of the group box only to the user who is permitted the use of the group user box, and requires various requirements that relate to the access control.

<User box access control (a group user box)>

After the user has been identified and authorized, the user ID is related to the task of acting a use by FIA\_ATD.1 and FIA\_USB.1 And after the account has been authorized, the account ID is related to the task of acting a use by FIA\_ATD.1 and FIA\_USB.1 FDP\_ACC.1[1] and FDP\_ACF.1[1] permits a task to act for the user to operate the list to the user box (group user box) where the user attribute corresponded with the Account Name (account ID) in the security attribute of the subject is set.

It is required to be a user who is permitted the use of the group user box to operate the user box file in the group user box. When the Account authentication method is "the method not synchronized", FIA\_UID.2[6] and FIA\_UAU.2[6] identifies and authenticates that it is a user who is permitted the use of the group user box. When the account authentication method is "synchronized method" and the Account that user belongs to is not registered, FIA\_UID.2[6] and FIA\_UAU.2[6] identifies and authenticates that it is a user who is permitted the use of the account.

FIA\_UAU.7 returns "\*" for each entered character as feedback protected by the panel and supports the authentication.

In the case of the failure authentication from the panel, FIA\_AFL.1[8] refuses all input acceptances from the panel for 5 seconds in every failure. When the authentication failure reaches 1-3 times, FIA\_AFL.1[7] locks the authentication function for that account from then on. This lock status is released by the administrator's release operation.

FMT\_MTD.1[3] permits only the administrator the setting of the threshold of the unauthorized access detection value that is the trial frequency of the failure authentication in the authentication of the user who is permitted the use of the group user box.

When FIA\_ATD.1 and FIA\_USB.1 relates to the user box ID under the task to act for user, FDP\_ACC.1[1] and FDP\_ACF.1[1] permits the user box file that has a corresponding object attribute to the account ID and the user box ID of the subject attribute the operation such as print, download, transmissions, movement and copy.

<Necessary requirement to manage the group box>

FMT\_MAS.1[3] permits the modification operation of the user attribute of the user box that is set "account ID" to the user who is permitted the access to the group user box.

For the user box attribute of the user box file, the user box attribute value of the selected user box as storage is set by FMT\_MSA.3[3].

<Necessary requirement to manage the subject attribute related with the group user box>

FMT\_MTD.1[11] restricts the registration of the account ID and account password only to the administrator. Also, FMT\_MTD.1[3] restricts the modification of the account ID and account password only to the administrator.

FMT\_MTD.1[12] restricts the registration of the belonging account assigned to the user, to the administrator and to the user who is permitted the use of the account.

FIA\_SOS.1[5] verifies the quality of the account password .

<Management of the account authentication method>

FMT\_MOF.1[3] restricts the behavior management of the account authentication function and the stop operation management to the administrator.

<Necessary requirement to keep the administrator secure>

→ refer to set.admin

<Necessary requirement to keep the service engineer secure>

→ refer to set.service

<Role and controlling function for each management>

As the role of doing these managements, FMT\_SMR.1[2] maintains an administrator and FMT\_SMR.1[6] maintains a user permitted the use of the group user box. FMT\_SMF.1 specifies these management functions.

This security objective is satisfied by the completion of these multiple functional requirements.

#### ● O.SECURE-PRINT (Secure print file)

These security objectives explain the policy for the secure print file.

First, for secure print file, this security objective limits the print of the secure print file only for the user, who is permitted the use of the secure print file, and requires various requirements that relate to the access control.

<Secure print file access control>

After the user has been identified and authorized, the user ID is related to the task of acting a use by FIA\_ATD.1 and FIA\_USB.1. FDP\_ACC.1[2] and FDP\_ACF.1[2] permits the list display operation of every secure print user box to the task of acting the user who has user ID. As it must be a user who is permitted the use of the secure print file to print it, FIA\_UID.2[4] and FIA\_UAU.2[4] identifies and authenticates that it is a user who is permitted the use of the secure print file.

FIA\_UAU.7 returns "\*" for each entered character as feedback protected by the panel and supports the authentication.

FIA\_AFL.1 [8] refuses all input acceptances from the panel for 5 seconds in every failure. When the authentication failure reaches 1-3 times, FIA\_AFL.1 [5] locks the authentication function for to the concerned secure print file. This lock status is released by the administrator's release operation.

FMT\_MTD.1[3] permits only to the administrator the setting of the threshold of the authentication failure frequency that is the trial frequency of the failure authentication in the authentication of the user who is permitted the use of the secure print file.

When FIA\_ATD.1 and FIA\_USB.1 relate the secure print internal control ID to the task of acting use, FDP\_ACC.1[2] and FDP\_ACF.1[2] permit the print operation to the secure print

file that has a corresponding object attribute to the secure print internal control ID of the subject attribute.

As for secure print internal control ID, FMT\_MSA.3[2] gives the value uniquely identified when the secure print file is registered.

<Secure print password>

FMT\_MTD.1[8] permits only to the user the registration of the secure print password used for the authentication. FIA\_SOS.1[5] verifies the quality of the secure print password.

<Necessary requirement to keep the administrator secure>

→ refer to set.admin

<Necessary requirement to keep the service engineer secure>

→ refer to set.service

<Role and controlling function for each management>

As the role of doing these managements, FMT\_SMR.1[2] maintains an administrator and FMT\_SMR.1[3] maintains a user. Moreover, FMT\_SMF.1 specifies these management functions.

This security objective is satisfied by the completion of these multiple functional requirements.

- **O.CONFIG (Access limitation to an management function)**

This security objective limits the setting related to the SMTP server, the setting related to the DNS server, the setting related to the Enhanced Security function, the backup function, and the restorations function to the administrator, and needs various requirements to limit the access to a series of setting function and the management function.

<Management of network setting>

When the administrator attribute is associated with the task of substituting the use, FDP\_ACC.1[3] and FDP\_ACF.1[3] permits the task of substituting the user to operate the SMTP server group object, the DNS server group object, the settings for the MFP address group object and PC-FAX operation setting object.

<Operation limitation of Backup and restoration function>

When the administrator attribute is related to the task of acting the use by FIA\_ATD.1 and FIA\_USB.1, the task of acting the user is permitted the back-up operation of;

- the user box files by FDP\_ACC.1[1] and FDP\_ACF.1[1].
- the secure print files by FDP\_ACC.1[2] and FDP\_ACF.1[2].

In addition, the restoration operation is permitted for

- SMTP server group object, DNS server group object, MFP address group object and PC-FAX operation setting object by FDP\_ACC.1[3] and FDP\_ACF.1[3].

Moreover, the restoration operation is permitted for

- the enhanced security setting data by FMT\_MOF.1[1]
- the operation setting data of user authentication function, encryption strength setting data

for S/MIME function and setting data of SNMP password authentication function by FMT\_MOF.1[2].

-the Trusted Channel setting data, encryption passphrase and account authentication function operation setting data by FMT\_MOF.1[3].

-the user attribute of the user box by FMT\_MSA.1[1], FMT\_MSA.1[2] and FMT\_MSA.1[3].

-the user password by FMT\_MTD.1[2].

-the user ID, the SNMP password, the panel auto logoff time, the authentication failure frequency, the secure print password, the external authentication setting data, the account ID, the account password, the S/MIME certificate, the transmission address data, the belonging account of user, administrator authentication lock time, TSI receiving setting by FMT\_MTD.1[3].

-the restoration operation (modification operation) is permitted only to the administrator for objective data of the user box password by FMT\_MTD.1[4]. FMT\_MTD.1[7] permits only to the administrator the backup operation (inquiry operation) of the SNMP password, the user password, the user box password, and the secure print password, the account password, encryption passphrase.

#### <Operational limitation of Enhanced Security function>

FMT\_MOF.1[1] permits only the administrator and service engineer to disable the setting for the enhanced security function. FMT\_MOF.1[4] permits only the service engineer to enable the operation setting (activation) for the maintenance function.

#### <Management of HDD lock password, encryption passphrase and CF lock password>

FMT\_MTD.1[3] permits the modification operation to the HDD lock password, the encryption passphrase and CF lock password. FIA\_SOS.1[4] verifies the quality of the HDD lock password, the encryption passphrase and CF lock password. In order to change the HDD lock password, encryption passphrase and CF lock password, FIA\_UAU.6 re-authenticates that a user is an administrator by collating with the registered HDD lock password and encryption Passphrase object. When the authentication is succeeded, the HDD lock password, encryption passphrase and CF lock password are allowed to be changed.

Moreover, FMT\_MTD.1[11] permits only to the administrator to register the encryption passphrase.

#### <Necessary requirement for accessing MIB object>

The SMTP server group object, the DNS server group object and the MFP address group object exists as an MIB object as well, so that the restriction is necessary even in the access from the SNMP.

FIA\_UID.2[2] and FIA\_UAU.2[2] identifies and authenticates that the user who accesses the MIB object is an administrator.

FIA\_AFL.1[3] locks the authentication function to access the MIB object when the failure authentication reaches 1-3 times. This lock is released by the start of TOE or the lock release operation by the administrator.

FMT\_MTD.1[3] restricts the threshold setting of the unauthorized access detection value that is the trial frequency of the failure authentication in the administrator authentication using the SNMP password only to the administrator

FMT\_MTD.1[3] restricts the change in the SNMP password to the administrator.  
FIA\_SOS.1[2] verifies the quality of the SNMP password.  
FMT\_MOF.1[2] restricts the method of the SNMP password authentication function only to the administrator.

<Operational Limit of Trusted Channel function setting data>

The behavior and the stop setting of Trusted Channel function are permitted only to the administrator by FMT\_MOF.1[3].

<Operational Limit for S/MIME function>

The registration of the S/MIME certificate and the transmission address data is permitted only to the administrator by FMT\_MTD.1[11]. The modification of the S/MIME certificate and the transmission address data is permitted only to the administrator by FMT\_MTD.1[3]. The behavior of the S/MIME function is permitted only to the administrator by the FMT\_MOF.1[2].

<Necessary requirements to keep the administrator secure>

→ refer to set.admin

<Necessary requirements to keep the service engineer secure>

→ refer to set.service

<Role and controlling function for each management>

As the role of doing these managements, FMT\_SMR.1[1] maintains a service engineer and FMT\_SMR.1[2] maintains an administrator. Moreover, FMT\_SMF.1 specifies these management functions.

This security objective is satisfied by the completion of these multiple functional requirements.

- **O.OVERWRITE-ALL (Complete overwrite deletion)**

This security objective regulates that it deletes all data areas of HDD and initializes the concealed information of NVRAM that is set by the user, and requires various requirements that relate to the deletion.

FAD\_RIP.1 guarantees that these objective information not to be able to use the content of any previous information by the deletion operation.

This security objective is satisfied by the completion of these multiple functional requirements.

- **O.CRYPT-KEY (Encryption key generation)**

This security objective regulates that, when the encryption protection chip is installed, the encryption key necessary to encrypt all the data written in HDD is generated, and needs various requirements that relate to the encryption key generation.

Using KonicaMinolta HDD encryption key generation mechanism (SHA256) according to KonicaMinolta encryption specification standard, FCS\_CKM.1 generates the 256bit

encryption key.

This security objective is satisfied by the completion of this function requirement.

- **O.CHECK-HDD (Validity confirmation of HDD)**

This security objective regulates that it verifies the validity of HDD in order to confirm the unauthorized HDD doesn't exist, and needs various requirements that relate to the verification of an external entity from TOE.

FIA\_EID.1[1] identifies HDD before the action from TOE to HDD, and cancels the scheduled action when the identification fails.

This security objective is satisfied by the completion of this function requirement.

- **O.CHECK-CF (Validity confirmation of CF)**

This security objective regulates that it verifies the validity of CF in order to confirm the unauthorized CF doesn't exist, and needs various requirements that relate to the verification of an external entity from TOE.

FIA\_EID.1[2] identifies CF before the action from TOE to CF, and cancels the scheduled action when the identification fails.

This security objective is satisfied by the completion of this function requirement.

- **O.TRUSTED-PASS(Usage of Trusted Channel)**

This security objective generates the Trusted Channel in the transmission and reception such as a user box file and a secure print file, and the requirement that relates with the Trusted Channel is necessary. FTP\_ITC.1 generates the Trusted Channel according to the requirement from the other Trusted IT product, and it is applied to the transmission and reception, such as the user box file and the secure print file.

This security objective is satisfied by the completion of this function requirement,

- **O.CRYPTO-MAIL (Usage of Encryption mail)**

This security objective regulates the encryption of a user box file when transmitting the user box file by e-mail, and various requirements related to the encryption are necessary.

FCS\_CKM.1 generates the encryption key (128bit, 168bit, 192bit or 256bit) by using Pseudorandom number Generation Algorithm according to FIPS 186-2.

FCS\_COP.1 encrypts the user box file by using AES (encryption key: 128bit, 192bit or 256bit) of FIPS PUB 197 (it becomes a transmission data of S/MIME). Also, the same requirement encrypts the user box file by using 3-Key-Triple-DES (encryption key: 168bit) of SP800-67. (By the same token, it becomes a transmission data of S/MIME.)

FCS-COP.1 encrypts these encryption keys are encrypted by RSA of FIPS 186-2 that is a public key of S/MIME certificate of each destination.

This security objective is satisfied by the completion of these plural function requirements.

- **O.AUTH-CAPABILITY (Support action to use user identification and authentication function)**

This security objective regulates that the user identification and authentication function is used by the user information management server that is the entity of a necessary IT environment for the security maintenance of TOE, and needs various requirements that relate to the encryption.

Applying FIT\_CAP.1[1], the inquiry and the acquirement function for the identification and authentication objective user are achieved for the user identification and authentication function by the ActiveDirectory of the user information management server.

This security objective is satisfied by the completion of this function requirement.

- **O.CRYPTO-CAPABILITY (Support action to use the encryption function)**

This security objective regulates that TOE's support action for the data stored in HDD is encrypted by the encryption kit that is the entity out of TOE, and needs various requirements that regulates the support of external entity action.

Applying FIT\_CAP.1[2], the support function to process the image file through encryption function is achieved for the encryption function of the encryption kit.

This security objective is satisfied by the completion of this function requirement.

- **O.LOCK-HDD-CAPABILITY (Support action to use the HDD lock function)**

This security objective regulates that TOE'S support action refuses the unauthorized access from MFP other than the one that is set by the HDD that is the entity out of TOE, and needs various requirements that regulates the support of external entity action.

Applying FIT\_CAP.1[3], the support function to change the HDD lock password and to release the HDD lock function for the HDD lock function achieved by the HDD.

This security objective is satisfied by the completion of this function requirement.

- **O.LOCK-CF-CAPABILITY (Support action to use the CF lock function)**

This security objective regulates that TOE'S support action refuses the unauthorized access from MFP other than the one that is set by the CF that is the entity out of TOE, and needs various requirements that regulates the support of external entity action.

Applying FIT\_CAP.1[4], the support function to change the CF lock password and to release the CF lock function for the CF lock function achieved by the CF.

This security objective is satisfied by the completion of this function requirement.

- **set.admin (Set of necessary requirement to keep administrator secure)**

<Identification and Authentication of an administrator>

FIA\_UID.2[2] and FIA\_UAU.2[2] identifies and authenticates that the accessing user is a administrator.

FIA\_UAU.7 returns "\*" for each character entered as feedback protected in the panel, and supports the authentication.

FIA\_AFL.1[8] refuses, in case of the failure authentication tried from the panel, all the input receipts from the panel for five seconds in every failure. When the failure authentication reaches 1-3 times, FIA\_AFL.1[2] logoffs if it's under authentication, and locks all the authentication functions that use the administrator password from then on. The release function is executed by starting TOE with turning OFF and ON the power supply, so that the lock is released after the administrator authentication lock time passed.

FMT\_MTD.1[3] permits only to the administrator the setting of the threshold of the authentication failure frequency which is the trial frequency of the failure authentication in the administrator authentication.

<Management of session of identified and authenticated administrator>

The duration of session of the administrator who is identified and authenticated contributes to reduce the chance of attacking associated with unnecessary session connection by ending the session after the panel automatic logoff time elapses by FTA\_SSL.3. if it logs in from the panel. The change in the panel auto logoff time is limited to the administrator by FMT\_MTD.1[3].

<Management of administrator's authentication information>

FIA\_SOS.1[1] verifies the quality of the administrator password. Moreover, FIA\_SOS.[6] verifies the quality of session information used to authenticate the administrator via the network, and FIA\_SOS.2 secures the quality of session information that is generated and used. FMT\_MTD.1[6] restricts the change in the administrator password to the administrator and the service engineer. When the administrator changes the administrator password, FIA\_UAU.6 re-authenticates it. In this re-authentication, when the failure authentication reaches 1-3 times, FIA\_AFL.1[2] logoffs it if it's under authentication, and releases the authentication status of the administrator from then on. And it locks all the authentication functions to use the administrator password. The release function is executed by starting TOE with turning OFF and ON the power supply, so that the lock is released after the administrator authentication lock time passed.

<Role and management function for each management>

FMT\_SMR.1[1] have service engineer maintain the role to do these management, and FMT\_SMR.1[2] have the administrator do the same. Additionally, FMT\_SMF.1 specifies these management functions.

➤ ***set.service* (Set of necessary requirement to keep service engineer secure)**

<Identification and Authentication of a service engineer>

FIA\_UID.2[1] and FIA\_UAU.2[1] identifies and authenticates that the accessing user is a service engineer.

FIA\_UAU.7 returns "\*" every one character entered as the feedback protected in the panel, and supports the authentication.

FIA\_AFL.1[8] refuses all the input receipts from the panel for five seconds at each failure, and when the failure authentication reaches 1-3 times, FIA\_AFL.1[1] logoffs it if it's under authentication, and locks all the authentication functions to use the CE password. The CE authentication lock release function is executed and the CE authentication lock time goes by, so that this lock status is released.

FMT\_MTD.1[3] permits only to the administrator the setting of the threshold of the authentication failure frequency that is the trial frequency of the failure authentication in the service engineer authentication. FMT\_MTD.1[9] permits only to the service engineer the setting of the CE authentication lock time.

<Management of service engineer's authentication information>

FIA\_SOS.1[1] verifies the quality of the CE password. FMT\_MTD.1[9] restricts the change in the CE password to the service engineer. Moreover, FIA\_UAU.6 re-authenticates it. In this re-authentication, when the failure authentication reaches 1-3 times, FIA\_AFL.1[1] releases the authentication status of the service engineer and locks all the authentication functions to use the CE password. The secret lock release function is executed and the CE authentication

lock time goes by, so that this lock status is released.

<Role and management function for each management>

FMT\_SMR.1[1] maintains the role to do these management as a service engineer.

FMT\_SMF.1 specifies these management functions.

### 6.2.1.3. 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 9 Dependencies of IT Security Functional Requirements Components**

N/A : Not Applicable

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4	<p>FCS_COP.1 (only partial event) &lt;The reason not to fulfill partially FCS_CKM.2 or FCS_COP.1&gt; The cryptographic operation is performed using key generated KonicaMinolta HDD cryptographic key generation algorithm in the IT environment by FIT_CAP.1[2]. TSF only uses this capability, and there is no necessity of the distribution and cryptographic operation.</p> <p>&lt;The reason not to apply FCS_CKM.4&gt; The encryption key is regularly kept for the stored data. Moreover, an arbitrary access to the storage medium is difficult, and there is no necessity of the encryption key cancellation.</p>
FCS_COP.1	FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2, FCS_CKM.4	<p>FCS_CKM.1 (only a part of the phenomenon) The satisfied events: The encryption key for enciphering the attached file by the S/MIME communication is generated. &lt;The reason not to satisfy a part of the FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2&gt; -It seems proper to use FDP_ITC.1 because the public key to encrypt the encryption key for the data encryption of S/MIME is imported outside of TSF control area, but S/MIME certificate is registered by the administrator's operation. In that case, it is unnecessary to consider whether it passes thorough the untrusted channel or not. There is not inevitability to apply the security requirement (The use under the condition that A.NETWORK is realized). -Also, the attribute information of imported encryption key doesn't apply to the security attribute used for the access control, etc., is not related to the initialization, etc., so there is no necessity to apply.</p>

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
		<p>-In FMT_MTD.1[11], it is expressed as registration of TSF data, and the object of import operation is assigned to an appropriate role.</p> <p>-As a result, the event corresponding to the key management is explained by using not the security requirement that is showed in the dependencies but other security requirement, so that it's no problem even if this dependencies is not satisfied.</p> <p>&lt;The reason not apply FCS_CKM.4&gt; The Encryption Key is stored constantly for the stored data. The arbitrary access to the storing media is difficult, so it is not necessary to cancel the Encryption Key.</p>
FDP_ACC.1[1]	FDP_ACF.1	FDP_ACF.1[1]
FDP_ACC.1[2]	FDP_ACF.1	FDP_ACF.1[2]
FDP_ACC.1[3]	FDP_ACF.1	FDP_ACF.1[3]
FDP_ACF.1[1]	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1[1], FMT_MSA.3[1], FMT_MSA.3[3]
FDP_ACF.1[2]	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1[2] FMT_MSA.3[2]
FDP_ACF.1[3]	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1[3] <The reason not to apply FMT_MSA.3> There is no necessity for applying this requirement because the object attribute doesn't exist.
FIA_AFL.1[1]	FIA_UAU.1	FIA_UAU.2[1]
FIA_AFL.1[2]	FIA_UAU.1	FIA_UAU.2[2]
FIA_AFL.1[3]	FIA_UAU.1	FIA_UAU.2[2]
FIA_AFL.1[4]	FIA_UAU.1	FIA_UAU.2[3]
FIA_AFL.1[5]	FIA_UAU.1	FIA_UAU.2[4]
FIA_AFL.1[6]	FIA_UAU.1	FIA_UAU.2[5]
FIA_AFL.1[7]	FIA_UAU.1	FIA_UAU.2[6]
FIA_AFL.1[8]	FIA_UAU.1	FIA_UAU.2[1], FIA_UAU.2[2], FIA_UAU.2[3], FIA_UAU.2[4], FIA_UAU.2[5], FIA_UAU.2[6]
FIA_ATD.1	None	N/A
FIA_SOS.1[1]	None	N/A
FIA_SOS.1[2]	None	N/A
FIA_SOS.1[3]	None	N/A
FIA_SOS.1[4]	None	N/A
FIA_SOS.1[5]	None	N/A
FIA_SOS.1[6]	None	N/A
FIA_SOS.2	None	N/A
FIA_UAU.2[1]	FIA_UID.1	FIA_UID.2[1]
FIA_UAU.2[2]	FIA_UID.1	FIA_UID.2[2]
FIA_UAU.2[3]	FIA_UID.1	FIA_UID.2[3]
FIA_UAU.2[4]	FIA_UID.1	FIA_UID.2[4]
FIA_UAU.2[5]	FIA_UID.1	FIA_UID.2[5]
FIA_UAU.2[6]	FIA_UID.1	FIA_UID.2[6]
FIA_UAU.6	None	N/A
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2[1], FIA_UAU.2[2], FIA_UAU.2[3], FIA_UAU.2[4], FIA_UAU.2[5], FIA_UAU.2[6]
FIA_UID.2[1]	None	N/A

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
FIA_UID.2[2]	None	N/A
FIA_UID.2[3]	None	N/A
FIA_UID.2[4]	None	N/A
FIA_UID.2[5]	None	N/A
FIA_UID.2[6]	None	N/A
FIA_UID.2[7]	None	N/A
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1[1]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[1], FMT_SMR.1[2]
FMT_MOF.1[2]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[2]
FMT_MOF.1[3]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[2]
FMT_MSA.1[1]	FDP_ACC.1 or FDP_IFC.1, FMT_SMF.1, FMT_SMR.1	FDP_ACC.1[1], FMT_SMF.1, FMT_SMR.1[2], FMT_SMR.1[3]
FMT_MSA.1[2]	FDP_ACC.1 or FDP_IFC.1, FMT_SMF.1, FMT_SMR.1	FDP_ACC.1[1], FMT_SMF.1, FMT_SMR.1[2], FMT_SMR.1[4]
FMT_MSA.1[3]	FDP_ACC.1 or FDP_IFC.1, FMT_SMF.1, FMT_SMR.1	FDP_ACC.1[1], FMT_SMF.1, FMT_SMR.1[2], FMT_SMR.1[6]
FMT_MSA.3[1]	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1[1], FMT_MSA.1[2], FMT_SMR.1[3]
FMT_MSA.3[2]	FMT_MSA.1, FMT_SMR.1	Neither is applicable.  <The reason not to apply FMT_MSA.1> This is the internal control ID that is identified uniquely, and this does not require the management such as change or deletion, after this is assigned once. <FMT_SMR.1> The assignment of FMT_MSA.3.2[2] is not applicable. FMT_SMR.1 is the dependency that is set relating to the following and so there is no necessity of application.
FMT_MSA.3[3]	FMT_MSA.1, FMT_SMR.1	Neither is applicable.  <The reason not to apply FMT_MSA.1> The user box attribute of a user box file always needs to correspond with the user box. Therefore, the value only has to be given at the time of storage. It is not necessary to change the value of this attribute at the time of other operational timing. Accordingly, the management requirement is unnecessary. <FMT_SMR.1> The assignment of FMT_MSA.3.2[3] is not applicable. FMT_SMR.1 is the dependency that is set relating to the following and so there is no necessity of application.

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
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[2] , FMT_SMR.1[3]
FMT_MTD.1[3]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[2]
FMT_MTD.1[4]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[2], FMT_SMR.1[4]
FMT_MTD.1[5]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[2], FMT_SMR.1[3]
FMT_MTD.1[6]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[1], FMT_SMR.1[2]
FMT_MTD.1[7]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[2]
FMT_MTD.1[8]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[3]
FMT_MTD.1[9]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]
FMT_MTD.1[10]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2], FMT_SMR.1[5]
FMT_MTD.1[11]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]
FMT_MTD.1[12]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2] FMT_SMR.1[6]
FMT_SMF.1	None	N/A
FMT_SMR.1[1]	FIA_UID.1	FIA_UID.2[1]
FMT_SMR.1[2]	FIA_UID.1	FIA_UID.2[2]
FMT_SMR.1[3]	FIA_UID.1	FIA_UID.2[3]
FMT_SMR.1[4]	FIA_UID.1	FIA_UID.2[5]
FMT_SMR.1[5]	FIA_UID.1	FIA_UID.2[7]
FMT_SMR.1[6]	FIA_UID.1	FIA_UID.2[6]
FTA_SSL.3	None	N/A
FTP_ITC.1	None	N/A
FNEW_RIP.1	None	N/A
FIA_EID.1[1]	None	N/A
FIA_EID.1[2]	None	N/A
FIT_CAP.1[1]	None	N/A
FIT_CAP.1[2]	None	N/A
FIT_CAP.1[3]	None	N/A
FIT_CAP.1[4]	None	N/A

### 6.2.2. 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 must 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.

The secure requirement dependency analysis is assumed to be appropriate because the package EAL has been selected, therefore details are not discussed.

## 7. TOE Summary Specification

The list of the TOE security function led from the TOE security function requirement is shown in the following Table 10. The detailed specification is explained in the paragraphs described below.

**Table 10 The list of the name and identifier of TOE Security function**

No.	TOE Security Function	
1	F.ADMIN	Administrator function
2	F.ADMIN-SNMP	SNMP administrator function
3	F.SERVICE	Service mode function
4	F.USER	User function
5	F.BOX	User box function
6	F.PRINT	Secure print function
7	F.OVERWRITE-ALL	All area overwrite deletion function
8	F.CRYPT	Encryption key generation function
9	F.VALIDATION-HDD	HDD validation function
10	F.VALIDATION-CF	CF validation function
11	F.RESET	Authentication Failure Reset function
12	F.TRUSTED-PASS	Trusted Channel function
13	F.S/MIME	S/MIME encryption processing function
14	F.SUPPORT-AUTH	External Server authentication operation support function
15	F.SUPPORT-CRYPTO	Cryption kit operation support function
16	F.SUPPORT-HDD	HDD lock operation support function
17	F.SUPPORT-CF	CF lock operation support function

### 7.1. F.ADMIN (Administrator Function)

F.ADMIN is a series of security function that administrator operates, such as an administrator identification authentication function in an administrator mode accessing from a panel or through a network, and a security management function that includes a change of an administrator password and a lock cancellation of a locked user box. (Nevertheless, all functions are not feasible functions through both a panel and a network.)

#### 7.1.1. Administrator identification authentication function

It identifies and authenticates the accessing user as the administrator in response to the access request to the administrator mode.

- Offers the administrator authentication mechanism authenticating by the administrator password that consists of the character shown in Table 11.
  - Offers the administrator authentication mechanism using the session information besides the administrator password, after the administrator is authenticated to the access from the network,
  - According to protocol, use the session information of more than  $10^{10}$ , or generate and use the session information more than  $10^{10}$ .
- Return "\*" for each character as feedback for the entered administrator password.

- Resets the number of authentication failure when succeeding in the authentication.
  - In the case of access from a panel, it doesn't accept the input from a panel for five seconds when failing in the authentication.
  - Locks all the authentication functions to use the administrator password when detecting the authentication failure that becomes 1~3 times at total in each authentication function by using the administrator password. (Refuse the access to the administrator mode)
    - The administrator specifies the failure frequency threshold by the unauthorized access detected threshold setting function.
  - F.RESET works and the lock release function of the administrator authentication function in F.SERVICE is carried out, and the lock of authentication function is released.
- As described above, FIA\_AFL.1[2], FIA\_AFL.1[8], FIA\_SOS.1[6], FIA\_SOS.2, FIA\_UAU.2[2], FIA\_UAU.7 and FIA\_UID.2[2] are realized.

**Table 11 character and number of digits used for password <sup>12</sup>**

Objectives	Number of digits	Characters
CE Password	8-digits	92 characters in total can be selected ASCII code (0x21 - 0x7E, except 0x22 and 0x2B) -Number : 0 - 9 -Alphabet : Capital letter and small letter -Symbols : !, #, \$, %, &, ', (, ), *, , , - , . , / , : , ; , < , = , > , ? , @ , [ , ¥ , ] , ^ , _ , ` , { ,   , } , ~
Administrator Password		
HDD Lock Password	20-digits	83 characters in total can be selected ASCII code (0x21-0x7E, except 0x22, 0x28, 0x29, 0x2C, 0x3A, 0x3B, 0x3E, 0x3F, 0x5B, 0x5C and 0x5D) - Number : 0 - 9 - Alphabets : Capital letter and small letter - Symbols : !, #, \$, %, &, ', * , + , - , . , / , < , = , @ , ^ , _ , ` , { ,   , } , ~
CF Lock Password	20-digits	84 characters in total can be selected ASCII code (0x21-0x7E, except 0x22, 0x28, 0x29, 0x2C, 0x3A, 0x3B, 0x3E, 0x3F, 0x5B, 0x5C and 0x5D) -Number : 0 - 9 - Alphabets : Capital letter and small letter - Symbols : !, #, \$, %, &, ', * , + , - , . , / , < , = , @ , ^ , _ , ` , { ,   , } , ~
Encryption passphrase		
User Password	8-digits or more	95 character in total can be selected ASCII code (0x21-0x7E) -Number : 0 - 9 -Alphabets : Capital letter and small letter -Symbols : !, #, \$, %, &, ', (, ), * , , , - , . , / , : , ; , < , = , > , ? , @ , [ , ¥ , ] , ^ , _ , ` , { ,   , } , ~ , " , + , SPACE
Account Password	8-digits	
Security Print Password		
User Box Password		

<sup>12</sup> Table 11 shows the minimum password space as the security specification. Therefore the excluded characters are permitted to use if possible, and some excluded characters according to each password are shown.

Objectives	Number of digits	Characters
SNMP Password -Privacy Password -Authentication Password	8-digits or more	93 characters in total can be selected ASCII code (0x20 - 0x7E, except 0x5C) -Number : 0 - 9 -Alphabets : Capital letter and small letter -Symbols : ! , # , \$ , % , & , ' , ( , ) , * , , , - , . , / , : , ; , < , = , > , ? , @ , [ , ] , ^ , _ , ` , { ,   , } , ~ , " , +

### 7.1.2. Auto logoff function of administrator mode

While accessing an administrator mode from a panel, if not accepting any operation during the panel automatic logoff time, it logs off the administrator mode automatically.

As described above, FIA\_SSL.3 is realized.

### 7.1.3. Function offered in Administrator mode

When a user is identified and authenticated as an administrator by the administrator identification authentication function at the accessing request to the administrator mode, the administrator authority is associated with the task substituting the user. And the following operations and the use of the functions are permitted.

As described above, FIA\_ATD.1 and FIA\_USB.1 are realized.

#### 7.1.3.1. Change of Administrator password

When a user is re-authenticated as an administrator by the panel and the new password satisfies the quality, the password is changed.

- Offers the administrator authentication mechanism that is authenticated by the administrator password which consists of the character shown in Table 11.
- Resets the number of authentication failure when succeeding in the re-authentication.
- Return "\*" for each character as feedback for the entered administrator password in the re-authentication by the access from the panel.
- When the authentication failure that becomes 1-3 times at total in each authentication function by using the administrator password is detected, it logoffs the administrator mode accessing from the panel, and locks all the authentication functions to use the administrator password. (The access to the administrator mode is refused.)
  - The administrator specifies the failure frequency threshold by the unauthorized access detection threshold setting function.
- F.RESET works or the lock release function of the administrator authentication function in F.SERVICE is carried out, so that the lock of the authentication function is released.
- Verify the new administrator password if the following qualities are satisfied.
  - It is composed of the characters and by the number of digits, shown in the Table 11.
  - It shall not be composed of one kind of character.
  - It doesn't match with the current value.

As described above, FIA\_AFL.1[2], FIA\_SOS.1[1], FIA\_UAU.6, FIA\_UAU.7, FMT\_MTD.1[6], FMT\_SMF.1 and FMT\_SMR.1[2] are realized.

### 7.1.3.2. User Settings

- User Registration (Only the user who uses with the machine authentication as User authentication method.)

User is registered by setting the user ID (Though user ID is composed of the user name and the authentication server information<sup>13</sup>, only user name is registered in case of the machine authentication.) and registering the user password. It verifies whether the user password newly set have been satisfied the following qualities.

- It is composed of the characters and by the number of digits, shown in the Table 11.
- It shall not be composed of one kind of character.

While the external server authentication is effective, the user password cannot be registered. Also register the belonging account (account ID), and relate. (The account setting is necessary beforehand.)

- Change of user password (Only the user who uses with the machine authentication as User authentication method.)

User password is changed. It verifies whether the user password newly set have been satisfied the following qualities.

- It is composed of the characters and by the number of digits, shown in the Table 11.
- It shall not be composed of one kind of character.

- User deletion

User ID and user password is deleted.

- When a personal user box that a concerned user owns exists, that personal user box is automatically set to the public user box of "user attributes: public."

- Change of the belonging account

The belonging account that related to user is changed

As described above, FIA\_SOS.1[3], FMT\_MTD.1[1], FMT\_MTD.1[2], FMT\_MTD.1[3], FMT\_MTD.1[10], FMT\_MTD.1[12], FMT\_SMF.1 and FMT\_SMR.1[2] are realized.

### 7.1.3.3. User Box Settings

- User Box Registration

When the administrator attribute is related, the view of the list of user boxes is permitted. To register a personal user box or a public user box by selecting the user attribute to the non-registration user box ID selected from the list of user boxes. When it's registered, it is possible to select "User ID" in the user attribute of the user box which have been specified "Public" as a default value.

- In the case of the personal user box, the arbitrary user ID registered is specified.
- In the case of the public user box, verify that a user box password registered satisfies the following conditions.

---

<sup>13</sup> It associates with the external server authentication setting data that is set in the case of the use of the external server (only Active Directly method is applicable) as the method of the user authentication function. Because it deals when there are plural user information management servers, there is the case which plural authentication server information are included in the external server information setting data.

- It is composed of the characters and by the number of digits, shown in the Table 11.
- It shall not be composed of one kind of character.
- Specify the arbitrary account ID registered when Group user box.
  
- Change of User Box Password
  - The user box password set to the public user box is changed.
  - It verifies whether the user box password newly set have been satisfied the following qualities.
    - It is composed of the characters and by the number of digits, shown in the Table 11.
    - It shall not be composed of one kind of character.
  
- Change of user attribute of user box
  - Specify the user attribute of a personal user box to the other user or the account that registered.
  - Specify the user attribute of group user box to the user or the other account that registered.
  - Specify the user attribute of public user box to the user or account that registered.
  - Specify the user attribute of a personal user box or group user box to public.
    - The registration of a user box password is necessary at the same time, and then the processing which is similar to a change of the above-mentioned user box password should be done.

As described above, FDP\_ACC.1[1], FDP\_ACF.1[1], FIA\_SOS.1[5], FMT\_MSA.1[1] , FMT\_MSA.1[2] , FMT\_MSA.1[3] , FMT\_MSA.3[1], FMT\_MTD.1[4], FMT\_MTD.1[5], FMT\_SMF.1 and FMT\_SMR.1[2] are realized.

#### 7.1.3.4. Release of Lock

Reset (0 clear) the number of authentication failure for each users.

- If there is a user to whom access is locked, the lock is released.  
Reset (0 clear) the number of authentication failure for all secure prints.
- If there is a secure print to which access is locked, the lock is released.  
Reset (0 clear) the number of authentication failure of each user boxes.
- If there is a user box to which access is locked, the lock is released.  
Reset (0 clear) the number of authentication failure of each account.
- If there is a user account to which access is locked, the lock is released.  
Reset (0 clear) the number of authentication failure of SNMP password.
- If there is a MIB object to which access is locked, the lock is released.

As described above, FIA\_AFL.1[3], FIA\_AFL.1[4], FIA\_AFL.1[5], FIA\_AFL.1[6] and FIA\_AFL.1[7] are realized.

#### 7.1.3.5. Setting of user authentication function

Set the following authentication method in a user authentication function.

- Machine authentication: Authentication method which utilizes a user password managed on MFP sides.
- External server authentication : Authentication method which utilizes a user password

managed with a user information management server connected through a network.(Only Active Directory method is object)

- When external server authentication is used, the external server authentication setting data(Contain the multiple authentication server information, such as domain name to which external server belongs) needs to be set.

Set the following authentication method in the account authentication function used with a user authentication function.

- Account authentication function : synchronized method  
The method which utilizes an account ID related to user ID beforehand.
- Account authentication function : method not synchronized  
The method to authenticate by the account ID and the account password at the time of access, without utilizing the account ID that related to user ID beforehand.
- Account authentication function : not use  
Utilize only the authentication function by user ID, and not utilize the authentication by account information.

As described above, FMT\_MOF.1[3], FMT\_MTD.1[3], FMT\_MOF.1[2], FMT\_SMF.1 and FMT\_SMR.1[2] are realized.

#### 7.1.3.6. Unauthorized access setting

- Setting of unauthorized access detection threshold  
The unauthorized access detection threshold in the authentication operation prohibition function is set for 1-3 times.
- Setting of Administrator Authentication Lock Time  
Set the Administrator Authentication Lock Time between 5-60 minutes.  
As described above, FMT\_MTD.1[3], FMT\_SMF.1 and FMT\_SMR.1[2] are realized.

#### 7.1.3.7. Setting of auto logoff function

The panel auto logoff time which is the setting data of the auto logoff function should be set within the following time range.

- panel auto logoff time : 1 - 9 minutes  
As described above, FMT\_MTD.1[3], FMT\_SMF.1 and FMT\_SMR.1[2] are realized.

#### 7.1.3.8. Network Settings

A setup operation of the following setting data is performed.

- A series of setup data that relates to SMTP server (IP address, Port Number, etc.)
- A series of setup data that relates to DNS server (IP address, Port Number, etc.)
- A series of setup data that relates to MFP address (IP address, NetBIOS Name, AppleTalk Printer Name, etc.)

As described above, FDP\_ACC.1[3] and FDP\_ACF.1[3] are realized.

### 7.1.3.9. Execution of back-up and restoration function

All the setting data stored in NVRAM, CF and HDD is backed-up and re-stored except the administrator password, the CE password, CF lock password, HDD lock password and Encryption passphrase. As the object related to security, due to the relation of confidentiality and completeness, the one shown by the following classifications is targeted.

<Type A : Object to which back-up and restoration should be limited>

- SNMP password
- User password
- Account password
- Secure print password
- User Box password
- Encryption passphrase

<Type B : Object to which restoration should be limited>

- A series of data that relates to SMTP server setting
- A series of data that relates to DNS server setting
- A series of data that relates to MFP address setting
- Operation setting data of SNMP password authentication function
- Setting data of Enhanced Security function
- Setting data of operation method of user authentication function
- Operation setting data of account authentication function
- Authentication failure frequency threshold of authentication operation prohibition function
- Panel auto logoff time
- User ID
- User attribute of user box
- User box ID
- S/MIME certificate
- Transmission address data
- Encryption strength setting data in S/MIME function
- Trusted Channel function setting data
- Belonging Account of user
- Administrator authentication lock time
- PC-FAX operation setting
- TSI receiving setting data
- External server authentication setting data

<Type C : Object to which back-up should be limited>

- Secure print file
- User box file

As described above, FDP\_ACC.1[1], FDP\_ACC.1[2], FDP\_ACC.1[3], FDP\_ACF.1[1], FDP\_ACF.1[2], FDP\_ACF.1[3], FMT\_MOF.1[1], FMT\_MOF.1[2], FMT\_MOF.1[3], FMT\_MSA.1[1], FMT\_MSA.1[2], FMT\_MSA.1[3], FMT\_MTD.1[2], FMT\_MTD.1[3], FMT\_MTD.1[4], FMT\_MTD.1[7], FMT\_SMF.1 and FMT\_SMR.1[2] are realized.

### 7.1.3.10. Operation setting function of HDD lock function

#### <Modification of HDD lock password>

Change the HDD lock password. By using the HDD lock password currently set, when it is re-authenticated as an administrator, and the new password satisfies the quality, it is changed.

- Offers the HDD lock password verification mechanism that verified the HDD lock password that consists of the character shown in Table 11.
- Return, in verification, "\*" for each character as feedback for the entered HDD lock password.
- Verify the HDD lock password newly set if the following qualities are satisfied.
  - It is composed of the characters and by the number of digits shown in Table 11.
  - It shall not be composed of one kind of character.
  - It shall not be matched with the current value.

As described above, FIA\_SOS.1[4], FIA\_UAU.7, FIA\_UAU.6, FMT\_MTD.1[3], FMT\_SMF.1 and FMT\_SMR.1[2] are realized.

### 7.1.3.11. Operation setting function of CF lock function

#### <Modification of CF lock password>

Change the CF lock password. By using the CF lock password currently set, when it is re-authenticated as an administrator, and the new password satisfies the quality, it is changed.

- Offers the CF lock password verification mechanism that verified the CF lock password that consists of the character shown in Table 11.
- Return, in verification, "\*" for each character as feedback for the entered CF lock password.
- Verify the CF lock password newly set if the following qualities are satisfied.
  - It is composed of the characters and by the number of digits shown in Table 11.
  - It shall not be composed of one kind of character.
  - It shall not be matched with the current value.

As described above, FIA\_SOS.1[4], FIA\_UAU.7, FIA\_UAU.6, FMT\_MTD.1[3], FMT\_SMF.1 and FMT\_SMR.1[2] are realized.

### 7.1.3.12. Operation setting of encryption function

(\* When an optional encryption board is installed to MFP, it can be operated.)

#### <Operation Setting ON>

When turning it ON from OFF, it verifies that the encryption passphrase newly set satisfies the following qualities, and F.CRYPT is performed.

- It is composed of the characters and by the number of digits shown in Table 11.
- It shall not be composed of one kind of character.

As described above, FIA\_SOS.1[4], FMT\_MTD.1[11], FMT\_SMF.1 and FMT\_SMR.1[2] are realized.

#### <Encryption Passphrase Change, Operation Setting OFF>

Change the encryption passphrase and operation setting OFF. It is permitted when using the encryption passphrase currently set and when it is re-authenticated as an administrator. To change the encryption passphrase, by using the encryption passphrase currently set, when it is re-authenticated as an administrator, and the new encryption passphrase satisfies the quality,

F.CRYPT is performed.

- In case of re-authentication, it offers the encryption passphrase verification mechanism that verified the encryption passphrase that consists of the character shown in Table 11.
- Return, in verification, "\*" for each character as feedback for the entered encryption passphrase.
- Verify the encryption passphrase newly set if the following qualities are satisfied.
  - It is composed of the characters and by the number of digits shown in Table 11.
  - It shall not be composed of one kind of character.
  - It shall not be matched with the current value.

As described above, FIA\_SOS.1[4], FIA\_UAU.7, FIA\_UAU.6, FMT\_MTD.1[3], FMT\_SMF.1 and FMT\_SMR.1[2] are realized.

#### 7.1.3.13. Change of SNMP password

The SNMP password (Privacy password and Authentication password) is changed. Verify that the SNMP password newly set satisfies the following qualities.

- It is composed of the characters and by the number of digits shown in Table 11.

As described above, FIA\_SOS.1[2], FMT\_MTD.1[3], FMT\_SMF.1 and FMT\_SMR.1[2] are realized.

#### 7.1.3.14. Setting of SNMP password authentication function

The authentication method in the SNMP password authentication function is set to "Only Authentication password" or the "Authentication password and Privacy password".

As described above, FMT\_MOF.1[2], FMT\_SMF.1 and FMT\_SMR.1[2] are realized.

#### 7.1.3.15. Account Settings

- Account registration
  - Account is registered by setting the account ID and registering the account password. It verifies whether the account password newly set have been satisfied the following qualities.
  - It is composed of the characters and by the number of digits, shown in Table 11.
  - It shall not be composed of one kind of character.
- Change of account ID and account password
  - Account ID and account password is changed. It verifies whether the account password newly set have been satisfied the following qualities.
  - It is composed of the characters and by the number of digits, shown in Table 11.
  - It shall not be composed of one kind of character.
- Account deletion
  - Account ID and account password are deleted.
  - When the Group box of the account ID exists, that group user box is automatically set to the public user box of "user attributes: public."

As described above, FIA\_SOS.1[5], FMT\_MSA.1[3], FMT\_MTD.1[3], FMT\_MTD.1[11], FMT\_SMF.1 and FMT\_SMR.1[2] are realized.

#### 7.1.3.16. Setting of Trusted Channel function

Set the setting data of Trusted Channel function by SSL/TLS

- Communication Encryption Strength Setting (Modification of the communication encryption method.)
- Operation and Stop Setting of the Trusted Channel function

As described above, FMT\_MOF.1[3], FMT\_SMF.1 and FMT\_SMR.1[2] are realized.

#### 7.1.3.17. Setting of S/MIME transmission function

Set the setting data which are used when the user box file is S/MIME transmitted.

- Transmission address data (e-mail address)
- Registration and modification of S/MIME certificate
- Setting of Encryption Strength for S/MIME function

As described above, FMT\_MOF.1[2], FMT\_MTD.1[3], FMT\_MTD.1[11], FMT\_SMF.1 and FMT\_SMR.1[2] are realized.

#### 7.1.3.18. Setting of PC-FAX

Set the setting data of FAX related settings as follows,

- PC-FAX operation Setting
  - Setting either of two modes at PC-FAX operation which are to store in each box and to store in common area for all users according to the designated information at FAX transmission.
- TSI receiving Setting
  - Setting the storing box at TSI receiving relating the transmitter's telephone number with the box as the identification information of transmitter's terminal.

As described above, FDP\_ACC.1[3], FDP\_ACP.1[3], FMT\_MTD.1[3], FMT\_SMF.1 and FMT\_SMR.1[2] are realized.

#### 7.1.3.19. Function related to Enhanced Security function

The function that influences the setting of the Enhanced Security function that the administrator operates is as follows. (\* It has explained the influence of the backup and restoration function in 7.1.3.9.)

- Operation setting of Enhanced Security function  
Function to set valid or invalid of Enhanced Security function.
- HDD logical format function  
Function to write the default value of management data using the file system of HDD. Along with the execution of this logical format, the setting of the Enhanced Security function is invalidated.
- All area overwrite deletion function  
The settings of enhanced security function are invalidated by executing the overwrite deletion of all area

As described above, FMT\_MOF.1[1], FMT\_SMF.1 and FMT\_SMR.1[2] are realized.

### 7.1.3.20. Function that relates to password initialization function

The function that relates to the initialization of the password that the administrator operates is as follows.

- All area overwrite deletion function

The settings of the administrator password and the SNMP password are initialized to the values at factory shipment by executing the overwrite deletion of all area

As described above, FMT\_MTD.1[3] , FMT\_MTD.1[6], FMT\_SMF.1 and FMT\_SMR.1[2] are realized.

## 7.2. F.ADMIN-SNMP (SNMP administrator function)

F.ADMIN-SNMP is a security function, which identifies and authenticates the administrator in the access through the network by using SNMP from client PC, and then permits the operation of a setting function of the network only to the administrator whose identification and authentication was succeeded.

### 7.2.1. Identification and authentication function by SNMP password

It identifies and authenticates by the SNMP password, that the user who accesses the MIB object through the network with the use of SNMP is an administrator

- Offers the SNMP authentication mechanism which authenticates by the SNMP password that consists of the character shown in Table 11.
  - Only Authentication password or both the Privacy password and the Authentication password is used.
  - In the case of SNMP, the SNMP password is used for every session without requiring the administrator authentication mechanism by the separate session information.
- Reset the authentication failure frequency if it succeeds in authentication.
  - In the case of both the Privacy password and the Authentication password are used, the authentication failure frequency is reset only when both passwords together succeeded in the authentication.
- When the authentication failure that becomes the 1-3 times at total in each authentication function by using the SNMP password is detected, all the authentication functions to use the SNMP password are locked. (The access to the MIB object is refused.)
  - The administrator specifies the failure frequency threshold by the unauthorized access detection threshold setting function.
  - In the case of both the Privacy password and the Authentication password are utilized, even though both passwords together fails in authentication, it is detected as one failure.
- To release the lock, the lock release function to the MIB object of F.ADMIN is performed or the F.RESET function operates.
- The lock status is released when the lock release function to the MIB object of F. ADMIN is performed.

As described above, FIA\_AFL.1[3] , FIA\_UAU.2[2] and FIA\_UID.2[2] are realized.

### 7.2.2. Management function using SNMP

When it is identified and authenticated that the user is an administrator by the SNMP password, the access to the MIB object is permitted, and then the operation of the setting data shown as followings is permitted to be done.

(1) Network Settings

Setting operation of the following setting data is performed.

- Setting data that relates to SMTP server (IP address, port number, etc.)
- Setting data that relates to DNS server (IP address, port number, etc.)
- A series of setting data that relates to MFP address (IP address, NetBIOS name, AppleTalk printer name, etc.)

As described above, FDP\_ACC.1[3] and FDP\_ACF.1[3] are realized

(2) Change of SNMP password

The SNMP password (Privacy password and Authentication password) is changed. Verify that the SNMP password newly set satisfies the following qualities.

- It is composed of the characters and by the number of digits shown in Table 11.

As described above, FIA\_SOS.1[2], FMT\_MTD.1[3] , FMT\_SMF.1 and FMT\_SMR.1[2] are realized.

(3) Setting of SNMP password authentication function

The authentication method in the SNMP password authentication function is set to the "Authentication password only" or the "Privacy password and the Authentication password".

As described above, FMT\_MOF.1[2] , FMT\_SMF.1 and FMT\_SMR.1[2] are realized.

### 7.3. F.SERVICE (Service mode function)

F.SERVICE is a series of security function that the service engineer operates, such as the service engineer identification authentication function in service mode accessing from a panel, and a security management function that includes a change in the CE password and the administrator password.

#### 7.3.1. Service engineer identification authentication function

It is identified and authenticated the accessing user as the service engineer in response to the access request to the service mode from the panel.

- Offers the CE authentication mechanism that is authenticated by the CE password that consists of the character shown in Table 11.
  - The CE authentication mechanism by the separate session information is not required because the service mode can only be accessed from the panel.
- Return "\*" for each character as feedback for the entered CE password.
- Resets the number of the authentication failure when succeeding in the authentication.
- Not accept the input from the panel for five seconds when the authentication failed.
- When the authentication failure that becomes 1-3 times at total in each authentication function by using the CE password is detected, it locks all the authentication functions to use

the CE password. (The access to the service mode is refused.)

- The administrator specifies the failure frequency threshold by the unauthorized access detection threshold setting function.
- Lock of authentication function is released with F.RESET function operated.  
As described above, FIA\_AFL.1[1], FIA\_AFL.1[8], FIA\_UAU.2[1], FIA\_UAU.7 and FIA\_UID.2[1] are realized.

### 7.3.2. Function offered in service mode

When a user is identified and authenticated as a service engineer by the service engineer identification authentication function at the access request to the service mode, the use of the following functions is permitted.

#### (1) Change of CE password

When a user is re-authenticated as a service engineer and the new password satisfies the quality, it is changed.

- Offers the CE authentication mechanism that is re-authenticated by the CE password that consists of the characters shown in Table 11.
- Resets the number of authentication failure when succeeding in the re-authentication.
- Return "\*" for each character as feedback for the entered service codes in the re-authentication.
- When the authentication failure that becomes 1-3 times at total in each authentication function by using the CE password is detected, it logoffs the service mode accessing from the panel, and locks all the authentication functions to use the CE password. (The access to the service mode is refused.)
  - The administrator specifies the failure frequency threshold by the unauthorized access detection threshold setting function.
- The F.RESET function operates to release the lock of the authentication function.
- It verifies that the CE password newly set satisfies the following qualities.
  - It is composed of the characters and by the number of digits, shown in the Table 11.
  - It shall not be composed of one kind of character.
  - It shall not be matched with the current value.

As described above, FIA\_AFL.1[1], FIA\_SOS.1[1], FIA\_UAU.6, FIA\_UAU.7, FMT\_MTD.1[9], FMT\_SMF.1 and FMT\_SMR.1[1] are realized.

#### (2) Change of administrator password

Change the administrator password. Verify that the administrator password newly set satisfies the following qualities.

- It is composed of the characters and by the number of digits, shown in the Table 11.
- It shall not be composed of one kind of character.
- It shall not be matched with the current value.

As described above, FIA\_SOS.1[1], FMT\_MTD.1[6], FMT\_SMF.1 and FMT\_SMR.1[1] are realized.

#### (3) Release of the lock of administrator authentication function

Reset (0 clear) the number of authentication failure for the administrator authentication.

- If access is locked, the lock is released.

As described above, FIA\_AFL.1[2] is realized.

(4) Setting of CE Authentication Lock Time

Set the CE Authentication Lock Time between 1 - 60 minutes.

As described above, FMT\_MTD.1[9], FMT\_SMF.1 and FMT\_SMR.1[1] are realized.

(5) Function that relates the operation setting of maintenance function

Set the operation of the maintenance function. (Available to change from the halt condition to startup condition)

As described above, FMT\_MOF.1[4], FMT\_SMF.1 and FMT\_SMR.1[1] are realized.

(6) Function that relates to Enhanced Security function

The functions that influence the setting of the Enhanced Security function that the service engineer operates are as follows.

- HDD logical format function

Function to write the value of management data using the file system of HDD. The setting of the Enhanced Security function is invalidated along with the execution of this logical format.

- HDD physical format function

A function to rewrite the entire disk in HDD with a regulated pattern including the signal rows such as the track and sector information. The setting of the Enhanced Security function is invalidated along with the execution of this physical format.

- Initialization function

Function to reset every setting value written in NVRAM to the factory default. The setting of the Enhanced Security function is invalidated by executing this initialization function.

As described above, FMT\_MOF.1[1], FMT\_SMF.1 and FMT\_SMR.1[1] are realized.

## 7.4. F.USER (User Function)

F.USER identifies and authenticates the user for the use of MFP various function. To the identified and authenticated user, it offers the management function of the user password that is managed in the MFP at the time of machine authentication, besides the permission of the use of functions such as F.BOX and F.PRINT.

### 7.4.1. User Identification and Authentication Function

<Account Authentication : User identification and authentication in the synchronized method>

When the access request for the user box and the request for the registration of the secure print file, it is identified and authenticated to be a user. Account Name (account ID) is associated with the concerned user ID that is set up beforehand besides the user ID for the identified and authenticated user, and the use of F.BOX and F.PRINT is permitted to the identified and authenticated user.

- Offers the user authentication mechanism that authenticates the user that consists of the characters shown in Table 11.

- After the user is authenticated to the access from the network, the user authentication mechanism using session information besides the user password is offered.
- According to the protocol, it uses the session information more than  $10^{10}$  or it generates and uses the session information more than  $10^{10}$ .
- Return "\*" for each character as feedback for the entered user password.
- Resets the number of authentication failure when succeeding in the authentication.
- Not accept the access from the panel for five seconds when the authentication failed.
- When the authentication failure that becomes 1-3 times at total for the concerned user is detected, it locks all the authentication functions to the user.
  - The administrator specifies the failure frequency threshold by the unauthorized access detection threshold setting function.
- To release the lock of the authentication function is to perform the lock release function to the user authentication of F.ADMIN.  
As described above, FIA\_AFL.1[4], FIA\_AFL.1[8], FIA\_UAU.2[3], FIA\_UAU.7 and FIA\_UID.2[3] are realized.

<Account Authentication : Account registration function when the belonging account of user is not registered in the synchronized method>

- Require the Account authentication after User identification and authentication.
- Register the successful account ID as account name when succeeding in the account authentication. (By this, FMT\_MTD.1[12], FMT\_SMS.1 and FMT\_SMR.1[6] are realized.)  
(The detail of the account authentication is the same as processing of the items explained in the following <Account authentication: User identification and authentication in the authentication method not synchronized>)

<Account Authentication :User identification and authentication in the authentication method not synchronized>

When the access request for the user box and the request for the registration of the secure print file, it is identified and authenticated to be a user. The detail of user authentication is the same as account authentication: user identification and authentication in the synchronized method. In the case of the access from the panel, the account authentication is required, Account Name is associated with the user ID if succeeding the account authentication, and the use of F.BOX and F.PRINT is permitted to the user who is identified and authenticated.

- Offers account authentication mechanism that is authenticated the account by the account password that consists of the characters shown in Table 11.
- Return "\*" for each character as feedback for the entered account password.
- Resets the number of authentication failure when succeeding in the authentication.
- Not accept the access from the panel for five seconds when the authentication failed.
- When the authentication failure that becomes 1-3 times at total for the concerned account is detected, it locks all the authentication functions to the account.
  - The administrator specifies the failure frequency threshold by the unauthorized access detection threshold setting function.
- The lock of the authentication function is to perform the lock release function to the concerned account of F.ADMIN.

As described above, FIA\_AFL.1[7], FIA\_AFL.1[8], FIA\_UAU.2[6], FIA\_UAU.7 and FIA\_UID.2[6] are realized.

When accessing from a network, the account is not authenticated after the user authentication but the user and the account are processed with one sequence. When authenticating the account, the account ID is associated with the user ID, and the user ID and the account ID are measured by the session information which is the same as user identification and authentication in the account authentication: the synchronized method.

As described above, FIA\_ATD.1, FIA\_SOS.1[6], FIA\_SOS.2 and FIA\_USB.1 are realized.

#### <Automatic registration of the User ID>

In the case of the "External server authentication" has been selected as the user authentic method, the identified and authenticated user is registered as an user ID with the user name and authentication server information that was used with identification and authentication.

As described above, FIA\_UID.2[7], FMT\_MTD.1[10], FMT\_SMF.1 and FMT\_SMR.1[5] are realized.

### 7.4.2. Auto logoff function in user identification and authentication domain

While the user who is identified and authenticated is accessing from a panel, if it does not accept any operations for more than the "panel automatic logoff time", it logs off from a user identification and authentication domain automatically.

As described above, FTA\_SSL.3 is realized.

### 7.4.3. Modification function of user password

When the identification and authentication are succeeded, and the access to the user identification and authentication domain is permitted, the user is permitted to change its own password. When the external server authentication is effective, this function cannot be applied.

When the user password newly set satisfies the following qualities, it is changed.

- It is composed of the characters and by the number of digits, shown in the Table 11.
- It shall not be composed of one kind of character.

As described above, FIA\_SOS.1[3], FMT\_MTD.1[2], FMT\_SMF.1 and FMT\_SMR.1[3] are realized.

## 7.5. F.BOX (User Box Function)

F.BOX is a series of security function related to the user box to the user who is identified and authenticated that you are the registered user, such as the permission of the operation and management of the personal user box of the user, the authentication to the user who is permitted the utilization of the user box in the access to the public box, and the access control function to permit various operations of the concerned user box and the user box file after the authentication.

#### <Registration of user box by user operation>

To register a personal user box, a group user box or public user box by selecting the user attribute to the non-registration user box ID selected. When it's registered, it is possible to select

"User ID" or "Account ID" in the user attribute of the user box which have been specified "Public" as a default value.

- In the case of the personal user box, the arbitrary user ID registered is specified.
- In the case of the public user box, verify that a user box password registered satisfies the following conditions.
  - It is composed of the characters and by the number of digits, shown in the Table 11.
  - It shall not be composed of one kind of character.
- In the case of group user box, the arbitrary account ID registered is specified.  
As described above, FIA\_SOS.1[5], FMT\_MSA.3[1], FMT\_MTD.1[5], FMT\_SMF.1 and FMT\_SMR.1[3] are realized.

<Automatic registration of user box>

- In the user box operation to store of the copy job and the print job, when the specified user box is unregistered, the personal user box which is set the user ID of the user who operates the job concerned is automatically registered.  
As described above, FMT\_MSA.3[1] and FMT\_SMF.1 are realized.

<Registration of user box file>

- In the new registration operation, move or copy operation of user box file, the user box ID equivalent to the user box specified as target storage is set to the user box attribute as the user box file.  
As described above, FMT\_MSA.3[3] is realized.

### 7.5.1. Personal User Box Function

#### (1) Access control function to personal user box

The task to act for the identified and authenticated user has "User ID" of the user who is identified and authenticated for the user attribute. This task is permitted the display of the list of the personal user box which has a corresponding user attribute with this user attribute. As described above, FIA\_ATD.1, FIA\_USB.1, FDP\_ACC.1[1] and FDP\_ACF.1[1] are realized.

#### (2) Access control function to a user box file in a personal user box

When the user box to operate is selected, "User Box ID" of the user box is related to the task as a user box attribute in addition to the user attribute. This task is permitted, to the user box file with the user box attribute corresponding to the user box attribute of itself, the printing, the E-mail transmission (include the S/MIME transmission), the FTP transmission, the FAX transmission, the SMB transmission, WebDAV transmission, download, the removing to other user boxes, and the copy operations to other user boxes.

As described above, FIA\_ATD.1, FIA\_USB.1, FDP\_ACC.1[1] and FDP\_ACF.1[1] are realized.

#### (3) User attribute change of a personal user box

The user attributes can be changed.

- If another registered user is specified, it becomes a personal user box that another user manages.
- If public is specified, it becomes a public user box. It is necessary to register the user box password. In this case, it is verified that the user box password meets the following

requirements.

- It is composed of the characters and by the number of digits shown in Table 11.
- It shall not be composed of one kind of character.
- If account ID is specified, it becomes a group user box that can be accessed by a user who is permitted the use of the concerned account.

As described above, FIA\_SOS.1[5], FMT\_MSA1.[1], FMT\_SMF.1 and FMT\_SMR.1[3] are realized.

### 7.5.2. Public User Box Function

When the user is identified and authenticated as a registered user, the task to act for the user who is identified and authenticated has "User ID" of the identified and authenticated user as the user attribute. This task is permitted the display of the list of the public user box which is set the public as the user attribute. The operation specification of each public user box is as follows.

(As described above, FIA\_ATD.1, FIA\_USB.1, FDP\_ACC.1[1] and FDP\_ACF.1[1] are realized.)

- Authentication function in access to a public user box

For the access request for each public user box, after the above-mentioned verification function is operated, the user who accesses is authenticated that it is a user permitted the use of a user box concerned respectively.

- Offers the user box authentication mechanism that is authenticated by the user box password that consists of the character shown in Table 11.
  - After the user box is authenticated to the access from the network, it offers the user box authentication mechanism using the session information besides the user box password.
- According to protocol, it utilizes the 10<sup>10</sup> session information or more, or generated and uses the 10<sup>10</sup> session information or more.
- Return "\*" for each character as feedback for the entered user box password.
- Resets the number of authentication failure when succeeding in the authentication.
- In case of the access from the panel, when it fails in the authentication, an input from the panel is not accepted for five seconds.
- When the authentication failure that becomes the 1-3 times in total is detected for the public user box concerned, the authentication function to the public user box concerned is locked.
  - The administrator specifies the failure frequency threshold by the unauthorized access detection threshold setting function.
- The lock of the authentication function is released by the lock release function to the public user box of F.ADMIN executed.

As described above, FIA\_AFL.1[6], FIA\_AFL.1[8], FIA\_SOS.1[6], FIA\_SOS.2, FIA\_UAU.2[5], FDP\_UAU.7 and FIA\_UID.2[5] are realized.

The following is a function that the user who is permitted the use of the user box is offered in the user box identification and authentication domain of the user box.

- Access control to a user box file in a public user box

The task to act for the user is related the "User Box ID" of the user box as a user box attribute

in addition to the user attribute. This task is permitted the user box file, which have a corresponding user box attribute to the user box attribute of the subject attribute, to do the printing, the E-mail transmission (include the S/MIME transmission), the FTP transmission, the fax transmission, the SMB transmission, WebDAV transmission, download, the movement to other user boxes, and the copy operations to other user boxes.

As described above, FIA\_ATD.1, FIA\_USB.1, FDP\_ACC.1[1] and FDP\_ACF.1[1] are realized.

- User attribute change of a public user box

The user attribute of the user box can be changed.

- Specify the registered user. And change to a personal user box for the registered user.
- Specify the account ID, and then it becomes a group user box that can be accessed by a user who is permitted the use of the concerned account.

As described above, FMT\_MSA.1[2], FMT\_SMF.1 and FMT\_SMR.1[4] are realized.

- Change of a public user box password

Change the user box password of the public user box. When the user box password newly set satisfies the following qualities, it is changed.

- It is composed of the characters and by the number of digits shown in Table 11.
- It shall not be composed of one kind of character.

As described above, FIA\_SOS.1[5], FMT\_MTD.1[4], FMT\_SMF.1 and FMT\_SMR.1[4] are realized.

### 7.5.3. Group User Box Function

#### (1) Access control function for Group User Box

The task to act for the identified and authenticated user has the "Account ID" as the Account Name that is related to the identified and authenticated user. This task is permitted the display of the list of the group user box which has a corresponding user attribute with this account ID.

As described above, FIA\_ATD.1, FIA\_USB.1, FDP\_ACC.1[1] and FDP\_ACF.1[1] are realized.

#### (2) Access control function to a user box file in a group user box

When the user box to operate is selected, "User Box ID" of the user box is related to the task as a user box attribute in addition to the user attribute. This task is permitted, to the user box file with the user box attribute corresponding to the user box attribute of subject attribute, the printing, the E-mail transmission (include the S/MIME transmission), the FTP transmission, the FAX transmission, the SMB transmission, WebDAV transmission, download, the removing to other user boxes, and the copy operations to other user boxes.

As described above, FIA\_ATD.1, FIA\_USB.1, FDP\_ACC.1[1] and FDP\_ACF.1[1] are realized.

#### (3) User attribute change of a group user box

The user attributes can be changed.

- If another account ID is specified, the user of another Account Name becomes an accessible group user box.
- If public is specified, it becomes a public user box. It is necessary to register the user box password. In this case, it is verified that the user box password satisfies the following

requirements.

- It is composed of the characters and by the number of digits shown in Table 11.
- It shall not be composed of one kind of character.

➤ Specify a registered user, and change to a personal user box for the registered user.

As described above, FIA\_SOS.1[5], FMT\_MSA.1[3], FMT\_SMF.1 and FMT\_SMR.1[6] are realized.

## 7.6. F.PRINT (Secure Print Function)

F.PRINT is a security function related to the secure print function.

It offers the access control function that allows the printing and displaying the list of the secure print file after authenticating if a user is the authorized person to use the secure print file for the access to the secure print file from the panel to the identified and authenticated user.

### 7.6.1. Secure Print Function

#### (1) Authentication function by the secure print password

When the user is identified and authenticated as the registered user, it authenticates that the accessing user is a user to whom the use of the secure print file concerned is permitted, in response to the access request to each secure print file.

- Offers the secure print password authentication mechanism that is authenticated by the secure print password that consists of the character shown in Table 11.

➤ The secure print authentication mechanism by the separate session information is not needed because it becomes only an access from the panel in the case of the secure print.

➤ Return "\*" for each character as feedback for the entered secure print password.

➤ Resets the number of authentication failure when succeeding in the authentication.

➤ The access from the panel is not accepted for 5 seconds when the authentication is failed.

➤ When the authentication failure that becomes the 1-3 times in total for the secure print file concerned is detected, the authentication function to the secure print file is locked.

- The administrator specifies the failure frequency threshold by the unauthorized access detection threshold setting function.

➤ The lock is released by the lock release function to the secure print file of F.ADMIN executed.

As described above, FIA\_AFL.1[5], FIA\_AFL.1[8], FIA\_UAU.2[4], FIA\_UAU.7 and FIA\_UID.2[4] are realized.

#### (2) Access control function to a secure print file

The secure print file access control operates when it is authenticated.

➤ The task to act for the user who is identified and authenticated has the authenticated secure print internal control ID as the file attribute.

➤ This task is permitted the printing to the secure print file with a corresponding file attribute to the file attribute of this task.

As described above, FIA\_ATD.1, FIA\_USB.1, FDP\_ACC.1[2] and FDP\_ACF.1[2] are realized.

#### (3) Registration function of a secure print file

When it is authenticated as a registered user in the registration request of the secure print file, the user is permitted to register the secure print password with the concerned secure print file.

As described above, FMT\_MTD.1[8] is realized.

➤ Registration of the secure print password

The registered secure print password is verified to meet the following requirements.

- It is composed of the characters and by the number of digits shown in Table 11.
- It shall not be composed of one kind of character.

As described above, FMT\_SOS.1[5], FMT\_SMF.1 and FMT\_SMR.1[3] are realized.

➤ Giving of the secure print internal control ID

When the verification of the secure print password is completed in a registration request of the secure print file, the secure print internal control ID uniquely identified is set to the concerned secure print file.

As described above, FMT\_MSA.3[2] is realized.

## 7.7. F.OVERWRITE-ALL (All area overwrite deletion function)

F.OVERWRITE-ALL executes the overwrite deletion in the data area of HDD and CF, and initializes the setting value of the password that is set to NVRAM and CF as well. The object for the deletion or the initialization is as follows.

<Object for the deletion : HDD>

- Secure print file
- User box file
- On memory image file
- Stored image file
- HDD remaining image file
- Image related file
- Transmission address data file
- User ID
- User password
- User box password
- Secure print password
- Account ID
- Account password
- S/MIME certificate
- Remaining TSF data

< Object for the deletion : CF>

- CF remaining image file

<Object for the initialization : NVRAM>

- Administrator Password
- Operation setting of HDD lock function (OFF) --- HDD lock password is deleted.
- Operation setting of CF lock function (OFF) --- CF lock password is deleted.

- Operation setting of Encryption function (OFF) --- Encryption Passphrase is deleted.
- Trusted Channel setting data --- Trusted Channel setting data is deleted, because initialization has no default value.

<Object for the initialization : CF>

- SNMP Password

The deletion methods such as the data written in HDD and the written frequency is executed according to the deletion method of all area overwrite deletion function set in F.ADMIN (Table 12). The HDD lock password, CF lock password and the encryption passphrase cannot be used for being turned off the operation setting of the HDD lock function, CF lock function and the encryption function. The setting of the Enhanced Security function becomes invalid in the execution of this function. (Refer to the description for the operation setting of the Enhanced Security function in F.ADMIN.)

As described above, FAD\_RIP.1 is realized.

**Table 12 A type of overwrite deletion of all area and the method of overwriting**

Method	Overwritten data type and their order
Mode:1	0x00
Mode:2	Random numbers → Random numbers → 0x00
Mode:3	0x00 → 0xFF → Random numbers → Verification
Mode:4	Random numbers → 0x00 → 0xFF
Mode:5	0x00 → 0xFF → 0x00 → 0xFF
Mode:6	0x00 → 0xFF → 0x00 → 0xFF → 0x00 → 0xFF → Random numbers
Mode:7	0x00 → 0xFF → 0x00 → 0xFF → 0x00 → 0xFF → 0xAA
Mode:8	0x00 → 0xFF → 0x00 → 0xFF → 0x00 → 0xFF → 0xAA → Verification

## 7.8. F.CRYPT (Encryption key generation function)

F.CRYPT is generated the encryption key to encrypt image data written in HDD by using the HDD encryption key generation algorithm (SHA-256) that is regulated by the KonicaMinolta encryption specification standard. KonicaMinolta HDD encryption key generation algorithm (SHA-256) is the algorithm to generate the encryption key by using the SHA-256 regulated by FIPS 180-2.

When the encryption passphrase is decided in the encryption functional operation setting to which the access is restricted in F.ADMIN, the encryption key of 256bit length is generated from the encryption passphrase by applying the SHA-256 algorithm.

As described above, FCS\_CKM.1 is realized.

## 7.9. F.VALIDATION-HDD (HDD verification function)

F.VALIDATION-HDD is a check function to permit reading from and writing in the HDD only when it is verified that the illegal HDD is not installed and is confirmed validity when the HDD lock password is set to HDD

When the HDD lock password is set to HDD, the status of HDD is confirmed in the HDD operation verifying at the time of TOE starting. When the HDD lock password certainly being

set is returned as the result of status confirmation, the access to HDD is permitted. If the HDD lock password not being set is returned, the access to HDD is refused because of an illegitimate possibility.

As described above, FIA\_EID.1[1] is realized.

#### 7.10. F.VALIDATION-CF (CF verification function)

F.VALIDATION-CF is a check function to permit reading from and writing in the CF only when it is verified that the illegal CF is not installed and is confirmed validity when the CF lock password is set to CF

When the CF lock password is set to CF, the status of CF is confirmed in the CF operation verifying at the time of TOE starting. When the CF lock password certainly being set is returned as the result of status confirmation, the access to CF is permitted. If the CF lock password not being set is returned, the access to CF is refused because of an illegitimate possibility.

As described above, FIA\_EID.1[2] is realized.

#### 7.11. F.RESET (Authentication Failure Frequency Reset Function)

F.RESET is a function that releases the lock by resetting the authentication failure frequency when the account locks in the administrator authentication and CE authentication.

##### (1) CE Authentication function lock release processing function

The function is executed by the specific operation, and the lock is released by clearing the failure frequency of the CE authentication to 0 after CE authentication lock time.

As described above, FIA\_AFL.1[1] is realized.

##### (2) Administrator authentication function lock release processing function

The function is executed by OFF/ON of the main power supply, and the lock is released by clearing the failure frequency of the administrator authentication to 0 after the administrator authentication lock time.

As described above, FIA\_AFL.1[2] is realized.

#### 7.12. F.TRUSTED-PASS (Trust Channel Function)

F.TRUSTED-PASS is a function that generates and achieves the Trusted Channel by using SSL or TSL protocol when transmitting and receiving the following image file between client PC and MFP.

- User box file (download from MFP to client PC)
- Image file that will be stored as a user box file (upload from client PC to MFP)
- Image file that will be stored as Secure Print file (upload from client PC to MFP)

As described above, FTP\_ITC.1 is realized.

#### 7.13. F.S/MIME (S/MIME Encryption Processing Function)

F.S/MIME is a function to encrypt the User box file when transmitting the User box file as S/MIME.

<User box file Encryption Key generation>

- The Encryption key is generated to encrypt the user box file by the pseudorandom number Generation Algorithm which FIPS 186-2 provides. (Encryption key length is 128bit, 168bit, 192bit or 256bit.)

As described above, FCS\_CKM.1 is realized.

<Encryption of User box file >

- It is encrypted by AES which FIPS PUB 197 provides by using encryption key (128bit, 168bit and 256bit) to encrypt the user box file.
- It is encrypted by the 3-Key-Triple-DES which SP800-67 provides by using the encryption key (168bit) to encrypt the user box file.

As described above, FCS\_COP.1 is realized.

<Encryption of User box file Encryption key>

- The encryption key to encrypt the user box file is encrypted by RSA which FIPS 186-2 provides.
- The key length of the encryption key used in this case is 1024 bit, 2048bit, 3072bit or 4096bit.

As described above, FCS\_COP.1 is realized.

#### 7.14. F.SUPPORT-AUTH (External Server authentication operation support function)

F.SUPPORT-AUTH is the function that realizes the user identification and authentication function in cooperation with the user information management server of ActiveDirectory. (the function that operates with F.USER.)

When the user information management server is used for user identification method, the inquiry for the identification of the user is done for the user information management server under the user's request of the identification and authentication process. After this inquiry, the user identification and authentication process is realized by getting the user identification information returned back from user information management server.

As described above, FCS\_CAP.1[1] is realized.

#### 7.15. F.SUPPORT-CRYPTO (Cryption kit operation support function)

F.SUPPORT-CRYPTO is the function that operates the cryption function by cryption kit under TOE support.

The encryption process for the image files written in HDD is achieved through the cryption kit by setting the encryption key that F.CRYPTO generates, on it.

Furthermore the decryption process for the image files read from HDD is achieved through the cryption kit by setting the encryption key, that F.CRYPTO generates, on it.

As described above, FCS\_CAP.1[2] is realized.

#### 7.16. F.SUPPORT-HDD (HDD lock operation support function)

F.SUPPORT-HDD is the function to operate HDD lock function of HDD from TOE.

<Release process of HDD lock state>

At the MFP power ON, the release process of HDD lock state of HDD lock function is achieved.

- Release process is requested to HDD by using HDD lock password stored in HDD.

<Modification process of HDD lock password>

F.ADMIN requests to change the HDD lock password.

- Modification process is requested to HDD by using HDD lock password stored in NVRAM and new HDD lock password.

As described above, FIT\_CAP.1[3] is realized.

## 7.17. F.SUPPORT-CF (CF lock operation support function)

F.SUPPORT-CF is the function to operate CF lock function of CF from TOE.

<Release process of CF lock state>

At the MFP power ON, the release process of CF lock state of CF lock function is achieved.

- Release process is requested to CF by using CF lock password stored in CF.

<Modification process of CF lock password>

F.ADMIN requests to change the CF lock password.

- Modification process is requested to CF by using CF lock password stored in NVRAM and new CF lock password.

As described above, FIT\_CAP.1[4] is realized.