bizhub 754 / bizhub 654 / ineo 754 / ineo 654
Control Software
A55V0Y0-0100-G00-10

Security Target

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

Version: 1.06

Issued on: July 2, 2013

Created by: KONICA MINOLTA, INC.

<Revision History>

Date	Ver.	Division	Approved	Checked	Created	Revision
2012/10/19	1.00	Office Products System Control Development Div. 1	Suzuki	Nagata	Chiba	Initial Version.
2013/1/11	1.01	Office Products System Control Development Div.1	Suzuki	Nagata	Chiba	Deal with typos.
2013/1/23	1.02	Office Products System Control Development Div. 1	Suzuki	Nagata	Chiba	Deal with typos.
2013/1/29	1.03	Office Products System Control Development Div. 1	Suzuki	Nagata	Chiba	Deal with typos.
2013/3/11	1.04	Office Products System Control Development Div. 1	Suzuki	Nagata	Chiba	Deal with typos.
2013/4/8	1.05	Office Products System Control Development Div. 1	Suzuki	Nakata	Chiba	Change Corporate Name. Deal with typos.
2013/7/2	1.06	Office Products System Control Development Div. 1	Suzuki	Nakata	Chiba	Guidance ver. up. Deal with typos.

---- [Contents] ----

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

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

1. ST Introduction

1.1. ST Reference

- ST Title	:	bizhub 754 / bizhub 654 / ineo 754 / ineo 654 Control Software A55V0Y0-0100-G00-10 Security Target
- ST Version	:	1.06
- Created on	:	July 2, 2013
- Created by	:	KONICA MINOLTA, INC.

1.2. TOE Reference

- TOE Name	:	Japanese： bizhub 754 / bizhub 654 / ineo 754 / ineo 654 Zentai Seigyo Software English： bizhub 754 / bizhub 654 / ineo 754 / ineo 654 Control Software
- TOE Version	:	A55V0Y0-0100-G00-10
- TOE Type	:	Software
- Created by	:	KONICA MINOLTA, INC.

1.3. TOE Overview

This paragraph explains the usage, main security functions, and operational environment of TOE.

1.3.1. TOE Type

bizhub 754 / bizhub 654 / ineo 754 / ineo 654 control software, which is the TOE, is an embedded software product installed in the SSD on the MFP controller to control the operation of the whole MFP.

1.3.2. Usage of TOE and Main Security Functions

bizhub 754, bizhub 654, ineo 754 and ineo 654 are digital multi-function products provided by KONICA MINOLTA, INC., composed by selecting and combining copy, print, scan and FAX functions. (Hereinafter all the products are referred to as "MFP".) TOE is the “control software for bizhub 754 / bizhub 654 / ineo 754 / ineo 654" that controls the entire operation of MFP, including the operation control processing and the image data management triggered by the panel of the main body of MFP or through the network.

TOE supports the protection from exposure of the highly confidential documents stored in MFP. Moreover, for the danger of illegally bringing out HDD, which stores image data in MFP, TOE can encrypt image data written in HDD using ASIC (Application Specific Integrated Circuit). Besides, TOE has the function that deletes data area including image data in HDD completely by deletion method compliant with various overwrite deletion standards at the time of abandonment or the lease returns and the function that controls the access from the public line against the danger using Fax function as a steppingstone to access internal network. So it

contributes to the prevention of information leakage of the organization that uses MFP. Also, TOE includes the audit log function and contributes to the detection of MFP illegal use.

1.4. TOE Description

1.4.1. Roles of TOE Users

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

- User
  An MFP user who is registered into MFP. (In general, the employee in the office is assumed.)

- Administrator
  An MFP user who manages the operations of MFP. Manages MFP's mechanical operations and users. (In general, it is assumed that the person elected from the employees in the office plays this role.)

- Service engineer
  A user who manages the maintenance of MFP. Performs the repair and adjustment of MFP. (In general, the person-in-charge of the sales companies that performs the maintenance service of MFP in cooperation with KONICA MINOLTA, INC. is assumed.)

- Responsible person of the organization that uses MFP
  A responsible person of the organization that manages the office where the MFP is installed. Assigns an administrator who manages the operation of MFP.

- Responsible person of the organization that manages the maintenance of MFP
  A responsible person of the organization that manages the maintenance of MFP. Assigns service engineers who manage the maintenance of MFP.

Besides this, though not a user of TOE, those who go in and out the office are assumed as accessible persons to TOE.

1.4.2. Physical Scope of TOE

1.4.2.1. Use Environment

Figure 1 shows a general environment in which the usage of MFP equipped with TOE is expected. Moreover, the matters expected to occur in the use environment are listed below.

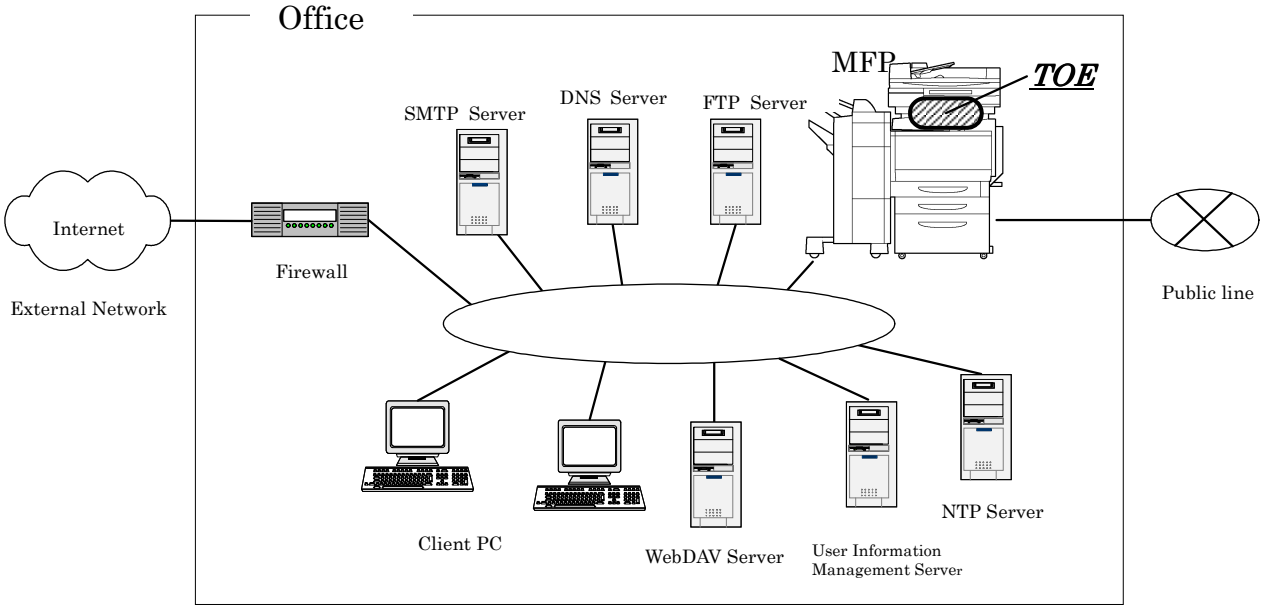

Figure 1 An example of MFP's use environments

- An intra-office LAN exists as a network in the office.
- MFP is connected to the client PCs via the intra-office LAN, and has mutual data communications.
- When a SMTP, FTP, or WebDAV server is connected to the intra-office LAN, MFP can carry out data communications with these servers, too. (The DNS service will be necessary when setting a domain name of the SMTP / FTP / WebDAV server.)
- It is also assumed to unify management of user IDs / passwords in a server. In this case, TOE can control access to the MFP by using the user registration information in the user information management server.
- It is also assumed to manage time in NTP server. In this case, TOE can record the date and time information on the audit log by using time information provided from NTP 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 applied.
- The intra-office LAN provides a network environment that cannot be intercepted by office operations including using switching hubs and installing wiretapping detectors.
- The public line connected with MFP is used for communications by Fax and the remote diagnostic function.

1.4.2.2. Operation Environment

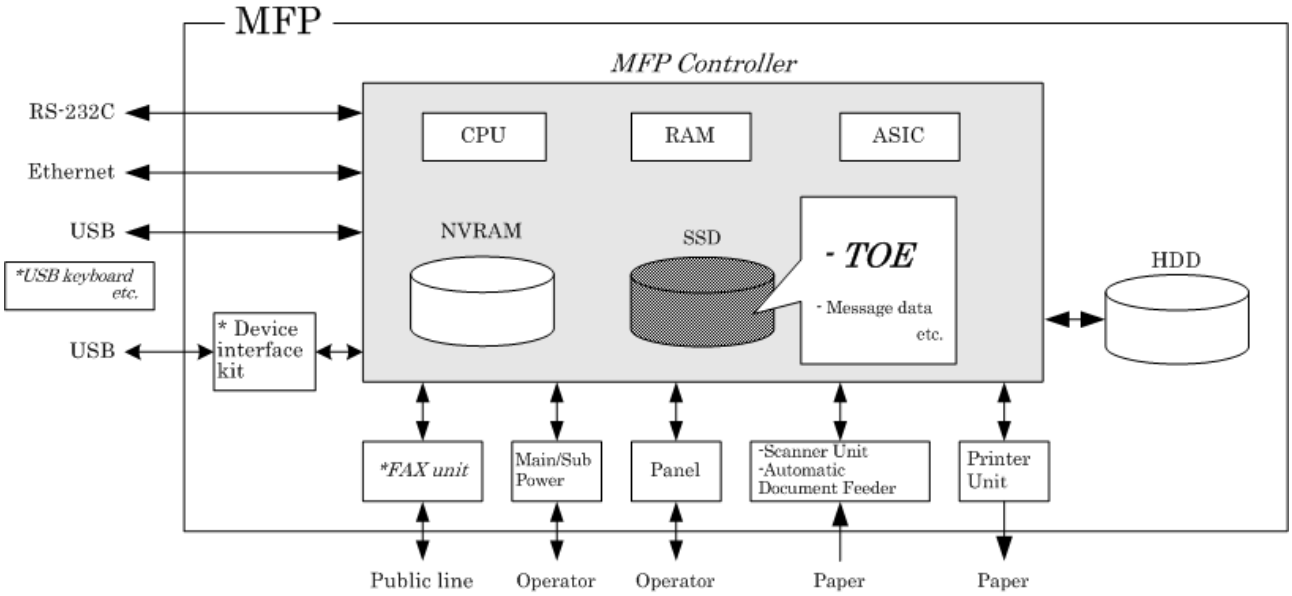

Figure 2 Hardware composition relevant to TOE

Figure 2 shows the structure of the hardware environment in MFP that TOE needs for the operation. The MFP controller is installed in the main body of MFP, and TOE exists in SSD on the MFP controller, loaded into the main memory.

The following explains about the unique hardware on the MFP controller, the hardware having interfaces to the MFP controller, and the connection using interfaces, shown in Figure 2.

- SSD

  A storage medium that stores the object code of the "MFP Control Software," which is the TOE. Additionally, stores the message data expressed in each country's language to display the response to access through the panel and network, and various settings that MFP needs for processing TOE.

- NVRAM

  A nonvolatile memory. This memory medium stores various settings that MFP needs for processing of TOE.

- ASIC

  An integrated circuit for specific applications which implements an HDD encryption functions for enciphering the image data written in HDD.

- HDD

  A hard disk drive of 250GB in capacity. This is used not only for storing image data as files but also as an area to save image data and destination data temporarily during extension conversion and so on.

- Main/sub power supply
  Power switches for activating MFP.

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

- Scan unit/automatic document feeder
  A device that scans images and photos from paper and converts them into digital data.

- Printer unit
  A device to actually print the image data which were converted for printing when receives a print request from the MFP controller.

- Ethernet
  Supports 10BASE-T, 100BASE-TX, and Gigabit Ethernet.

- USB
  Copying image file to an external memory, copying or printing image file from an external memory, and update of TOE, etc. can be performed through this interface. This is also usable as a connection interface of the optional parts. There is the device interface kit which is need for copy or print from Bluetooth device and the USB keyboard[1] to complement key entry from the panel. Including an external memory, it is necessary to be able to use them.

- RS-232C
  Serial connection using D-sub 9-pin connectors is usable. The maintenance function is usable through this interface in the case of failure. It is also possible to use the remote diagnostic function (described later) by connecting with the public line via a modem.

- FAX unit (* optional part)
  A device that has a port of Fax public line and is used for communications for FAX-data transmission and remote diagnostic (described later) via the public line. Is not pre-installed in MFP as a standard function according to the circumstances in sales, but sold as an optional part. Fax unit is purchased when the organization needs it, and the installation is not indispensable.

1.4.2.3. Guidance

- bizhub 754 / 654 Service Manual Security Functions (Japanese) Ver.1.03
- bizhub 754 / 654 SERVICE MANUAL SECURITY FUNCTION Ver.1.03
- ineo 754 / 654 SERVICE MANUAL SECURITY FUNCTION Ver.1.03
- bizhub 754 / 654 User's Guide Security Functions (Japanese) Ver.1.03
- bizhub 754 / 654 User's Guide [Security Operations] Ver.1.03
- ineo 754 / 654 User's Guide [Security Operations] Ver.1.03

[1] It is usable when the display language is English, French, Italian, German or Spanish. It does not affect the operation of security functions.

1.4.3. Logical Scope of TOE

Users use a variety of functions of TOE from the panel and a client PC via the network. Hereafter, this section 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 administrators, the service engineer function manipulated by service engineers, and the function operated in the background without user's awareness.

1.4.3.1. Basic Function

In MFP, a series of functions for the office work concerning the image such as copy, print, scan, and FAX exists as basic functions, 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 image files, and stores them in RAM and HDD. (For print image files from client PCs, multiple types of conversion are applied.) These image files are converted into data to be printed or sent, and transmitted to the device outside of the MFP controller concerned.

Operations of copy, print, scan, and FAX are managed by the unit of job, so that operation priority can be changed, finishing of print jobs can be changed, and such operations can be aborted, by giving directions from the panel.

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

- Secure Print Function
  When a Secure Print password is received together with printing data, the image file is stored as standby status. Then, printing is performed by a print direction and password entry from the panel.
  When printing is requested by a client PC, this function eliminates the possibility that other users stole a glance at the printing of highly confidential data, or such data is slipped into the other printings.

- ID & Print Function
  When this function is set up, usual print data are saved in the print waiting state, and printed by the user authentication processing from the panel. Even when this function is not set up, if it is specified on the print data to activate this function, the system will operate in the same manner as this function is set up by a user.

1.4.3.2. User Box Function

A directory called a "user box" can be created as an area to store image files in HDD. Three types of user box are usable; the first is the personal user box which a user possesses, the second is the public user box which is shared by registered users who made a certain number of groups, and the third is the group box which is shared by the users belonging to same account. 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 the group

box limits operations only for the users of the account that are permitted to use it.

TOE processes the following operation requests to a user box or image files in the user box that is transmitted from the panel or the network unit through a network from a client PC.

- Print, transmit, and download from a client PC, of image files in a user box
  - The encryption of user box file is possible in the E-mail that is one of the transmission methods.
- Delete an image file in a user box, move/copy it to other user boxes and copy it to external memory
- Set a storing period of image files in a user box (delete automatically after the period passes.)
- Change the name and password of a user box, or delete a user box
- Set attributes of a user box (change the type of a personal user box, public user box, or group user box)

1.4.3.3. User Authentication Function

TOE can limit the user who uses MFP. For access through the panel or the network, TOE identifies and authenticates 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 user authentication like below are supported.

(1) Machine authentication[2]
A method to authenticate user at MFP by registering a user ID and a user password into HDD on the MFP controller.

(2) External server authentication
A method to authenticate user at MFP by using the user ID and the user password that are registered on the user information management server which is connected with the intra-office LAN without managing the user ID and user password on the MFP side. Though multiple methods called Active Directory[3], NTLM[4], and NDS are supported, the method of the external server authentication assumed in this ST is applied only to the case of using Active Directory.

1.4.3.4. Account Authentication Function[5]

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
Set an Account ID on a user beforehand, and associate the user with the account ID of the user's account when he/she is authenticated.

---

[2] When user is set "Pause" by administrator function, authentication function for the user does not work.

[3] A method of directory service that Windows Server 2000 (or later) supports to uniformly manage user information in the network environment of Windows platform.

[4] An abbreviation of NT LAN Manager. An authentication method used in directory service that Windows NT supports to uniformly manage user information in network environment of Windows platform.

[5] When account is set "Pause" by administrator function, authentication function for the account does not work.

(2) Method not synchronized with User Authentication

Associate a user with his/her account ID when the user is authenticated by the account password set for each 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 MFP 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 functions related to the security.

- User registration management
  - Registration or change of user IDs/passwords, deletion of users, and pause/resume of users
  - Change of the association between users and account IDs
- Account registration management
  - Registration or change of account IDs/passwords and pause/resume of accounts.
- Management of user box settings
  - Registration or change of user box passwords, and management of user attributes
- Operational setup of automatic system reset
  - Setup of the function that logs out automatically when the setting time passed.
- Management of network settings
  - Connection setting of the intra-office LAN (setting of DNS server)
  - SMTP setting (setting of the SMTP server utilized by E-mail transmission)
  - IP addresses, NetBIOS names, and AppleTalk printer names etc.
- Backup or restore function of NVRAM, SSD and HDD
  - This is performed through the network by using a backup/restore application for the management installed in the client PC.
- All area overwrite deletion function of HDD
  - There are data deletion methods conformed to various military standards (ex. Military Standard of United States Department of Defense)
  - When this function is started up, in conformity with a set method, the overwrite deletion is executed for the data area including image data in HDD.
- Format function of HDD
  - A logical format is executable.
- Access and deletion function of Audit Log
  - Export the audit log, and the access and the deletion of log are executable.
- Management of date/time information settings
  - Setting of the date and time information held by TOE. When the event for audit occurred, this date/time information is recorded as the audit log.
- Management of FAX setup (* Fax unit is installed.)
  - Setup of TSI[6] receiving
  - Setup of FAX output at PC-FAX receiving (Storing in user box or common area for all users are available.)

[6] An abbreviation of Transmitting Subscriber Identification. The same meaning of Identification of Subscriber's Terminal. TSI receiving is the function that can designate the user box to be stored for each subscriber.

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

- Method setup of a user authentication function
  - Machine authentication, external server authentication, or user authentication stop is selected.
  - Combination with Account Authentication is set up. (Method synchronized with User Authentication, Method not synchronized with User Authentication)
- Setup of access when the user attribute is public
  - It is selected whether to permit or prohibit MFP utilization of the user who is not identified by user ID.
- Setup of a password policy function
  - It is selected whether to enable or disable the function to check the several conditions of the password, such as the number of valid digits of various passwords.
- Setup of the authentication method of Secure Print and the authentication operation prohibition function.
  - When secure print files are authenticated, the authentication operation prohibition function operates in a mode, and does not operate in the other mode.
  - The operation mode of the function detecting unsuccessful authentication in each authentication function is also synchronous with the above mode.
  - The above-mentioned operational modes are selected.
- Setup of the network setting modification function by SNMPv1 and v2.
  - It is selected whether to enable or disable the function to change MIB by SNMPv1 and v2.
- Operational Setup of Authentication Function when writing using SNMPv3
  - The security levels of authentication or skipping authentication is selected.
  - For the security levels, either "only authentication password" or "authentication password + privacy password" is available.
- Setup of the HDD encryption function
  - Whether to activate or stop the function is selected.
  - An encryption passphrase is registered or changed when the function is activated.
- Setup of the user box collective management function
  - It is selected whether to enable or disable this function.
- Setup of the print capture function
  - A function to verify the print data received by MFP when the print function is faulty.
  - It is selected whether to enable or disable this function.
- Setup of the network setting management reset function
  - This function resets a series of items to factory default values
  - It is selected whether to enable or disable this function.
- Setup of the trusted channel (SSL/TLS encryption communications) function
  - SSL/TLS server certificates are generated or imported.
  - The encryption method used for communications is set up.
- Setup of the transmission address data
  - A transmission address or method used for box file transmission etc. is selected.
  - S/MIME certificates are imported.
- Setup of the FTP server function
  - Whether to activate or stop the function is selected.

- Setup of the S/MIME function
  - Whether permit or prohibit the S/MIME certificate automatic registration function is selected.
  - The encryption method used for data encryption is selected.
- Setup of the ID & print function
  - Whether to activate the ID & print function or not in normal printing is selected.
- Setup of the HDD data overwrite deletion function
  - The deletion method is selected.
- Operational Setup of the Audit log when it is full.
  - The operational setting of the audit log when it is full is selected.

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 security.

- Modification function of administrator password

The following is a set of operation setting functions related especially to the behavior of the security function.

- Authentication setup of the service engineer with the CE[7] password.
  - Whether to activate or stop the function is selected.
- Setup of remote diagnostic function (later description)
  - Able to select permission or prohibition.
- Setup of a TOE update function via Internet
  - Able to select permission or prohibition.
- Setup 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 settings 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.

- Encryption key generation function
  Performs encryption/decryption by ASIC when writing image data in HDD or reading image

[7] An abbreviation of Customer Service engineer

data from HDD.
The operational setup of this function is performed by the administrator function. When activated, TOE generates the encryption key by the encryption passphrase that was entered on the panel.

- Remote diagnostic function
  MFP's equipment information such as operating state and the number of printed sheets is managed by making use of the connection by a port of FAX public line, by a modem through RS-232C or by E-mail or WebDAV to communicate with the support center of MFP produced by KONICA MINOLTA, INC. In addition, if necessary, appropriate services (shipment of additional toner packages, account claim, dispatch of service engineers due to the failure diagnosis, etc.) are provided.

- 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 external memory.

- 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 operational setup of this function is performed by the administrator function.

- 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.

- HDD data overwrite deletion function
  The overwrite deletion is executed to the data area of image unnecessary in HDD. The deletion pattern is set in the administrator function.

- Audit log function
  It is the function to generate the log, which is audit log, and store them in HDD, when the event for audit occurred. The operation of the log is limited only to the administrator and the export and the deletion of log can be performed.

The standard is that MFP is not installed Fax unit and does not have a port of Fax public line, so there is not the access to the internal network through MFP. TOE provides the following function, provided that Fax unit is installed in MFP.

- Fax unit control function
  TOE prohibits access to the internal network, where MFP was connected to, from a port of Fax public line through Fax unit.

TOE makes effective use of the security function (HDD encryption function) of ASIC, which is an external entity. The following explains typical functions related to the external entity.

- Utilization of ASIC
  ASIC, an external entity, activates a function to encrypt the image data in HDD as a function to protect unauthorized bring-out of data and so on when an encryption passphrase is set up.

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". Alert screen is displayed if each value set is changed to the vulnerable one individually. Also, the use of the update function of TOE through the network, the initializing function of the network setting, and the setting change by remote diagnostic function is prohibited, or alert screen is displayed when it is used.

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.

- User authentication function : Valid (Both authentication by the main body and the external server are usable)
- User : access of PUBLIC : Prohibited
- User Name List : Prohibited
- Print without authentication : Prohibited
- Simple print authentication : Prohibited
- Password policy function : Valid
- Setup of Authentication Operation Prohibition function
  : The panel and account are locked out for 5 seconds when authentication has failed (failure frequency threshold: 1-3).
- Secure print access method : Work with the setting of Authentication operation prohibition function
- User box management function : Prohibited
- SNMP v1/v2c Write function : Prohibited
- WriteUser Authentication by SNMPv3 : Valid
- Setup of HDD encryption function : Valid
- Print data capture function : Prohibited
- Address registration user change function : Prohibited
- Setup of limitation of SSL encryption severity: Valid (Only 3DES and, AES are user-selectable)
- SSL protocol setting : Valid
- Setup of operation prohibition release time of Administrator authentication
  : Setup prohibited for 1-4 minutes
- Setup of operation prohibition release time of CE authentication
  : Setup prohibited for 1-4 minutes
- FTP Server function : Prohibited
- Automatic registration of S/MIME certificate : Prohibited
- Setup of limitation of S/MIME encryption severity
  : Valid (Only 3DES and AES are user-selectable.)
- Image log transmission : Prohibited
- Remote panel function : Prohibited

- External application connection : Prohibited

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 Version 3.1 Revision 4 (Japanese Translation v1.0)
Part 2: Security functional components Version 3.1 Revision 4 (Japanese Translation v1.0)
Part 3: Security assurance components Version 3.1 Revision 4 (Japanese Translation v1.0)

- 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 to Package: EAL3. There is no additional assurance component.

2.4. Reference

- Common Criteria for Information Technology Security Evaluation Part 1:Introduction and general model Version 3.1 Revision 4 CCMB-2012-09-001
- Common Criteria for Information Technology Security Evaluation Part 2:Security functional components Version 3.1 Revision 4 CCMB-2012-09-002
- Common Criteria for Information Technology Security Evaluation Part 3:Security assurance components Version 3.1 Revision 4 CCMB-2012-09-003
- Common Methodology for Information Technology Security Evaluation
  Evaluation methodology Version 3.1 Revision 4 CCMB-2012-09-004

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.

- Secure Print file
  An image file registered by Secure Print.
- ID & print file
  An image file saved as an ID & print file when print data are registered by the ID & print function.
- User Box file
  An 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 store of a secure print file or an ID & print file and the transmission of a user box file, making in the preparation for the threat thought when unauthorized MFP or mail server is connected by any chance, or when operational setup of PC-FAX is changed even if without unauthorized MFP, the setting of MFP (IP address, transmission address data etc.) and operation setting of PC-FAX require not to be modified illegally. Therefore, the setting of MFP (IP address, transmission address data etc.) and operation setting of PC-FAX are considered as subsidiary protected assets.

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

- Secure Print File
- ID & print File
- User Box File
- Stored Image File
  - Stored image files other than secure print file, user box file, or ID & print file

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.

3.3. Threats

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

T.DISCARD-MFP (Lease-return and discard of MFP)

When leased MFPs are returned or discarded MFPs are collected, secure print files, user box files, ID & print files, and stored image files can leak by the person with malicious intent when he/she analyzes the HDD in the MFP.

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

- Secure print files, user box files, ID & print files, and stored image files can leak by a malicious person or a user illegally when he/she brings out the files to analyze the HDD in a MFP.
- A person or a user with malicious intent illegally replaces the HDD in MFP. In the replaced HDD, newly created files such as secure print files, user box files, ID & print files, and stored image files are accumulated. A person or a user with malicious intent takes out to analyze the replaced HDD, so that such image files will 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 operates the user box file, such as copies, moves, downloads, prints, transmits, and so on.

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

Exposure of the user box file when a person or a user with malicious intent accesses the public user box which is not permitted to use, and operates the user box file, such as copies, moves, downloads, prints transmits, and so on.

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 a user with malicious intent accesses the group user box which the account where a user does not belong to owns, and operates the user box file, such as copies, moves, downloads, prints transmits, and so on.

T.ACCESS-SECURE-PRINT (Unauthorized access to the secure print file or ID & print file by utilizing the user function)

- Secure print files are exposed by those malicious including users when he/she operates (prints etc.) ones to which access is not allowed.
- ID & print files are exposed by those malicious including users when he/she operates (prints etc.) ones which were stored by other users.

T.UNEXPECTED-TRANSMISSION (Transmission to unintended address)

- Malicious person or user changes the network settings that are related to the transmission of a user box file. Even an address 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 settings which are 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 settings which set in MFP to identify MFP itself where TOE installed, by setting to the value of the entity such as another unauthorized MFP from the value of MFP (NetBIOS name, AppleTalk printer name, IP address etc) that TOE is originally installed, so that secure print files or ID & print files are 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 reception 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 setting of PC-FAX reception 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 files, secure print files, or ID & print files rises because those malicious including users change the settings related to the enhanced security function.

T.BACKUP-RESTORE (Unauthorized use of backup function and restoration function)

User box files, secure print files, or ID & print files can leak by those malicious including users using the backup function and the restoration function illegally. Also highly confidential data such as passwords can be exposed, so that settings might be falsified.

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. Moreover, although a accumulated data in a client PC and a server existing in internal network, and a general data traveling across the internal network are not protected assets, TOE security environment that corresponds to the organization that prohibited the access to internal network via MFP from Fax public line portal is assumed.

Also, there are a lot of organizations that want to decrease the motivation of illegal operations such as the unauthorized use of MFP by an attacker and the exposure and falsification of image files which are the assets. Since the audit log function can track the illegal uses and operations, motivation of an attacker is expected to decrease. TOE security environment that corresponds to the organizations and users that desire to manage MFP with this function is assumed. Obtaining logs related to security are two. One is obtaining the log of all authentication functions. In order to use the functions of MFP except the confirmation of stopped state of user and account, it is necessary to succeed in authentication, and so the illegal actions (operations after permission time) of MFP user could be reduced. Another thing is obtaining the log of operations (jobs) related to the user box files, the secure print files, and the ID & print files which are the assets registered in MFP. The illegal operations could be reduced by auditing the access of user to the assets.

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 files (secure print files, user box files, and ID & print files) which transmitted or received between IT equipment must be communicated via a trusted path to the correct destination, or encrypted when the organization or the user expects to be protected.

P.REJECT-LINE (Access prohibition from public line)

An access to internal network from public line via the Fax public line portal must be prohibited.

P.AUDIT-LOGGING (Acquisition and management of Audit log)

The generation of the audit log related to all authentication functions and to all jobs necessary to be audited must be maintained. Also, the audit log must be protected from a person who does not have the authority of disclosure or change, and it must be set to be accessed by a person who has the authority.

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 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 permitted user)

TOE permits the use of MFP installed TOE only to the user who succeeded in the identification and authentication.

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

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

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

- TOE permits the user who succeeded in identification and authentication 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 that 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 that this account owns only to the user who is permitted the use of this account.

O.SECURE-PRINT (Access control for secure print files and ID & print files)

- TOE permits the user function of a secure print file only to the user who was allowed to use the file.
- TOE permits the user function of an ID & print file only to the user who stored that 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 Trusted Channel function setting data
- The setting functions of certificates, transmission address data, etc used for the S/MIME function.
- The setting function of TSI receiving
- The setting function of PC-FAX reception
- Counter management function
- All area overwrite deletion function

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 (Overwrite deletion)

TOE overwrites image data regions of assets stored in the HDD in the MFP with deletion data, and makes it unable to restore.

O.CRYPT-KEY (Encryption key generation)

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

O.TRUSTED-PATH (The use of Trusted Channel)

TOE provides 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 files
- Image file that will be stored as secure print files
- Image files that will be stored as ID & print files

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

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

O.FAX-CONTROL (Fax unit control)

TOE provides the control function that prohibits an access to internal network which the MFP connects with, from public line via the Fax public line portal.

O.AUTH-CAPABILITY (The support operation to utilize user authentication function)

TOE supports the necessary operation to utilize the user authentication function by user information management server using Active Directory.

O.CRYPTO-CAPABILITY (The support operation to utilize HDD encryption function)

TOE supports necessary mechanical operations to utilize the HDD encryption function by ASIC.

O.AUDIT-LOGGED (Acquisition and management of Audit log)

TOE maintains the generation of the audit log related to all authentication functions and jobs, necessary to be audited. And, it provides the function to protect the audit log from a person who does not have the authority of disclosure or change.

4.2. Security Objectives for the Operational Environment

In this section, the security objectives for TOE operational environment are described.

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, which provides appropriate protected feedback to the user password, user box password, account password, administrator password, secure print password, and SNMP password, which will be entered.

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 instead 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 secure print files, ID & print files, and the user box and user box files ends, 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 responsible person 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 responsible person in the organization managing the maintenance of MFP educates a service engineer in order to faithfully carry out the given role for the installation of the TOE, the setup 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 responsible person 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 responsible person 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.FAX-UNIT (Utilization of Fax unit)

The service engineer installs the Fax unit on MFP which is the optional parts and sets to utilize the function of the Fax unit.

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 users who commonly utilize 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.

- Avoid setting an easy-to-guess value on the administrator password, account password, SNMP password, and encryption passphrase.
- Keep the administrator password, account password, SNMP password, and encryption passpharse confidential.
- Change the administrator password, account password, SNMP password, and encryption passphrase appropriately.

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 (Security related Setting, Maintenance, Operation)

The administrator performs the setting along with the guidance including the enhanced security function to TOE before user uses, and the settings are kept while TOE is used. Also, when leased MFPs are returned or discarded, the administrator operates along with the guidance for TOE.

OE.AUDIT-STORAGE-PROTECTED (Audit log protection)

The administrator protects the audit log from deletion and change by a person who does not have the operation authority of the exporting log to reliable IT products.

OE.AUDIT-ACCESS-AUTHORIZED (Access authority to audit log)

The administrator manages that only a person who has the operation authority of the exporting log to reliable IT products can access.

OE.AUDIT-REVIEWED (Examination of audit log)

The administrator carries out the examination of the audit log at appropriate intervals to detect the compromise and abnormal condition.

4.3. Security Objectives Rationale

4.3.1. Necessity

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

Table 1 Conformity of security objectives to assumptions, threats, and organization security policies

Organization security policies / Assumptions / Threats / Security objectives	A.ADMIN	A.SERVICE	A.NETWORK	A.SECRET	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	P.COMMUNICATION-DATA	P.REJECT-LINE	P.AUDIT-LOGGING
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					X											
O.CRYPTO-KEY						X										
O.TRUSTED-PATH														X		
O.CRYPTO-MAIL														X		
O.FAX-CONTROL															X	
O.CRYPTO-CAPABILITY						X										
O.AUTH-CAPABILITY							X	X	X	X						
O.AUDIT-LOGGED																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.FAX-UNIT															X	
OE.SECRET				X												
OE.SETTING-SECURITY					X	X	X	X	X	X	X	X	X	X		
OE.AUDIT_STORAGE-PROTECTED																X
OE.AUDIT_ACCESS-AUTHORIZED																X
OE.AUDIT-REVIEWED																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 and no access by an unspecified person from an external network to the intra-office LAN.
  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, user box password, user password, and account password and that the administrator executes the operation rule concerning the administrator 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.

4.3.3. Sufficiency of Threats

The security objectives against threats are described as follows.

- **T.DISCARD-MFP (Lease return and discard of MFP)**
  This threat assumes the possibility of leaking information from MFP collected from the user.
  O.OVERWRITE is that TOE provides the function to overwrite the image data area of the protected assets in HDD by data for deletion, so that the possibility of the threat is reduced by executing this function before MFP is collected. Also, OE.SETTING-SECURITY indicates the operation of the function to overwrite the image data area of the protected assets in HDD

provided by TOE by data for deletion, so that the possibility of the threat is reduced by operating it before MFP is collected.
Accordingly, this threat is countered sufficiently.

- **T.BRING-OUT-STORAGE (Unauthorized bringing out 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 O.CRYPTO-KEY assumes that TOE generates an encryption key to encrypt the data written in the HDD, a mechanical operation to use the HDD encryption function by ASIC is supported by O.CRYPTO -CAPABILITY, and OE. SETTING-SECURITY performs the setting along with the description of guidance including the enhanced security function, and the operation related to the maintenance.
  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 succeed identification and authentication 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 external user information management server is used, the possibility of the threat is reduced because the user identification and authentication is operated through O.AUTH-CAPABILITY supporting the operation for the user authentication function by the user information management server of Active Directory and through OE.SERVER setting to use the user management by Active Directory by the administrator.
  OE. SETTING-SECURITY performs the setting along with the description of guidance including the enhanced security function, and the operation related to the maintenance, and E.FEED-BACK uses the application regulating to return the protected feedback for the entered password in the user's authentication, and OE.SESSION also requires the log-out 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 succeed identification and authentication 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 external user information management server is used, the possibility of the threat is reduced because the user identification and authentication is operated through O.AUTH-CAPABILITY supporting the operation for the user authentication function by the user information management server of Active Directory and through OE.SERVER setting to

use the user management by Active Directory by the administrator.
OE. SETTING-SECURITY performs the setting along with the description of guidance including the enhanced security function, and the operation related to the maintenance, and 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.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 user 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 TOE permits only the user who succeeded the identification and authentication 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 external user information management server is used, the possibility of the threat is reduced because the user identification and authentication is operated through O.AUTH-CAPABILITY supporting the operation for the user authentication function by the user information management server of Active Directory and through OE.SERVER setting to use the user management by Active Directory by the administrator.
  OE. SETTING-SECURITY performs the setting along with the description of guidance including the enhanced security function, and the operation related to the maintenance, and 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.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 or an ID & print file using the user function)**
  This threat assumes the possibility that an unauthorized operation is done to the secure print and ID & print using user function.
  O.REGISTERED-USER assumes that TOE permits only the user who succeeded the identification and authentication to use MFP installing TOE, furthermore, the operations of the secure print and ID & print are limited only to the authorized user by O.SECURE-PRINT, so that the possibility of the threat is reduced. When the external user information management server is used, the possibility of the threat is reduced because the user identification and authentication is operated through O.AUTH-CAPABILITY supporting the operation for the user authentication function by the user information management server of Active Directory and through OE.SERVER setting to use the user management by Active Directory by the administrator.
  OE. SETTING-SECURITY performs the setting along with the description of guidance including the enhanced security function, and the operation related to the maintenance, and 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.SESSION requires the log-out 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 or an ID & print file which is required to be concealed from other users in the office is transmitted to the unauthorized entity.
  In addition to this, the setting of PC-FAX reception and the setting of TSI reception assumes the possibility of unintended user 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 reception and the setting of TSI reception are limited to the administrator, and so the possibility of this threat is removed.
  OE. SETTING-SECURITY performs the setting along with the description of guidance including the enhanced security function, and the operation related to the maintenance, and OE.FEED-BACK uses the application regulating that the feedback protected is returned for the entered password by the administrator's authentication and OE.SESSION requires to logout 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 files, secure print files, or ID & print files by having been changed the specific function setting which relates to security.
  O.CONFIG regulates that only the administrator and the service engineer are permitted to perform the setup 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. SETTING-SECURITY performs the setting along with the description of guidance including the enhanced security function, and the operation related to the maintenance, and 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.SESSION is also requested to logout 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 user box files, secure print files, or ID & print files may leak when the back-up function or the restoration function is illegally used. Moreover, this assumes that confidential data such as passwords might leak or various settings are falsified, so that user box files, secure print files, or ID & print files 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. SETTING-SECURITY performs the setting along with the description of guidance including the enhanced security function, and the operation related to the maintenance, and OE.FEED-BACK uses the application regulating that the protected feedback is returned for the entered password by the administrator authentication and OE.SESSION is also requested the log-out operation after the operation ends, and so O.CONFIG is sufficiently supported.
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 path 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-PATH provides Trusted Channel to a correct destination in the transmission and reception of an image between MFP and client PCs for user box files, secure print files, and ID & print files that save confidential images, so that the organizational security policies is achieved.
  Also, the security objective provides 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, 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 out after the operations of the administrator mode ends, that O.CONFIG is supported. Also, OE. SETTING-SECURITY performs the setting along with the description of guidance including the enhanced security function, and the operation related to the maintenance.
  Accordingly, this organizational security policy is sufficiently to achieve.

- **P.REJECT-LINE (Access prohibition from public line)**

  This organizational security policy prohibits being accessed to a stored data in a client PC and a server existing in internal network or a general data flowing on internal network from public line via the port of Fax public line on Fax unit installed to MFP.
  This means that communication, like remote diagnostic function or illegal operation

command, except image data which is sent from public line network and forwarded to internal network via the port of Fax public line of MFP is not forwarded to internal network, even though Fax unit is installed on MFP at the request of the organization.
O.FAX-CONTROL prohibits the access to the data existing in internal network including a general data from public line via the Fax public line portal.
Also, OE.FAX-UNIT is regulated to install Fax unit which is the optional part on MFP by service engineer, so that O.FAX-CONTROL is supported.
Accordingly, this organizational security policy is achieved.

- **P.AUDIT-LOGGING (Acquisition and management of Audit log)**

This organizational security policy must maintain the generation of the audit log related to all authentication functions and jobs, necessary to be audited. Also, it regulates that it protects the audit log from a person who does not have the authority of disclosure or change, and a person who has the authority could access the audit log.
O.AUDIT-LOGGED regulates that it maintains the generation of the audit log related to all authentication functions and jobs, necessary to be audited, and it provides the function to protects the audit log from a person who does not have the authority of disclosure or change.
Also, the administrator is regulated the followings. OE.AUDIT_STORAGE-PROTECTED protects the audit log from access, deletion and change by a person who does not have the operation authority of the exporting log to reliable IT products.
OE.AUDIT_ACESS-AUTHORIZED manages that only a person who has the operation authority of the exporting log to reliable IT products can access. And OE.AUDIT-REVIEWED carries out the examination of the audit log at appropriate intervals to detect the compromise and abnormal condition, so that O.AUDIT-LOGGED is supported.
Accordingly, this organizational security policy is achieved.

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.

- **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.1)

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

5.1.1. FIT_CAP.1 Definition

- **Class name**
  FIT: Support for IT environment entity
  Meaning of abbreviation: FIT (Functional requirement for IT environment support)

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

- **Component leveling**

FIT_CAP Capability of using IT environment entity	1

  Meaning of abbreviation: CAP (**CAP**ability of using IT environment)

  FIT_CAP.1: "Capability of using security service of IT environment entity" corresponds to the substantiation of capability needed to use the security function correctly provided by IT environment entity.

Audit : FIT_CAP.1
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)
Management : FIT_CAP.1
The following actions could be considered for the management functions in FMT. There is no management activity expected

FIT_CAP.1	**Capability of using security service of IT environment entity**
FIT_CAP.1.1	
TSF shall provide the necessary capability to use the service for [assignment: *security service provided by IT environment entity*]. : [assignment: *necessary capability list for the operation of security service*]	
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 Functional Requirements

6.1.1.1. Cryptographic Support

FCS_CKM.1	**Cryptographic key generation**
FCS_CKM.1.1	
The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].	
[assignment: *list of standards*] : ***Listed in "Table2 Cryptographic key generation Relation of Standards-Algorithm-Key sizes"***	
[assignment: *cryptographic key generation algorithm*] : ***Listed in "Table2 Cryptographic key generation Relation of Standards-Algorithm-Key sizes"***	
[assignment: *cryptographic key sizes*] : ***Listed in "Table2 Cryptographic key generation Relation of Standards-Algorithm-Key sizes"***	
Hierarchical to : No other components Dependencies : FCS_CKM.2 or FCS_COP.1 (FCS_COP.1), 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
FIPS 186-2	***Pseudorandom number Generation Algorithm***	***- 128 bits*** ***- 192 bits*** ***- 168 bits*** ***- 256 bits***
Konica Minolta Encryption specification standard	***Konica Minolta HDD Encryption Key Generation Algorithm***	***- 256 bits***

FCS_COP.1	**Cryptographic operations**
FCS_COP.1.1	
The TSF shall perform [assignment: *list of Cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: *list of standards*].	
[assignment: *list of standards*] : ***Listed in "Table3 Cryptographic operation Relation of Algorithm-Key sizes-Cryptographic operation"***	
[assignment: *cryptographic algorithm*] : ***Listed in "Table3 Cryptographic operation Relation of Algorithm-Key sizes-Cryptographic operation"***	
[assignment: *cryptographic key sizes*] : ***Listed in "Table3 Cryptographic operation Relation of Algorithm-Key sizes-Cryptographic operation"***	
[assignment: *list of cryptographic operation*] : ***Listed in "Table3 Cryptographic operation Relation of Algorithm-Key sizes-Cryptographic operation"***	
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-Key sizes-Cryptographic Operation

List of standards	Cryptographic Algorithm	Cryptographic key sizes	Contents of Cryptographic operation
FIPS PUB 197	***AES***	***- 128 bits*** ***- 192 bits*** ***- 256 bits***	***Encryption of S/MIME transmission data***
SP800-67	***3-Key-Triple-DES***	***- 168 bits***	***Encryption of S/MIME transmission data***
FIPS 186-2	***RSA***	***- 1024 bits*** ***- 2048 bits*** ***- 3072 bits*** ***- 4096 bits***	***Encryption of cryptographic key to encrypt S/MIME transmission data***

6.1.1.2. User Data Protection

FDP_ACC.1[1]	**Subset access control**
FDP_ACC.1.1[1]	
The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].	
[assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*] : ***Listed in "Table4 User box access control operational list "***	
[assignment: *access control SFP*] : ***User Box access control***	
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
A task to act for a user	***User Box***	***- List***
	User Box File	***- 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*** ***- Copy to external memory*** ***- Backup***

FDP_ACC.1[2]	**Subset access control**
FDP_ACC.1.1[2]	
The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].	
[assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*] : ***Listed in "Table 5 Secure print file access control operational list"***	
[assignment: *access control SFP*] : ***Secure print file access control***	
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
A task to act for a user	***Secure Print File***	***- List*** ***- Print*** ***- Back-Up***

FDP_ACC.1[3]	**Subset access control**
FDP_ACC.1.1[3]	
The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].	
[assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*] :	

Listed in "Table6 Setting management access control operational list"		
[assignment: *access control SFP*] : ***Setting management access control***		
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
A task to act for a user	***- SMTP Server Group Object*** ***- DNS Server Group Object*** ***- MFP Address Group Object*** [8] ***- PC-FAX reception setting Object*** ***- Transmission Address Data Object***	***- Settings*** ***- Restore***

FDP_ACC.1[4]	**Subset access control**	
FDP_ACC.1.1[4]		
The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by SFP*].		
[assignment: *list of subjects, objects, and operations among subjects and objects covered by SFP*] : ***Listed in "Table7 ID & print file Access Control operational list"***		
[assignment: *access control SFP*] : ***ID & print file access control***		
Hierarchical to	:	No other components
Dependencies	:	FDP_ACF.1 (FDP_ACF.1[4])

Table 7 ID & Print file Access Control: Operational List

Subject	Object	Operational list
A task to act for a user	***ID & print File***	***- List*** ***- Print*** ***- Backup***

FDP_ACF.1[1]	**Security attribute based access control**
FDP_ACF.1.1[1]	
The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *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*].	
[assignment: *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*] : ***<Subject>*** → ***<Subject attributes>*** ***- A task to act for a user*** → ***- User Attribute (User ID)*** ***- Account Name (Account ID)*** ***- User Box Attribute (User Box ID)*** ***- Administrator Attribute*** --- ***<Object>*** → ***<Object attributes>*** ***- User Box*** → ***- User Attribute (User ID or Public or Account ID)*** ***- User Box File*** → ***- User Box Attribute (User Box ID)***	
[assignment: *access control SFP*] :	

[8] 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.

User Box access control
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: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].
[assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*] : ***<Operation control to Personal user box>*** ***A task to act for a user is permitted to do the list display operation to the user box with the user attribute of an object attribute corresponding to the user attribute (user ID) of the subject attribute.*** ***<Operation control to Group user box>*** ***A task to act for a user is permitted to do the list display operation to the user box with the Account Name of an object attribute corresponding to the Account Name (account ID) of the subject attribute.*** ***<Operation control to Public user box>*** ***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.*** ***<Operational control to User box file>*** ***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, copy to the other user boxes and copy to external memory, 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 of the subject attribute.***
FDP_ACF.1.3[1]
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].
[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects] : ***- A task to act for the user that has an administrator attribute is permitted to operate displaying of user box list.*** ***- A task to act for the user that has an administrator attribute is permitted to operate the back-up the user box file.***
FDP_ACF.1.4[1]
The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes that explicitly deny access of subjects to objects].
[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects] : ***None***
Hierarchical to : No other components Dependencies : FDP_ACC.1 (FDP_ACC.1[1]) , FMT_MSA.3 (FMT_MSA.3[1], FMT_MSA.3[3])

FDP_ACF.1[2] **Security attribute based access control**
FDP_ACF.1.1[2]
The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *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*].
[assignment: *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*] : ***<Subject>*** ***<Subject attributes>*** ***- A task to act for a user*** → ***- File attributes (Secure print internal control ID)*** ***- User attributes (User ID)*** ***- Administrator attributes*** --- ***<Object>*** ***<Object attributes>*** ***- Secure print file*** → ***- File attributes (Secure print internal control ID)***
[assignment: *access control SFP*] :

Secure print file access control
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: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].
[assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*] : ***- A task to act for a user who has a user attribute (user ID) is permitted to display the list of all the secure print files.*** ***- 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).***
FDP_ACF.1.3[2]
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].
[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects] : ***A task to act for a user who has an administrator attribute is permitted to back up secure print file.***
FDP_ACF.1.4[2]
The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].
[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects] : ***None***
Hierarchical to : No other components Dependencies : FDP_ACC.1 (FDP_ACC.1[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: *access control SFP*] to objects based on the following: [assignment: *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*].
[assignment: *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*] : ***<Subject>*** ***<Subject attributes>*** ***- A task to act for a user*** → ***- Administrator attributes*** --- ***<Object>*** ***- SMTP server group object*** ***- DNS server group object*** ***- MFP address group object*** ***- PC-FAX reception setting object*** ***- Transmission Address data object*** **** No Object Attribute***
[assignment: *access control SFP*] : ***Setting management access control***
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: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].
[assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*] : ***- 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, the PC-FAX reception setting object, and the transmission address data object and to operate the restoration.***
FDP_ACF.1.3[3]
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].

[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects] : ***None***
FDP_ACF.1.4[3]
The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].
[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects] : ***None***
Hierarchical to : No other components Dependencies : FDP_ACC.1 (FDP_ACC.1[3]) , FMT_MSA.3 (N/A)

FDP_ACF.1[4]	**Security attribute based access control**

FDP_ACF.1.1[4]
The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of the subjects and objects controlled under the indicated SFP, and for each, SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].
[assignment: *list of the subjects and objects controlled under the indicated SFP, and for each, SFP-relevant security attributes, or named groups of SFP-relevant security attributes*] : ***<Subject>*** ***<Subject attributes>*** ***- A task to act for a user*** → ***- User attributes (user ID)*** ***- Administrator attributes*** --- ***<Object>*** ***<Object attributes>*** ***- ID & print file*** → ***- User attributes (user ID)***
[assignment: *access control SFP*] : ***ID & print file access control***
FDP_ACF.1.2[4]
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].
[assignment: *rules governing access used for controlled operations to controlled objects among controlled subjects and controlled objects*] : ***- A task to act for a user is permitted to list and print the ID & print file whose user attributes of the object attributes are equal to those of the subject attributes (user ID).***
FDP_ACF.1.3[4]
The TSF shall explicitly authorise access of subjects to objects based on the following supplemental rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].
[assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*] : ***A task to act for a user with the administrator attributes is permitted to back up ID & print files.***
FDP_ACF.1.4[4]
The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].
[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*] : ***None***
Hierarchical to : No other components Dependencies : FDP_ACC.1 (FDP_ACC.1[4]) , FMT_MSA.3 (FMT_MSA.3[4])

FDP_IFC.1	**Subset information flow control**

FDP_IFC.1.1
The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*].
[assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*] :

<Subject> ***- Reception from Fax unit*** ***<Information>*** ***- Received data from public line*** ***<Operation>*** ***- Send to internal network***
[assignment: *information flow control SFP*] : ***Fax information flow control***
Hierarchical to : No other components Dependencies : FDP_IFF.1(FDP_IFF.1)

FDP_IFF.1	**Simple security attributes**

FDP_IFF.1.1
The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*].
[assignment: *information flow control SFP*] : ***Fax information flow control***
[assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*] : ***<Subject>*** ***- Reception from Fax unit*** ***<Information>*** ***- Received data from public line*** ***<Security attribute>*** ***- Image data attribute*** ***- Data attribute other than image data***
FDP_IFF.1.2
The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*].
[assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*] : ***Does not send data other than image data received from FAX unit to internal network.***
FDP_IFF.1.3
The TSF shall enforce the [assignment: *additional information flow control SFP rules*].
[assignment: *additional information flow control SFP rules*] : ***None***
FDP_IFF.1.4
The TSF shall explicitly authorise an information flow based on the following rules: [*assignment: rules, based on security attributes, that explicitly authorise information flows*].
[*assignment: rules, based on security attributes, that explicitly authorise information flows*] : ***None***
FDP_IFF.1.5
The TSF shall explicitly deny an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly deny information flows*].
[assignment: *rules, based on security attributes, that explicitly deny information flows*] : ***None***
Hierarchical to : No other components Dependencies : FDP_IFC.1(FDP_IFC.1) , FMT_MSA.3 (N/A)

FDP_RIP.1	**Subset residual information protection**

FDP_RIP.1.1
The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: [assignment: *list of objects*].
[assignment: *list of objects*] : ***- User box files*** ***- Secure print files*** ***- ID & print files*** ***- Stored image files***
[selection: *allocation of the resource to, deallocation of the resource from*] : ***Deallocation of the resource from***
Hierarchical to : No other components Dependencies : No dependencies

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: *[assignment: positive integer number], 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*] : ***- Authentication for accessing the service mode*** ***- Re-authentication for changing the CE password.***
[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] ***[assignment: range of acceptable values] : an administrator configurable positive integer within 1-3***
FIA_AFL.1.2[1]
When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].
[selection: *met, surpassed*] : ***Met***
[assignment: *list of actions*] : ***<Action when it is detected>*** ***- Log out from the authentication status of the service mode if it is, and lock the authentication function which uses the CE password.*** ***- If it's not under the authentication status, lock the authentication function which uses the CE password.*** ***<Operation for recovering the normal condition>*** ***Perform the lock release function of CE authentication by specific operation.*** ***(When time set in the release time setting of operation prohibition for CE authentication passed from specific operation, the release process is performed.)***
Hierarchical to : No other components
Dependencies : FIA_UAU.1 (FIA_UAU.2[1])

FIA_AFL.1[2] Authentication failure handling
FIA_AFL.1.1[2]
The TSF shall detect when [selection: *[assignment: positive integer number], 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*] :

- Authentication for accessing the administrator mode ***- Re-authentication for changing the administrator password***
[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] : ***[assignment: range of acceptable values] : an administrator configurable positive integer within 1-3***
FIA_AFL.1.2[2]
When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].
[selection: *met, surpassed*] : ***Met***
[assignment: *list of actions*] : ***<Action when it is detected>*** ***- Log out from the authentication status of the administrator mode if it is, and lock the authentication function which uses the administrator password.*** ***- If it's not under the authentication status, lock the authentication function which uses the administrator password.*** ***<Operation for recovering the normal condition>*** ***- Perform the boot process of the TOE. (Release process is performed after time set in the release time setting of operation prohibition for Administrator authentication passed by the boot process.)***
Hierarchical to : No other components
Dependencies : FIA_UAU.1 (FIA_UAU.2[2])

FIA_AFL.1[3]	**Authentication failure handling**

FIA_AFL.1.1[3]
The TSF shall detect when [selection: *[assignment: positive integer number], 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*]: ***- Authentication for accessing the MIB object through SNMP***
[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] : ***[assignment: range of acceptable values] : an administrator configurable positive integer within 1-3***
FIA_AFL.1.2[3]
When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].
[selection: *met, surpassed*] : ***Met***
[assignment: *list of actions*] : ***<Action when it is detected>*** ***Deny the access to the MIB object and lock the authentication function to use SNMP password.*** ***<Operation for recovering the normal condition>*** ***- Perform the delete function of authentication failure frequency offered within the administrator mode.***
Hierarchical to : No other components
Dependencies : FIA_UAU.1 (FIA_UAU.2[2])

FIA_AFL.1[4]	**Authentication failure handling**

FIA_AFL.1.1[4]
The TSF shall detect when [selection: *[assignment: positive integer number], 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*] : ***- Authentication for accessing the TOE by user*** ***- Re-authentication when a user changes his/her own user password***

[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] **:** ***[assignment: range of acceptable values] : an administrator configurable positive integer within 1-3***
FIA_AFL.1.2[4]
When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the TSF shall [assignment: *list of actions*].
[selection: *met, surpassed*] : ***Met***
[assignment: *list of actions*] : ***<Action when it is detected>*** ***- While authentication is performed, log out from the authentication status of the user, and lock the authentication function for the user.*** ***- Otherwise, lock the authentication function for using the user password.*** ***<Operation for recovering the normal condition>*** ***- Perform the delete function of authentication failure frequency offered within the administrator mode.***
Hierarchical to : No other components
Dependencies : FIA_UAU.1 (FIA_UAU.1[1])

FIA_AFL.1[5]	**Authentication failure handling**

FIA_AFL.1.1[5]
The TSF shall detect when [selection: *[assignment: positive integer number], 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*] : ***Authentication for accessing the secure print file***
[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] : ***[assignment: range of acceptable values] : an administrator configurable positive integer within 1-3***
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: *met, surpassed*] : ***Met***
[assignment: *list of actions*] : ***<Action when it is detected>*** ***Deny the access to the secure print file and lock the authentication function for the secure print file.*** ***<Operation for recovering the normal condition>*** ***- Perform the delete function of authentication failure frequency offered within the administrator mode.***
Hierarchical to : No other components
Dependencies : FIA_UAU.1 (FIA_UAU.2[3])

FIA_AFL.1[6]	**Authentication failure handling**

FIA_AFL.1.1[6]
The TSF shall detect when [selection: *[assignment: positive integer number], 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*]. : ***- Authentication for accessing a public user box*** ***- Re-authentication when a user authorized to access a public user box changes the user box password of the public user box***
[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] : ***[assignment: range of acceptable values] : an administrator configurable positive integer within 1-3***

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: *met, surpassed*] : ***Met***
[assignment: *list of actions*] : ***<Action when it is detected>*** ***- While authentication is performed, log out from the authentication status of the user box, and lock the authentication function for the concerned user box.*** ***- Otherwise, lock the authentication function which uses the user box password.*** ***<Operation for recovering the normal condition>*** ***- Perform the delete function of authentication failure frequency offered within the administrator mode.***
Hierarchical to : No other components
Dependencies : FIA_UAU.1 (FIA_UAU.2[4])

FIA_AFL.1[7]	**Authentication failure handling**

FIA_AFL.1.1[7]
The TSF shall detect when [selection: *[assignment: positive integer number], 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*] : ***- Account authentication: Account authentication when the belonging account of the user who accesses in the synchronized method is not registered.*** ***- Account authentication: Account authentication of the user who accesses in the method not synchronized.***
[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] : ***[assignment: range of acceptable values] : an administrator configurable positive integer within 1-3***
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*] : ***Met***
[assignment: *list of actions*] : ***<Action when it is detected>*** ***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.*** ***<Operation for recovering the normal condition>*** ***Perform the delete function of authentication failure frequency offered within the administrator mode.***
Hierarchical to : No other components
Dependencies : FIA_UAU.1 (FIA_UAU.1[2])

FIA_AFL.1[8]	**Authentication failure handling**

FIA_AFL.1.1[8]
The TSF shall detect when [selection: *[assignment: positive integer number], 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*] : ***- Authentication when it accesses service mode from the panel*** ***- Authentication when it accesses administrator mode from the panel*** ***- User authentication when user accesses TOE from the panel*** ***- Account authentication when user accesses TOE from the panel*** ***- Authentication when it accesses secure print file from the panel***

- Authentication when it accesses Public user box from the panel
[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] : ***[assignment: positive integer number] : 1***
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*] : ***Met***
[assignment: *list of actions*] : ***<Action when it is detected>*** ***Deny all access from the panel.*** ***<Operation for recovering the normal condition>*** ***Automatically release the lock after 5 seconds.***
Hierarchical to : No other components
Dependencies : FIA_UAU.1(FIA_UAU.2[1], FIA_UAU.2[2], FIA_UAU.1[1], FIA_UAU.2[3], FIA_UAU.2[4], FIA_UAU.1[2])

FIA_ATD.1	**User attribute definition**

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*] : ***- User attributes (User ID)*** ***- User box attributes (User box ID)*** ***- File attributes (Secure print internal control ID)*** ***- Account name (Account ID)*** ***- Administrator Attribute***
Hierarchical to : No other components
Dependencies : No dependencies

FIA_SOS.1[1]	**Verification of secrets**

FIA_SOS.1.1[1]
The TSF shall provide a mechanism to verify that secrets ***(User Password, Administrator Password, CE Password, secure print password, user box password, and account password)*** meet [assignment: *a defined quality metric*].
[assignment: *a defined quality metric*] : ***- Number of digits: 8 or more and up to 64-digits*** ***- Character type: possible to choose from 94 or more characters*** ***- Rule :*** ***(1) Do not compose by only one and the same character.*** ***(2) Do not set the same password as the current setting after change.***
Hierarchical to : No other components
Dependencies : No dependencies

FIA_SOS.1[2]	**Verification of secrets**

FIA_SOS.1.1[2]
The TSF shall provide a mechanism to verify that secrets ***(SNMP Password)*** meet [assignment: *a defined quality metric*].
[assignment: *a defined quality metric*] : ***- Number of digits: 8 or more and up to 32-digits*** ***- Character type: possible to choose from 90 or more characters*** ***- Rule :***

	(1) Do not compose by only one and the same character. ***(2) Do not set the same password as the current setting after change.***
Hierarchical to :	No other components
Dependencies :	No dependencies

FIA_SOS.1[3]	**Verification of secrets**
FIA_SOS.1.1[3]	
The TSF shall provide a mechanism to verify that secrets ***(Encryption passphrase)*** meet [assignment: *a defined quality metric*].	
[assignment: *a defined quality metric*] : ***- Number of digits: 20- digits*** ***- Character type: possible to choose from 83 or more characters*** ***- Rule :*** ***(1) Do not compose by only one and the same character.*** ***(2) Do not set the same passphrase as the current setting after change.***	
Hierarchical to :	No other components
Dependencies :	No dependencies

FIA_SOS.1[4]	**Verification of secrets**
FIA_SOS.1.1[4]	
The TSF shall provide a mechanism to verify that secrets ***(Session Information)*** meet [assignment: *a defined quality metric*].	
[assignment: *a defined quality metric*]: ***10^{10} and above***	
Hierarchical to :	No other components
Dependencies :	No dependencies

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

FIA_UAU.1[1]	**Timing of authentication**
FIA_UAU.1.1[1]	
The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.	
[assignment: *list of TSF mediated actions*] ***Confirm the stopped state of user's use (Method of user authentication: Machine authentication only)***	

FIA_UAU.1.2[1]		
The TSF shall require each user ***(User)*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user ***(User)***.		
Hierarchical to	:	No other components
Dependencies	:	FIA_UID.1(FIA_UID.2[3])

FIA_UAU.1[2]	**Timing of authentication**

FIA_UAU.1.1[2]
The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.
[assignment: *list of TSF mediated actions*] ***Confirm the stopped state of the account.***
FIA_UAU.1.2[2]
The TSF shall require each user ***(User who is permitted to use account)*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user ***(User who is permitted to use account)***.
Hierarchical to : No other components
Dependencies : FIA_UID.1(FIA_UID.2[3])

FIA_UAU.2[1]	**User authentication before any action**

FIA_UAU.2.1[1]		
The TSF shall require each user ***(Service Engineer)*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user ***(Service Engineer)***.		
Hierarchical to	:	FIA_UAU.1
Dependencies	:	FIA_UID.1 (FIA_UID.2[1])

FIA_UAU.2[2]	**User authentication before any action**

FIA_UAU.2.1[2]		
The TSF shall require each user ***(Administrator (User who is authenticated by Administrator password, User who is authenticated by SNMP password))*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user ***(Administrator (User who is authenticated by Administrator password, User who is authenticated by SNMP password))***.		
Hierarchical to	:	FIA_UAU.1
Dependencies	:	FIA_UID.1 (FIA_UID.2[2])

FIA_UAU.2[3]	**User authentication before any action**

FIA_UAU.2.1[3]		
The TSF shall require each user ***(User who is permitted to use secure print file)*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user ***(User who is permitted to use secure print file)***		
Hierarchical to	:	FIA_UAU.1
Dependencies	:	FIA_UID.1 (FIA_UID.2[4])

FIA_UAU.2[4]	**User authentication before any action**

FIA_UAU.2.1[4]
The TSF shall require each user ***(User who is permitted to use the public user box)*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user ***(User who is permitted to use the public user box)***

Hierarchical to	:	FIA_UAU.1
Dependencies	:	FIA_UID.1 (FIA_UID.2[5])

FIA_UAU.6	**Re-authenticating**

FIA_UAU.6.1
The TSF shall re-authenticate the user under the conditions [assignment: *list of conditions under which re-authentication is required*].
[assignment: *list of conditions under which re-authentication is required*] ***- When the service engineer modifies the CE password.*** ***- When the administrator modifies the administrator password.*** ***- When the user modifies his/her user password.*** ***- When a user permitted to use a public user box modifies the user box password of the public user box.***

Hierarchical to	:	No other components
Dependencies	:	No dependencies

FIA_UAU.7	**Protected authentication feedback**

FIA_UAU.7.1
The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.
[assignment: *list of feedback*] : ***Display "*" every character data input.***

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

FIA_UID.2[1]	**User identification before any action**

FIA_UID.2.1[1]
The TSF shall require each user ***(Service Engineer)*** to be successfully identified before allowing any other TSF-mediated actions on behalf of that user ***(Service Engineer).***

Hierarchical to	:	FIA_UID.1
Dependencies	:	No dependencies

FIA_UID.2[2]	**User identification before any action**

FIA_UID.2.1[2]
The TSF shall require each user ***(Administrator)*** to be successfully identified before allowing any other TSF-mediated actions on behalf of that user ***(Administrator).***

Hierarchical to	:	FIA_UID.1
Dependencies	:	No dependencies

FIA_UID.2[3]	**User identification before any action**

FIA_UID.2.1[3]
The TSF shall require each user ***(User)*** to be successfully identified before allowing any other TSF-mediated actions on behalf of that user ***(User).***

Hierarchical to	:	FIA_UID.1
Dependencies	:	No dependencies

FIA_UID.2[4]	**User identification before any action**

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

FIA_UID.2[5]	**User identification before any action**

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

FIA_UID.2[6]	**User identification before any action**

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

FIA_UID.2[7]	**User identification before any action**

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

FIA_USB.1	**User-subject binding**

FIA_USB.1.1
The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment; *list of user security attributes*].
[assignment; *list of user security attributes*]: ***- User attributes (User ID)*** ***- User box attributes (User box ID)*** ***- File attributes (Secure print internal control ID)*** ***- Account name (Account ID)*** ***- Administrator Attribute***
FIA_USB.1.2
The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*].
[assignment: *rules for the initial association of attributes*]: ***<User box attribute>*** ***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.*** ***<Account Name>*** ***- 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.***

- 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. ***<File attribute>*** ***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.*** ***<User attribute>*** ***The user ID of the concerned user associates to the task acting on the behalf of users when authenticated as the user.*** ***<Administrator attribute>*** ***The Administrator's attributes associate to the task acting on the behalf of users when authenticated as the Administrator.***
FIA_USB.1.3
The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *rules for the changing of attributes*].
[assignment: *rules for the changing of attributes*]. ***None***
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: *determine the behavior of, disable, enable, modify the behavior of*] the functions [assignment: *list of functions*] to [assignment: *the authorized identified roles*].
[assignment: *list of functions*] : ***- Enhanced Security Setting***
[selection: *determine the behavior of, disable, enable, modify the behavior of*] : ***disable***
[assignment: *the authorized identified roles*] : ***- Administrator*** ***- Service Engineer***
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 behaviour**
FMT_MOF.1.1[2]
The TSF shall restrict the ability to [selection: *determine the behavior of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorized identified roles*].
[assignment: *list of functions*] : ***- User Authentication Function*** ***- S/MIME function*** ***- SNMP password authentication function*** ***- ID & print function*** ***- HDD data overwrite deletion function*** ***- Audit log function***
[selection: *determine the behavior of, disable, enable, modify the behavior of*] : ***modify the behavior of***
[assignment: *the authorized identified roles*] : ***Administrator***
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: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorized identified roles*].	
[assignment: *list of functions*] : ***- Account Authentication Function (For administrator)*** ***- Trusted Channel Function***	
[selection: *determine the behavior of, disable, enable, modify the behaviour of*] : ***modify the behavior of, disable***	
[assignment: *the authorized identified roles*] : ***Administrator***	
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: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorized identified roles*].	
[assignment: *list of functions*] : ***- All area overwrite deletion function***	
[selection: *determine the behavior of, disable, enable, modify the behaviour of*] : ***Enable***	
[assignment: *the authorized identified roles*] : ***Administrator***	
Hierarchical to :	No other components
Dependencies :	FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2])

FMT_MOF.1[5]	**Management of security functions behavior**
FMT_MOF.1.1[5]	
The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorized identified roles*].	
[assignment: *list of functions*] : ***- Account Authentication Function (For user)***	
[selection: *determine the behavior of, disable, enable, modify the behaviour of*] : ***modify the behavior of***	
[assignment: *the authorized identified roles*] : ***User who is permitted to use that account***	
Hierarchical to :	No other components
Dependencies :	FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[6])

FMT_MSA.1[1]	**Management of security attributes**
FMT_MSA.1.1[1]	
The TSF shall enforce the [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete*, [assignment: *other operations*]] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorized identified roles*].	
[assignment: *list of security attributes*] : ***User attributes of the user box that is set user's own [user ID].***	
[selection: *change_default, query, modify, delete*, [assignment: *other operations*]] :	

***Modify* (modify to other user's [User ID], [account ID] or [public])**		
[assignment: *the authorized identified roles*] : ***- User*** ***- Administrator***		
[assignment: *access control SFP, information flow control SFP*] : ***User box access control***		
Hierarchical to	:	No other components
Dependencies	:	FDP_ACC.1 or FDP_IFC.1 (FDP_ACC.1[1]) , FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2], FMT_SMR.1[3])

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

FMT_MSA.1[3]		**Management of security attributes**
FMT_MSA.1.1[3]		
The TSF shall enforce the [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete*, [assignment: *other operations*]] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorized identified roles*].		
[assignment: *list of security attributes*] : ***User attributes of user box that is set the [Account ID].***		
[selection: *change_default, query, modify, delete*, [assignment: *other operations*]] : ***modify* (modify to [user ID], [public] or other [account ID])**		
[assignment: *the authorized identified roles*] : ***- User who is permitted to use that account*** ***- Administrator***		
[assignment: *access control SFP, information flow control SFP*] : ***User box access control***		
Hierarchical to	:	No other components
Dependencies	:	FDP_ACC.1 or FDP_IFC.1 (FDP_ACC.1[1]) , FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2], FMT_SMR.1[6])

FMT_MSA.3[1]	**Static attribute initialization**
FMT_MSA.3.1[1]	
The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes (***User attributes of the user box***) that are used to enforce the SFP.	

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

FMT_MSA.3[2]	**Static attribute initialization**

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

FMT_MSA.3[3]	**Static attribute initialization**

FMT_MSA.3.1[3]
The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes (***User box attributes of user box file***) that are used to enforce the SFP.
[selection, choose one of: *restrictive, permissive, [assignment: other property]*] : ***[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.***
[assignment: *access control SFP, information flow control SFP*] : ***User box access control***
FMT_MSA.3.2[3]
The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.
[assignment: *the authorized identified roles*] ***None***
Hierarchical to : No other components
Dependencies : FMT_MSA.1 (N/A) , FMT_SMR.1 (N/A)

FMT_MSA.3[4]	**Static attribute initialization**
FMT_MSA.3.1[4]	
The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection: choose one of: *restrictive, permissive, [assignment: other property]*] default values for the security attributes (***User attributes of ID & print file***) that are used to enforce the SFP.	
[selection: choose one of: *restrictive, permissive, [assignment: other property]*] : ***[assignment: other property]: Shall be equal to the values of the user attributes of the user who stores that ID & print file.***	
[assignment: *access control SFP, information flow control SFP*] : ***ID & print file access control***	
FMT_MSA.3.2[4]	
The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.	
[assignment: *the authorized identified roles*] ***None***	
Hierarchical to	: No other components
Dependencies	: FMT_MSA.1 (N/A) , FMT_SMR.1 (N/A)

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

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

FMT_MTD.1[3]	**Management of TSF data**
FMT_MTD.1.1[3]	
The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].	
[assignment: *list of TSF data*] :	

- User ID ***- Account ID*** ***- Account password*** ***- Secure print password*** ***- System auto reset time*** ***- Threshold Number of authentication failure*** ***- External server authentication setting data*** ***- S/MIME certificate[9]*** ***- Belonging Account of User*** ***- Release time of operation prohibition for Administrator authentication*** ***- Encryption passphrase*** ***- SNMP password*** ***- TSI receiving setting data***
[selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] : ***Modify***
[assignment: *the authorized identified roles*] : ***Administrator***
Hierarchical to : No other components
Dependencies : FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2])

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

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

FMT_MTD.1[6] **Management of TSF data**
FMT_MTD.1.1[6]

[9] It intends the operation of replacing a settable digital certificate for each user in stead of the modification of the value itself.

The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].
[assignment: *list of TSF data*] : ***Administrator password***
[selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] : ***modify***
[assignment: *the authorized identified roles*] : ***- Administrator*** ***- Service Engineer***
Hierarchical to : No other components
Dependencies : FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[1], FMT_SMR.1[2])

FMT_MTD.1[7]	**Management of TSF data**

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

FMT_MTD.1[8]	**Management of TSF data**

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

FMT_MTD.1[9]	**Management of TSF data**

FMT_MTD.1.1[9]
The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].
[assignment: *list of TSF data*] : ***- CE password*** ***- Release time of operation prohibition for CE authentication***
[selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] : ***modify***
[assignment: *the authorized identified roles*] : ***Service Engineer***

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

FMT_MTD.1[10]	**Management of TSF data**

FMT_MTD.1.1[10]

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

[assignment: *list of TSF data*] :
User ID

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

[assignment: *the authorized identified roles*] :
Administrator, External server

Hierarchical to	:	No other components
Dependencies	:	FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2], FMT_SMR.1[5])

FMT_MTD.1[11]	**Management of TSF data**

FMT_MTD.1.1[11]

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

[assignment: *list of TSF data*] :
- Account ID
- Account password
- S/MIME certificate
- Data of TSI reception setting
- Data of external server authentication setting

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

[assignment: *the authorized identified roles*] :
Administrator

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

FMT_MTD.1[12]	**Management of TSF data**

FMT_MTD.1.1[12]

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

[assignment: *list of TSF data*] :
Belonging Account of a user oneself

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

[assignment: *the authorized identified roles*]:
Administrator, the user who is permitted to use of the account[10]

Hierarchical to	:	No other components
Dependencies	:	FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2], FMT_SMR.1[6])

FMT_MTD.1[13]	**Management of TSF data**

FMT_MTD.1.1[13]

[10] 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.

The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].		
[assignment: *list of TSF data*] : ***User ID*** ***Account ID***		
[selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] : ***[assignment: other operations] : Pause and resume***		
[assignment: *the authorized identified roles*]: ***Administrator***		
Hierarchical to	:	No other components
Dependencies	:	FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2], FMT_SMR.1[5])

FMT_MTD.1[14]	**Management of TSF data**

FMT_MTD.1.1[14]		
The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].		
[assignment: *list of TSF data*] : ***Audit log***		
[selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] : ***query, delete***		
[assignment: *the authorized identified roles*]: ***Administrator***		
Hierarchical to	:	No other components
Dependencies	:	FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2])

FMT_MTD.1[15]	**Management of TSF data**

FMT_MTD.1.1[15]		
The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].		
[assignment: *list of TSF data*] : ***Date and time information***		
[selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] : ***modify***		
[assignment: *the authorized identified roles*]: ***Administrator***		
Hierarchical to	:	No other components
Dependencies	:	FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2])

FMT_SMF.1	**Specification of Management Functions**

FMT_SMF.1.1
The TSF shall be capable of performing the following management functions: [assignment: *list of management functions to be provided by the TSF*].
[assignment: *list of management functions to be provided by the TSF*] : ***- Stop Function of Enhanced security function by administrator*** ***- Operation setup function of ID & print 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*** [11]

[11] A part of the backup function corresponds to the inquiry function of TSF data.

- *Restoration Function by administrator* [12]
- *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-out 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*
- *Registration function of user box by administrator*
- *Modification function of user attributes of the user box by the administrator*
- *Registration function of user ID by administrator*
- *Stop function of user by administrator*
- *Resume function of user by administrator*
- *Stop function of account by administrator*
- *Resume function of account 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*
- *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 Release time of operation prohibition for Administrator authentication by administrator*
- *Modification function of Encryption passphrase by administrator*
- *Modification function of TSI receiving setting data by administrator*
- *Operation setting function of HDD data overwrite deletion function by administrator*
- *All area overwrite deletion function by administrator*
- *Operation function of audit log by administrator*
- *Operation setting function when audit log is full by administrator*
- *Modification function of date and time information by administrator*
- *Modification function of CE password by service engineer*
- *Modification function of administrator password by service engineer*
- *Stop function of Enhanced Security function by service engineer*
- *Modification function of Release time of operation prohibition for CE authentication by service engineer*
- *Overwrite function for the default value of the user attribute of the user box by the user.*
- *Operation method setting function of user's own account authentication function when method of account authentication is set for each user by 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*
- *Registration function of Belonging Account of user oneself by user who is permitted the use of the account*
- *User box registration function by user*
- *Automatic Personal user box registration function by user box stored job that specifies unregistered box by user*
- *Machine non-registered users' user ID automatic registration function with external server when user authentication method is external server authentication*
- *Registration function of secure print password according to secure print file registration by user*
- *Modification function of user attribute of user box by user who is permitted the use of public user box*

[12] A part of the restoration function corresponds to the modification function of TSF data.

- Modification function of user box password of the user box by user who is permitted the use of public user box
- Modification function of the concerned user box's user attribute by user who is permitted the use of the group user box
Hierarchical to : No other components
Dependencies : No dependencies

FMT_SMR.1[1] **Security roles**
FMT_SMR.1.1[1]
The TSF shall maintain the roles [assignment: *the authorised identified roles*].
[assignment: *the authorised identified roles*] : ***Service Engineer***
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])

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

FMT_SMR.1[3] **Security roles**
FMT_SMR.1.1[3]
The TSF shall maintain the roles [assignment: *the authorised identified roles*].
[assignment: *the authorised identified roles*] : ***User***
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])

FMT_SMR.1[4] **Security roles**
FMT_SMR.1.1[4]
The TSF shall maintain the roles [assignment: *the authorised identified roles*].
[assignment: *the authorised identified roles*] : ***User who is permitted to use that public user box***
FMT_SMR.1.2[4]
The TSF shall be able to associate users with roles.
Hierarchical to : No other components
Dependencies : FIA_UID.1 (FIA_UID.2[5])

FMT_SMR.1[5] **Security roles**
FMT_SMR.1.1[5]

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

FMT_SMR.1[6]	**Security roles**

FMT_SMR.1.1[6]
The TSF shall maintain the roles [assignment: *the authorised identified roles*].
[assignment: *the authorised identified roles*] : ***The user who is permitted to use of the account***
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

FTA_SSL.3	**TSF-initiated termination**

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

6.1.1.6. Trusted Path/Channel

FTP_ITC.1	**Inter-TSF trusted channel**

FTP_ITC.1.1
The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2
The TSF shall permit [selection: *the TSF, another trusted IT product*] to initiate communication via the trusted channel.
[selection : *the TSF, another trusted IT product*] ***The other trusted IT product***
FTP_ITC.1.3
The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].
[assignment : *list of functions for which a trusted channel is required*] ***- Download of the user box file.*** ***- Upload of the image file that will be stored as a user box file.*** ***- Upload of the image file that will be the secure print file.*** ***- Upload of the image file that will be the ID & Print file.***
Hierarchical to : No other components

Dependencies	:	No dependencies

6.1.1.7. Security Audit

FAU_GEN.1	**Audit data generation**
FAU_GEN.1.1	
The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and c) [assignment: *other specifically defined auditable events*].	
[selection, choose one of: *minimum, basic, detailed, not specified*] ***not specified***	
[assignment: *other specifically defined auditable events*]: ***Listed in "Table 8 Auditable events list"***	
FAU_GEN.1.2	
The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].	
[assignment: *other audit relevant information*]: ***Listed in "Table 8 Auditable events list"***	
Hierarchical to	: No other components
Dependencies	: FPT_STM.1

Table 8 Auditable events list

Auditable events	Relevant functional requirement	Audit Level	Additional Information
Start and end of job (necessary to be audited)	***FDP_ACF.1***	***not specified***	***Type of job***
Success or failure of all authentication functions	***FIA_UAU.2***	***basic***	***None***

FAU_GEN.2	**User identity association**
FAU_GNE.2.1	
For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.	
Hierarchical to	: No other components
Dependencies	: FAU_GEN.1 FIA_UID.1 (FIA_UID.2[1], FIA_UID.2[2], FIA_UID.2[3], FIA_UID.2[4], FIA_UID.2[5], FIA_UID.2[6])

FAU_SAR.1	**Audit review**
FAU_SAR.1.1	
The TSF shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of audit information*] from the audit records.	
[assignment: *authorised users*]: ***Administrator***	

[assignment: *list of audit information*]: ***Audit log listed in "Table 8 Auditable events list"***		
FAU_SAR.1.2		
The TSF shall provide the audit records in a manner suitable for the user to interpret the information.		
Hierarchical to	:	No other components
Dependencies	:	FAU_GEN.1

FAU_SAR.2	**Restricted audit review**

FAU_SAR.2.1		
The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.		
Hierarchical to	:	No other components
Dependencies	:	FAU_SAR.1

FAU_STG.1	**Protected audit trail storage**

FAU_STG.1.1		
The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.		
FAU_STG.1.2		
The TSF shall be able to [selection, choose one of: *prevent, detect*] unauthorised modifications to the stored audit records in the audit trail.		
[selection, choose one of: *prevent, detect*]: ***prevent***		
Hierarchical to	:	No other components
Dependencies	:	FAU_GEN.1

FAU_STG.4[1]	Prevention of audit data loss

FAU_STG.4.1[1]		
The TSF shall [selection, choose one of: *"ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*] and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full **(if the audit trail is full, in the state where operation when the audit trail was full was set as "overwrite prohibition")**.		
[selection, choose one of: *"ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*]: ***ignore audited events***		
[assignment: *other actions to be taken in case of audit storage failure*]: ***Stop accepting jobs***		
Hierarchical to	:	No other components
Dependencies	:	FAU_STG.1

FAU_STG.4[2]	Prevention of audit data loss

FAU_STG.4.1[2]		
The TSF shall [selection, choose one of: *"ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*] and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full **(if the audit trail is full, in the state where operation when the audit trail was full was set as "overwrite permission")**.		
[selection, choose one of: *"ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*]: ***overwrite the oldest stored audit records***		
[assignment: *other actions to be taken in case of audit storage failure*]: ***none***		
Hierarchical to	:	No other components

Dependencies	:	FAU_STG.1

FPT_STM.1	Reliable time stamps
FPT_STM.1	
The TSF shall be able to provide reliable time stamps.	
Hierarchical to	: No other components
Dependencies	: No. dependencies

6.1.1.8. Extension: Capability of Using IT Environment Entity

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

FIT_CAP.1[2]	**Capability of using security service of IT environment entity**
FIT_CAP.1.1[2]	
TSF shall provide the necessary capability to use the service for [assignment: *security service provided by IT environment entity*]. : [assignment: *necessary capability list for the operation of security service*]	
[assignment: *security service provided by IT environment entity*] : ***HDD encryption function achieved by ASIC***	
[assignment: *necessary capability list for the operation of security service*] : ***Support function of the image file processing by HDD encryption function***	
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 9 TOE Security Assurance Requirements

TOE Security Assurance Requirements		Component
ADV: Development	Security architecture description	ADV_ARC.1

TOE Security Assurance Requirements		Component
	Functional specification with complete summary	ADV_FSP.3
	Architectural design	ADV_TDS.2
AGD: Guidance documents	Operational user guidance	AGD_OPE.1
	Preparative procedures	AGD_PRE.1
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
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
ATE: Tests	Analysis of coverage	ATE_COV.2
	Testing: basic design	ATE_DPT.1
	Functional testing	ATE_FUN.1
	Independent testing - sample	ATE_IND.2
AVA: Vulnerability Assessment	Vulnerability analysis	AVA_VAN.2

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 10 Conformity of IT Security Functional Requirements to Security Objectives

Security Objectives / Security Functional Requirements	O.REGISTERED-USER	O.PRIVATE-BOX	O.PUBLIC-BOX	O.GROUP-BOX	O.SECURE-PRINT	O.CONFIG	O.OVERWRITE	O.CRYPTO-KEY	O.TRUSTED-PATH	O.CRYPTO-MAIL	O.FAX-CONTROL	O.AUTH-CAPABILITY	O.CRYPTO-CAPABILITY	O.AUDIT-LOGGED	* set.admin	* set.service
set.admin	X	X	X	X	X	X										
set.service	X	X	X	X	X	X										
FAU_GEN.1														X		

Security Objectives / Security Functional Requirements	O.REGISTERED-USER	O.PRIVATE-BOX	O.PUBLIC-BOX	O.GROUP-BOX	O.SECURE-PRINT	O.CONFIG	O.OVERWRITE	O.CRYPTO-KEY	O.TRUSTED-PATH	O.CRYPTO-MAIL	O.FAX-CONTROL	O.AUTH-CAPABILITY	O.CRYPTO-CAPABILITY	O.AUDIT-LOGGED	* set.admin	* set.service
FAU_GEN.2														X		
FAU_SAR.1														X		
FAU_SAR.2														X		
FAU_STG.1														X		
FAU_STG.4														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_ACC.1[4]					X	X										
FDP_ACF.1[1]		X	X	X		X										
FDP_ACF.1[2]					X	X										
FDP_ACF.1[3]						X										
FDP_ACF.1[4]					X	X										
FDP_IFC.1											X					
FDP_IFF.1											X					
FDP_RIP.1							X									
FIA_AFL.1[1]																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	X	X									X	X
FIA_SOS.1[2]						X										
FIA_SOS.1[3]	X															
FIA_SOS.1[4]						X										
FIA_SOS.2	X		X												X	
FIA_UAU.2[1]																X
FIA_UAU.2[2]						X									X	
FIA_UAU.1[1]	X															
FIA_UAU.2[3]					X											
FIA_UAU.2[4]			X													
FIA_UAU.1[2]				X												
FIA_UAU.6	X		X			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										

Security Objectives / Security Functional Requirements	O.REGISTERED-USER	O.PRIVATE-BOX	O.PUBLIC-BOX	O.GROUP-BOX	O.SECURE-PRINT	O.CONFIG	O.OVERWRITE	O.CRYPTO-KEY	O.TRUSTED-PATH	O.CRYPTO-MAIL	O.FAX-CONTROL	O.AUTH-CAPABILITY	O.CRYPTO-CAPABILITY	O.AUDIT-LOGGED	* set.admin	* set.service
FMT_MOF.1[2]	X				X	X										
FMT_MOF.1[3]				X		X										
FMT_MOF.1[4]						X										
FMT_MOF.1[5]				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_MSA.3[4]					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_MTD.1[13]	X			X												
FMT_MTD.1[14]						X										
FMT_MTD.1[15]						X										
FMT_SMF.1	X	X	X	X	X	X									X	X
FMT_SMR.1[1]						X									X	X
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												
FPT_STM.1														X		
FTA_SSL.3	X														X	
FTP_ITC.1									X							
FIT_CAP.1[1]												X				
FIT_CAP.1[2]													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 permitted user)**

This security objective limits the utilization of MFP installing TOE to only the user who succeeded in identification and authentication, and needs various requirements regarding user identification and authentication.

<Necessary requirement for identification and authentication of the user>
It identifies and authenticates that the user who accesses is a permitted user by FIA_UID.2 [3] and FIA_UAU.1 [1].
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 [4] 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 system auto reset time elapses with FTA_SSL.3. when it logs in from the panel. The change in the system auto reset 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, pause and resumption of use in the user registration is permitted to the administrator by FMT_MTD.1 [10] and FMT_MTD.1 [13]. 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 registration and change operation of an external server setting is limited to only the administrator by FMT_MTD.1 [3] and FMT_MTD.1 [11].

The quality of the user password is verified by FIA_SOS.1 [1]. 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]. In addition, when a user changes his/her own user password, the user is re-authenticated by FIA_UAU.6.

<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 authenticated, the user ID is associated with 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 associated with 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 and administrator to give the initial value to change the public attribute. 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.
  As for the user box attribute of the user box file, the value consistent with the user box

attribute of the user box which was selected as the file saved is set up 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 [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 function 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 regarding access control.

<User box access control (a public user box)>
After the user has been identified and authenticated, the user ID is associated with 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 on the user attributes 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 [4] 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 setup 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 [4] 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 and the administrator to operate the change of the user attribute of user 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 [1] verifies the quality of the user box password. If a user permitted to use a public user box changes the user box password of the public user box, FIA_UAU.6 re-authenticates the user.
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 and administrator to give the initial value to change the user attribute. 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 user box only to the user who is permitted the use of the account. It also limits the set of the group user box which is not a pause status of use and the operation of the user function of the user box file in the group user 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 authenticated, the user ID is associated with the task of acting a use by FIA_ATD.1 and FIA_USB.1. And after the account has been authenticated, the account ID is associated with 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 which is not a pause status of use. When the Account authentication method is "the method not synchronized", FIA_UID.2 [6] and FIA_UAU.1 [2] 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.1 [2] 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 setup 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] permit 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.

<Management of the group user 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 and 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].

<Management of the subject attribute related with the group user box>
FMT_MTD.1[11] and FMT_MTD.1[13] restricts the registration, pause of use and resumption of use 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 [1] 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 (for administrator) and the stop operation management only to the administrator.
On FMT_MOF.1[3], the administrator selects the operation method of the account authentication function (for administrator) to “user set,” and so the operation method of the account authentication function is left to the account authentication function (for user).
FMT_MOF.1[5] restricts the behavior management of the account authentication function (for user) to the user self who is permitted to use that account. However, FMT_MOF.1[5] is the subset of FMT_MOF.1[3] and the settings do not compete.

<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 (Access control of secure print file and ID & 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 authenticated, the user ID is associated with 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 file 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 [3] 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 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 setup 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 stored.

<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 [1] verifies the quality of the secure print password.

Next, for ID & print file, this security objective limits the print of the ID & print file only for the user who stored that file, so that various requirements regarding access control are necessary.

<ID & print file access control>
FDP_ACC.1[4] and FDP_ACF.1[4] permit the task substituting for a user with a user ID to

list and print the ID & print file with the user attribute consistent with the user ID.
For the user attribute set in the ID & print file, the user ID of the user who stores the file when the file is stored is set by FMT_MSA.3 [4].

<Operation management of the ID & print function>
Management of this operation mode is limited only to the administrator by FMT_MOF.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 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 setting of SMTP server group object, DNS server group object, MFP address group object, PC-FAX reception setting object, and transmission address data object.

<Operation limitation of Backup and restoration function>
When the administrator attribute is associated with 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].
- the ID & print files by FDP_ACC.1 [4] and FDP_ACF.1 [4].

In addition, the restoration operation is permitted for
- SMTP server group object, DNS server group object, MFP address group object, PC-FAX operation setting object, and transmission address data object by FDP_ACC.1[3] and FDP_ACF.1[3].

Moreover, the restoration operation (modification operation) is permitted only to the administrator for the following data:
- 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 the operation setting data of SNMP password authentication function by FMT_MOF.1[2].
- the Trusted Channel setting data, encryption passphrase and the operation setting data of account authentication function by FMT_MOF.1[3].
- the users 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 system auto reset 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 belonging account of user, release time of operation prohibition for administrator authentication, and TSI receiving setting by FMT_MTD.1[3].
- 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, and the account password.

<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.

<Management of encryption passphrase >
FMT_MTD.1 [3] permits only administrator the modification operation to the encryption passphrase. FIA_SOS.1 [3] verifies the quality of 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 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 of 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 is permitted only to the administrator by FMT_MTD.1 [11]. The modification of the registered S/MIME certificate is permitted only to the administrator by FMT_MTD.1 [3]. In addition, the setup of transmission address data is permitted only to the administrator by FDP_ACC.1 [3] and FDP_ACF.1 [3]. The behavior of the S/MIME function is permitted only to the administrator by the FMT_MOF.1 [2].

<Operational Limit for FAX function>
The registration of the user box to be stored in TSI reception (TSI reception setting) is permitted only to the administrator by FMT_MTD.1 [11]. The modification of the registered TSI reception setting is permitted only to the administrator by FMT_MTD.1 [3]. In addition, the setting of the area stored when PC-FAX is received (PC-FAX reception setting) is permitted only to the administrator by FDP_ACC.1 [3] and FDP_ACF.1 [3].

<Operational Limit of deletion method of HDD data overwrite deletion function>
The deletion method of HDD data overwrite deletion function is limited the operation only to the administrator by FMT_MOF.1[2].

<Operational Limit of All area overwrite deletion function>
The start up of all area overwrite deletion function is permitted only to the administrator by FMT_MOF.1[4].

<Operational Limit of Audit Log>
The inquiry and deletion operation of audit log is permitted only to the administrator by FMT_MTD.1[14].

<Operational Limit of Operation setup of the Audit log when it is full>
The operational setting of the audit log when it is full is permitted only to the administrator by FMT_MOF.1[2].

<Operational Limit of Date/time information>
The modification of Date/time information is permitted only to the administrator by FMT_MTD.1[15].

<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 (Overwrite deletion)**

  This security objective regulates that it deletes image data area of the protected assets stored in HDD 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.

  Therefore, this security objective is satisfied.

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

  This security objective regulates that the encryption key necessary to encrypt image data written in HDD by ASIC is generated, and needs various requirements that relate to the encryption key generation.

  Using Konica Minolta HDD encryption key generation algorism according to the Konica Minolta encryption specification standard, FCS_CKM.1 generates an encryption key 256 bits long. In addition, the encryption key is generated on RAM that is a volatility memory with the power supply ON and is disappeared with the power supply OFF.

  This security objective is satisfied by this functional requirement.

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

  This security objective generates the Trusted Channel in the transmission and reception such as a user box file, a secure print file, and an ID & 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, the secure print file, and the ID & print file.

  This security objective is satisfied by this functional 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 (128, 168, 192 or 256 bits) by using Pseudorandom number Generation Algorithm according to FIPS 186-2.

  FCS_COP.1 encrypts the user box file by using AES (encryption key: 128, 192 or 256 bits) 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: 168 bits) of SP800-67. (By the same token, it becomes a transmission data of S/MIME.) FCS_COP.1 encrypts these encryption keys by RSA of FIPS 186-2 by using a public key of S/MIME certificate of each destination (1024, 2048, 3072 or 4096 bits).

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

- **O. FAX-CONTROL (Fax unit control)**

  This security objective regulates to prohibit an access to internal network which the MFP concerned connects with, from public line via the Fax public line portal.

  This means that communication, like remote diagnostic function or illegal operation command, except image data which is sent from public line network and forwarded to internal network via MFP is not forwarded to internal network, and various requirements related to the flow control of Fax unit are necessary.

  Applying FDP_IFC.1 and FDP_IFF.1, the flow control not to send data, except the image data

which the reception function from a public line received, to internal network is achieved.
This security objective is satisfied by this functional requirement.

- **O.AUTH-CAPABILITY (Support action to use user authentication function)**
  This security objective regulates that TOE supports the user authentication function using an user information management server that is the entity outside TOE, and needs various requirements that regulate to support the external entity action.
  Applying FIT_CAP.1 [1], the inquiry and the acquirement function for the identification and authentication objective user are achieved for the user authentication function by the Active Directory of the user information management server.
  This security objective is satisfied by this functional requirement.

- **O.CRYPTO-CAPABILITY (Support action to use the HDD encryption function)**
  This security objective regulates that TOE supports the action to encrypt the data stored in HDD by ASIC that is the entity outside TOE, and needs various requirements that regulates to support the external entity action.
  Applying FIT_CAP.1[2], a support function to process image data in HDD through the HDD encryption function implemented by ASIC is achieved for that HDD encryption function.
  This security objective is satisfied by this functional requirement.

- **O.AUDIT-LOGGED (Acquisition and management of Audit log)**
  This security objective regulates that TOE maintains the generation of the audit log related to all authentication functions and to all jobs necessary to be audited, and protects the audit log from a person who does not have the authority of disclosure or change, and needs requirement that relates to the audit log.
  Applying FAU_GEN.1 and FAU_GEN.2, the function to generate the audit log related to all authentication functions and jobs, necessary to be audited, applying FAU_SAR.1,FAU_SAR.2, FAU_STG.1, FAU_STG.4[1], FAU_STG.4[2], the function to protects the audit log from a person who does not have the authority of disclosure or change are achieved.
  In order to provide user information and date/time information that are necessary for the audit information, this is supported by FIA_UID.2[1], FIA_UID.2[2], FIA_UID.2[3], FIA_UID.2[4], FIA_UID.2[5], FIA_UID.2[6] and FPT_STM.1
  This security objective is satisfied by this functional 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 an 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] logs out 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 release time of operation prohibition for administrator authentication 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 and change of the release time of operation prohibition for 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 system auto reset time elapses by FTA_SSL.3. if it logs in from the panel. The change in the system auto reset 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.1[4] 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] logs out 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 release time of operation prohibition for administrator authentication 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] logs out 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 release time of operation prohibition for CE authentication elapses, 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 release time of operation prohibition for CE authentication.

<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 CE authentication lock release function is executed and the release time of operation prohibition for CE authentication elapses, so that this lock status is released.

<Role and management function for each management>
FMT_SMR.1 [1] maintains the role to do these managements as a service engineer. FMT_SMF.1 specifies these management functions.

6.2.1.3. Dependencies of IT Security Functional Requirements

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

Table 11 Dependencies of 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
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2[1], FIA_UID.2[2], FIA_UID.2[3] FIA_UID.2[4], FIA_UID.2[5], FIA_UID.2[6]
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4	FCS_COP.1 (only partial event) <The reason not to fulfill partially FCS_CKM.2 or FCS_COP.1> The cryptographic operation is performed using key generated by Konica Minolta HDD cryptographic key generation algorithm in the IT environment by FIT_CAP.1[1]. TSF only uses this capability, and there is no necessity of the distribution and cryptographic operation. <The reason not to apply FCS_CKM.4> The encryption key temporarily exists in the volatile memory area, but there is no necessity of the encryption key cancellation since it is automatically destroyed without the necessity of access from the outside.
FCS_COP.1	FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2, FCS_CKM.4	FCS_CKM.1 (only partial event) The satisfied events: The encryption key for enciphering the attached file by the S/MIME communication is generated.

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
		<The reason not to satisfy a part of the FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2> - 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. - 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. - 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 dependency is not satisfied. <The reason not apply FCS_CKM.4> The encryption key temporarily exists in the volatile memory area, but there is no necessity of the encryption key cancellation since it is automatically destroyed without the necessity of access from the outside.
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_ACC.1[4]	FDP_ACF.1	FDP_ACF.1[4]
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.
FDP_ACF.1[4]	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1[4] FMT_MSA.3[4]
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1 <The reason not to apply FMT_MSA.3> There is no necessity for applying this requirement because the security attribute is initialized on the outside.

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
FDP.RIP.1	None	N/A
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.1[1]
FIA_AFL.1[5]	FIA_UAU.1	FIA_UAU.2[3]
FIA_AFL.1[6]	FIA_UAU.1	FIA_UAU.2[4]
FIA_AFL.1[7]	FIA_UAU.1	FIA_UAU.1[2]
FIA_AFL.1[8]	FIA_UAU.1	FIA_UAU.2[1], FIA_UAU.2[2], FIA_UAU.1[1], FIA_UAU.2[3], FIA_UAU.2[4], FIA_UAU.1[2]
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.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.1[1]	FIA_UID.1	FIA_UID.2[3]
FIA_UAU.2[3]	FIA_UID.1	FIA_UID.2[4]
FIA_UAU.2[4]	FIA_UID.1	FIA_UID.2[5]
FIA_UAU.1[2]	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.1[1], FIA_UAU.2[3], FIA_UAU.2[4], FIA_UAU.1[2]
FIA_UID.2[1]	None	N/A
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_MOF.1[4]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[2]
FMT_MOF.1[5]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[6]
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]

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
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.
FMT_MSA.3[4]	FMT_MSA.1, FMT_SMR.1	Neither is applicable. <The reason not to apply FMT_MSA.1> It is the concept of ID & print that the object is a print object to which only the person who stored it can access, so it is not assumed that the object is transferred to any other user. Consequently, it is not necessary to change the value of the attribute when the user performs operations other than store, so that the management requirement is unnecessary. <FMT_SMR.1> The assignment of FMT_MSA.3.2[4] 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_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_SMF.1,

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
	FMT_SMR.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_MTD.1[13]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]
FMT_MTD.1[14]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]
FMT_MTD.1[15]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]
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]
FPT_STM.1	None	N/A
FTA_SSL.3	None	N/A
FTP_ITC.1	None	N/A
FIT_CAP.1[1]	None	N/A
FIT_CAP.1[2]	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 TOE 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 Table 12 below. The detailed specification is explained in the paragraphs described below.

Table 12 Names and Identifiers 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, ID & print function
7	F.CRYPTO	Encryption key generation function
8	F.RESET	Authentication Failure Frequency Reset function
9	F.TRUSTED-PATH	Trusted Channel function
10	F.S/MIME	S/MIME encryption processing function
11	F.FAX-CONTROL	Fax unit control function
12	F.SUPPORT-AUTH	External Server authentication operation support function
13	F.SUPPORT-CRYPTO	ASIC support function
14	F.OVERWRITE	HDD data overwrite deletion function
15	F.AUDIT-LOGGED	Audit log 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.

- Provides the administrator authentication mechanism authenticating by the administrator password that consists of the character shown in Table 13.
  - Provides 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 of authentication function is released.

As described above, FIA_AFL.1[2], FIA_AFL.1[8], FIA_SOS.1[4], FIA_SOS.2. FIA_UAU.2[2], FIA_UAU.7 and FIA_UID.2[2] are realized.

Table 13 Characters and Number of Digits for Password [13]

Objectives	Number of digits	Characters
User Password CE Password Administrator Password Account Password User Box Password	8 - 64	Selectable from 161 or more characters in total (Alphabet, numeric, and symbols (Some are not included.), Special characters (Some are not included.))
Encryption passphrase	20	Selectable from 83 or more characters in total (Alphabet, numeric, and symbols (Some are not included.)
Secure Print Password	8- 64	Selectable from 94 or more characters in total (Alphabet, numeric, symbols (Some are not included.))
SNMP Password - Privacy Password - Authentication Password	8 - 32	Selectable from 90 or more characters in total (Alphabet, numeric, and symbols (Some are not included.)

7.1.2. Auto Logout Function of Administrator Mode

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

As described above, FIA_SSL.3 is realized.

7.1.3. Function Supported 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 attribute 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.

[13] Table 12 shows the minimum password space as the security specification. Therefore, although some excluded characters are shown depending on the password type, the excluded characters are permitted to use if possible.

7.1.3.1. Change of Administrator Password

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

- Provides the administrator authentication mechanism that is authenticated by the administrator password which consists of the character shown in Table 13.
- 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.
- When the authentication failure that becomes 1-3 times at total in each authentication function by using the administrator password is detected, it logouts the administrator mode accessing, 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, 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 administrator password of Table 13.
  - 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 Setup

- 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[14], 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 user password of the Table 13.
  - 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

[14] 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 a case in which plural sets of authentication server information are included in the external server information setting data.

satisfied the following qualities.

- It is composed of the characters and by the number of digits, shown in the user password of the Table 13.
- It shall not be composed of one kind of character.
- It shall not be equal to the value which is currently set.

- User deletion
  User ID and user password are deleted.
  - When a personal user box that a concerned user owns exists, it is selected whether that personal user box is set to the public user box of "user attributes: public" or it is deleted.

- Pause/resume of User (Only in the machine authentication as User authentication method.)
  Specify the User ID and pause the user or resume the user in the pause state. The user in the pause state is not identified and not authenticated, so that the user cannot use the user function after identification and authentication.

- Change of the belonging account
  The belonging account that related to user is changed

As described above, FIA_SOS.1[1], FMT_MTD.1[1], FMT_MTD.1[2], FMT_MTD.1[3], FMT_MTD.1[10], FMT_MTD.1[12], FMT_MTD.1[13], FMT_SMF.1 and FMT_SMR.1[2] are realized.

7.1.3.3. User Box Setup

- User Box Registration
  When the administrator attribute is related, the view of the list of user boxes is permitted. A personal user box, a group user box, and a public user box are registered by selecting the user attribute to the non-registration user box ID selected from the list of user boxes. When they are registered, “public” is specified on the user attribute of the user box by default, however, a user ID or an account ID can be selected.
  - 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 user box password of the Table 13.
    - 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 user box password of the Table 13.
    - It shall not be composed of one kind of character.
    - It shall not be equal to the value which is currently set.

- 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.
    - If a user box password is not registered at the same time, the password shall be registered, and the same processing as the change of user box password mentioned above is performed.

As described above, FDP_ACC.1[1], FDP_ACF.1[1], FIA_SOS.1[1], 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 (clear all) the number of times of authentication failure for each users.
  - If there is a user to whom access is locked, the lock is released.
- Reset (clear all) the number of times of authentication failure for all secure print passwords.
  - If there is a secure print password to which access is locked, the lock is released.
- Reset (clear all) the number of times of authentication failure of each user boxes.
  - If there is a user box to which access is locked, the lock is released.
- Reset (clear all) the number of times of authentication failure of each account.
  - If there is a user account to which access is locked, the lock is released.
- Reset (clear all) the number of times of authentication failure of SNMP password.
  - If the access to a MIB object 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. Setup 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 (for administrator) : synchronized method
  The method which utilizes an account ID associated with user ID beforehand.
- Account authentication function (for administrator) : 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 associated with user ID beforehand.

- Account authentication function (for administrator) : not use
  Utilize only the authentication function by user ID, and not utilize the identification and authentication by account information.
- Account authentication function (for administrator) : Synchronize by User
  Registered user sets “Synchronize or Do Not synchronize” for User Authentication & Account Track.

As described above, FMT_MOF.1 [2], FMT_MOF.1[3], FMT_MTD.1[3], FMT_MTD.1[11], FMT_SMF.1 and FMT_SMR.1[2] are realized.

7.1.3.6. Unauthorized Access Setup

- Setup of unauthorized access detection threshold
  The unauthorized access detection threshold in the authentication operation prohibition function is set for 1-3 times.
- Setup of the release time of operation prohibition for Administrator Authentication
  Set the release time of operation prohibition for Administrator Authentication 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. Setup of Auto Logout Function

The system auto reset time which is the setting data of the auto logout function should be set within the following time range.

- System auto reset 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 Setup

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, SSD and HDD are backed-up and re-stored except the administrator password, the CE 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

<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
- System auto reset time
- User ID
- User attribute of user box
- Account ID
- S/MIME certificate
- Transmission address data
- Encryption strength setting data in S/MIME function
- SSL certificate
- Belonging Account of user
- Release time of operation prohibition for Administrator authentication
- PC-FAX reception 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
- ID & print file

As described above, FDP_ACC.1[1], FDP_ACC.1[2], FDP_ACC.1[3], FDP_ACC.1[4], FDP_ACF.1[1], FDP_ACF.1[2] , FDP_ACF.1[3], FDP_ACF.1[4], 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 Setup of HDD Encryption Function

<Encryption Passphrase Change>

The encryption passphrase is changed. It is changed when the newly setup encryption passphrase satisfies quality requirements, and F.CRYPTO is performed

- Verify that the encryption passphrase newly set satisfies the following qualities.
  - It is composed of the characters and by the number of digits shown in the encryption passphrase of the Table 13.
  - 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[3], FMT_MTD.1[3], FMT_SMF.1 and FMT_SMR.1[2] are realized.

7.1.3.11. Change of SNMP Password

The SNMP password (Privacy password and Authentication password) is changed. This is performed when the newly setup password satisfies quality requirements.

- Verifies that the SNMP password which is newly set satisfies the following qualities.
  - It is composed of the characters and by the number of digits shown in SNMP password of the Table 13.
  - 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[2], FMT_MTD.1[3], FMT_SMF.1, and FMT_SMR.1[2] are realized.

7.1.3.12. Setup 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.

7.1.3.13. Account Setup

- 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 the account password of the Table 13.
  - 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 the account password of the Table 13.
  - It shall not be composed of one kind of character.
  - It shall not be matched to the current setting.

- Account deletion

  Account ID and account password are deleted.
  - When the group user box of the account ID exists, it is selected weather that group user box is set to the public user box of "user attributes: public" or it is deleted.

- Pause/resume of Account

  Account ID is specified, and the use of the account is paused or the use of the account in the pause state is resumed. The account in the pause state is not done the identification and

authentication, and becomes impossible to use the user function to need the identification and authentication of account.

As described above, FIA_SOS.1[1], FMT_MSA.1[3], FMT_MTD.1[3], FMT_MTD.1[11], FMT_MTD.1[13], FMT_SMF.1 and FMT_SMR.1[2] are realized.

7.1.3.14. Setup 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.

7.1.3.15. Setup 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
- Setup of Encryption Strength for S/MIME function

As described above, FDP_ACC.1[3], FDP_ACF.1[3], FMT_MOF.1[2], FMT_MTD.1[3], FMT_MTD.1[11], FMT_SMF.1, and FMT_SMR.1[2] are realized.

7.1.3.16. Setup of FAX

Set the setting data of FAX related settings as follows,

- PC-FAX reception Setting
  - Setting either of two modes at PC-FAX operation which are to store in each user box and to store in common area for all users according to the designated information at FAX transmission.
- TSI reception Setting
  - Setting the storing user box at TSI reception by relating the transmitter's telephone number with the user 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_MTD.1[11], FMT_SMF.1 and FMT_SMR.1[2] are realized.

7.1.3.17. Function Related to Enhanced Security Function

The function that influences the setup 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.)

- Operational setup of Enhanced Security function
  Function to set valid or invalid of Enhanced Security function.

Other than the operational setup of Enhanced Security function, the setting could be invalid by executing the followings; HDD logical format function, all area overwrite deletion function, etc. These operations are limited to all administrators.

As described above, FMT_MOF.1[1], FMT_SMF.1 and FMT_SMR.1[2] are realized.

7.1.3.18. Function Related 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.

7.1.3.19. Operational Setup of the ID & Print Function

The operation modes of the ID & print function are set up as follows:

- ID & print automatic operation mode
  An operation mode that stores a print file sent from a client PC as an ID & print file even if printing is requested by the normal print setup.
- ID & print specified operation mode
  An operation mode that stores a print file sent from a client PC as an ID & print file only when it is requested to store that file as an ID & print file.

As described above, FMT_MOF.1[2], FMT_SMF.1, and FMT_SMR.1[2] are realized.

7.1.3.20. Operational Setup of the HDD data overwrite deletion Function

This sets the deletion methods of the HDD data overwrite deletion function to “Mode1” or “Mode2”. (Refer to table 15 for details of “Mode1” and “Mode2”)
As described above, FMT_MOF.1[2], FMT_SMF.1, and FMT_SMR.1[2] are realized.

7.1.3.21. Function Related to the Audit Log Function

- Access and delete of Audit log
  This exports the audit log obtained by the audit log function. (Audit log is deleted at the time of export.) Also, there is the deletion operation of audit log other than the deletion by the export operation. Both are operated only by administrator.
- Operational setup when the audit log is full
  Either is set up for the operation of audit log when it is full; “Permit Overwrite” setting to overwrite from the oldest audit log, “Prohibit overwrite” setting to stop the acceptance of job.

As described above, FMT_MOF.1[2], FMT_MTD.1[14], FMT_SMF.1, and FMT_SMR.1[2] are realized.

7.1.3.22. Setting of date and time information

- Set the date and time information. The date and time information is set only by administrator.

If each value is not in the value in a parenthesis, the setting cannot be determined; Year (00-37), Month (01-12), Day (01-31), Hour (00-23), Minute (00-59). Also, refer to the time function in MFP and time information of NTP server, that administrator sets.

As described above, FMT_MTD.1[15], FMT_SMF.1, FMT_SMR.1[2], and FPT_STM1are realized.

7.1.3.23. All Area Overwrite Deletion Function

All Area Overwrite Deletion Function executes the overwrite deletion in the data area of HDD, and initializes the settings such as passwords on NVRAM and SSD as well. The object for the deletion or the initialization is as follows.

<Object for the deletion: HDD>
- Secure print file
- User box file
- ID & print file
- Stored image file
- Transmission address data file
- User ID
- User password
- User box password
- Secure print password
- Account ID
- Account password
- S/MIME certificate
- SSL certificate

<Object for the initialization: NVRAM, SSD>
- Administrator Password
- SNMP password
- Encryption passphrase --- Encryption Passphrase is deleted, and the operational setting of HDD encryption function is turned OFF.

The deletion methods such as the data overwritten in HDD and the writing frequency is executed according to the deletion method of the overall area overwrite deletion function set by F.ADMIN (Table 15). For the HDD encryption function, the encryption passphrase which was set is disabled by turning off the operational setup. The setup of the Enhanced Security function becomes invalid in the execution of this function. (Refer to the description for the operational setup of the Enhanced Security function in F.ADMIN.)

As described above, FAD_RIP.1, FMT_MOF.1[4], FMT_SMF.1, and FMT_ SMR.1[2] is realized.

Table 14 Types and Methods of Overwrite Deletion of Overall Area

Method	Overwritten data type and their order

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

7.2. 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

- Provides the SNMP authentication mechanism which authenticates by the SNMP password that consists of the character shown in Table 13.
  - 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 fail in authentication, it is detected as one failure.
- 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 below is permitted to be done.

(1) Network Setup

Setup 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 the SNMP password of the Table 13.
- This password is not composed of one character only.
- This password is not matched to the currently setup password.

As described above, FIA_SOS.1[2], FMT_MTD.1[3] , FMT_SMF.1 and FMT_SMR.1[2] are realized.

(3) Setup 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.

- Provides the CE authentication mechanism that is authenticated by the CE password that consists of the character shown in Table 13.
  - 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 Supported 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.

7.3.2.1. Change of CE Password

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

- Provides the CE authentication mechanism that is re-authenticated by the CE password that consists of the characters shown in Table 13.
- Resets the authentication failure frequency when succeeding in the re-authentication.
- Return "*" for each character as feedback for the entered CE password 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 logouts 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 unlocks 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 CE password of the Table 13.
  - 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.

7.3.2.2. 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 administrator password of the Table 13.
- 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.

7.3.2.3. Setup of the release time of operation prohibition for CE Authentication

Set the release time of operation prohibition for CE Authentication between 5 - 60 minutes.
As described above, FMT_MTD.1[9], FMT_SMF.1 and FMT_SMR.1[1] are realized.

7.3.2.4. Function Related 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 initial 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
  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 and SSD to the factory default. The setup 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 provides 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 Authentication Function

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

When the access request for the user box and the store request for the secure print file, it is identified and authenticated to be a permitted 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.

- 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 operation setting of the authentication operation prohibition function.
- The lock of authentication function is released by performing the lock release function to the concerned user of F.ADMIN.

As described above, FIA_AFL.1[4], FIA_AFL.1[8], FIA_ATD.1, FIA_UAU. 1[1], FIA_UAU.7 FIA_UID.2[3] and FIA_USB.1 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_SMF.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 store request for the secure print file, it is identified and authenticated to be a permitted 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.

- Provides account authentication mechanism that is authenticated the account by the account password that consists of the characters shown in Table 13.
- 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 operation setting of the authentication operation prohibition function.
- The lock of the authentication function is released by performing the lock release function to the concerned account of F.ADMIN.

As described above, FIA_AFL.1[7], FIA_AFL.1[8], FIA_ATD.1, FIA_UAU.1[2], FIA_UAU.7 FIA_UID.2[6] and FIA_USB.1 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.

- Provides the user authentication mechanism that authenticates the user by the user password that consists of the characters shown in Table 13.
  - After the user is authenticated to the access from the network, the user authentication mechanism using session information besides the user password is provided.
  - 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}.

As described above, FIA_ATD.1, FIA_SOS.1[4], FIA_SOS.2 and FIA_USB.1 are realized.

<Account authentication: User identification and authentication when it does not used>

When the access request for the user box and the store request of the secure print file, it is identified and authenticated to be a permitted user. The detail of the user authentication is the same as account authentication: user identification and authentication in the synchronized method. The use of F.BOX and F.PRINT is permitted to the user who is identified and authenticated.

As described above, FIA_AFL.1[4], FIA_AFL.1[8], FIA_ATD.1, FIA_UAU. 1[1], FIA_UAU.7 FIA_UID.2[3] 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 authentication method, the identified and authenticated user is registered as a 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. Operation Method Setup Function of Account Authentication Function

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

- Account Authentication Function (for user): synchronized method
  The method which utilizes an account ID associated with user ID beforehand.
- Account Authentication Function (for user): 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 associated with user ID beforehand.

As described above, FMT_MOF.1[5], FMT_SMF.1 and FMT_SMR.1[6] are realized.

7.4.3. Auto Logout 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 logout time", it logs out from a user identification and authentication domain automatically.

As described above, FTA_SSL.3 is realized.

7.4.4. 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.

The user password is changed when it is re-authenticated that the user is a user and the newly setup password satisfies the quality.

- Provides user authentication mechanism that is authenticated the user by the user password that consists of the characters shown in Table 13.
- Resets the number of authentication failure when succeeding in the re-authentication.
- Return "*" for each character as feedback for the entered user password, in the case of access from the panel at the re-authentication.

- When the authentication failure that becomes 1-3 times at total for the concerned account is detected by each authentication function utilizing the user password, all the authentication functions utilizing the user password of the user are locked out. (Login by the user is denied. Change operation of the user password is denied.)
  - The administrator specifies the failure frequency threshold by the unauthorized access detection threshold setting function.
- The lock of the authentication function is released by performing the lock release function to the concerned account of F.ADMIN
- Changed when the user password newly set satisfies the following qualities.
  - It is composed of the characters and by the number of digits, shown in the user password of the Table 13.
  - It shall not be composed of one kind of character.
  - This password is not matched to the currently setup password.

As described above, FIA_AFL.1[4], FIA_SOS.1[1], FIA_UAU.6, FIA_UAU.7, FMT_MTD.1[2], FMT_SMF.1, and FMT_SMR.1[3] are realized.

7.5. F.BOX (User Box Function)

F.BOX permits a user who was identified and authenticated as a permitted user to operate and manage his/her personal user box. When the account authentication is used, F.BOX permits the user to operate and manage the group user box associated with the account to which the user belongs. F.BOX is a series of security function such as the access control function allowing that the user is permitted to use the public user box when he/she tries to access that public user box and permitting various operations of the public user box and the user box files after the authentication succeeds.

<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 user box password of the Table 13.
  - 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[1], 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 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.

<Storing of user box file>

- In the new storing 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

7.5.1.1. 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.

7.5.1.2. Access Control Function to User Box File in Personal User Box

When the user box to operate is selected, "User Box ID" of the user box is associated with 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, the copy operations to other user boxes, and the copy operations to an external memory.

As described above, FIA_ATD.1, FIA_USB.1, FDP_ACC.1[1] and FDP_ACF.1[1] are realized.

7.5.1.3. User Attribute Change of 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 satisfies the following requirements.
  - It is composed of the characters and by the number of digits shown in the user box password of the Table 13.
  - 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[1], 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 permitted 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.)

7.5.2.1. Authentication Function in Access to 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.

- Provides the user box authentication mechanism that is authenticated by the user box password that consists of the character shown in Table 13.
- After the user box is authenticated to the access from the network, it provides the user box authentication mechanism using the session information besides the user box password.
  - According to protocol, it utilizes the 10^{10} session information or more, or generated and uses the 10^{10} 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[4], FIA_SOS.2, FIA_UAU.2[4], 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 provided in the user box identification and authentication domain of the user box.

7.5.2.2. Access Control to User Box File in 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, the WebDAV transmission, download, the movement to other user boxes, the copy operations to other user boxes, and the copy operations to an external memory.

As described above, FIA_ATD.1, FIA_USB.1, FDP_ACC.1[1] and FDP_ACF.1[1] are realized.

7.5.2.3. User attribute change of 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.

7.5.2.4. Change of Public User Box Password

The user box password of the public user box is changed. This is performed when it is re-authenticated that the user has a permission to use the public user box and the user box password newly set satisfies the following quality:

- Provides the user box authentication mechanism which authenticates the user by user box password consisting of the characters shown in Table 13.
- Resets the number of authentication failure when succeeding in the re-authentication.
- Return "*" for each character as feedback for the entered user box password, in the case of access from the panel at the re-authentication.
- When the authentication failure that becomes 1-3 times at total for the concerned public user box is detected by each authentication function utilizing the user box password, all the authentication functions utilizing the user box password of the public user box are locked out. (Deny the login of the public user box. Deny the change operation of the user box password of the public user box.)
  - 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.
- Changed when the user box password newly set satisfies the following qualities.
  - It is composed of the characters and by the number of digits, shown in the user password of the Table 13.
  - It shall not be composed of one kind of character.
  - This password is not matched to the currently setup password.

As described above, FIA_AFL.1[6], FIA_SOS.1[1], FIA_UAU.6, FIA_UAU.7, FMT_MTD.1[4], FMT_SMF.1, and FMT_SMR.1[4] are realized.

7.5.3. Group User Box Function

7.5.3.1. 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 associated with 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.

7.5.3.2. Access Control Function to User Box File in Group User Box

When the user box to operate is selected, "User Box ID" of the user box is associated with 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, the copy operations to other user boxes, and the copy operations to an external memory.

As described above, FIA_ATD.1, FIA_USB.1, FDP_ACC.1 [1] and FDP_ACF.1[1] are realized.

7.5.3.3. User Attribute Change of Group User Box

The user attributes can be changed.

- If another account ID is specified, it becomes a group user box that the user of another Account Name can access.
- 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 the user box password of the Table 13.
  - 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 [1], FMT_MSA.1[3], FMT_SMF.1 and FMT_SMR.1[6] are realized.

7.6. F.PRINT (Secure Print Function, ID & Print Function)

F.PRINT is a security function related to the secure print function and ID & print function.

It provides 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.

Moreover, for the user who was identified and authenticated as a permitted user, when ID & print files are accessed from the panel, F.PRINT provides the access control function that allows the printing and displaying the list of only the ones stored by the user.

7.6.1. Secure Print Function

7.6.1.1. Authentication Function by Secure Print Password

When the user is identified and authenticated as the permitted user, it authenticates that the accessing user is a user to whom the use of the secure print file is permitted, in response to the access request to each secure print file.

- Provides the secure print authentication mechanism that is authenticated by the secure print password that consists of the character shown in Table 13.
- 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[3], FIA_UAU.7 and FIA_UID.2[4] are realized.

7.6.1.2. Access Control Function to 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.

7.6.1.3. Registration Function of Secure Print File

When it is authenticated as a permitted user in the store request of the secure print file, the user is permitted to register the secure print password with the concerned secure print file.

- 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 13.
  - It shall not be composed of one kind of character.

- Giving of the secure print internal control ID
  When the verification of the secure print password is completed in a store 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_SOS.1 [1], FMT_MSA.3[2], FMT_MTD.1[8], FMT_SMF.1 and FMT_SMR.1[3] are realized.

7.6.2. ID & print Function

7.6.2.1. ID & Print File Registration Function

For the storing request of ID & print file, if the user is authenticated as a registered user, ID & print file is stored.

- The user ID of the user who tries to store the file is set as a user attribute of that ID & print file.

As described above, FIA_MSA.3 [4] is realized,

7.6.2.2. ID & Print File Access Control Function

When the user is authenticated, the ID & print file access control operates.

- The task substituting for the identified and authenticated user has a user ID as a user attribute.

- This task is allowed to list and print ID & print files with the user attribute which is equal to this user attribute.

As described above, FIA_ATD.1, FIA_USB.1, FDP_ACC.1[4], and FDP_ACF.1[4] are realized,

7.7. F.CRYPT (Encryption Key Generation Function)

F.CRYPT generates an encryption key to encrypt image data written in HDD by using the Konica Minolta HDD encryption key generation algorithm that is regulated by the Konica Minolta encryption specification standard.

When the encryption passphrase is decided in the HDD encryption functional operation setting to which the access is restricted in F.ADMIN, an encryption key 256 bits long is generated from the encryption passphrase by applying the Konica Minolta HDD encryption key generation algorithm.

As described above, FCS_CKM.1 is realized.

7.8. 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 the release time of operation prohibition for CE authentication.

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 release time of operation prohibition for Administrator authentication.

As described above, FIA_AFL.1[2] is realized.

7.9. F.TRUSTED-PATH (Trust Channel Function)

F.TRUSTED-PATH 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)
- Image file that will be stored as an ID & print file (upload from client PC to MFP)

As described above, FTP_ITC.1 is realized.

7.10. 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 128, 168, 192 or 256 bits.)

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 (128, 192 and 256 bits) to encrypt the user box file.
- It is encrypted by the 3-Key-Triple-DES which SP800-67 provides by using the encryption key (168 bits) to encrypt the user box file.

As described above, FCS_COP.1 is realized.

<Encryption of User box files 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, 2048, 3072 or 4096 bits.

As described above, FCS_COP.1 is realized.

7.11. F.FAX-CONTROL (FAX Unit Control Function)

F.FAX-CONTROL is the function that prohibits an access to internal network connected to MFP through the FAX unit by TOE control.

TOE controls the function that transfer the data received from public line to internal LAN. The prohibition of access (data forwarding except image data) from public line to internal network is realized by TOE control.

As described above, FDP_IFC.1 and FDP_IFF.1 are realized.

7.12. F.SUPPORT-AUTH (External Server Authentication Operation Support Function)

F.SUPPORT-AUTH is the function that realizes the user authentication function in cooperation with the user information management server of Active Directory. (the function that operates with F.USER.)

When the “external server authentication” is selected for user authentication method, the inquiry for the authentication information 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 authentication information returned back from user information management server.

As described above, FCS_CAP.1 [1] is realized.

7.13. F.SUPPORT-CRYPTO (ASIC Support Function)

F.SUPPORT-CRYPTO is the function that operates the HDD encryption function that utilizes ASIC from TOE.

For image data written in HDD, an encryption key generated by F.CRYPTO is set in ASIC,

and encryption is performed by the ASIC. On the other hand, for the encrypted data read out of the HDD, the encryption key generated by F.CRYPTO is set in ASIC in the same manner as above, and decryption is performed by the ASIC.

As described above, FCS_CAP.1 [2] is realized.

7.14. F.OVERWRITE (HDD Data Overwrite Deletion Function)

F.OVERWRITE executes the overwrite deletion in the data area in order not to be able to use the image data unnecessary in HDD again.

- The image data that is the object for the overwrite deletion is as follows. Also, the following image files that are stored in the HDD temporary area and the swap area are the objects for the overwrite deletion.
  - User box file
  - Secure print file
  - ID & print file
  - Stored image file

- The operating timing of the overwrite deletion is as follows.
  - When job such as print or scan is completed or stopped
  - When the data becomes unnecessary to be kept by the deletion operation
  - When the remaining information exists in the temporary area and swap area when the power is on at the time of the unexpected power-off.
- The deletion methods such as the data overwritten in HDD and the writing frequency is executed according to the deletion method of the HDD data overwrite deletion function set by F.ADMIN(Table 15).

As described above, FAD_RIP.1 is realized.

Table 15 Types and Methods of Overwrite Deletion of Temporary data

Method	Overwritten data type and their order
Mode:1	0x00
Mode:2	0x00 → 0xFF → 0x61 → Verification

7.15. F.AUDIT-LOGGED (Audit log function)

F.AUDIT-LOGGED is the function to generate audit record log when the auditable event related to security occurred. This generates the record of following events.

(1) Start-up / Shut-down
This obtains the record of start up and end of MFP and the record of ON/OFF of the audit log function.

(2) Start and end of job (necessary to be audited)

This obtains the operation logs of user box file, secure print file and ID & print file which are the protected assets registered in MFP. These operations are necessary to be audited and the record of the start and end timing is obtained.

- User box file

  Jobs related to the user box file are as follows. The record of following jobs is obtained.
  - ✧ Panel job
    Save in User box from the operation panel in Copy, Scan and User Box mode
  - ✧ Saved job in User box via driver / network
    Save in User box through the printer driver or network
  - ✧ Saved job in User box via USB / Bluetooth
    Save in User box through USB or Bluetooth
  - ✧ Saved job in FAX RX user box
    Save in User box through Fax-receiving
  - ✧ Output job from User box
    Print from the operation panel in User box mode. Send from the operation panel and network in User box mode.
- Secure Print file, ID & Print file

  Jobs related to the secure print file and ID & Print file are as follows. The record of following job is obtained.
  - ✧ Saved job in user box via driver and network
    Save in User box through the printer driver or network
  - ✧ Output job from User box
    Print from the operation panel

(3) Success and failure of all authentication function
- Administrator / CE Identification authentication
- User authentication, account track
- Public user box authentication
- Secure print access authentication

.

Also, “Date / time information” “User ID” “Job name (job type)” and “Result” are recorded as the log obtained item. The Date / time information that is set by the administrator by F.ADMIN is recorded. The administrator is able to export log file through the network and the log is deleted when it’s exported. User other than administrator cannot perform the export and deletion of log. When the audit record becomes full, it is overwritten from the oldest audit log in order or prohibited the behavior of TOE. This behaves according to the setup of F.ADMIN.

As described above, FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, and FAU_STG.4 are realized.

---End---