bizhub 754e / bizhub 654e
PKI Card System Control Software
Security Target

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

Version: 1.01

Issued on: February 24, 2014

Created by: KONICA MINOLTA, INC.

<Revision History>

Date	Ver.	Division	Approved	Checked	Created	Revision
2013/06/10	1.00	Office Products System Control Development Div.1	Nabeshima	Nakata	Chiba	Initial Version.
2014/02/24	1.01	Office Products System Control Development Div.1	Nabeshima	Nakata	Chiba	Deal with typos.

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

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

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

1. ST Introduction

1.1. ST Reference

- ST Title	:	bizhub 754e / bizhub 654e PKI Card System Control Software Security Target
- ST Version	:	1.01
- Created on	:	February 24,2014
- Created by	:	KONICA MINOLTA, INC.

1.2. TOE Reference

- TOE Name	:	bizhub 754e / bizhub 654e PKI Card System Control Software
- TOE Version	:	A55V0Y0-0100-G00-60pki
- 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 754e / bizhub 654e PKI Card System 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 754e / bizhub 654e 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 “bizhub 754e / bizhub 654e PKI Card System Control Software" 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 function to print the encryption print realized by using a special printer driver and IC card by using exclusive driver (loadable driver) and the IC card that is used generating that encryption print for a printer data transmitted to MFP from client PC among the highly confidential document transmitted between MFP and client PC. Also, it provides a function of protecting the scanned image data transmitted by mail from MFP by S/MIME through the use of a loadable driver and an IC card. Both of these security functions are realized by the combined TOE and an IC card.

Moreover, for the danger of illegally bringing out HDD that is medium that temporarily stores image data processed 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 stored in HDD completely by deletion method compliant with various overwrite deletion standards and the function that controls the access from the FAX 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 organisation that uses MFP.

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 owns IC card. (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 organisation that uses MFP
  A responsible person of the organisation that manages the office where the MFP is installed. Assigns an administrator who manages the operation of MFP.

- Responsible person of the organisation that manages the maintenance of MFP
  A responsible person of the organisation 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.

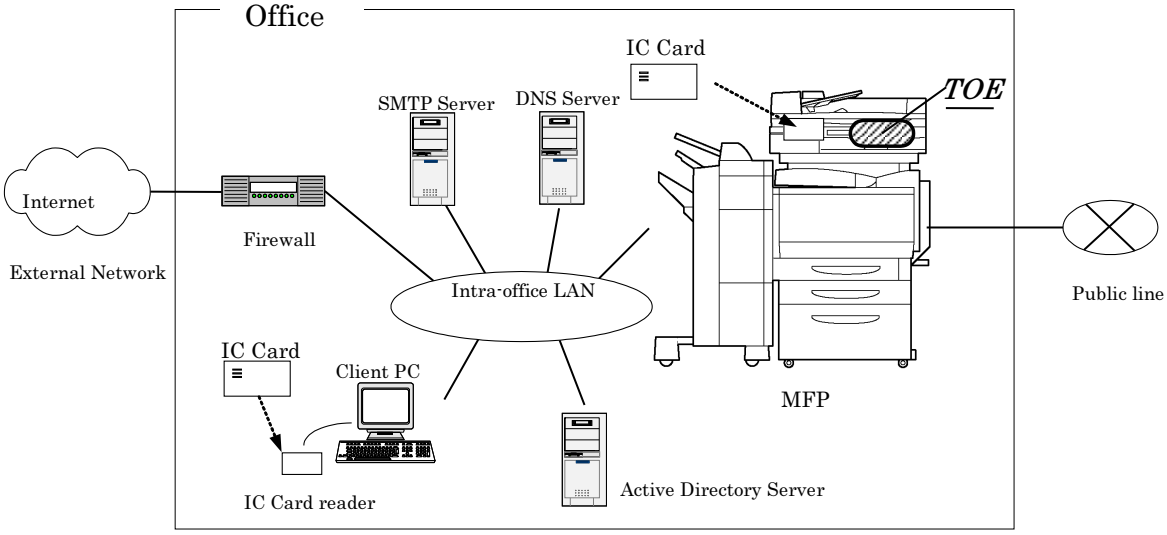

Figure 1 An example of MFP's use environments

- 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.
- An IC card and an IC card reader of the client PC is used to transmit the encrypted print file to MFP using the exclusive printer driver and decrypt the scanned image data transmitted from MFP.
- Active Directory sever is connected to an intra-office LAN and it is used to the authentication of IC card.
- When a SMTP server is connected to the intra-office LAN, MFP can carry out data communication with these servers, too. (The DNS service will be necessary when setting a domain name of the SMTP 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 public line connected with MFP is used for communications by FAX.

1.4.2.2. Operation Environment

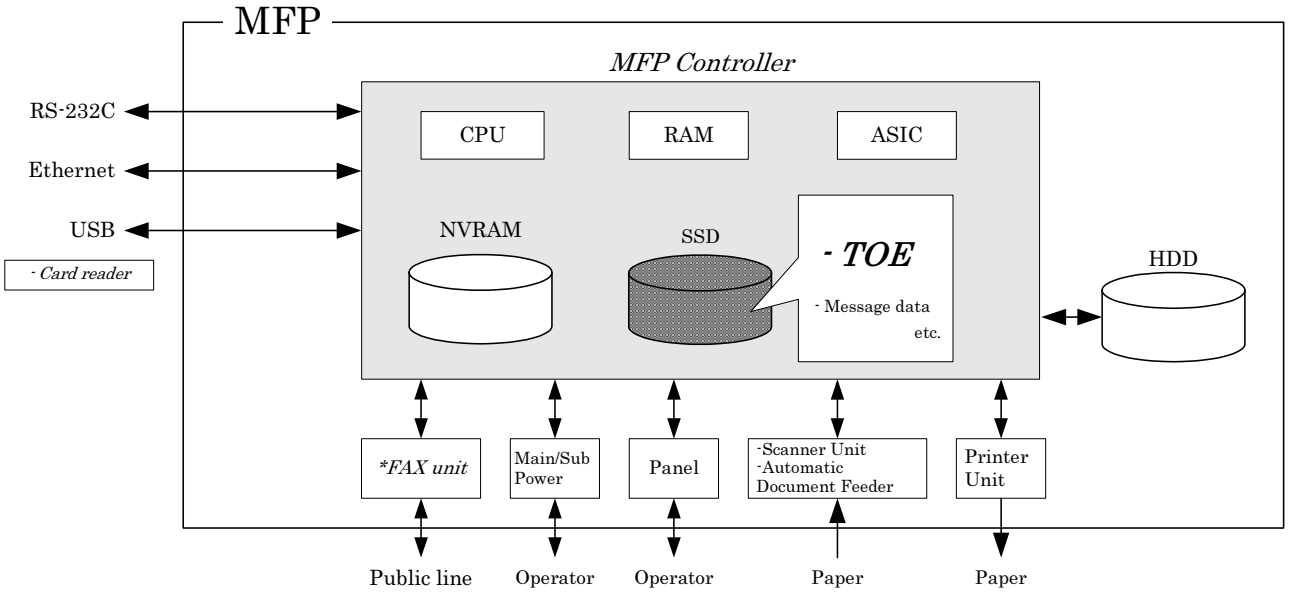

Figure 2 Hardware composition relevant to TOE

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 by using RS-232C, shown in Figure 2.

- SSD
  A storage medium that stores the object code of the "MFP PKI Card System 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 of 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 encrypting 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 temporarily during extension conversion and so on. Also, the loadable drivers for accessing an IC card are stored here.

- 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, numeric keypad, 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
  It can be connected with a card reader corresponded to IC card. A card reader is not pre-installed in MFP as a standard according to the circumstances in sales, but sold as an optional part. It is an essential component under this ST assumption.

- IC card
  An IC card that supports the standard specification of Common Access Card (CAC) and Personal ID Verification (PIV)

- 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.

- FAX unit (* optional part)
  A device that has a port of Fax public line and is used for communications for FAX-data transmission via the public line. This 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 organisation needs it, and the installation is not indispensable.

1.4.2.3. Guidance

- bizhub 754e / 654e for PKI Card System SERVICE MANUAL SECURITY FUNCTION Ver.1.01
- bizhub 754e / 654e for PKI Card System User's Guide [Security Operations] Ver.1.01

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 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. Also, various functions are realized with IC card.

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.

- Encryption Print Function

  A print file is stored as standby status remaining encrypted when the encrypted print file, which is generated from the exclusive printer driver of the client PC, is received.

  Printing is performed by a print direction from the panel by decrypting an encrypted print file through the PKI processing using IC card.

  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.

- Scan To Me Function

  IC card owner can transmit scan images from MFP to own e-mail address through PKI processing using IC card. Following two functions are usable.

  - S/MIME Encryption Function

    Scanned image is encrypted as S/MIME mail data file when transmitting an image file scanned by user to mail address.

    This function eliminates the possibility that other users stole a glance at highly confidential image on the communication.

  - Digital Signature Function

    Signature data is added to verify a mail sender and guarantee a mail data as S/MIME mail data file, when transmitting image files scanned by a user to mail address. This function eliminates the possibility to receive a falsified file erroneously on the communication.

1.4.3.2. Administrator Function

TOE provides the functions such as the management of various settings of the network, image quality, etc in the administrator mode that only authenticated administrator can manipulate from the panel.

The following shows the functions related to the security.

- Operational setup of automatic system reset
  - Setup of the function that logs out automatically when the setting time passed in an idle state.
- 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 stored in HDD.
- 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 encryption method applying to S/MIME process
- Setup of message digests method using signature applying to S/MIME process.
- Setup of giving a signature applying to S/MIME process
- Setup of the authentication operation prohibition function
  - Function to emphasize strength of authentication function when inputting various passwords
  - Suspending authentication for five seconds when inputting a password incorrectly and prohibiting authentication when failing it more than certain number of times.
  - Above operating types can be set.

1.4.3.3. 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 (Setting data of administrator password, setting of HDD encryption function etc.)

- Authentication setup of the service engineer with the CE[1] password.
  - Whether to activate or stop the function is selected.
- 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 physical format that initializes HDD status is executable.
- Initialization function
  - The various settings that the user or the administrator has set and the data that the user has stored are deleted.

[1] An abbreviation of Customer Service engineer

1.4.3.4. 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 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.

- Updating function of TOE
  TOE facilitated with the function to update itself. As for the update means, there are a method that downloads from FTP server through Ethernet (TOE update function via Internet) and a method that performs the connection of external memory.

TOE is not accessed to the internal network through the MFP since Fax unit is not installed as a standard and Fax public line portal does not exist. However, when Fax unit is installed, the following functions are supported.

- 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 of ASIC and IC card, 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 image data in HDD as a function to protect unauthorized bring-out of data and so on when an encryption passphrase is set up.

- Utilization of IC card
  IC card, an external entity, activates functions to encrypt or sign as a function to protect a data disclosed against the intention of a user when the encryption print or the E-mail transmission is performed.

1.4.3.5. 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 and the initializing function of the network setting 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 : access of PUBLIC : Prohibited
- User Name List : Prohibited
- Print without 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 :Operate with the setting of Authentication operation prohibition function
- User Box administrator function : Prohibited
- SNMP v1 / v2c Write function : Prohibited
- Use of SNMPv3 : Prohibited
- Setup of HDD encryption function : Valid
- Print data capture function : Prohibited
- Address registration user change function : Prohibited
- 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
- Network Server Function : Prohibited
- Setup of limitation of S/MIME encryption severity
  : Valid (Only 3DES and AES are user-selectable).
- Transmission of Image log : Prohibited
- Remote Panel Function : 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 organisational 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.

- Encryption print file
  An encrypted image file stored in MFP by generated and sent from a client PC by using the exclusive printer driver and IC card.
- Scanned image file
  An image file scanned on the spot by MFP. This assumes the operation of transmitting to scanned user's mail address by E-mail (S/MIME).

Image files other than the above-mentioned, such as a image file of a job kept as a wait state by copy, and a image file of a job kept that prints the remainder of copies becoming as a wait state for confirmation of the finish, are not intended to be protected in the general use of MFP, so that it is not treated as the 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.

- Encrypted Print File
- Scanned Image File
- Stored Image File
  - Stored image files other than encrypted 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)

When the intra-office LAN where the MFP with the TOE will be installed is connected to an external network, access from the external network to the MFP is not allowed.

A.SECRET (Operational condition about secret information)

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

A.IC-CARD (Operational condition about IC card)

IC card is owned by rightful 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, encrypted print files, scanned image 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)

- Encrypted print files, scanned image 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 encrypted print files, scanned image 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.

3.4. Organisational Security Policies

This ST assumes a TOE security environment corresponding to an organisation or user such as demanding the encryption of files and permitting access only to mail messages to which a signature is appended as an intra-office LAN security measure for protected assets that requires considering confidentiality. Moreover, although a stored data in a client PC and a server existing in internal network or a general data flowing on internal network is not protected assets, TOE security environment that corresponds to the organisation and users that prohibit the access to internal network via Fax public line of MFP is assumed. The security policies applied in the organisation that uses TOE are identified and described as follows.

P.COMMUNICATION-CRYPTO (Encryption communication of image file)

Highly confidential image file (encrypted print files, scanned image files) which transmitted or received between IT equipment must be encrypted.

P.COMMUNICATION-SIGN (Signature of image file)

Digital signature must be added to a mail including highly confidential image files (scanned image files).

P.DECRYPT-PRINT (Decryption of image file)

Highly confidential image files (encrypted print file) received by MFP are permitted to print only to a user who generated that files.

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.

4. Security Objectives

In this chapter, in relation to the assumptions, the threats, and the organisational security policy identified in Chapter 3, the required security objectives for the TOE and the environment for the usage of the TOE are described. This is described by being divided into the categories of the security objectives for the TOE and the security objectives for the environment below.

4.1. Security Objectives for the TOE

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

O.DECRYPT-PRINT (Decryption of encrypted print file)

TOE permits only the IC card used for generating encrypted print files to print the concerned encrypted print files.

O.OVERWRITE (Overwrite deletion)

TOE overwrites image data regions of assets stored in HDD in 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 all the data written in the HDD in the MFP including image files.

O.MAIL- CRYPTO (The use and encryption of S/MIME)

TOE encrypts scanned images according to user's demand for E-mail transmission of scanned images.

O.MAIL-SIGN (The use and signature of S/MIME)

TOE generates message digest of E-mail data including encrypted scanned images required for the digital signature process according to user's demand for E-mail transmission of scanned images.

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.PKI-CAPABILITY (The support operation to utilize PKI function)

TOE supports necessary mechanical operations for card reader and IC card using Active Directory in order to allow for the use of the encrypted print file function and Scan To Me function that are realized by the combined use of a card reader and IC card.

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.

4.2. Security Objectives for the Operational Environment

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

OE.ADMIN (A reliable administrator)

The responsible person in the organisation 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 organisation 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 organisation 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.CARD-USER (Utilization of IC card)

The owner of IC card uses IC card and exclusive printer driver when encrypting an encrypted print file, and uses the IC card when encrypting a scanned image file.

OE.IC-CARD (Possessive conditions of IC card)

- A responsible person of an organisation that uses MFP distributes an IC card issued for use in the organisation to those users who are permitted to possess the IC card.
- A responsible person of an organisation that uses MFP prohibits the user of an IC card from transferring or leasing the IC card to others and strictly obligates the user to notify if the user has lost the IC card.

OE.SECRET (Appropriate management of confidential information)

The administrator executes the following operation.

- Set the value of eight-digits or more for the administrator password
- Avoid setting an easy-to-guess value on the administrator password and encryption passphrase.
- Keep the administrator password and encryption passphrase confidential.
- Change the administrator 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.
- Set the value of eight-digits or more when changing the administrator password.
- When the service engineer changes the administrator password, make the administrator to change it promptly.

OE.SIGN (Persist of signature giving)

- Owner of IC card must add the signature when transmitting highly confidential image data to client PC from MFP.
- Administrator sets up the setting of the method of giving a digital signature to compulsory or arbitrarily adds the signature.

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, it operates along with the guidance for TOE.

OE.DRIVER (Utilization of exclusive printer driver)

The owner of IC card installs exclusive printer driver that satisfies the following requirements to client PC.

- Support the generation of random common key using for encrypting documents.
- Support the encryption process of the common key using public key in IC card.
- Support the encryption algorithm and key length that suit SP800-67.

OE.FAX-UNIT (Utilization of Fax unit)

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

4.3. Security Objectives Rationale

4.3.1. Necessity

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

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

Organisation security policies / Assumptions / Threats \ Security objectives	A.ADMIN	A.SERVICE	A.NETWORK	A.SECRET	A.IC-CARD	T.DISCARD-MFP	T.BRING-OUT-STORAGE	P.COMMUNICATION-CRYPTO	P.COMMUNICATION-SIGN	P.DECRYPT-PRINT	P.REJECT-LINE
O.DECRYPT-PRINT										X	
O.OVERWRITE						X					
O.CRYPTO-KEY							X				
O.MAIL-CRYPTO								X			
O.MAIL-SIGN									X		
O.CRYPTO-CAPABILITY							X				
O.PKI-CAPABILITY									X	X	
O.FAX-CONTROL											X
OE.ADMIN	X										
OE.SERVICE		X									
OE.CARD-USER								X			
OE.IC-CARD					X			X	X	X	
OE.NETWORK			X								
OE.SECRET				X							
OE.SIGN									X		
OE.SETTING-SECURITY						X	X	X			
OE.DRIVER								X			
OE.FAX-UNIT											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 organisation that uses the MFP assigns personnel who are reliable in the organisation that uses the MFP to administrator, 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 organisation 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 access by an unspecified person from an external network to the intra-office LAN.
  OE.NETWORK 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 executes the operation rule concerning the administrator password and encryption passphrase. It also regulates that the service engineer executes the operation rule concerning the CE password, and that the service engineer makes the administrator to execute the operation rule concerning the administrator password, so that this condition is realized.

- **A.IC-CARD (Operating condition concerning IC Card)**
  This condition assumes IC card used for the use of TOE is managed properly and IC card owner is the rightful user.
  OE.IC-CARD regulates that the responsible person in the organisation gives out and collects the IC cards issued by reliable PKI environment properly. It also regulates that the responsible person in the organisation keeps the user informed about how to correspond when expiring or losing the IC card, so that the unexpected user who the responsible person in the organisation does not intend must not own the activated IC card. This means that the owners of IC cards are appropriate users and 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 image data area of assets in HDD by deletion data. Also, OE.SETTING-SECURITY is that TOE operates along with the guidance, so that the possibility of the threat is removed by executing the same function, TOE provides, 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, etc., 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 image data written in the HDD, and a mechanical operation to use the HDD encryption function by ASIC is supported by O.CRYPTO-CAPABILITY. And also OE.SETTING-SECURITY performs the operations related to the setting and the maintenance along with the guidance including the enhanced security function.
  Accordingly, this threat is countered sufficiently.

4.3.4. Sufficiency of Organisational Security Policies

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

- **P.COMMUNICATION-CRYPTO (Encryption communication of image file)**
  This organisational security policy assumes that the highly confidential image files to be communicated on the network (encrypted print files, scanned image files) are encrypted so as to secure the confidentiality of the files.
  O.MAIL-CRYPTO supports the function to encrypt scanned image files transmitted by e-mail from MFP to user's own client PC. OE.CARD-USER requires the use of IC card for transmission to client PC from MFP, and the use of IC card and exclusive printer driver for transmission from client PC to MFP. In addition, OE.DRIVER demands to use the exclusive printer driver keeping image data secure. Moreover, OE.IC-CARD requests IC card owner is the rightful user. Also, the operation related to the setting and the maintenance along with the guidance including the enhanced security function is performed by OE.SETTING -SECURITY. Accordingly, this organisational security policy is sufficiently achieved.

- **P.COMMUNICATION-SIGN (Signature of image file)**
  This organisational security policy assumes that signature is added to the highly confidential image files (scanned image files) which are transferred by e-mail (S/MIME).
  OE.SIGN supports the addition of signature on scanned image files transmitted by e-mail to the client PC from MFP certainly. O.MAIL-SIGN and O.PKI-CAPABILITY supports the function to add signature to scanned image files sent by mail to user's own client PC from

MFP by using IC card. Moreover, OE.IC-CARD requires that IC card owner is the rightful user. Accordingly, this organisational security policy is sufficiently achieved.

- **P.DECRYPT-PRINT (Decryption of image file)**
  This organisational security policy assumes that only the user (IC card owner) who generated files is allowed to print the encrypted print file.
  O.DECRYPT-PRINT assumes that TOE allows the printing of encrypted print files only by IC card that generated those encrypted print files. In addition, OE.IC-CARD demands to manage the IC card owner appropriately.
  O.PKI-CAPABILITY supports the mechanical operation that the decryption process of encrypted print files uses an IC card, which is the external entity.
  Accordingly, this organisational security policy is sufficiently to achieve.

- **P.REJECT-LINE (Access prohibition from public line)**
  This organisational 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 Fax public line portal on Fax unit installed to MFP.
  This means that communication (illegal operation command) except image data which is sent from public line network and forwarded to internal network via the Fax public line portal of MFP is not forwarded to internal network, even though Fax unit is installed on MFP at the request of the organisation.
  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 of Fax unit. Also, OE.FAX-UNIT requires installing and operating Fax unit which is the optional part on MFP by service engineer, so that O.FAX-CONTROL is supported.
  Accordingly, this organisational 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 for TOE 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(only partial event)), FCS_CKM.4 (N/A)	

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

List of Standards	Cryptographic Key Generation Algorithm	Cryptographic Key sizes
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 partial event)), 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* *Decryption of encrypted print file*
FIPS 186-2	*RSA*	*- 1024 bits* *- 2048 bits* *- 3072 bits* *- 4096 bits*	*Encryption of common key (encryption key) to encrypt S/MIME transmission data*
FIPS 180-2	*SHA-1*	*N/A*	*Generation of message digest*
FIPS 180-2	*SHA-256*	*N/A*	*Generation of message digest*

6.1.1.2. User Data Protection

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*] : *- Encrypted print files* *- Scanned image 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 service mode from the panel*** ***-Authentication for accessing the administrator mode 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[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 of all input from the panel*** ***<Operation for recovering the normal condition>*** ***- Release automatically after five seconds passed.***	
Hierarchical to :	No other components
Dependencies :	FIA_UAU.1 (FIA_UAU.2[1], FIA_UAU.2[2])

FIA_SOS.1[1]	Verification of secrets

FIA_SOS.1.1[1]
The TSF shall provide a mechanism to verify that secrets *(CE 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 161 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 *(Administrator 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 161 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 password as the current setting after change.*
Hierarchical to : No other components
Dependencies : No dependencies

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

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.***	
Hierarchical to	: No other components
Dependencies	: No dependencies

FIA_UAU.7	**Protected authentication feedback**
FIA_UAU.7.1	
The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.	
[assignment: *list of feedback*] : ***Display "*" for every character data input.***	
Hierarchical to	: No other components
Dependencies	: FIA_UAU.1 (FIA_UAU.2[1], FIA_UAU.2[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 ***(IC card of IC card owner)*** to be successfully identified before allowing any other TSF-mediated actions on behalf of that user ***(IC card of IC card owner).***	
Hierarchical to	: FIA_UID.1
Dependencies	: No dependencies

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 function*
[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*] : - *All area overwrite deletion function*
[selection: *determine the behavior of, disable, enable, modify the behavior 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[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*] : - *Addition of Digital Signature*
[selection: *determine the behavior of, disable, enable, modify the behaviour 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_MTD.1[1] Management of TSF data
FMT_MTD.1.1[1]
The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].
[assignment: *list of TSF data*] : - *Panel Auto Log-out Time* - *Authentication Failure Frequency Threshold* - *S/MIME Encryption Strength (Encryption Algorithm)* - *S/MIME Message Digest Method* - *Release time of operation prohibition for Administrator Authentication* - *Encryption Passphrase*
[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[2]	**Management of TSF data**

FMT_MTD.1.1[2]
The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the 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[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*] : ***- 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_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*] : ***- Modification function of administrator password by administrator*** ***- Modification function of Release time of operation prohibition for Administrator authentication by administrator*** ***- Modification function of Panel Auto Log-out Time by administrator*** ***- Modification function of authentication failure frequency threshold by administrator in the authentication operation prohibition function*** ***- Modification function of S/MIME encryption strength (encryption algorithm) by administrator*** ***- Modification function of S/MIME message digest method by administrator*** ***- Modification function of encryption passphrase by administrator*** ***- All area overwrite deletion function by administrator*** ***- Digital signature giving function by administrator*** ***- Disable function of Enhanced security function by administrator*** ***- Disable function of Enhanced security function by service engineer*** ***- Modification function of CE password by service engineer*** ***- Modification function of administrator password by service engineer*** ***- Modification function of Release time of operation prohibition for CE authentication by service engineer***

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])

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 panel auto logoff time (1-9 minute/s) while a administrator is operating on the panel***
Hierarchical to : No other components
Dependencies : No dependencies

6.1.1.6. 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*] : ***HDD encryption function achieved by ASIC***
[assignment: *necessary capability list for the operation of security service*] : ***- Support function of the image files processing by HDD encryption function***
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*] : ***Following functions achieved by IC card*** ***(1) Decryption function of common key to encrypt the encrypted print file*** ***(2) Message digest encryption function for signing the scanned image by S/MIME function*** ***(3) Support function for using public key***	
[assignment: *necessary capability list for the operation of security service*] : ***- Request function of transmission of encrypted common key for above (1) and of decryption process of encrypted common key*** ***- Request function of transmission of message digest for above (2) and of encryption process of message digest*** ***- Inquiring function of public key for above (3)***	
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 4 TOE Security Assurance Requirements

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

TOE Security Assurance Requirements		Component
	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 5 Conformity of IT Security Functional Requirements to Security Objectives

Security Objectives / Security Functional Requirements	O.DECRYPT-PRINT	O.OVERWRITE	O.CRYPTO-KEY	O.MAIL-CRYPTO	O.MAIL-SIGN	O.CRYPTO-CAPABILITY	O.PKI-CAPABILITY	O.FAX-CONTROL	* set.admin	* set.service
set.admin				X	X	X				
set.service				X	X	X				
FCS_CKM.1			X	X						
FCS_COP.1	X			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	X
FIA_SOS.1[1]										X
FIA_SOS.1[2]									X	
FIA_SOS.1[3]						X				
FIA_UAU.2[1]										X
FIA_UAU.2[2]									X	
FIA_UAU.6									X	X
FIA_UAU.7									X	X
FIA_UID.2[1]										X
FIA_UID.2[2]									X	
FIA_UID.2[3]							X			
FMT_MOF.1[1]									X	X
FMT_MOF.1[2]									X	
FMT_MOF.1[3]									X	
FMT_MTD.1[1]				X	X	X			X	X
FMT_MTD.1[2]									X	
FMT_MTD.1[3]										X
FMT_SMF.1				X	X				X	X

Security Objectives / Security Functional Requirements	O.DECRYPT-PRINT	O.OVERWRITE	O.CRYPTO-KEY	O.MAIL-CRYPTO	O.MAIL-SIGN	O.CRYPTO-CAPABILITY	O.PKI-CAPABILITY	O.FAX-CONTROL	* set.admin	* set.service
FMT_SMR.1[1]									X	X
FMT_SMR.1[2]				X	X				X	
FTA_SSL.3									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.DECRYPT-PRINT (Decryption of Encrypted Print File)**

  This security objective explains the policy for encrypted print files.
  If the action of printing an encrypted print file is taken through the use of an IC card identified through O.PKI-CAPABILITY, a proper common key (encryption key) to decrypting the encrypted print file is provided from IC card through O.PKI-CAPABILITY, and the process of decrypting the encrypted print file operates through FCS_COP.1.
  Therefore, this security objective is satisfied.

- **O.OVERWRITE (Overwrite deletion)**

  This security objective regulates that it erases image data areas of assets stored in HDD, and requires various requirements that relate to the deletion.
  FDP_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.MAIL-CRYPTO (Usage and Encryption of S/MIME)**

  This security objective regulates that the image data scanned directly on MFP is encrypted when it is sent to the user's own mail address 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 scanned image 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 scanned image 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 common keys (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) using IC card which is identified by O.PKI-CAPABILITY. Also, the setting of encryption algorithm is limited to administrator by FMT_MTD.1[1].

  This security objective is satisfied by these functional requirements.

  <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>
  As the role of doing these managements, FMT_SMR.1[1] maintains a service engineer and FMT_SMR.1[2] maintains an administrator. In addition, FMT_SMF.1 specifies these management functions.

- **O.MAIL-SIGN (Usage and signature of S/MIME)**

  This security objective regulates that a message digest is generated under the assumption that a digital signature will be appended to the image data scanned directly through MFP when it is sent to the user's own mail address by mail. And various requirements related to the message digest are required.

  Through FSC_COP.1, message digest required for the signature processing is generated by the hash function regulated by FIPS 180-2 (SHA-1 or SHA-256). In addition, FMT_MTD.1[1] limits the setting of message digest method to administrators.

  This security objective is satisfied by these functional requirements.

  <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>
  As the role of doing these managements, FMT_SMR.1[1] maintains a service engineer and FMT_SMR.1[2] maintains an administrator. In addition, FMT_SMF.1 specifies these

management functions.

- **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[1], a support function to process image data in HDD by HDD encryption function is achieved for the HDD encryption function implemented by ASIC. Also, encryption passphrase used for an encryption is verified the quality by FIA_SOS.1[3]. The setting is limited to the administrator by FMT_MTD.1[1].
  This security objective is satisfied by this functional requirement.

  <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>
  As the role of doing these managements, FMT_SMR.1[1] maintains a service engineer and FMT_SMR.1[2] maintains an administrator. In addition, FMT_SMF.1 specifies these management functions.

- **O.PKI-CAPABILITY (Support action to use the PKI function)**
  This security objective regulates that TOE supports the action of giving signature to scanned images by the IC card identified by FIA_UID.2[3] that is the entity out of TOE, and the action of decrypting common key for decrypting the encrypted print files. Also, it needs various requirements that regulate the support of external entity action.
  Applying FIT_CAP.1[2], the support function to process scanned images and encrypted print files by PKI function for the PKI function achieved by the IC card is realized.
  This security objective is satisfied by this functional requirement.

- **O. FAX-CONTROL (Fax unit control)**
  This security objective regulates to prohibit an access to internal network which the MFP connects with, from public line via the Fax public line portal. This means that communication (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. 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.

- ***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[3] 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 upper limit (1-3 times) consecutively, FIA_AFL.1[2] logouts if it is 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[1] 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 panel automatic logout time elapses by FTA_SSL.3 if it logs in from the panel. The change in the panel auto logout time is limited to the administrator by FMT_MTD.1[1].

<Management of administrator's authentication information>
FIA_SOS.1[2] verifies the quality of the administrator password. FMT_MTD.1[2] 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 the upper limit (1-3 times), FIA_AFL.1[2] logouts it if it is under authentication, and releases the authentication status of the administrator 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.

<Role and management 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. In addition, FMT_SMF.1 specifies these management functions and FMT_MOF.1[1], FMT_MOF.1[2], and FMT_MOF.1[3] manages those behaviors.

- ***set.service*** **(Set of necessary requirements 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 "*" for every one character entered as the feedback protected in the panel, and supports the authentication.
  FIA_AFL.1[3] refuses all the input receipts from the panel for five seconds at each failure, and when the failure authentication reaches the upper limit (1-3 times) consecutively, FIA_AFL.1[1] logouts 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 when the release time of operation prohibition for CE authentication passes, this lock status is

released.
FMT_MTD.1[1] 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[3] 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[3] 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 the upper limit (1-3 times) consecutively, 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 function lock release function is executed and when the release time of operation prohibition for CE authentication passes, 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. In addition, FMT_SMF.1 specifies these management functions and FMT_MOF.1[1] manages those behaviors.

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 6 Dependencies of IT Security Functional Requirements Components

N/A : Not Applicable

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4	FCS_COP.1 (only partial event) The satisfied events: Operating the key that is generated by the Pseudorandom number generation algorithm <Reason not to satisfy FCS_CKM.2 or FCS_COP.1 partially> - The encryption operation is performed using the key generated by the KONICA MINOLTA HDD encryption 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 encryption operation. <Reason not to apply FCS_CKM.4) - The key generated by the Pseudorandom number algorithm temporarily exists in the volatile memory area, but there is no necessity of the encryption key

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
		cancellation since it is automatically destroyed without the necessity of access from the outside. - The key generated by KONICA MINOLTA HDD encryption key generation algorithm 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: Generating the common key for encrypting the S/MIME transmission data. <The reason not to satisfy a part of the FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2> - FIT_CAP.1[2] imports the common key that decrypts the encrypted print file, and so there is no necessity of the key generation or importing from the outside. - FIT_CAP.1[2] supports the public key that performs the encryption of common key that encrypts the S/MIME transmission data, and so there is no necessity of the key generation or importing from the outside. - The message that is used for generating the message digest is the generated document data itself, and so there is no necessity of key generation or importing from the outside. <The reason not apply FCS_CKM.4> - The keys for encrypting S/MIME transmission data and for decrypting the encrypted print file 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. - The public key that performs the encryption of common key that encrypts the S/MIME transmission data is the public information, and so there is no necessity of the encryption key cancellation.
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.
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[1], FIA_UAU.2[2]
FIA_SOS.1[1]	None	N/A
FIA_SOS.1[2]	None	N/A
FIA_SOS.1[3]	None	N/A

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
FIA_UAU.2[1]	FIA_UID.1	FIA_UID.2[1]
FIA_UAU.2[2]	FIA_UID.1	FIA_UID.2[2]
FIA_UAU.6	None	N/A
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2[1], FIA_UAU.2[2]
FIA_UID.2[1]	None	N/A
FIA_UID.2[2]	None	N/A
FIA_UID.2[3]	None	N/A
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_MTD.1[1]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[2]
FMT_MTD.1[2]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[1] , FMT_SMR.1[2]
FMT_MTD.1[3]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[1]
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]
FTA_SSL.3	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 7 below. The detailed specification is explained in the paragraphs described below.

Table 7 Names and Identifiers of TOE Security Function

No.	TOE Security Function	Relationship with Logical Scope of the TOE
7.1	F.ADMIN (Administrator function)	Administrator function
7.2	F.SERVICE (Service mode function)	Service engineer function
7.3	F.CARD-ID (IC card identification function)	Basic function
7.4	F.PRINT (Encryption print function)	Basic function
7.5	F.OVERWRITE (All area overwrite deletion function)	Administrator function
7.6	F.CRYPTO (Encryption key generation function)	Other function
7.7	F.RESET (Authentication failure frequency reset function)	Administrator function, Service engineer function
7.8	F.S/MIME (S/MIME encryption processing function)	Basic function
7.9	F.SUPPORT-CRYPTO (ASIC support function)	Other function
7.10	F.SUPPORT-PKI (PKI support function)	Other function
7.11	F.FAX-CONTROL (FAX unit control function)	Other 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 and a security management function that includes a change of an administrator password.

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 8.
- Return "*" for each character as feedback for the entered administrator password.
- Resets the number of authentication failure when succeeding in the authentication.
- Not 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 releases the lock of authentication function.

As described above, FIA_AFL.1[2], FIA_AFL.1[3], FIA_UAU.2[2], FIA_UAU.7 and FIA_UID.2[2] are realized.

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.

Table 8 Characters and Number of Digits for Password [2]

Objectives	Number of digits	Characters
Administrator Password	8-64	Selectable from 161 or more characters in total
CE Password	8-64	Selectable from 161 or more characters in total
Encryption passphrase	20	Selectable from 83 or more characters in total

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.

7.1.3.1. Change of Administrator Password

When a user is re-authenticated as an administrator by the panel and when the password newly set satisfies the qualities, the password is changed.

- Provides the administrator authentication mechanism that is re-authenticated by the administrator password which consists of the character shown in Table 8.
- 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 from the panel, and locks all the authentication functions to use the administrator password. (The access to the administrator mode is refused.)
  - The administrator specifies the failure frequency threshold by the unauthorized access detection threshold setting function.
- F.RESET works, so that the lock of the authentication function is released.
- Verify that the administrator password newly set satisfies the following qualities.
  - It shall be composed of the characters and by the number of digits shown in the administrator password of Table 8.
  - 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], FIA_AFL.1[2], FIA_UAU.6, FIA_UAU.7, FMT_MTD.1[2],

[2] Table 8 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.

FMT_SMF.1 and FMT_SMR.1[2] are realized.

7.1.3.2. 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[1], FMT_SMF.1, and FMT_SMR.1[2] are realized.

7.1.3.3. 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 [1], FMT_SMF.1 and FMT_SMR.1[2] are realized.

7.1.3.4. Operation Setup of HDD Encryption Function

<Encryption Passphrase Change>
The encryption passphrase is changed. It is changed when the newly setup encryption passphrase satisfies the quality requirements, and F.CRYPTO is performed

- Verify that the encryption passphrase newly set satisfies the following qualities.
  - It shall be composed of the characters and by the number of digits shown in the encryption passphrase of the Table 8.
  - 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[1], FMT_SMF.1 and FMT_SMR.1[2] are realized.

7.1.3.5. Setup of S/MIME Transmission Function

The functions related to the S/MIME function that the administrator operates, are as follows.

- Setup of Digital signature giving
  Able to select the setting of digital signature when using the S/MIME function, from “be always valid,” “select when the transmission” and “be always invalid.”
- Modification of S/MIME Encryption Strength (Encryption Algorithm)
- Algorithm modification of method of S/MIME message digest

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

7.1.3.6. Function related to Enhanced Security Function

The function that affects to the setting of enhanced security function that the administrator operates is as follows.

- Operation setting of Enhanced security function
  Function to set the enhanced security function to valid or invalid.

Other than the operation setting of the enhanced security function, it is possible to set invalid the setting of enhanced security function by executing the HDD logical format function, the all area overwrite deletion function, etc.. All these operations are limited only to the administrator.

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

7.1.3.7. Function related to Password Initialization Function

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

- All area overwrite deletion function
  Setting the administrator password to the initial value at factory shipment by executing the overwrite deletion to all area.

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

7.2. 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.

7.2.1. 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 8.
- 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[3], FIA_UAU.2[1], FIA_UAU.7 and

FIA_UID.2[1] are realized.

7.2.2. 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.

7.2.2.1. Change of CE Password

When a user is re-authenticated as a service engineer and the newly set password satisfies the qualities, it is changed.

- Provides the CE authentication mechanism that is re-authenticated by the CE password that consists of the characters shown in Table 8.
- 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 releases the authentication function.
- Verify that the CE password newly set satisfies the following qualities.
  - It shall be composed of the characters and by the number of digits, shown in the CE password of the Table 8.
  - 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[3], FMT_SMF.1 and FMT_SMR.1[1] are realized.

7.2.2.2. Change of Administrator Password

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

- It shall be composed of the characters and by the number of digits, shown in the administrator password of the Table 8.
- 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[2], FMT_SMF.1 and FMT_SMR.1[1] are realized.

7.2.2.3. 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[3], FMT_SMF.1 and FMT_SMR.1[1] are realized.

7.2.2.4. Function related to the Enhanced Security Function

The functions that affect the setting of the enhanced security function that the service engineer operates are as follows.

- HDD logical format function
  Function to write on HDD the initial value of the management data that is used for the file system. This logical formatting deactivates the setting of the enhanced security function.
- HDD physical format function
  Function to rewrite the entire disk of HDD including the signal rows such as the track and sector information with a regulated pattern. This physical formatting deactivates the setting of enhanced security function.
- Initialization function
  Function to reset every setting value written in NVRAM and SSD to the factory shipment default. The setting of enhanced security function is deactivated by executing this initialization function.

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

7.3. F.CARD-ID (IC Card Identification Function)

F.CARD-ID is the function that MFP identifies the IC card connected to MFP before using the encryption print function and Scan To Me function.

As described above, FIA_UID2[3] is realized.

7.4. F.PRINT (Encryption Print Function)

F.PRINT is a security function related to the encryption print function. It operates the decryption process to the print operation by the common key (encryption key) that is obtained by F.SUPPORT-PKI.

- The common key (encryption key) (168 bits) to decrypt the encrypted print file is decrypted by RSA that is regulated by the FIPS186-2.

As described above, FCS_COP.1 is realized.

7.5. F.OVERWRITE (All Area Overwrite Deletion Function)

F.OVERWRITE executes the overwrite deletion in the data area including image data stored in HDD, and initializes the settings value such as passwords set on NVRAM and SSD as well. The object for the deletion or the initialization is as follows.

<Object for the deletion: HDD>

- Encrypted print file
- Scanned image file
- Stored image file

<Object for the initialization: NVRAM / SSD>

- Administrator Password
- Operation setting of HDD encryption function (OFF) --- Encryption Passphrase is deleted

The deletion methods such as the data overwritten in HDD and the writing frequency is executed according to the deletion method of the all area overwrite deletion function set by F.ADMIN (Table 9). For the HDD encryption function, the encryption passphrase which was set is disabled by turning off the operational setup.

As described above, FDP_RIP.1 is realized.

Table 9 Types and Methods of Overwrite Deletion of All Area

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

7.6. F.CRYPTO (Encryption Key Generation Function)

F.CRYPTO 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.

7.7. F.RESET (Authentication Failure Frequency Reset Function)

F.RESET is a function that releases the lock by resetting the counted 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 is elapsed.

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

7.8. F.S/MIME (S/MIME Encryption Processing Function)

F.S/MIME is a function to encrypt the scanned image and add signature when transmitting the scanned image to user's own self by S/MIME. Signature generation is performed by IC card by F.SUPPORT-PKI, but on this function the message digest for signature is generated.

<Encryption Key generation>

- The common key (encryption key) is generated to encrypt the scanned image 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 Scanned image >

- Scanned image is encrypted by AES which FIPS PUB 197 provides by using common key (encryption key) (128, 192 and 256 bits).
- Scanned image is encrypted by the 3-Key-Triple-DES which SP800-67 provides by using the common key (encryption key) (168 bits).

As described above, FCS_COP.1 is realized.

<Encryption of Encryption key>

- The common key (encryption key) to encrypt the scanned image is encrypted by RSA which FIPS 186-2 provides.
- The key length of the common key (encryption key) used in F.SUPPORT-PKI is 1024, 2048, 3072 or 4096 bits.

As described above, FCS_COP.1 is realized.

<Message Digest Generation>

- For scanned image, message digest is generated by hash function (SHA-1 or SHA-256) which FIPS 180-2 provides.

As described above, FCS_COP.1 is realized.

7.9. 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 image data read out of the HDD, the encryption key generated by F.CRYPTO is set in ASIC and decryption is performed by the ASIC.

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

7.10. F.SUPPORT-PKI (PKI Support Function)

F.SUPPORT-PKI is the function to operate the IC card identified by F.CARD-ID from TOE.

<Decryption process request>

- The encrypted common key (encryption key) is sent to IC card, the decryption processing of the common key (encryption key) is done by IC card, and the common key (encryption key) that is correctly decrypted is received.

<Signature process request>

- The message digest (hash value of the message) generated by F.S/MIME is sent to IC card, the signature processing is done, and correct signature to the message digest is received.

<Public key obtain request>

- Inquiring to IC card is performed and public key (digital certificate) in the IC card is received.

As described above, FIT_CAP.1[2] 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.