bizhub C353 PKI Card System Control Software
Security Target

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

Version: 1.07

Issued on: August 5, 2009

Created by: KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

<Revision History>

Date	Ver.	Division	Approved	Checked	Created	Revision
Dec. 12, 2008	1.00	Development Div. 12	Hirota	Nakajima	Yoshida	Initial Version
Jan. 15, 2009	1.01	Development Div. 12	Hirota	Nakajima	Yoshida	Deal with typos.
Jan. 27, 2009	1.02	Development Div. 12	Hirota	Nakajima	Yoshida	Deal with typos.
Feb. 24, 2009	1.03	Development Div. 12	Hirota	Nakajima	Yoshida	Deal with typos.
Apr. 2, 2009	1.04	Office Software Development Division 1	Hirota	Nakajima	Yoshida	Deal with typos.
May 22, 2009	1.05	Office Software Development Division 1	Hirota	Nakajima	Yoshida	Deal with typos.
Jun. 9, 2009	1.06	Office Software Development Division 1	Hirota	Nakajima	Yoshida	Change of TOE version
August 5, 2009	1.07	Office Software Development Division 1	Hirota	Nakajima	Yoshida	Deal with typos.

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

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

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

1. ST Introduction

1.1. ST Identification

-ST Title	:	bizhub C353 PKI Card System Control Software Security Target
-ST Version	:	1.07
-Created on	:	August 5, 2009
-Created by	:	KONICA MINOLTA BUSINESS TECHNOLOGIES, INC. Eiichi Yoshida

1.2. TOE Identification

-TOE Name	:	bizhub C353 PKI Card System Control Software
-TOE Version	:	A02E0Y0-0100-GM0-U4
-TOE Type	:	Software
-Created by	:	KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

1.3. TOE Overview

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

1.3.1. TOE Type

bizhub C353 PKI Card System Control Software, which is the TOE is an embedded software product installed in the flash memory on the MFP controller to control the operation of the whole MFP.

1.3.2. Usage of TOE and Main Security Functions

bizhub C353 is digital multi-function products provided by Konica Minolta Business Technologies, 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 C353 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 exchanged between MFP and client PC. Also, it provides the protection function for scan image data transmitted by mail from MFP by S/MIME using loadable driver and IC card. All are coordinated with IC card and TOE and realizes these security functions.

Moreover, for the danger of illegally bringing out HDD, which stores image data temporarily in MFP, TOE can use HDD lock function loaded on the HDD or encrypt all the data written in HDD including image data using the encryption board. Besides, TOE has a deletion method compliant

with various overwrite deletion standards. It deletes all the data of HDD completely and it contributes to the prevention of information leakage of the organization that uses MFP by using this method at the time of abandonment or the lease returns.

1.4. TOE Description

1.4.1. Roles of the TOE Users

The roles of the personnel related to the use of the 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 engineers
  A user who manages the maintenance for 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 Business Technologies, Inc. is assumed.)

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

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

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

1.4.2. Physical Scope of TOE

1.4.2.1. Use Environment

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

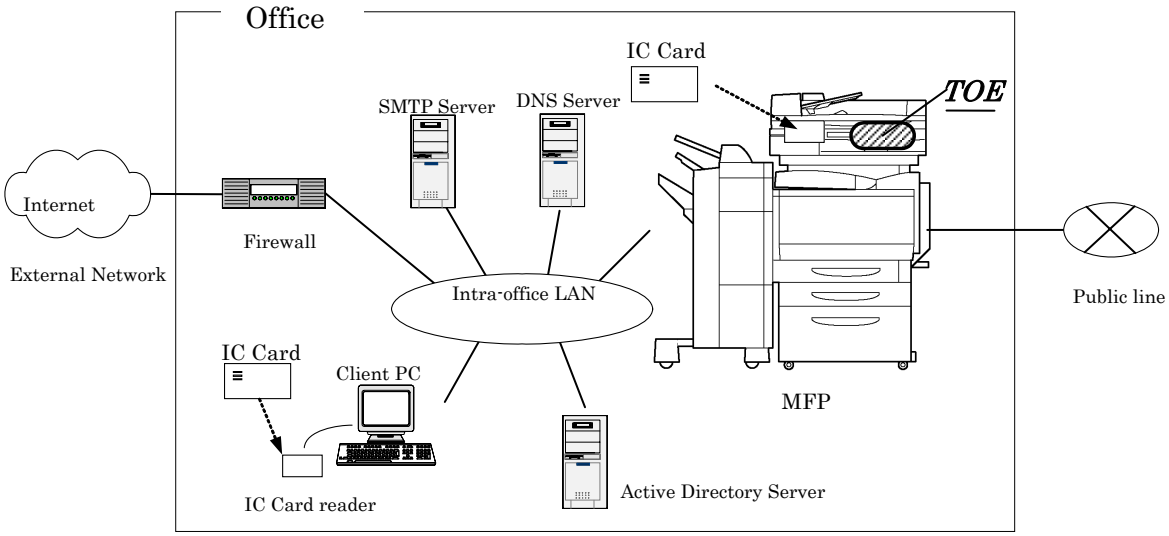


Figure 1 An example of MFP's use environments

- An intra-office LAN exists as a network in the office.
- MFP is connected to the client PCs via the intra-office LAN, and has mutual data communications.
- 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 scan image data transmitted from MFP.
- Active Directory 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 and the remote support function.

1.4.2.2. Operation Environment

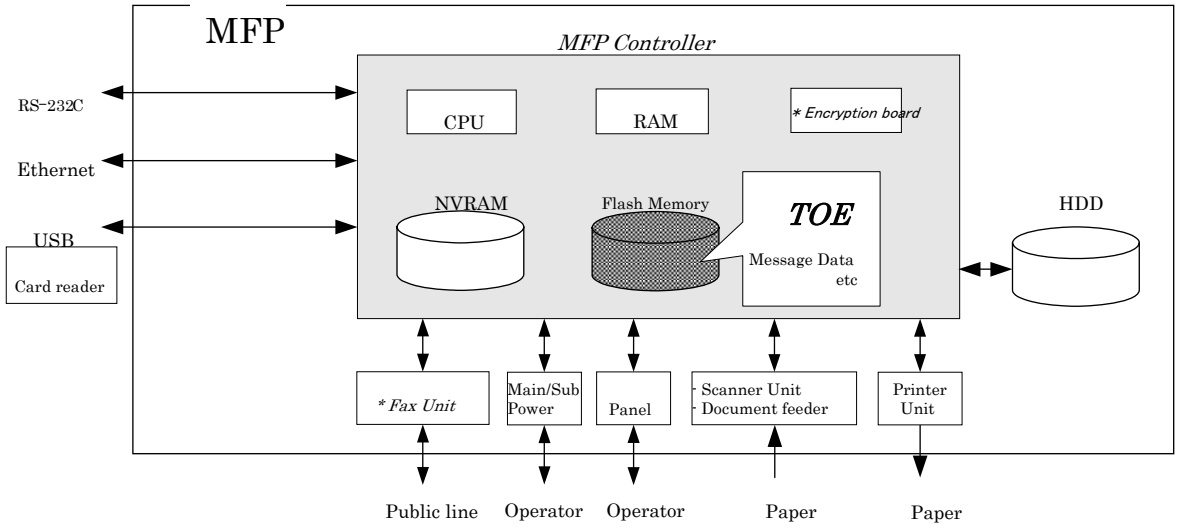


Figure 2 Hardware composition relevant to TOE

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

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

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

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

- Encryption Board (*Option)
  An integrated circuit for specific purposes which implements an encryption function for enciphering all data written in HDD.

- HDD
  A hard disk drive of 60GB 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 exclusive drivers for accessing an IC card are stored here.
  As a feature function, security function (HDD lock function) is installed, being possible to set a password and not being possible to read and write unless it agrees to the password. Furthermore, when the frequency of uniformity of it becomes unsuccessful in password collation, the function is also ready to lock the password collation function.

- Main/sub power supply
  Power switches for activating MFP

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

- Scan Unit/ automatic manuscript 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
  Besides a printing from a USB memory, 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 pins connectors is usable. The maintenance function is usable through this interface in the case of failure. It is also possible to use the remote diagnostic function (described later) by connecting with the public line via a modem.

- FAX unit (* optional part)
  A device used for communications for FAX-data transmission and remote diagnostic (described later) via the public line. Is not pre-installed in MFP as a standard function according to the circumstances in sales, but sold as an optional part.

1.4.2.3. Guidance

- bizhub C353 for PKI Card System User's Guide [Security Operations]
- bizhub C353 for PKI Card System SERVICE MANUAL SECURITY FUNCTION

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 registers 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. In addition, 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 a 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

    Scan 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 typical function related to the security.

- Operational setup of automatic system reset
  - Setting of the function that logs out automatically when the setting time passed.
- Complete 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 overall area of HDD.
- Setup of the HDD lock function
  - Whether to activate or stop the function is selected.
  - An HDD lock password is registered or changed when the function is activated.
- Setup of the encryption function (* only when the encryption board installed)
  - 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 digest method using signature applying to S/MIME process
- Setup of giving a signature applying to S/MIME process
- Setup of the prohibit function of authenticating operations
  - 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 typical functions related to security.

- Modification function of administrator password

The following is a set of operation setting functions of affecting functions especially to the behavior of the security function (Setting data of administrator password, setting of HDD lock function, setting of 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 remote diagnostic function (later description)

[1]Abbreviation of Customer Service engineer

- Able to select permission or prohibition.

- Setup of a TOE update function via Internet
  - Able to select permission or prohibition.
- Setup of maintenance function
  - Able to select permission or prohibition.
- The format function of HDD
  - A physical format that initializes the HDD status is executable.
- Initialization function
  - The various setting values that the user or the administrator has set and the data that the user has stored are deleted.

1.4.3.4. 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 encryption board when writing data in HDD or reading data from HDD. (TOE does not process the encryption and description itself.)
  The operational setup of this function is performed by the administrator function. When activated, TOE generates the encryption key by the encryption passphrase that was entered on the panel.

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

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

TOE uses effectively security function of external entity as encryption board, HDD and IC card. The following explains the major functions related to external entity. In addition, it is necessary to activate either encryption function by the encryption board or HDD lock function at least.

- Utilization of encryption board
  Encryption board, an external entity, activates a function to encrypt the 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 HDD Lock Function
  HDD, an external entity, activates a HDD lock function as a function to protect unauthorized bring-out when the password 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.

2. Conformance Claims

2.1. CC Conformance Claim

This ST conforms to the following standards.

Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and general model 2006/9 Version 3.1 Revision 1 (Translation v1.2)
Part 2: Security functional requirements 2007/9 Version 3.1 Revision 2 (Translation v2.0)
Part 3: Security assurance requirements 2007/9 Version 3.1 Revision 2 (Translation v2.0)

- Security function requirement : Part 2 Extended
- Security assurance requirement : Part 3 Conformant

2.2. PP Claim

There is no PP that is referenced by this ST.

2.3. Package Claim

This ST conforms to Package: EAL 3. There is no additional assurance component.

2.4. Reference

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

3. Security Problem Definition

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

3.1. Protected Assets

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

- Encrypted print file
  An encrypted image file generated, sent and stored in MFP by using the exclusive printer driver and IC card from client PC.
- 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).

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

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 being disposed, 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
- On-memory Image File
  - Image file of job in the wait state
- Stored Image File
  - Stored image files other than encrypted print file
- HDD remaining Image File
  - The file which remains in the HDD data area that is not deleted only by general deletion operation (deletion of a file maintenance area)
- Image-related File
  - Temporary data file generated in image file processing

.

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.

A.SETTING (Operational setting condition about security)

- Prohibit administrator authentication operation when failing the input of administrator password consecutively constant frequency.
- Disable the use of the remote diagnostic function
- Disable the use of the TOE update function via an internet.
- Disable the use of the maintenance function.
- Activate login authentication of service engineer.
- Activate the encryption function or HDD lock function.
- Disable the setting of administrator function excluding panel.

3.3. Threats

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

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

When leased MFPs are returned or discarded MFPs are collected, encrypted print files, scanned image files, on-memory image files, stored image files, HDD remaining image files, image-related files, and highly confidential information such as the setup various passwords can leak by the person with malicious intent when he/she analyzes the HDD or NVRAM in the MFP.

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

- Encrypted print files, scanned image files, on-memory image files, stored image files, HDD-remaining image files, image-related files, and various passwords which were set up 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, on-memory

image files, stored image files, HDD-remaining image files, image-related files, and various passwords which were set up 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. Organizational Security Policies

In this ST, TOE security environment that corresponds to organizations and users such as file encryption is demanded and only the signed mail is permitted to read is assumed as the security measures in the intra-office LAN corresponding to the Protected Assets considering the confidentiality. The security policies applied in the organization 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) are permitted to print only to a user who generated that files.

4. Security Objectives

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

4.1. Security Objectives for the TOE

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

O.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-ALL (Complete overwrite deletion)

TOE overwrites all the data regions of HDD in MFP with deletion data, and makes all image data unable to restore. In addition, TOE provides a function to initialize settings such as the highly confidential passwords on NVRAM (administrator passwords, HDD lock passwords, and encryption passphrases).

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

TOE verifies that correct HDD is installed.

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 encryption function)

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

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

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

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

TOE supports necessary mechanical operations for card reader and IC card using Active

Directory to utilize the encrypted print file function and the Scan To Me function, that is realized in cooperation with the card reader and the IC card.

4.2. Security Objectives for the Operation Environment

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

OE.ADMIN (A reliable administrator)

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

OE.SERVICE (The service engineer's guarantee)

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

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

- The responsible person in the organization who uses MFP carries out the measures for the unauthorized access from the outside by setting up the equipment such as the firewall to intercept the access from an external network to MFP with TOE.

OE.CARD-USER (Utilization of IC card)

The owner of IC card uses IC card and exclusive driver to encrypt encrypted print files and uses only IC card to encrypt scanned image files.

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

- The responsible person in the organization who uses MFP gives the IC card issued to use for the organization out to an appropriate user who is allowed to own that IC card.
- The responsible person in the organization who uses MFP prohibits users from handing over or renting the IC card to others, and keeps users informed about written report when losing.

OE.SECRET (Appropriate management of confidential information)

The administrator has the user implemented the following operation.

- Set the value of eight-digits or more for the administrator password.
- Should not set the value that can be guessed for the administrator password, HDD lock password and encryption passphrase.
- Keep the administrator password, HDD lock password and encryption passphrase confidential.
- Change the administrator password, HDD lock 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 (Operation setting of security)

- Administrator makes "Valid" the setting of authentication operation prohibition function. (Prohibit authentication operation)
- Service engineer makes "Invalid" the remote diagnostic function.
- Service engineer makes "Invalid" the TOE update function via the internet.
- Service engineer makes "Invalid" the maintenance function.
- Service engineer makes "Valid" the service engineer authentication function.
- Administrator makes "Valid" the HDD lock function or encryption function. [2]
- Administrator makes "Invalid" the setting from the administrator function via the network.

OE.DRIVER (Utilization of exclusive driver)

The owner of IC card installs exclusive 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 of IC card.
- Support the encryption algorithm and key length that suit SP800-67.

[2] Required to buy encryption board for the use of encryption function (Installed to MFP by service engineer)

4.3. Security Objectives Rationale

4.3.1. Necessity

The correspondence between the assumptions, threats, and organizational 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 organizational security policy.

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

Organizational security policies / Assumptions / Treats / Security objectives	A.ADMIN	A.SERVICE	A.NETWORK	A.SECRET	A.IC-CARD	A.SETTING	T.DISCARD-MFP	T.BRING-OUT-STORAGE	P.COMMUNICATION-CRYPTO	P.COMMUNICATION-SIGN	P.DECRYPT-PRINT
O.DECRYPT-PRINT											X
O.OVERWRITE-ALL							X				
O.CRYPTO-KEY								X			
O.CHECK-HDD								X			
O.MAIL-CRYPTO									X		
O.MAIL-SIGN										X	
O.CRYPTO-CAPABILITY								X			
O.LOCK-HDD-CAPABILITY								X			
O.PKI-CAPABILITY										X	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					
OE.DRIVER									X		

4.3.2. Sufficiency of Assumptions

The security objectives for the assumptions are described as follows.

- **A.ADMIN (Personnel Conditions to be an Administrator)**
  This condition assumes that administrators are not malicious.
  With OE.ADMIN, the organization that uses the MFP assigns personnel who are reliable in the organization that uses the MFP, so the reliability of the administrator is realized.

- **A.SERVICE (Personnel Conditions to be a Service Engineer)**
  This condition assumes the service engineer are not malicious.
  With OE.SERVICE, the organization that manages the maintenance of the MFP educates the service engineer. Also, the administrator needs to observe the maintenance of the MFP, so that the reliability of service engineers is assured.

- **A.NETWORK (Network Connection Conditions for the MFP)**
  This condition assumes that there are no access by an unspecified person from an external network of 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 organization gives out and collects the IC cards issued by reliable PKI environment properly. It also regulates that the responsible person in the organization 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 organization 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.

- **A.SETTING (Operational setting condition concerning the security)**
  This condition assumes the following setting satisfies the operational setting condition concerning security is done for TOE.
  - Enable password lock for the administrator
  - Prohibit remote diagnostic of service engineer

- Prohibit TOE update via the internet of service engineer
- Prohibit maintenance function of service engineer
- Enable service engineer authentication function
- Enable HDD lock function or encryption function
- Prohibit setting function by administrator function via the network

OE.SETTING-SECURITY regulates that settings described above is done for all items as above, so that this condition is realized.

4.3.3. Sufficiency of Threats

The security objectives against threats are described as follows.

- **T.DISCARD-MFP (Lease return and disposal of MFP)**
  This threat assumes the possibility of leaking information from MFP collected from the user. O.OVERWRITE-ALL is that TOE provides the function to overwrite data for the deletion of all area of HDD and initializes the information of NVRAM, so that the possibility of the threat is removed by executing this function before MFP is collected.
  Accordingly, this threat is countered sufficiently.

- **T.BRING-OUT-STORAGE (Unauthorized bring-out of HDD)**
  This threat assumes the possibility that the image data in HDD leaks by being stolen from the operational environment under MFP used or by installing the unauthorized HDD and taking away with the data accumulated in it.
  For the above, the possibility of the threat is reduced by supporting the operation to use the HDD lock function by O.LOCK-HDD-CAPABILITY. In addition, when the encryption board is installed, the possibility of the threat is reduced because O.CRYPTO-KEY generates an encryption key to encrypt data written in the HDD, and a mechanical operation to use the encryption function by encryption board is supported by O.CRYPTO-CAPABILITY.
  The danger of leaking exists by bring out the HDD and replacing another HDD without the HDD lock function, but the validity of HDD installed by TOE is verified by O.CHECK-HDD, data is not written in the HDD replaced secretly. The possibility of the threat is removed consequently.
  Accordingly, this threat is countered sufficiently.

4.3.4. Sufficiency of Organizational Security Policies

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

- **P.COMMUNICATION-CRYPTO (Encryption communication of image file)**
  This organizational security policy assumes highly confidential image file (encrypted print files, scanned image files) which flows on network is encrypted to ensure the confidentiality. O.MAIL-CRYPTO supports the function to encrypt scanned image files transmitted by 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 driver for

transmission from client PC to MFP. In addition, OE.DRIVER demands to use the exclusive driver keeping image data secure. Moreover, OE.IC-CARD requests IC card owner is the rightful user.
Accordingly, this organizational security policy is sufficiently to achieve.

- **P.COMMUNICATION-SIGN (Signature of image file)**
  This organizational security policy assumes signature is added to highly confidential image files (scanned image files) which flow by mail (S/MIME).
  OE.SIGN supports the addition of signature on scanned image files transmitted by mail to the client PC from MFP certainly. O.MAIL-SIGN and O.PKI-CAPABILITY supports the function to add signature on scanned image files transmitted to user's own client PC from MFP by mail by using IC card. Moreover, OE.IC-CARD requires that IC card owner is the rightful user.
  Accordingly, this organizational security policy is sufficiently to achieve.

- **P.DECRYPT-PRINT (Decryption of image file)**
  This organizational security policy assumes only the user (IC card owner) who generated files can perform the printing of encrypted print files.
  By O.DECRYPT-PRINT, 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 operations to use IC card, which is external entity, for the decryption process of encrypted print files.
  Accordingly, this organizational security policy is sufficiently to achieve.

5. Extended Components Definition

5.1. Extended Function Component

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

- **FAD_RIP.1**

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

  - Necessity of extension

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

  - Reason for applied class (FAD)

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

  - Reason for applied family (RIP)

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

- **FIA_EID.1**

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

  - Necessity of extension

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

  - Reason for applied class (FIA)

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

  - Reason for applied family (EID)

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

- **FIT_CAP.1**

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

  - Necessity of extension

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

  - Reason for applied class (FIT)

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

  - Reason for applied family (CAP.1)

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

5.1.1. FAD_RIP.1 Definition

- **Class name**
  FAD: Protection of all data
  Meaning of abbreviation: FAD (Functional requirement for All Data protection)

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

  - Remaining Information Protection of All Data (FAD_RIP);

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

- **Component leveling**

FAD_RIP Residual Information Protection of All Data	1

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

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

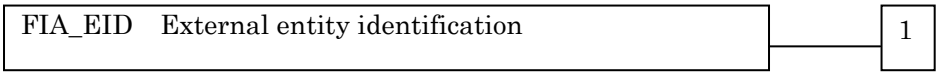
FAD_RIP.1	**Residual Information Protection of All Data after the explicit deletion operation**
FAD_RIP.1	
TSF shall ensure that the content of the information allocated to source before shall not be available after the explicit deletion operation against the object and TSF data.: [assignment: object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

5.1.2. FIA_EID.1 Definition

- **Family behaviour**

  This family corresponds to the necessity to ensure that IT environment entity is not illegally replaced when IT environment entity out of TOE provides the security functions.
  This family requires the verification of the authentication of IT environment entity.

- **Component leveling**



Meaning of abbreviation: EID (External entity IDentification)

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

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

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

5.1.3. FIT_CAP.1 Definition

- **Class name**

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

- **Class behaviour**

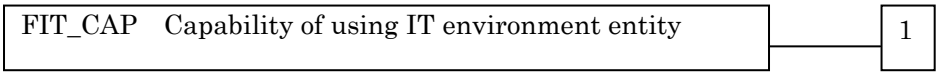
  This class contains a family specifying the requirement related with the use of the security service provided by IT environment entity. One family exists here.

- Use of IT environment entity (FIT_CAP);

- **Family behaviour**

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

- **Component leveling**



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

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

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

FIT_CAP.1	**Capability of using security service of IT environment entity**
FIT_CAP.1	
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 does not compete with CC part 2.

< Method of specifying security function requirement "Operation" >

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

<Method of clear indication of dependency>

The label in the parentheses "( )" in the dependent section indicates a label for the security functional requirements used in this ST. When it is a dependency that is not required to be used in this ST, it is described as "N/A" in the same parentheses.

6.1. TOE Security Requirements

6.1.1. TOE Security Function Requirements

6.1.1.1. Cryptographic Support

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 (SHA-1)*	*128 bits*

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

Table 3 Cryptographic Operation Relation of Algorithm-Key sizes-Cryptographic Operation

List of standards	Cryptographic algorithm	Cryptographic key sizes	Contents of Cryptographic operation
FIPS PUB 197	*AES*	*- 128 bits* *- 192 bits* *- 256 bits*	*Encryption of S/MIME transmission data*
SP800-67	*3-Key-Triple-DES*	*- 168 bits*	*Encryption of S/MIME transmission data* *Decryption of encrypted print file*
FIPS 186-2	*RSA*	*- 1024 bits* *- 2048 bits* *- 3072 bits* *- 4096 bits*	*Encryption of common key (encryptographic 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. 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 1~5***	
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 off from the authentication status of the service mode if it is, and lock the authentication function, which uses the CE password.*** • ***If it is 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 CE authentication lock time 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 1~5***	
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 off from the authentication status of the administrator mode if it is, and lock the authentication function, which uses the administrator password.*** • ***If it is not under the authentication status, lock the authentication function, which uses the administrator password.***	

<Operation for recovering the normal condition> ***- Perform the lock release function offered within the service mode.*** ***- Perform the boot process of the TOE. (Release process is performed after Administrator authentication lock time 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 5 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-digits*** ***-Character type: possible to choose from 92 or more characters***
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*] : ***-Character type: possible to choose from 92 or more characters***
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 ***(HDD Lock Password, 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 the same type of characters.*** ***(2) Do not match the value after it changes with the current setting value when changing.***
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 use under the conditions [assignment: *list of conditions under which re-authentication is required*].	
[assignment: *list of conditions under which re-authentication is required*] ***- When the service engineer modifies the CE password.*** ***- When the administrator modifies the administrator password*** ***- When the administrator changes the HDD lock setting.*** ***- When the administrator changes the Encryption function setting.***	
Hierarchical to : No other components	
Dependencies : No dependencies	

FIA_UAU.7	**Protected authentication feedback**
FIA_UAU.7.1	
The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.	
[assignment: *list of feedback*] : ***Display "*" every character data input.***	
Hierarchical to : No other components	
Dependencies : FIA_UAU.1 (FIA_UAU.2[1], FIA_UAU.2[2])	

FIA_UID.2[1]	**User identification before any action**
FIA_UID.2.1[1]	
The TSF shall require each user ***(Service Engineer)*** to identify itself 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 identify itself 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 identify itself 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

6.1.1.3. Security management

FMT_MOF.1[1]	**Management of security functions behaviour**
FMT_MOF.1.1[1]	
The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorized identified roles*].	
[assignment: *list of functions*] : ***- Remote Diagnostic Function*** ***- TOE Update Function via Internet*** ***- Maintenance Function*** ***- HDD Format Function (Physical format)*** ***- Initialization Function***	
[selection: *determine the behavior of, disable, enable, modify the behavior of*] : ***Enable***	
[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_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 behavior of*] the functions [assignment: *list of functions*] to [assignment: *the authorized identified roles*].	
[assignment: *list of functions*] : ***- Complete Overwrite Deletion Function*** ***- Management Function via Network***	
[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 behaviour
FMT_MOF.1.1[3]	
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*] : ***- Digital Signature Giving*** ***- Authentication Operation Prohibition*** ***- HDD Lock Function*** ***- Encryption Function***	
[selection: *determine the behavior of, disable, enable, modify the behavior of*] : ***disable***	
[assignment: *the authorized identified roles*] : ***Administrator***	
Hierarchical to :	No other components
Dependencies :	FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2])

FMT_MOF.1[4]	Management of security functions behaviour
FMT_MOF.1.1[4]	
The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorized identified roles*].	
[assignment: *list of functions*] : ***Service engineer Authentication Function***	
[selection: *determine the behavior of, disable, enable, modify the behavior of*] : ***Disable***	
[assignment: *the authorized identified roles*] : ***Service engineer***	
Hierarchical to :	No other components
Dependencies :	FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[1])

FMT_MTD.1[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-off Time*** ***- Authentication Failure Frequency Threshold*** ***- S/MIME Encryption Strength (Encryption Algorithm)*** ***- S/MIME Message Digest Method*** ***- Administrator Authentication Lock time*** ***- HDD Lock Password*** ***- 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*** ***- CE Authentication Lock Time***
[selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] : ***modify***
[assignment: *the authorized identified roles*] : ***Service engineer***
Hierarchical to : No other components
Dependencies : FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[1])

FMT_MTD.1[4] Management of TSF data
FMT_MTD.1.1[4]
The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].
[assignment: *list of TSF data*] : ***- Encryption Passphrase*** ***- HDD Lock Password***
[selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] : ***[assignment: other operations] : Registration***
[assignment: *the authorized identified roles*] : ***Administrator***
Hierarchical to : No other components
Dependencies : FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2])

FMT_SMF.1 Specification of Management Functions
FMT_SMF.1.1
The TSF shall be capable of performing the following security management functions: [assignment: *list of security management functions to be provided by the TSF*].
[assignment: *list of security management functions to be provided by the TSF*] : ***- Modification function of administrator password by administrator*** ***- Modification function of Administrator authentication lock time by administrator*** ***- Modification function of Panel Auto Log-off 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 by administrator*** ***- Modification function of S/MIME message digest method by administrator*** ***- Registration function of Encryption passphrase by administrator***

- Modification function of Encryption passphrase by administrator *- Registration function of HDD Lock password by administrator* *- Modification function of HDD Lock password by administrator* *- Complete overwrite deletion function by administrator* *- Digital signature giving function by administrator* *- Authentication operation prohibition function by administrator* *- HDD Lock setting function by administrator* *- Encryption setting function by administrator* *- Management function via Network by administrator* *- Modification function of service engineer password by service engineer-* *- Modification function of administrator password by service engineer* *- Modification function of CE authentication lock time by service engineer* *- Service engineer authentication setting function by service engineer* *- Remote diagnostic function by service engineer* *- TOE update function via Internet by service engineer* *- Maintenance function by service engineer* *- HDD format function by service engineer (physical format)* *- Initialization function 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 authorized identified roles*].	
[assignment: *the authorized 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 authorized identified roles*].	
[assignment: *the authorized 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])

6.1.1.4. 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

6.1.1.5. Extension: Residual information protection of all data

FAD_RIP.1	**Residual Information Protection of All Data after the explicit deletion operation**
FAD_RIP.1.1	
TSF shall guarantee not to be able to use the content of any information before having been assigned to the resource on the explicit deleting operation to the following objects and the TSF data: [assignment: *list of object and list of TSF data*].	
[assignment : *List of object and list of TSF data*] : ***<Objects>*** ***-Encrypted print file*** ***-Stored image file*** ***-HDD remaining image file*** ***-Image-related file*** ***<TSF data>*** ***-Encryption passphrase*** ***-HDD lock password*** ***-Administrator password***	
Hierarchical to	: No other components
Dependencies	: No dependencies

6.1.1.6. Extension: Approval of access destination

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

6.1.1.7. Extension: Capability of using IT environment entity

FIT_CAP.1[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*]	
[assignment: *security service provided by IT environment entity*] : ***Encryption function achieved by encryption board***	
[assignment: *necessary capability list for the operation of security service*] : ***Support function of the image files processing by 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*] : ***HDD lock function achieved by HDD***
[assignment: *necessary capability list for the operation of security service*] : ***-Support function of modifying HDD lock password*** ***-Support function of releasing HDD lock function***
Hierarchical to : No other components
Dependencies : No dependencies

FIT_CAP.1[3]	**Capability of using security service of IT environment entity**

FIT_CAP.1.1[3]
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
Development	Security architecture description	ADV_ARC.1
	Functional specification with complete summary	ADV_FSP.3
	Architectural design	ADV_TDS.2
Guidance documents	Operational user guidance	AGD_OPE.1
	Preparative procedures	AGD_PRE.1
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
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
Tests	Analysis of coverage	ATE_COV.2
	Testing: basic design	ATE_DPT.1
	Functional testing	ATE_FUN.1
	Independent testing - sample	ATE_IND.2
Vulnerability Assessment	Vulnerability analysis	AVA_VLA.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-ALL	O.CRYPTO-KEY	O.CHECK-HDD	O.MAIL-CRYPTO	O.MAIL-SIGN	O.CRYPTO-CAPABILITY	O.LOCK-HDD-CAPABILITY	O.PKI-CAPABILITY	* set.admin	* set.service
set.admin					X	X	X	X			
set.service					X	X	X	X			
FCS_CKM.1			X		X						
FCS_COP.1	X				X	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	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
FMT_MOF.1[2]										X	
FMT_MOF.1[3]										X	
FMT_MOF.1[4]											X
FMT_MTD.1[1]					X	X	X	X		X	X
FMT_MTD.1[2]										X	
FMT_MTD.1[3]											X
FMT_MTD.1[4]							X	X			
FMT_SMF.1					X	X				X	X
FMT_SMR.1[1]										X	X
FMT_SMR.1[2]					X	X				X	
FTA_SSL.3										X	
FAD_RIP.1		X									
FIA_EID.1				X							
FIT_CAP.1[1]							X				
FIT_CAP.1[2]								X			
FIT_CAP.1[3]									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)**
  This security objective explains the policy for encrypted print files.
  O.PKI-CAPABILITY provides an appropriate common key (encryption key) to decrypt encrypted print files from the IC card and FCS_COP.1 performs the decryption process of encrypted print files, when the printing operation of those files are performed by using the IC card identified by O.PKI-CAPABILITY.
  Therefore, this security objective is satisfied.

- **O.OVERWRITE-ALL (Complete overwrite deletion)**
  This security objective regulates that it deletes all data areas of HDD and initializes the concealed information of NVRAM that is set by the user, and requires various requirements that relate to the deletion.
  FAD_RIP.1 guarantees that these objective information not to be able to use the content of any previous information by the deletion operation.
  Therefore, this security objective is satisfied.

- **O.CRYPTO-KEY (Encryption key generation)**
  This security objective regulates that the encryption key necessary to encrypt all the data written in HDD by using encryption board is generated, and needs various requirements that relate to the encryption key generation.
  Using Konica Minolta HDD encryption key generation mechanism (SHA-1) according to the Konica Minolta encryption specification standard, FCS_CKM.1 generates an encryption key 128bits long.
  This security objective is satisfied by the completion of this function requirement.

- **O.CHECK-HDD (Validity confirmation of HDD)**
  This security objective regulates that it verifies the validity of HDD in order to confirm the unauthorized HDD doesn't exist, and needs various requirements that relate to the verification of an external entity from TOE.
  FIA_EID.1[1] identifies HDD before the action from TOE to HDD, and cancels the scheduled action when the identification fails.
  This security objective is satisfied by the completion of this function requirement.

- **O.MAIL-CRYPTO (Usage and encryption of S/MIME)**
  This security objective regulates that it encrypts when transmitting images scanned by using MFP to the user's own mail address, and various requirements related to encryption are necessary.
  FCS_CKM.1 generates encryption keys (128bits, 168bits, 192bits or 256bits) by using Pseudo-random number Generation Algorithm according to FIPS 186-2.
  FCS_COP.1 encrypts the scanned images by using AES (encryption key: 128bits, 192bits or 256bits) of FIPS PUB 197. (It becomes transmission data of S/MIME). In addition, the same requirement encrypts scanned images by using 3-Key-Triple-DES (encryption key: 168bits) of SP800-67. (Similarly, it becomes transmission data of S/MIME.) FCS-COP.1 encrypts these

common keys (encryption keys) by RSA of FIPS 186-2 that is public key of S/MIME certificate of each destination (1024bits, 2048bits, 3072bits or 4096bits) by using the IC card identified by O.PKI-CAPABILITY. Also, FMT_MTD.1[1] limits the settings of encryption algorithm to administrators.
This security objective is satisfied by the completion of these function 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 it generates the message digest assumed to give the signature when transmitting images scanned by using MFP to user's own mail address by mail, and various requirements related to the message digest are required.
FSC_COP.1 generates the message digest that is required for the signature process, by the hash function regulated by FIPS 180-2 (SHA-1 or SHA-256), by using the IC card identified by O.PKI-CAPABILITY. In addition, FMT_MTD.1[1] limits the setting of message digest method to administrators.
This security objective is satisfied by the completion of these function 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 controlling function for each management>
As the role of doing these managements, FMT_SMR.1[1] maintains a service engineer and FMT_SMR.1[2] maintains an administrator. In addition, FMT_SMF.1 specifies these management functions.

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

This security objective regulates that TOE's support action for the data stored in HDD is encrypted by the encryption board that is the entity out of TOE, and needs various requirements that regulates the support of external entity action.
Applying FIT_CAP.1[1], the support function to process all data in HDD through the encryption function is achieved for the encryption function realizing with the encryption board. In addition, FIA_SOS.1[3] verifies the quality of the encryption passphrase used for the encryption and FMT_MTD.1[1] and FMT_MTD.1[4] limits the settings to administrators.
This security objective is satisfied by the completion of this function 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 controlling function for each management>
As the role of doing these managements, FMT_SMR.1[1] maintains a service engineer and FMT_SMR.1[2] maintains an administrator. In addition, FMT_SMF.1 specifies these management functions.

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

This security objective regulates that TOE's support action refuses the unauthorized access from MFP other than the one that is set by the HDD that is the entity out of TOE, and needs various requirements that regulates the support of external entity action.
Applying FIT_CAP.1[2], the support function to change the HDD lock password and to release the HDD lock function for the HDD lock function realized by HDD is achieved. FIA_SOS.1[3] verifies the quality of the HDD lock password and FMT_MTD.1[1] and FMT_MTD.1[4] limits the setting to the administrator.
This security objective is satisfied by the completion of this function 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 controlling function for each management>
As the role of doing these managements, FMT_SMR.1[1] maintains a service engineer and FMT_SMR.1[2] maintains an administrator. 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 encrypting and giving signature to images scanned 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 regulates the support of external entity action.
Applying FIT_CAP.1[3], 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 the completion of this function requirement.

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

<Identification and Authentication of an administrator>
FIA_UID.2[2] and FIA_UAU.2[2] identifies and authenticates that the accessing user is 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 (1-5 times) consecutively, FIA_AFL.1[2] logoffs 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 administrator authentication lock time 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.

<Management of session of identified and authenticated administrator>
The duration of session of the administrator who is identified and authenticated contributes to reduce the chance of attacking associated with unnecessary session connection by ending the session after the panel automatic logoff time elapses by FTA_SSL.3 if it logs in from the panel. The change in the panel auto logoff time is limited to the administrator by FMT_MTD.1[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 (1-5 times), FIA_AFL.1[2] logoffs 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 administrator authentication lock time passed.

<Role and management function for each management>
FMT_SMR.1[1] have service engineer maintain the role to do these management, and FMT_SMR.1[2] have the administrator do the same. Additionally, FMT_SMF.1 specifies theses management functions and FMT_MOF.1[2] and FMT_MOF.1[3] manage those behavior.

- ***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 "*" 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 (1-5 times) consecutively, FIA_AFL.1[1] logoffs it if it's under authentication, and locks all the authentication functions to use the CE password. The CE authentication lock release function is executed and the CE authentication lock time goes by, so that this lock status is released.

FMT_MTD.1[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 CE authentication lock time.

<Management of service engineer's authentication information>
FIA_SOS.1[1] verifies the quality of the CE password. FMT_MTD.1[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 (1-5 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 the CE authentication lock time goes by, so that this lock status is released.

<Role and management function for each management>
FMT_SMR.1[1] maintains the role to do these managements as a service engineer. In addition, FMT_SMF.1 specifies these management functions and FMT_MOF.1[1] and FMT_MOF.1[4] manage those behavior.

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: The generated key by the Pseudo-random number Generation Algorithm is operated. <The reason not to fulfill partially FCS_CKM.2 or FCS_COP.1> - 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. <The reason not to apply FCS_CKM.4> - The key generated by the Pseudo-random number Generation Algorithm is thought that exists in the volatile storage area temporarily, but there is no necessity to think about the cancellation since there is no access from the outside and it is destroyed automatically. - The key generated by the Konica Minolta HDD encryption key generation algorithm is stored constantly since it is the stored data. In addition, the arbitrary access to the storage media is difficult and there is no necessity of the cancellation of the encryption key.
FCS_COP.1	FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2, FCS_CKM.4	FCS_CKM.1 (only a part of the phenomenon) The satisfied events: The common key for encrypting the S/MIME transmission data is generated. <The reason not to satisfy a part of the FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2> - FIT_CAP.1[3] 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[3] 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

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
		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 key that is used for the encryption of S/MIME transmission data, the decryption of encrypted print file and the generation of message digest is thought that exists in the volatile storage area temporarily, but there is no necessity to think about the cancellation since there is no access from the outside and it is destroyed automatically. - 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 encrypted key cancellation.
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
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_MOF.1[2]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[2]
FMT_MOF.1[3]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[2]
FMT_MOF.1[4]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[1]
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_MTD.1[4]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]
FMT_SMF.1	None	N/A
FMT_SMR.1[1]	FIA_UID.1	FIA_UID.2[1]
FMT_SMR.1[2]	FIA_UID.1	FIA_UID.2[2]
FTA_SSL.3	None	N/A
FAD_RIP.1	None	N/A
FAD_EID.1	None	N/A
FIT_CAP.1[1]	None	N/A
FIT_CAP.1[2]	None	N/A

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
FIT_CAP.1[3]	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 high level design, and analysis of the strength of function and a search for vulnerabilities are required. In addition, it is desirable that it has a development environment control, a configuration management for the TOE and a secure distribution procedure. And therefore, the selection of EAL3, which provides an adequate assurance level, is reasonable.

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

7. TOE Summary Specification

The list of the TOE security function led from the TOE security function requirement is shown in the following Table 7. 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 (All area overwrite deletion function)	Administrator function
7.6	F.CRYPTO (Encryption key generation function)	Other function
7.7	F.VALIDATION-HDD (HDD validation function)	Other function
7.8	F.RESET (Authentication Failure Frequency Reset function)	Administrator function, Service engineer function
7.9	F.S/MIME (S/MIME encryption processing function)	Basic function
7.10	F.SUPPORT-CRYPTO (Encryption board support function)	Other function
7.11	F.SUPPORT-HDD (HDD lock operation support function)	Other function
7.12	F.SUPPORT-PKI (PKI support 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.
- It does 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 1~5 times consecutively 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 or the lock release function of the administrator authentication function in F.SERVICE is carried out, and the lock of authentication function is released.

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

7.1.2. Auto Logoff Function of Administrator Mode

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

As described above, FIA_SSL.3 is realized.

Table 8 Characters and Number of Digits for Password [3]

Objectives	Number of digits	Characters
- Administrator Password	(0 - 8)	Selectable from 92 or more characters in total
- CE Password	8	Selectable from 92 or more characters in total
- Encryption passphrase - HDD lock password	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

[3] 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.

administrator authority is associated with the task substituting the user. In addition, 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, 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 by the access from the panel.
- When the authentication failure that becomes 1-5 times consecutively in each authentication function by using the administrator password is detected, it logoffs the administrator mode accessing from the panel, and locks all the authentication functions to use the administrator password. (The access to the administrator mode is refused.)
  - The administrator specifies the failure frequency threshold by the unauthorized access detection threshold setting function.
- F.RESET works or the lock release function of the administrator authentication function in F.SERVICE is carried out, so that the lock of the authentication function is released.
- Verify the new administrator password if it is composed of the characters and by the number of digits, shown in the Table 8.

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

7.1.3.2. Unauthorized Access Setup

- Setup of unauthorized access detection
  Whether to activate or stop the authentication operation prohibition function is selected.
- Setup of unauthorized access detection threshold
  The unauthorized access detection threshold in the authentication operation prohibition function is set for 1-5 times.
- Setup of Administrator Authentication Lock Time
  Set the Administrator Authentication Lock Time between 1-60 minutes.

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

7.1.3.3. Setup of Auto Logoff Function

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

- panel auto logoff time : 1 - 9 minutes

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

7.1.3.4. Setting function of HDD lock function

<Operation setting ON>
When turning it ON from OFF, it verifies that the newly set HDD lock password satisfies the

following quality.

- The characters and the number of digits of HDD lock password conform to those specified in Table 8.
- This password is not composed of one character only.

As described above, FIA_SOS.1[3], FMT_MOF.1[3], FMT_MTD.1[4], FMT_SMF.1 and FMT_SMR.1[2] are realized.

<Modification of HDD lock password>

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

- Provides the HDD lock password verification mechanism that verified the HDD lock password that consists of the character shown in Table 8.
- Return, in verification, "*" for each character as feedback for the entered HDD lock password.
- Verify the HDD lock password newly set if the following qualities are satisfied.
  - The characters and the number of digits of this password conform to those specified in Table 8.
  - This password is not composed of one character only.
  - This password is not equal to the currently setup password.

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

7.1.3.5. Operation Setup of Encryption Function

(* When the encryption board to encrypt is installed in MFP, it can be operated.)

<Operation Setting ON>

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

- It is composed of the characters and by the number of digits shown in Table 8.
- It shall not be composed of one kind of character.

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

<Encryption Passphrase Change>

The encryption passphrase is changed. F.CRYPTO is performed when it is re-authenticated by the currently setup encryption passphrase that the user is an administrator, and the newly setup encryption passphrase satisfies quality requirements.

- It provides the encryption passphrase verification mechanism that verified the encryption passphrase that consists of the character shown in Table 8.
- Return, in verification, "*" for each character as feedback for the entered encryption passphrase.
- Verify the encryption passphrase newly set if the following qualities are satisfied.
  - It is composed of the characters and by the number of digits shown in Table 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], FIA_UAU.7, FIA_UAU.6, FMT_MTD.1[1], FMT_SMF.1

and FMT_SMR.1[2] are realized.

7.1.3.6. 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 giving 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.

7.1.3.7. Function Related to Password Initialization Function

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

- All area overwrite deletion function
  The settings of the administrator password is initialized to the values at factory shipment by executing the overwrite deletion of all area

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

7.1.3.8. Operation Setup Related to Security

The operation setup functions related to the security that the administrator operates, are as follows.

- Valid and invalid setting of the administrator function from the network
  By making the administrator function from the network valid, it can use the administrator function via the network.

As described above, FMT_MOF.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.
- Reset 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 1-5 times consecutively 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 new password satisfies the quality, it is changed.

- Provides the CE authentication mechanism that is re-authenticated by the CE password that consists of the characters shown in Table 8.
- Resets the authentication failure frequency when succeeding in the re-authentication.
- Return "*" for each character as feedback for the entered service codes in the re-authentication.
- When the authentication failure that becomes 1-5 times consecutively in each authentication function by using the CE password is detected, it logs off 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.
- F.RESET function unlocks the authentication function.
- It verifies that the CE password newly set is composed of the characters and by the number of digits, shown in the Table 8.

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

7.2.2.3. Release of the Lock of Administrator Authentication Function

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

- If access is locked, the lock is released.

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

7.2.2.4. Setup of CE Authentication Lock Time

Set the CE Authentication Lock Time between 1 - 60 minutes.
As described above, FMT_MTD.1[3], FMT_SMF.1 and FMT_SMR.1[1] are realized.

7.2.2.5. Setup of Service Engineer Authentication Function

Set the service engineer authentication function to valid or invalid.
As described above, FMT_MOF.1[4], FMT_SMF.1 and FMT_SMR.1[1] are realized.

7.2.2.6. Management of the function affecting the TSF data

The functions affecting the other TSF data that are operated by the service engineer are as follows.

- HDD format function (physical format)
  Function to write in HDD the initial value of the management data that is used for the file system
- Initialization function
  Function to return the various set values written in NVRAM to the factory shipment state
- Maintenance function
  Function to perform the maintenance of breakdown etc. by connecting serial through RC-232C
- Remote diagnostic function
  Function to manage the device information such as the MFP operating status and the number of prints by communicating with support center of MFP
- TOE update function via the internet
  Function to download the TOE through Ethernet

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 by the common key (encryption key) that is obtained by F.SUPPORT-PKI to the print operation.

- The common key (encryption key) (168 bits) to decrypt the encrypted print file is

decrypted by the 3-Key-Triple-DES that is regulated by the SP800-67.

As described above, FCS_COP.1 is realized.

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

F.OVERWRITE-ALL executes the overwrite deletion in the data area of HDD, and initializes the settings such as passwords set in NVRAM as well. The object for the deletion or the initialization is as follows.

<Object for the deletion : HDD>

- Encrypted print file
- Stored image file
- HDD remaining image file
- Image related file

<Object for the initialization : NVRAM>

- Administrator Password
- Operation setting of HDD lock function (OFF) --- HDD lock password is deleted.
- Operation setting of Encryption function (OFF) --- Encryption Passphrase is deleted.

The deletion methods such as the data overwritten in HDD and the written frequency is executed according to the deletion method of overwrite area deletion function set by F.ADMIN (Table 9). The HDD lock password and the encryption passphrase, which are set, cannot be used by being turned off the operation setting of the HDD lock function and the encryption function.

As described above, FAD_RIP.1 is realized.

Table 9 Types and Methods of Overwrite Deletion of Overall 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 all data written in HDD by using the HDD encryption key generation algorithm (SHA-1) that is regulated by the Konica Minolta encryption specification standard. Konica Minolta HDD encryption key generation algorithm (SHA-1) is the algorithm to generate the encryption key by using the SHA-1 regulated by FIPS 180-2.

When the encryption passphrase is decided in the encryption functional operation setting to

which the access is restricted in F.ADMIN, an encryption key 128bits long is generated from the encryption passphrase by applying the Konica Minolta HDD encryption key generation algorithm (SHA-1).

As described above, FCS_CKM.1 is realized.

7.7. F.VALIDATION-HDD (HDD Verification Function)

F.VALIDATION-HDD is a check function to permit reading from and writing in the HDD only when it is verified that the illegal HDD is not installed and is confirmed validity when the HDD lock password is set to HDD

When the HDD lock password is set to HDD, the status of HDD is confirmed in the HDD operation verifying at the time of TOE starting. When the HDD lock password certainly being set is returned as the result of status confirmation, the access to HDD is permitted. If the HDD lock password not being set is returned, the access to HDD is refused because of an illegitimate possibility.

As described above, FIA_EID.1 is realized.

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

F.RESET is a function that releases the lock by resetting the authentication failure frequency when the account locks in the administrator authentication and CE authentication.

(1) CE Authentication function lock release processing function

The function is executed by the specific operation, and the lock is released by clearing the failure frequency of the CE authentication to 0 after CE authentication lock time.

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

(2) Administrator authentication function lock release processing function

The function is executed by OFF/ON of the main power supply, and the lock is released by clearing the failure frequency of the administrator authentication to 0 after the administrator authentication lock time.

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

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

F.S/MIME is a function to encrypt and sign the scanned image when transmitting the scanned image to the user by S/MIME. The IC card generates the signature by F.SUPPORT-PKI, but this generates the message digest using for the signature on this function.

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

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

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 used by F.SUPPORT-PKI in this case is 1024bits, 2048bits, 3072bits or 4096bits.

As described above, FCS_COP.1 is realized.

<Message Digest Generation>

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

As described above, FCS_COP.1 is realized.

7.10. F.SUPPORT-CRYPTO (Encryption Board Support Function)

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

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

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

7.11. F.SUPPORT-HDD (HDD lock Operation Support Function)

F.SUPPORT-HDD is the function to operate HDD lock function of HDD from TOE.

<Release process of HDD lock state>

At the MFP power ON, the release process of HDD lock state of HDD lock function is achieved.

- Release process is requested to HDD by using HDD lock password stored in NVRAM.

<Modification process of HDD lock password>

F.ADMIN requests to change the HDD lock password.

- Modification process is requested to HDD by using HDD lock password stored in NVRAM and new HDD lock password.

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

7.12. 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[3] is realized.