bizhub 4750 / bizhub 4050
PKI Card System Control Software
Security Target

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

Version: 1.09

Issued on: 24 July, 2015

Created by: Konica Minolta, Inc.

<Revision History>

Date	Ver	Division	Approved	Checked	Created	Revision
4/30/2014	1.00	Office Products System Control Development Division 2	Horimoto	Konishi	Tsuyama	Initial Version
8/26/2014	1.01	Office Products System Control Development Division 2	Horimoto	Konishi	Toda	- Review and correct the description concerning S/MIME. (PSWC is disabled when Enhanced encryption mode is enabled.) - Review concerning Boot control. - Add description concerning evaluation environment. - Deal with typos.
9/8/2014	1.02	Office Products System Control Development Division 2	Horimoto	Konishi	Toda	-Modify the name of TOE.
9/26/2014	1.03	Office Products System Control Development Division 2	Horimoto	Konishi	Toda	- Review and correct whole description.
10/8/2014	1.04	Office Products System Control Development Division 2	Horimoto	Konishi	Toda	- Deal with typos.
10/23/2014	1.05	Office Products System Control Development Division 2	Horimoto	Konishi	Toda	- Deal with typos. (Client PC environment)
11/11/2014	1.06	Office Products System Control Development Division 2	Horimoto	Konishi	Toda	- Deal with typos.
12/3/2014	1.07	Office Products System Control Development Division 2	Horimoto	Konishi	Toda	- Review and correct the description concerning protected assets and dependency of encryption support. - Deal with typos.
12/22/2014	1.08	Office Products System Control Development Division 2	Horimoto	Konishi	Toda	- Correct the TOE version.
7/24/2015	1.09	Office Products System Control Development Division 2	Horimoto	Konishi	Tamukai	- Correct Guidance.

— [Table of Contents] ————————————————————

— [List of Figures] —

— [List of Tables] —

1. ST Introduction

1.1. ST Reference

- ST Title	:	bizhub 4750 / bizhub 4050 PKI Card System Control Software Security Target
- ST Version	:	1.09
- Created on	:	July 24, 2015
- Created by	:	Konica Minolta, Inc.

1.2. TOE Reference

- TOE Name	:	bizhub 4750 / bizhub 4050 PKI Card System Control Software
- TOE Version	:	A6F730G0273999P (Description of TOE version: Controller firmware)
- TOE Type	:	Software
- Created by	:	Konica Minolta, Inc.

1.3. TOE Overview

This section explains the type, usage and main security functions of TOE. The usage and operational environments will be described in the Section “1.4”.

1.3.1. TOE Type

bizhub 4750 / bizhub 4050 PKI Card System Control Software, which is the TOE, is an embedded software product installed in the eMMC on the mfp controller to control the operation of the whole mfp.

1.3.2. Usage of TOE and Main Security Functions

bizhub 4750 / bizhub 4050 are digital multi-function products provided by Konica Minolta, Inc., composed by selecting and combining copy, print, scan and FAX functions. (Hereinafter all the products are referred to as "mfp".) TOE is the “bizhub 4750 / bizhub 4050 PKI Card System Control Software" that controls the entire operation of mfp, including the operation control processing and the image data management triggered by the panel of the main body of mfp or through the network.

TOE supports the function to print the encryption print realized by using a special printer driver and IC card by using exclusive driver (loadable driver) and the IC card that is used generating that encryption print for a printer data transmitted to mfp from client PC among the highly confidential document transmitted between mfp and client PC. Also, it provides a function of protecting the scanned image data transmitted by mail from mfp by S/MIME through the use of a loadable driver and an IC card. Both of these security functions are realized by the combined TOE and an IC card.

Moreover, for the danger of illegal access to HDD that is medium that temporarily stores image data processed in mfp, TOE can encrypt image data written in HDD. Besides, TOE has the function that completely deletes all data area of HDD including stored image data by deletion method compliant with various overwrite deletion standards. So it contributes to the prevention of information leakage of the organization that uses mfp.

1.4. TOE Description

1.4.1. Roles of TOE Users

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

- User
  An mfp user who owns IC card. (In general, the employee in the office is assumed.)

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

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

- Responsible person of the 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.

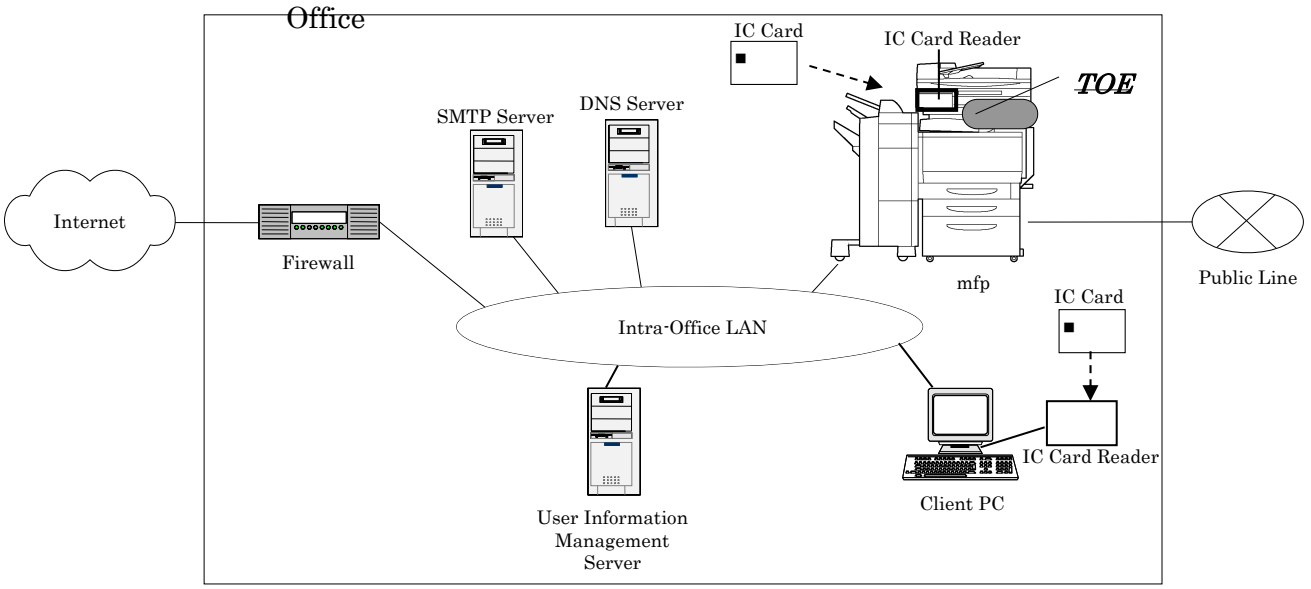

Figure 1 An example of mfp's use environments

- 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 scanned image data transmitted from mfp.
- User information management server is connected to an intra-office LAN and it is used to the authentication of IC card. As a user information management server, Windows Server OS which can use Active Directory (Kerberos authentication protocol) is used for TOE verification.
- When a SMTP server is connected to the intra-office LAN, mfp can carry out data communication with these servers, too. (The DNS service will be necessary when setting a domain name of the SMTP server)
- When the intra-office LAN connects to an external network, measures such as connecting via a firewall are taken, and an appropriate setup to block access requests to the mfp from the external network is applied.
- The public line connected with mfp is used for communications by FAX.

1.4.2.2. Operation Environment

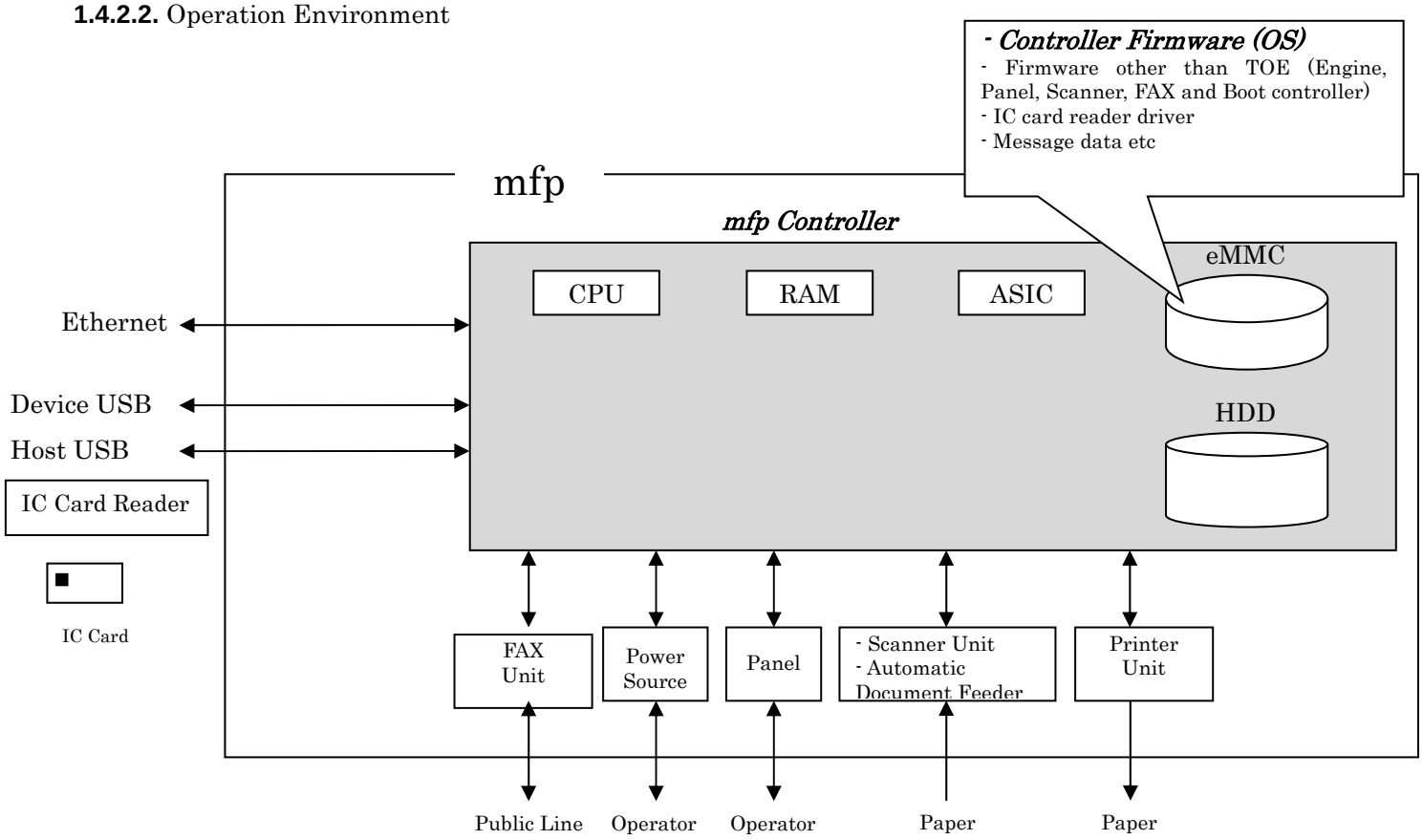

Figure 2 Hardware composition relevant to TOE

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

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

- RAM
  An encryption key which is used for HDD encryption is stored.

- eMMC（Embedded MultiMedia Card）
  An NAND type flash memory. A storage medium which stores object code of controller firmware for PKI Card System Control Software, which is TOE, object code of Engine, Panel and Boot controller, which are firmware other than TOE, IC card reader driver and message data. It also stores an administrator password and CE[1] password, which are used for TOE processing.

- ASIC
  An integrated circuit designed for overall image processing. It also processes image development and color adjustment when the image is printed.

[1] An abbreviation for Customer Service engineer; Also CE is used as a service engineer.

- HDD
  Image data is stored as a file as well as IC card ID. All image files and IC card ID are encrypted when stored.

- Power source
  Power switches for activating mfp.

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

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

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

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

- Device USB
  A port on the back of the mfp for local printing.

- Host USB
  A USB port on the panel side of mfp. It can be used for TOE update, print from USB flash drive connected to USB interface or storing scanned data. Note that the encryption print and S/MIME encryption processing functions which are described in this ST are not included in this print and scan.
  User can access to mfp with IC card if IC card reader is connected. Although IC card reader is not a standard feature of mfp but an optional accessory for sales reasons, this ST assumes it as indispensable component.

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

- IC card reader
  An equipment connecting to mfp and client PC to read IC card.
  The supported product type is AU-211P/Identive SCR-3310/SCR-3310v2.

- IC card reader driver
  A driver to access to IC card reader.
  The IC card reader driver which corresponds to the type of IC card and IC card reader is required.
  The following driver is used for TOE evaluation of mfp.
  IC card reader driver A6F70Y0-A401-G00-00

- FAX unit
  A device that has a port of Fax public line and is used for communications for FAX-data transmission via the public line.

- Software on client PC
  The software versions of client PC for TOE evaluation are as follows:
  (1) Windows 7 Professional SP1
  (2) Internet Explorer Ver.11
  (3) printer driver : Windows Printer Driver KONICA MINOLTA 4750 Series PCL6 v1.1.5.0
  (4) ActivClinet v7.0.2.25

1.4.2.3. Guidance

- bizhub 4750/4050 for PKI Card System
  SERVICE MANUAL [SECURITY FUNCTION] Ver. 1.03
- bizhub 4750/4050 for PKI Card System
  User's Guide [Security Operations] Ver. 1.04

1.4.3. Logical Scope of TOE

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

1.4.3.1. Basic Function

In mfp, a series of functions for the office work concerning the image such as copy, print, scan, and fax exists as basic functions, and TOE performs the core control in the operation of these functions. It converts the raw data acquired from the external device of the mfp controller into image files, and stores them in RAM and HDD. (For print image files from client PCs, multiple types of conversion are applied.) These image files are converted into data to be printed or sent, and transmitted to the device outside of the mfp controller concerned. Also, various functions are realized with IC card.

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

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

- Encryption Print Function

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

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

  When printing is requested by a client PC, this function eliminates the possibility that other users stole a glance at the printing of highly confidential data, or such data is slipped into the other printings.

- Scan To Me Function

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

  - S/MIME Encryption Function

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

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

  - Digital Signature Function

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

1.4.3.2. Administrator Function

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

The following shows the functions related to the security.

- Operational setup of automatic system reset
  - Setup of the function that logs out automatically when the setting time passed in an idle state.
- Setup of password rules function
  - Whether to activate or stop the function to check the conditions of password such as effective digit of various passwords is selected.
- HDD encryption function settings
  - Operation settings of HDD encryption function
- Encryption key generation for encrypting HDD
  - When mfp is powered on, a key is generated with a encryption passphrase to store volatile memory (RAM).
- Data Complete Deletion Function
  - There are data deletion methods conformed to various military standards (e.g. Military Standard of United States Department of Defence)
  - When this function is started up, in conformity with a set method selected by administrator, the overwrite deletion is executed for the overall area of HDD. (All area overwrite deletion function of HDD)
  - Administrator password and encryption passphrase of eMMC is initialized. (eMMC initialization function)
  - The above two are collectively called Data Complete Deletion Function.
  - Data Complete Deletion Function is activated from the panel.
- Setup of the HDD encryption function
  - Whether to activate or stop the function is selected.
  - An encryption passphrase is registered or changed when the function is activated.
- HDD logical format function
  - A logical format through the panel is executable.
  - The logical format is used to initialize HDD.
- HDD encryption function
  - When the operation setting of HDD encryption function is “Enable”, data written on HDD such as all image file and password is encrypted.
  - An administrator enters a character string (20-digit) when using the encryption function. The string is stored on eMMC with an encryption passphrase.

1.4.3.3. Service Engineer Function

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

- Modification function of administrator password

The following is a set of operation setting functions related especially to the behavior of the security function (Setting data of administrator password, setting of HDD encryption function etc.)

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.

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

TOE makes effective use of the security function of IC card, which is an external entity. The following explains typical functions related to the external entity.

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

1.4.3.5. Enhanced Security Function

Various setting functions related to the behavior of the security function for the Administrator function and the Service engineer function can be set collectively to the secure values by the operation settings of the "Enhanced Security Function". Alert screen is displayed if each value set is changed to the vulnerable one individually. Also the use of the update function of TOE through the network and the initializing function of the network setting is prohibited, or alert screen is displayed when it is used.

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

- User : access of PUBLIC: Prohibited
- Print without authentication: Invalid
- User Name List: Prohibited
- Password policy function: Valid
- User Box administrator function: Prohibited
- SNMP v1 / v2c Write function: Prohibited
- Use of SNMPv3: Prohibited
- Setup of HDD encryption function: Valid
- Print data capture function: Prohibited
- Address registration user change function: Prohibited

- Network Server Function: Prohibited
- Setup of limitation of S/MIME encryption severity: Valid
  (Only 3DES and AES are selectable.)
  (SHA-256 becomes Valid.)
- Transmission of Image log: Prohibited
- Remote Panel Function: Prohibited

The following function becomes the following setting when the enhanced security function is enabled. In contrast to the above function group, however, the setting can be changed individually.

- FTP server function setting: Prohibited

2. Conformance Claims

2.1. CC Conformance Claim

This ST conforms to the following standards.

Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and general model Version 3.1 Revision 4 (Japanese Translation v1.0)
Part 2: Security functional components Version 3.1 Revision 4 (Japanese Translation v1.0)
Part 3: Security assurance components Version 3.1 Revision 4 (Japanese Translation v1.0)

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

2.2. PP Claim

There is no PP that is referenced by this ST.

2.3. Package Claim

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

2.4. Reference

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

3. Security Problem Definition

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

3.1. Protected Assets

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

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

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

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

- Encrypted Print File
- Scanned Image File
- Stored Image File
  Stored image files other than encrypted print file
- Image file of job in the waiting state
  Image file of job in the waiting state and existing in the HDD data area
- 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
- Administrator Password
  Administrator password stored in eMMC
- Encryption Passphrase
  Encryption passphrase registered in eMMC

3.2. Assumptions

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

A.ADMIN (Personnel conditions to be an administrator)

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

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

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

A.NETWORK (Network connection conditions for mfp)

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

A.SECRET (Operational condition about secret information)

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

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

IC card is owned by rightful user in the use of TOE.

3.3. Threats

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

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

When leased mfps are returned or discarded mfps are collected, encrypted print files, scanned image files and stored image files as well as administrator password and encryption passphrase can be leaked by the person with malicious intent when he/she analyzes the HDD and eMMC in the mfp.

T.ACCESS-HDD (Unauthorized access to HDD)

Data stored on HDD such as all image files and password can be disclosed by a malicious person or a user when s/he illegally access to the HDD.

3.4. Organizational Security Policies

This ST assumes a TOE security environment corresponding to an organization or user such as demanding the encryption of files and permitting access only to mail messages to which a signature is appended as an intra-office LAN security measure for protected assets that requires considering confidentiality. 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 files) received by mfp are permitted to print only to a user who generated those 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 for the TOE and the environment for the usage of the TOE are described. This is described by being divided into the categories of the security objectives for the TOE and the security objectives for the environment below.

4.1. Security Objectives for the TOE

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

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

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

O.OVERWRITE-ALL (Data Complete Deletion

TOE disables reproduction of data stored on data area of HDD in mfp such as encrypted print file, scanned image file, image file of job in the waiting state, stored image file, HDD remaining image file, image-related file, and administrator password and encryption passphrase on eMMC set by an administrator.

O.CRYPTO-HDD (HDD encryption)

To protect all data written in HDD in mfp such as image data and password, TOE provides a function to generate an encryption key using an encryption passphrase and to encrypt and decrypt data such as image file and password. In addition, it provides a function to verify the quality of the encryption passphrase. Moreover, the function related to the setting of HDD encryption function (encryption passphrase) is provided only to an administrator.

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

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

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

4.2. Security Objectives for the Operational Environment

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

OE.ADMIN (A reliable administrator)

The responsible person in the 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)

When requesting maintenance to TOE, the responsible person or administrator in the organization who uses mfp concludes a maintenance contract with a company who performs maintenance. In the maintenance contract, it is clearly stated not to commit improper act. Before maintenance work, the administrator checks an ID of maintenance staff whether s/he is the service engineer coming from the regular maintenance company, and the administrator observes the maintenance.

OE.CARD-USER (Utilization of IC card)

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

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

A responsible person of an organization that uses mfp must follow the following operation manners:

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

OE.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.SECRET (Appropriate management of confidential information)

The administrator executes the following operation.

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

The service engineer executes the following operation.

- Should not set the value that can be guessed for the CE password.
- Keep the CE password confidential.
- The CE password should be properly changed.
- 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.

OE.SETTING-SECURITY (Security related Setting, Maintenance, Operation)

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

OE.DRIVER (Utilization of exclusive printer driver)

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

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

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 organization security policies

Organization security policies / Assumptions / Threats / Security objectives	A.ADMIN	A.SERVICE	A.NETWORK	A.SECRET	A.IC-CARD	T.DISCARD-mfp	T.ACCESS-HDD	P.COMMUNICATION-CRYPTO	P.COMMUNICATION-SIGN	P.DECRYPT-PRINT
O.DECRYPT-PRINT										X
O.OVERWRITE-ALL						X				
O.CRYPTO-HDD							X			
O.MAIL-CRYPTO								X		
O.MAIL-SIGN									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	X	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 to administrator, so the reliability of the administrator is satisfied.

- **A.SERVICE (Personnel Conditions to be a Service Engineer)**
  This condition assumes the service engineer does not commit any improper act.
  With OE.SERVICE, the organization that introduces TOE concludes a maintenance contract which clearly states that the maintenance staff of TOE does not commit any improper act, the administrator confirms the identity of the service engineer with his ID before the maintenance work, and the administrator observes the maintenance work, so the reliability of this condition is satisfied.

- **A.NETWORK (Network Connection Conditions for the mfp)**
  This condition assumes that there are no access by an unspecified person from an external network to the intra-office LAN.
  OE.NETWORK regulates the unauthorized access prevention from external by the installation of devices such as firewall in order to block access to the mfp from the external networks, so that this condition is satisfied.

- **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 satisfied.

- **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 satisfied.

4.3.3. Sufficiency of Threats

The security objectives against threats are described as follows.

- **T.DISCARD-MFP (Lease return and discard of mfp)**
  This threat assumes the possibility of leaking information from mfp collected from the user.
  O.OVERWRITE-ALL provides the function that TOE overwrites data for the deletion of image data area of protected assets in HDD and administrator password and encryption passphrase in eMMC. Also, OE.SETTING-SECURITY is that TOE operates along with the guidance, so that the possibility of the threat is removed by executing the function of overwriting and initializing, TOE provides, before mfp is collected.
  Accordingly, this threat is countered sufficiently.

- **T.ACCESS-HDD (Unauthorized access to HDD)**
  This threat assumes the possibility of disclosing all data written in HDD of mfp such as image file and password by unauthorized access to HDD.
  With O.CRYPTO-HDD, the possibility of the threat is reduced because an encryption key is generated with an encryption passphrase and all data such as image file and password are encrypted when they written in HDD and decrypted when they properly read out.
  Also the possibility of the threat is reduced with an encryption passphrase because its quality is verified.
  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 that the highly confidential image files to be communicated on the network (encrypted print files, scanned image files) are encrypted so as to secure the confidentiality of the files.
  O.MAIL-CRYPTO supports the function to encrypt scanned image files transmitted by e-mail from mfp to user's own client PC. OE.CARD-USER requires the use of IC card for transmission to client PC from mfp, and the use of IC card and exclusive printer driver for transmission from client PC to mfp. In addition, OE.DRIVER demands to use the exclusive printer driver keeping image data secure. Moreover, OE.IC-CARD requests IC card owner is the rightful user. Also, the operation related to the setting and the maintenance along with the guidance including the enhanced security function is performed by OE.SETTING -SECURITY. Accordingly, this organizational security policy is sufficiently achieved.

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

- **P.DECRYPT-PRINT (Decryption of image file)**

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

5. Extended Components Definition

5.1. Extended Function Component

In this ST, two 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 family 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.

- 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 security functions of external IT entity, the security function of external IT entity 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 (FIT_CAP)

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

5.1.1. FAD_RIP.1 Definition

- **Class name**

  FAD: Protection of all data

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

- **Class behavior**

  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.

  - Residual Information Protection of All Data (FAD_RIP);

- **Family behavior**

  This family (FAD_RIP) corresponds to the necessity never to access the deleted data or to guarantee that any data included in the resource is invalid when it is reallocated to other user data or TSF data. 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 user data and TSF data controlled by TSF cannot utilize any remaining information of every resource under the allocation of resource or the release of it.

Management : FAD_RIP.1
No expected management activity
Audit : FAD_RIP.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST. a) Minimal: The use of the user identification information with the explicit deletion operation

FAD_RIP.1	**Residual Information Protection of All Data after the explicit deletion operation**
Hierarchical to	: No other components
Dependencies	: No dependencies
FAD_RIP.1.1	
TSF shall ensure that the content of the information allocated to source before shall not be available after [assignment: Residual release request of resource allocation] against the user data and TSF data.: [assignment: *list of user data and list of TSF data*]	

5.1.2. FIT_CAP.1 Definition

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

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

  - Use of External IT entity (FIT_CAP);

- Family behavior
  This family (FIT_CAP) corresponds to the capability definition for TOE at the use of security function of external IT entity.

- Component leveling

FIT_CAP Capability of using external IT entity	1

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

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

Management : FIT_CAP.1
There is no management activity expected
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 external IT entity; b) Basic Use all operation of external IT entity (success, failure)

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

6. IT Security Requirements

In this chapter, the TOE security requirements are described.

<Definition of Label>

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

< Method of specifying security function requirement "Operation" >

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

<Method of clear indication of dependency>

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

<Definition of Term>

Here lists the terms used in this chapter.

Table 2 Definition of term used in SFR

Term	Definition
Encryption passphrase	A passphrase used for HDD encryption key generation
Data Complete Deletion of HDD	In conformity with a method selected by administrator, the overwrite deletion is executed for the overall area of HDD.
eMMC initialization function	A function for an administrator to initialize an administrator password and an encryption passphrase on eMMC from the panel
CE password	A password for a service engineer
Modification of CE password	A service engineer modifies a CE password from the panel.
Administrator password	A password for an administrator
Modification of Administrator password	- An administrator modifies an administrator password from a client PC. - A service engineer modifies (initializes) an administrator password from the panel.
Administrator password initialization	An administrator initializes an administrator password by Data Complete Deletion from the panel or network.
External server	External authentication server
Automatic system reset time	The function to log out automatically when the setting time passed in an idle state

Term	Definition
Modification of automatic system reset time	An administrator modifies automatic system reset time from the panel.
User information management server	Synonymous with external server
Active Directory	A directory service method offered by Windows Server 2000 (or after) to unify management of user information in the network environment of Windows platform
S/MIME certificate	A certificate to use for sending image file by E-mail
S/MIME Encryption Function	A function to encrypt scanned image to send by E-mail.
Decryption function of common key	A function to decrypt common key to encrypt an encrypted print file
Message digest encryption function	An encryption function with S/MIME function to add signature to scanned image

6.1. TOE Security Requirements

6.1.1. TOE Security Functional Requirements

6.1.1.1. Cryptographic Support

FCS_CKM.1	**Cryptographic key generation**
FCS_CKM.1.1	
The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].	
[assignment: *list of standards*] : ***Listed in "Table 3 Cryptographic key generation: Relation of Standards-Algorithm-Key sizes"***	
[assignment: *cryptographic key generation algorithm*] : ***Listed in "Table 3 Cryptographic key generation: Relation of Standards-Algorithm-Key sizes"***	
[assignment: *cryptographic key sizes*] : ***Listed in "Table 3 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 3 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*
FIPS180-3	*SHA-256*	*- 256bit*

FCS_COP.1	**Cryptographic operations**
FCS_COP.1.1	
The TSF shall perform [assignment: *list of Cryptographic operations*] in accordance with a specified	

cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: *list of standards*].
[assignment: *list of standards*] : ***Listed in Table 4 Cryptographic Operation: Relation of Algorithm-Key sizes-Cryptographic Operation***
[assignment: *cryptographic algorithm*] : ***Listed in Table 4 Cryptographic Operation: Relation of Algorithm-Key sizes-Cryptographic Operation***
[assignment: *cryptographic key sizes*] : ***Listed in Table 4 Cryptographic Operation: Relation of Algorithm-Key sizes-Cryptographic Operation***
[assignment: *list of cryptographic operation*] : ***Listed in Table 4 Cryptographic Operation: Relation of Algorithm-Key sizes-Cryptographic Operation***
Hierarchical to : No other components Dependencies : FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 (FCS_CKM.1 (only partial event)), FCS_CKM.4 (N/A)

Table 4 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 bit* *- 192 bit* *- 256 bit*	*Encryption of S/MIME transmission data*
SP800-67	*3-Key-Triple-DES*	*- 168 bit*	*Encryption of S/MIME transmission data* *Decryption of encrypted print file*
FIPS 186-2	*RSA*	*- 2048 bit* *- 3072 bit* *- 4096 bit*	*Encryption of common key (encryption key) to encrypt S/MIME transmission data*
FIPS 180-2	*SHA-256*	*N/A*	*Generation of message digest*
FIPS PUB 197	*AES*	*- 256 bit*	*- Encryption of all data (image file, password, etc) stored on HDD when they are written* *- Decryption of all data (image file, password, etc) stored on HDD when they are read out*

6.1.1.2. Identification and Authentication

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: 12 or more and up to 16- digits*** ***- Character type: possible to choose from 94 characters*** ***- Rule : (1) Do not compose by only one and the same character.*** ***(2) Do not set the same password as the current setting after change.*** **** CE password is applied to access via panel.***	
Hierarchical to	: No other components
Dependencies	: No dependencies

FIA_SOS.1[2]	**Verification of secrets**
FIA_SOS.1.1[2]	
The TSF shall provide a mechanism to verify that secrets ***(Administrator Password)*** meet [assignment: *a*	

defined quality metric].		
[assignment: *a defined quality metric*] : ***- Number of digits: 12 or more and up to 16- digits*** ***- Character type: possible to choose from 94 characters*** ***- Rule : (1) Do not compose by only one and the same character.*** ***(2) Do not set the same password as the current setting after change.*** **** Administrator password is applied to access via panel.***		
Hierarchical to	:	No other components
Dependencies	:	No dependencies

FIA_SOS.1[3]	**Verification of secrets**
FIA_SOS.1.1[3]	
The TSF shall provide a mechanism to verify that secrets ***(Encryption passphrase)*** meet [assignment: *a defined quality metric*].	
[assignment: *a defined quality metric*] : ***- Number of digits: 20- digits*** ***- Character type: possible to choose from 95 characters*** ***- Rule : (1) Do not compose by only one character.*** ***(2) Do not compose by the same characters.***	
Hierarchical to	: No other components
Dependencies	: No dependencies

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

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

FIA_UAU.6	**Re-authenticating**
FIA_UAU.6.1	
The TSF shall re-authenticate the user under the conditions [assignment: *list of conditions under which re-authentication is required*].	
[assignment: *list of conditions under which re-authentication is required*] ***- When the service engineer modifies the CE password.*** ***- When the administrator modifies the administrator password.***	
Hierarchical to	: No other components
Dependencies	: No dependencies

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

FIA_UID.2[1]	**User identification before any action**
FIA_UID.2.1[1]	
The TSF shall require each user ***(Service Engineer)*** to be successfully identified before allowing any other TSF-mediated actions on behalf of that user ***(Service Engineer).***	
Hierarchical to	: FIA_UID.1
Dependencies	: No dependencies

FIA_UID.2[2]	**User identification before any action**
FIA_UID.2.1[2]	
The TSF shall require each user ***(Administrator)*** to be successfully identified before allowing any other TSF-mediated actions on behalf of that user ***(Administrator).***	
Hierarchical to	: FIA_UID.1
Dependencies	: No dependencies

FIA_UID.2[3]	**User identification before any action**
FIA_UID.2.1[3]	
The TSF shall require each user ***(IC card of IC card owner)*** to be successfully identified before allowing any other TSF-mediated actions on behalf of that user ***(IC card of IC card owner).***	
Hierarchical to	: FIA_UID.1
Dependencies	: No dependencies

6.1.1.3. Security Management

FMT_MOF.1[1]	**Management of security functions behavior**
FMT_MOF.1.1[1]	
The TSF shall restrict the ability to [selection: *determine the behavior of, disable, enable, modify the behavior of*] the functions [assignment: *list of functions*] to [assignment: *the authorized identified roles*].	
[assignment: *list of functions*] : ***- Enhanced security function, HDD encryption function***	
[selection: *determine the behavior of, disable, enable, modify the behavior of*] : ***Disable*** , ***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[1], FMT_SMR.1[2])

FMT_MOF.1[2]	**Management of security functions behaviour**
FMT_MOF.1.1[2]	
The TSF shall restrict the ability to [selection: *determine the behavior of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorized identified roles*].	
[assignment: *list of functions*] : ***・HDD overwrite deletion function*** ***・eMMC initialization function***	
[selection: *determine the behavior of, disable, enable, modify the behavior of*] : ***Enable***	
[assignment: *the authorized identified roles*] : ***Administrator***	
Hierarchical to :	No other components
Dependencies :	FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2])

FMT_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*] : ***- Automatic system reset time*** ***- Length of password***	
[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***	
[selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] : ***Modify***	
[assignment: *the authorized identified roles*] : ***Service engineer***	
Hierarchical to :	No other components
Dependencies :	FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[1])

FMT_SMF.1	**Specification of Management Functions**
FMT_SMF.1.1	
The TSF shall be capable of performing the following management functions: [assignment: *list of management functions to be provided by the TSF*].	
[assignment: *list of management functions to be provided by the TSF*] : ***- Modification function of administrator password by administrator*** ***- Modification function of automatic system reset time by administrator*** ***- HDD overwrite deletion function and eMMC initialization function by administrator*** ***- Disable and enable function of enhanced security function by administrator*** ***- Disable and enable function of HDD encryption function by administrator*** ***- Modification function of length of password by administrator*** ***- Modification function of CE password by service engineer*** ***- Modification function of administrator password by service engineer***	
Hierarchical to :	No other components
Dependencies :	No dependencies

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

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

6.1.1.4. 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 an administrator is operating on the panel***	
Hierarchical to :	No other components
Dependencies :	No dependencies

6.1.1.5. Extension: Remaining All Information Protection

FAD_RIP.1	**Protection of all remaining information after explicit deletion operation**
Hierarchical to :	No other components
Dependencies :	No dependencies
FAD_RIP.1.1	
TSF shall ensure that the content of the information allocated to source before shall not be available after the[assignment: *request of explicit release of resource*] against the user data and TSF data.: [assignment: *user data and list of TSF data*]	
[assignment: *request of explicit release of resource*] ***Explicit deletion operation by administrator***	
[assignment: *user data and list of TSF data*]: ***<User data>*** ***- Encrypted print file*** ***- Stored image file*** ***- Image file of job in the waiting state*** ***- HDD remaining image file*** ***- Image-related file*** ***<TSF data>*** ***- Administrator password (Initialization)*** ***- Encryption passphrase***	

6.1.1.6. Extension: Capability of Using IT Environment Entity

FIT_CAP.1	**Capability of using security service of external IT environment entity**
Hierarchical to :	No other components
Dependencies :	No dependencies
FIT_CAP.1.1	
TSF shall provide the necessary capability to use the service for [assignment: *security service provided by external IT environment entity*]. : [assignment: *necessary capability list for the operation of security service*]	
[assignment: *security service provided by external 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 processing of encrypted common key***	

- *Request function of transmission of message digest for above (2) and of encryption processing of message digest*
- *Inquiring function of public key for above (3)*

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 5 TOE Security Assurance Requirements

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

6.2. IT Security Requirements Rationale

6.2.1. Rationale for IT Security Functional Requirements

6.2.1.1. Necessity

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

Table 6 Conformity of IT Security Functional Requirements to Security Objectives

Security Objectives / Security Functional Requirements	O. DECRYPT-PRINT	O.OVERWRITE-ALL	O.CRYPTO-HDD	O.MAIL-CRYPTO	O.MAIL-SIGN	O.PKI-CAPABILITY	※ set.admin	※ set.service
set.admin		X	X	X				
set.service		X	X	X				
FCS_CKM.1			X	X				
FCS_COP.1	X		X	X	X			
FIA_SOS.1[1]								X
FIA_SOS.1[2]							X	
FIA_SOS.1[3]			X					
FIA_UAU.2[1]								X
FIA_UAU.2[2]							X	
FIA_UAU.6							X	X
FIA_UAU.7							X	X
FIA_UID.2[1]								X
FIA_UID.2[2]							X	
FIA_UID.2[3]						X		
FMT_MOF.1[1]			X	X			X	
FMT_MOF.1[2]		X					X	
FMT_MTD.1[1]							X	
FMT_MTD.1[2]							X	
FMT_MTD.1[3]								X
FMT_SMF.1		X	X	X			X	X
FMT_SMR.1[1]		X	X	X			X	X
FMT_SMR.1[2]		X	X	X			X	
FTA_SSL.3							X	
FAD_RIP.1		X	X					
FIT_CAP.1						X		

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

6.2.1.2. Sufficiency

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

- **O.DECRYPT-PRINT (Decryption of Encrypted Print File)**

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

- **O.OVERWRITE-ALL (Data Complete Deletion)**

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

< Data Complete Deletion Function and operation restriction>
FAD_RIP.1 (except encryption passphrase) and FMT_MOF.1[2] guarantee that these objective information not to be able to use the content of any previous information by the deletion operation.
FMT_SMF.1 provides the administrator the management of administrator password, HDD Data Complete Deletion Function and eMMC initialization function.

<Role and management function for each management>
As the role of doing these managements, FMT_SMR.1[1] maintains a service engineer and FMT_SMR.1[2] maintains an administrator. In addition, FMT_SMF.1 specifies these management functions and FMT_MOF.1[2] manages those behaviors.

<Necessary requirement to keep the administrator secure>
→ refer to set.admin

<Necessary requirement to keep the service engineer secure>
→ refer to set.admin

Therefore, this security objective is satisfied.

- **O.CRYPTO-HDD (HDD encryption)**

This security objective regulates that it protects all data written on HDD such as image file and password, and requires requirements that relate to the encryption.
Using SHA-256 algorism of FIPS180-3, FCS_CKM.1 generates an encryption key (256 bits) from encryption passphrase.
The encryption key exists in the volatile memory area, but there is no necessity of the encryption key destruction since it is automatically destroyed without the necessity of access from the outside.
Using AES of FIPS PUB 197 (encryption key: 256 bits). FCS_COP.1 encrypts all image files and passwords written on HDD. Also, the same requirement decrypts all image files and passwords whey they are read out from HDD.

The operation setup and disabling setting of HDD encryption function is permitted by FMT_MOF.1[1] only to administrator. An encryption passphrase is verified the quality by FIA_SOS.1[3] with operation setup and deleted by FAD_RIP.1 (encryption passphrase) with disabling setting.
The management of HDD encryption function (encryption passphrase) is provided to the administrator by FMT_SMF.1.
This security objective is satisfied by 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 and FMT_MOF.1[1] manages those behavior.

- **O.MAIL-CRYPTO (Usage and Encryption of S/MIME)**

This security objective regulates that the image data scanned directly on mfp is encrypted when it is sent to the user's own mail address by e-mail, and various requirements related to the encryption are necessary
FCS_CKM.1 generates the encryption key (128, 168, 192 or 256 bits) by using Pseudorandom number Generation Algorithm according to FIPS 186-2.
FCS_COP.1 encrypts the scanned image by using AES (encryption key: 128, 192 or 256 bits) of FIPS PUB 197 (it becomes a transmission data of S/MIME). Also, the same requirement encrypts the scanned image by using 3-Key-Triple-DES (encryption key: 168 bits) of SP800-67. (By the same token, it becomes a transmission data of S/MIME.) FCS_COP.1 encrypts these common keys (encryption keys) by RSA of FIPS 186-2 by using a public key of S/MIME certificate of each destination (2048, 3072 or 4096 bits) using IC card which is identified by O.PKI-CAPABILITY. S/MIME encryption method is limited to 3DES, AES (these two can be selected) and SHA-256 by activating enhanced security function by FMT_MOF.1[1].

This security objective is satisfied by these functional requirements.

<Necessary requirement to keep the administrator secure>
→ refer to set.admin

<Necessary requirement to keep the service engineer secure>
→ refer to set.service

<Role and management function for each management>
As the role of doing these managements, FMT_SMR.1[1] maintains a service engineer and FMT_SMR.1[2] maintains an administrator. In addition, FMT_SMF.1 specifies these management functions and FMT_MOF.1[1] manages those behaviors.

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

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

  Through FSC_COP.1, message digest required for the signature processing is generated by the hash function regulated by FIPS 180-2 (SHA-256).

  This security objective is satisfied by these functional requirements.

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

  This security objective regulates that TOE supports the action of giving signature to scanned images by the IC card identified by FIA_UID.2[3] that is the entity out of TOE, and the action of decrypting common key for decrypting the encrypted print files. Also, it needs various requirements that regulate the support of external entity action.

  Applying FIT_CAP.1, the support function to process scanned images and encrypted print files by PKI function for the PKI function achieved by the IC card is realized.

  This security objective is satisfied by this functional requirement.

- ***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.

  <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 automatic system reset elapses by FTA_SSL.3 if it logs in from the panel. The change in the automatic system reset 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.

  The change in password length is limited to the administrator by FMT_MTD.1[1].

  <Role and management function for each management>

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

- ***set.service*** **(Set of necessary requirements to keep service engineer secure)**

  <Identification and Authentication of a service engineer>

  FIA_UID.2[1] and FIA_UAU.2[1] identifies and authenticates that the accessing user is a service engineer.

FIA_UAU.7 returns "*" for every one character entered as the feedback protected in the panel, and supports the authentication.

<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.

<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.

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 7 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 The satisfied events: Operating the key that is generated by the Pseudorandom number generation algorithm SHA-256. <Reason not to apply FCS_CKM.4) The keys for encrypting scan image file and HDD temporarily exist in the volatile memory area, but there is no necessity of the encryption key destruction since it is automatically destroyed without the necessity of access from the outside.
FCS_COP.1	FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2、FCS_CKM.4、	FCS_CKM.1 (only partial event) The satisfied events: Generating the common key for encrypting the S/MIME transmission data and the encryption key for encrypting HDD. <The reason not to satisfy a part of the FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2> - FIT_CAP.1 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 supports the public key that performs the encryption of common key that encrypts the S/MIME transmission data, and so there is no necessity of the key generation or importing from the outside. - The message that is used for generating the message digest is the generated document data itself, and so there is no necessity of key generation or importing from the outside.

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
		<The reason not apply FCS_CKM.4> - The keys for encrypting S/MIME transmission data and for decrypting the encrypted print file temporarily exists in the volatile memory area, but there is no necessity of the encryption key destruction since it is automatically destroyed without the necessity of access from the outside. - The public key that performs the encryption of common key that encrypts the S/MIME transmission data is the public information, and so there is no necessity of the encryption key destruction. The key for encrypting HDD temporarily exists in the volatile memory area, but there is no necessity of the encryption key destruction since it is automatically destroyed without the necessity of access from the outside.
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[2]
FMT_MOF.1[2]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MTD.1[1]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MTD.1[2]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[1]、FMT_SMR.1[2]
FMT_MTD.1[3]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]
FMT_SMF.1	None	N/A
FMT_SMR.1[1]	FIA_UID.1	FIA_UID.2[1]
FMT_SMR.1[2]	FIA_UID.1	FIA_UID.2[2]
FTA_SSL.3	None	N/A
FAD_RIP.1	None	N/A
FIT_CAP.1	None	N/A

6.2.2. Rationale for IT Security Assurance Requirements

This TOE is installed and used in an environment where adequate security is maintained in terms of the physical, personnel, and connectivity. Nonetheless, adequate effectiveness in the environment where the TOE is used must be assured. As a general commercial office product,

the execution of tests based on function specifications and TOE design, and analysis of the strength of function and a search for vulnerabilities are required. In addition, it is desirable that it has a development environment control, a configuration management for the TOE and a secure distribution procedure. And therefore the selection of EAL3, which provides an adequate assurance level, is reasonable.

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

7. TOE Summary Specification

The list of the TOE security function led from the TOE security function requirement is shown in Table 8 below. The detailed specification is explained in the sections described below.

Table 8 Names and Identifiers of TOE Security Function

No.	TOE Security Function	Relation with Logical Scope of 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) 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.	Basic function
7.4	F.PRINT (Encryption Print function)	Basic function
7.5	F.OVERWRITE-ALL (Data Complete Deletion Function)	Administrator function
7.6	F.S/MIME (S/MIME encryption processing function)	Basic function
7.7	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 processing 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 processing 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 acquisitionrequest> ● Inquiring to IC card is performed and public key (digital certificate) in the IC	Other function

	card is received. As described above, FIT_CAP.1 is realized.	
7.8	F.CRYPTO-HDD (HDD encryption function)	Basic 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 9.
- Return "*" for each character as feedback for the entered administrator password.

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

7.1.2. Auto Logout Function of Administrator Mode

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

As described above, FIA_SSL.3 is realized.

Table 9 Characters and Number of Digits for Password [2]

Objectives	Number of digits	Characters
Administrator Password	12-16	Selectable from 94 or more characters in total (Alphanumeric characters and symbols) ASCII code: 0x20-0x7e 0x22(") cannot be selected.
CE Password		

7.1.3. Function Supported in Administrator Mode

[2] Table 9 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.

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

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

7.1.3.1. Change of Administrator Password

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

- Provides the administrator authentication mechanism that is re-authenticated by the administrator password which consists of the character shown in Table 9.
- Return "*" for each character as feedback for the entered administrator password in the re-authentication.
- Verify that the administrator password newly set satisfies the following qualities.
  - It shall be composed of the characters and by the number of digits shown in the administrator password of Table 9.
  - It shall not be composed of one kind of character.
  - It shall not be matched with the current value.

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

7.1.3.2. Setup of Auto Logout Function

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

- system auto reset time : 1 - 9 minutes

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

7.1.3.3. Function Related to Enhanced Security and HDD Encryption

<Enhanced security function>

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

- Operation setting of enhanced security function
  Function to set the enhanced security function to valid or invalid through panel
- HDD logical format function
  Function to write on HDD the initial value of the management data that is used for the file system through panel. This logical formatting deactivates the setting of the enhanced security function.
- Data Complete Deletion Function
  The setting of the enhanced security function is deactivated by executing the all area overwrite deletion through panel.

This function is permitted only to the administrator.

The above function provides the management function for the enhanced security function.

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

<HDD encryption function>

The settings of HDD encryption function that the administrator operates are as follows:

- Operation setting of HDD encryption function

  Function to verify the quality and set the operation of encryption passphrase, and to delete and stop the operation of encryption passphrase through panel

<Quality of encryption passphrase>

The quality metric of encryption passphrase is as follows:

Table 10 Characters and Number of Digits for Encryption Passphrase

Objectives	Number of digits	Characters
Encryption passphrase	20	Selectable from 95 or more characters in total (Alphanumeric characters and symbols) ASCII code: 0x20-0x7e

- It shall be composed of the characters by the number of digits shown in the encryption passphrase of Table 10.
- It shall not be composed by only one type of character.
- It shall not be composed by the same characters.

The quality of encryption passphrase is verified when it is registered.

This function is permitted only to the administrator.

The above function provides the management function for HDD encryption function.

As described above, FIA_SOS.1[3], FMT_MOF.1[1], FMT_SMF.1 and FAD_RIP.1 (encryption passphrase) are described.

7.1.3.4. Password Length Setting

The minimum length of password used for administrator password and CE password should be set within the following length range:

- Password length: 12-16 digits

The password length setting should be configured after increasing the length of administrator password or CE password which is currently set.

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

7.1.3.5. Management of Data Complete Deletion Function

The execution of Data Complete Deletion Function is permitted only to the administrator via panel.

The data which is deleted or initialized by execution of Data Complete Deletion Function is described in “7.5”.

The above function provides the management functions for the HDD overwrite deletion function, eMMC initialization function and administrator password.

As described above, FMT_MOF.1[2], FMT_MTD.1[2] and FMT_SMF.1 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 9.
- Return "*" for each character as feedback for the entered CE password.
  As described above, 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 accessing request to the service mode, the service engineer attribute is associated with the task substituting the user. And the following uses of the functions are permitted.

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

7.2.2.1. Change of CE Password

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

- Provides the CE authentication mechanism that is re-authenticated by the CE password that consists of the characters shown in Table 9.
- Return "*" for each character as feedback for the entered CE password in the re-authentication.
- Verify that the CE password newly set satisfies the following qualities.
  - It shall be composed of the characters and by the number of digits, shown in the CE password of the Table 9.
  - It shall not be composed of one kind of character.
  - It shall not be matched with the current value.

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

7.2.2.2. Change of Administrator Password

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

- It shall be composed of the characters and by the number of digits, shown in the administrator password of the Table 9.
- It shall not be composed of one kind of character.
- It shall not be matched with the current value.

As described above, FIA_SOS.1[2], FMT_MTD.1[2], FMT_SMF.1 and FMT_SMR.1[2] 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 processing to the print operation by the common key (encryption key) that is obtained by F.SUPPORT-PKI.

- The common key (encryption key) (168 bits) to decrypt the encrypted print file is decrypted by RSA that is regulated by the FIPS186-2.
  As described above, FCS_COP.1 is realized.

7.5. F.OVERWRITE-ALL (Data Complete Deletion Function)

F.OVERWRITE-ALL executes the overwrite deletion in the data area of HDD by the explicit deletion operation of administrator, and initializes the settings value such as passwords set on eMMC. The object for the deletion or the initialization is as follows.

<Object for the deletion: HDD>

- Encrypted print file
- Image file of job in the waiting state
- Stored image file
- HDD remaining image file
- Image related file

<Object for the initialization: eMMC>

- Administrator Password

The deletion methods such as the data overwritten in HDD and the writing frequency is executed according to the deletion method of Data Complete Deletion Function set by F.ADMIN (Table 11). When this function is executed, the enhanced security function is disabled. (See the description of the operation setting of the enhanced security function for F.ADMIN.)

This function is permitted only to the administrator.

As described above, FAD_RIP.1 is realized. (Except encryption passphrase)

Table 11 Types and Methods of Data Complete Deletion

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.S/MIME (S/MIME encryption processing function)

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

<Encryption Key generation>

- The common key (encryption key) is generated to encrypt the scanned image by the pseudorandom number Generation Algorithm which FIPS 186-2 provides. (Encryption key length is 128, 168, 192 or 256 bits.)
  As described above, FCS_CKM.1 is realized.

<Encryption of Scanned image >

- Scanned image is encrypted by AES which FIPS PUB 197 provides by using common key (encryption key) (128, 192 and 256 bits).
- Scanned image is encrypted by the 3-Key-Triple-DES which SP800-67 provides by using the common key (encryption key) (168 bits).
  As described above, FCS_COP.1 is realized.

<Encryption of Encryption key>

- The common key (encryption key) to encrypt the scanned image is encrypted by RSA which FIPS 186-2 provides.
- The key length of the common key (encryption key) used in F.SUPPORT-PKI is 2048, 3072 or 4096 bits.
  As described above, FCS_COP.1 is realized.

<Message Digest Generation>

- For scanned image, message digest is generated by hash function (SHA-256) which FIPS 180-2 provides.
  As described above, FCS_COP.1 is realized.

7.7. 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 processing 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 processing 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 acquisitionrequest>

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

As described above, FIT_CAP.1 is realized.

7.8. F.CRYPTO-HDD (HDD encryption function)

F.CRYPTO-HDD is the function to encrypt the data such as image file and password when they are written on HDD.

<Encryption key generation for HDD encryption>

- A key 256 bits long to encrypt/decrypt all image files and passwords written on HDD is generated from the encryption passphrase by applying the SHA-256 algorithm that is regulated by FIPS180-3.
  The encryption key is generated when mfp is powered on.
  As described above, FCS_CKM.1 is realized.

<HDD encryption and decryption>

- An encryption key (256 bits) encrypts all image files and passwords when they are written on HDD by AES which FIPS PUB 197 provides.
- An encryption key (256 bits) decrypts all image files and passwords when they are read out from HDD by AES which FIPS PUB 197 provides.
  As described above, FCS_COP.1 is realized.

---END---