MX-FRX8

Security Target

Version 0.07

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

SHARP CORPORATION

Revision history

Date	Ver.	Revision	Author	Reviewed	Approved
2007-10-31	0.01	• Original draft	Nakagawa	Iwasaki	Tsujii
2007-02-15	0.02	• Consistency errors are modified: in Sections 1.3, 1.4, 3.1, 3.2, 3.3, 4.1, 4.3, 6.2, 6.4, 7.3, 7.6 and 8.2.	Nakagawa	Iwasaki	Tsujii
2008-03-13	0.03	• Consistency errors are modified: in Sections 1.3, 3.1, 4.1, 4.2, 4.3 and 6.4. • Other errors are corrected: in Sections 6.2 and 7.1.	Nakagawa	Iwasaki	Tsujii
2008-03-24	0.04	• Consistency errors are modified: in Sections 1.3 and 6.4.	Nakagawa	Iwasaki	Tsujii
2008-04-25	0.05	• Consistency errors are modified: in Sections 1.4, 6.2, 6.4, 7.3, 7.5, 7.6 and 8.2.	Nakagawa	Iwasaki	Yakushiji
2008-05-14	0.06	• Overall review	Nakagawa	Iwasaki	Yakushiji
2008-06-30	0.07	• Consistency errors are modified and other errors are corrected: in Sections 4.2, 4.3, 6.4 and 8.1.	Nakagawa	Iwasaki	Yakushiji

Table of Contents

List of Tables

List of Figures

1 ST Introduction

In accordance with the Common Criteria (CC) identified in Section 2.1, this chapter identifies this Security Target (ST) and the Target of Evaluation (TOE) claiming conformance to this ST. For that, this chapter presents ST reference, TOE reference, TOE overview and TOE description. See Sections 8.1 and 0 for terminology used in this ST.

1.1 ST Reference

This section provides information needed to identify this Security Target (ST).

ST title: MX-FRX8 Security Target

Version: 0.07

Publication Date: 2008-06-30

Author: Sharp Corporation

1.2 TOE Reference

This section provides information needed to identify the Target of Evaluation (TOE) claiming conformance to this ST.

TOE Identification: MX-FRX8 Version M.10

Developer: Sharp Corporation

1.3 TOE Overview

1.3.1 TOE Type

The TOE is an IT product to protect data in a Multi Function Device (MFD) and the main part of the TOE is the firmware in ROMs for the MFD. The HDC, a hardware part in the MFD, is also a part of the TOE and is controlled by the firmware.

MFDs, Multi Function Devices, are office machines mainly with copier, printer, scanner and fax functions. When installed, the TOE replaces the MFD standard firmware ROM.

1.3.2 Required non-TOE hardware/software/firmware

The TOE operates on the MFD made by Sharp Corporation, namely, MX-M850, MX-M860, MX-M950 and MX-M1100.

The abilities required for the Web browser, printer driver and PC-Fax driver used for communication to and from the MFD are as follows. The above models are delivered together with a printer driver and a PC-Fax driver both of which have the following abilities:

- Providing authentication feedback protection when a password is entered; typed password shall not be displayed and information other than the number of the typed characters shall not be disclosed.

- When the SSL mentioned in the next section is used, the SSL protocol (SSL 3.0, TLS 1.0 or higher) shall be supported.

Support by "Internet Explorer 6.0 SP2", a Web browser of Microsoft, has been confirmed for the operation of the TOE security functions identified by this ST. Users are advised to confirm the abilities of a browser before use, although other widely used Web browsers are presumed to have the above abilities.

1.3.3 Main Security Functions

The TOE provides the following functions aiming to protect user data (see Section 1.4.4 for details.) including image data. Their purpose is to counter unauthorized attempts of obtaining user data which is stored or remains in the non-volatile memory devices (such as the HDD) in the MFD. Another purpose is to counter attempts to wiretap user data when the MFD inputs and outputs the data over the network (LAN).

a) Cryptographic operation function: encrypts image data before written to the MFD internal storage such as HDD, either when the MFD temporarily writes image data of a current job, or when a user saves image data of a document as a file into the HDD.

6

b) Data clear function: automatically overwrites image data in the HDD and other storage devices when the image data becomes no longer required. All data are overwritten as necessary by the operation of the administrator on a daily basis or when MFDs are disposed.

c) Confidential files function: provides password protection for files where users save their job's image data, not to be reused by others.

d) IP/MAC address filter function: rejects unauthorized accesses over the network.

e) SSL function: protects data from wiretapping during transmission.

1.3.4 TOE Usage

The TOE provides MFD functions such as copier, printer, scanner, fax transmission and reception, and PC-Fax in the same way as the standard firmware. This section describes an overview of how to invoke the security functions described in the previous section. Descriptions on MFD functions are discussed later.

a) Users' operation of MFD functions such as copier triggers an automatic operation of the cryptographic operation function and the data clear function of the TOE. The MFD temporality spools the image data to the MSD (the HDD or the Flash memory) in the MFD while a job such as copy is in the process. The MFD reads out the image data to process the job and deletes the image data when the job is completed. The TOE encrypts image data to be spooled by the cryptographic operation function and decrypts when it reads it out. The TOE overwrites image data to be deleted by the data clear function.

b) Users can save image data as a "confidential file" (with password protection) in the HDD in the MFD using the confidential file function of the TOE. Later they can reuse the confidential file (for printing, fax transmission, transferring the image file to a client and other proposes) and prevent with the password the confidential file from being reused by others.

• When users enter a job such as copy into the MFD, they select to save the image data and specify a password. This allows the TOE to save the image data of the job in the HDD along with the password after job completion.

• Users set an original on the MFD, select "Scan to HDD" on the operation panel of the MFD and specify a password. This allows the TOE to scan the original and obtain image data from the MFD scanner unit, and save the image data in the HDD along with the password.

• Users select a confidential file saved in the HDD, enter the password and specify a file manipulation (including print, send, delete) on the operation panel of the MFD or from a client connected to the network. The TOE checks the password entered and, when the password is verified, performs the file manipulation. The TOE disables the file manipulation if incorrect passwords are entered three times in a row.

c) When users save a confidential file using the confidential file function of the TOE and when they reuse it, the cryptographic operation function automatically operates. The TOE encrypts the image data and the password to be saved in the HDD by the cryptographic operation function. When the TOE checks a password entered to reuse a confidential file, the TOE reads out the password from the HDD and decrypts it. When a print job or a send job is executed after verification of the password, the TOE reads out the image data and decrypts it.

d) When users delete a confidential file using the confidential file function of the TOE, the data clear function of the TOE automatically operates.

e) When users communicate with the MFD from a client over the network, the SSL function of the TOE can be used. When a print job is sent from a client, the image data to be printed is protected using the IPP-SSL protocol from wiretapping during transmission. When users access the Web page provided by the MFD (TOE) for remote operation such as reusing a confidential file, the SSL (HTTPS) protocol can be used to protect information including the password from wiretapping during transmission.

f) The administrator operates on the operation panel of the MFD as necessary (including when the MFD is disposed) to execute "Clear All Memory". Then, the TOE overwrites all image data in the MFD by the data clear function.

g) The administrator configures the filter settings on the TOE Web. The administrator can specify IP address ranges to accept or reject communication with the MFD, and specify MAC addresses to accept communication with the MFD. When the filter settings are configured, the TOE does not respond to communication from IP addresses other than those specified to accept, IP addresses specified to reject and MAC addresses other than those specified to accept.

1.3.5 Overview of the MFD Functions and Applications

The usage environment of the MFD that the TOE is installed to is shown in Figure 1.
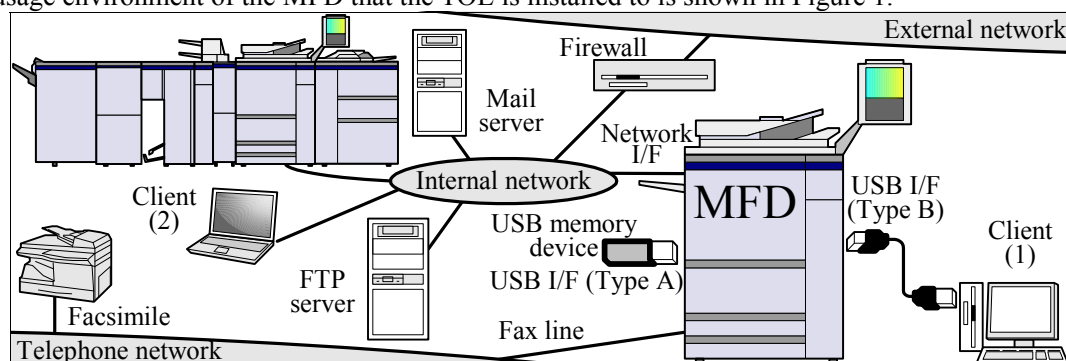
Figure 1: Usage environment of the MFD

Each MFD function of the TOE is explained below. Most functions are available on the operation panel of the MFD. Some functions run when receiving data. Moreover, some functions are available on the TOE Web, which is a Web site that the TOE serves for remote operation.

1.3.5.1 Job function

The job function receives the image data from the MFD's scanner unit or from outside of the MFD, spools the image data to the MSD in the MFD, and sends the image data to the MFD's engine unit (printing) or to the outside of the MFD (transmission). The job control function and the MFD control function implement the job function.

a) Copier: reads the original and prints that image by the operation from the operation panel. If Tandem Copy mode is selected, it sends the image data to the MFD that the administrator specified beforehand.

b) Printer: prints the data received from the outside of the MFD.

- Printer driver: generates the print data at a client and sends to the MFD via network or USB. If Tandem Print mode is selected, the printer driver sends the image data to two MFDs.

- Push print: is to send print data from a client to the MFD via E-mail, FTP or Web. Tandem print requests from another MFD are printed in the same manner.

- Pull print: acquires the print data in an FTP server or a USB memory device by operations on the operation panel.

c) Network scanner: scans an original to obtain image data through operations on the operation panel, and transmits the image data file in either of the following ways:

- E-mail: transmits it as an attachment to an E-mail.

- File server: transmits it to an FTP server.

- Desktop: transmits it via FTP to a client running the software tool delivered together with the MFD.

- Network folder: transmits it into a shared folder of Microsoft Windows over the network.

- USB memory: puts it into a USB memory device plugged into the MFD.

- PC scan: transmits it via TWAIN to a client running the software tool delivered together with the MFD.

- Internet Fax: transmits it as an attachment to an E-mail according to the Internet Fax standard specification.

d) Fax transmission: scans an original to obtain image data through operations on the operation panel, and transmits the image data as a facsimile.

e) Fax reception: receives a facsimile from another fax machine and prints it.

f) PC-Fax: transmits image data from a client as a facsimile or an internet fax.

1.3.5.2 Document filing function

The document filing function provides the following functions that allow users to save image data to the HDD in the MFD and operate it from the operation panel or the client via Web later. This function is implemented by the job control function.

● File a job: when a user enters a job such as copy into the MFD, the image data of the job can optionally be saved. When the user set a password at the time of saving, the file is saved as a confidential file.

● Scan to HDD: scans the original and does only store it, while neither prints nor transmits it.

● Operation on saved files: calls up the saved image data and operate it/them in the following ways.

   • Print: prints the saved image data to the paper. If Tandem Print mode is selected, this function sends the image data to the MFD that the administrator specified beforehand.

   • Send: transmits the saved image data either by any medium available for the network scanner function or by facsimile.

   • Preview: displays the rough outline of the saved image data.

   • Property change: changes the availability of the confidential file password of a file.

   • Password change: changes the confidential file password.

   • Delete: removes a saved image data file that the user no longer needs, and overwrites it.

   • Backup (export): transfers the saved image data to the client as binary data, from which the user can restore (import) the image data later.

The printer driver allows its job to be saved without being printed. Similarly, Scan to HDD may be considered as a network scanner job saved without being transmitted.

1.3.5.3 Address book function

The Address book function stores the destination fax number and E-mail address. This simplifies the operation for transmission. The data is stored in the HDD and storing, modifying and deleting are available by the operation from the operation panel or Web. This function is realized by the job control function.

1.3.6 Operating/managing the TOE

The TOE contains the following management function to keep the secure operation. Only the administrator cans operate the TOE by using the following management function below.

● Setting for authentication:
   • Change (modify) the administrator password

● Network access limitation settings:
   • IP Address Filter Settings
   • MAC Address Filter Settings

● Settings for security:
   • SSL Settings
   • Number of Times Auto Clear at Job End Program is Repeated
   • Number of Times Data Clear is Repeated
   • The data areas to be cleared by Power Up Auto Clear
   • Number of Times Power Up Auto Clear Program is Repeated
   • Disabling of Document Filing
   • Disabling of Print Jobs Other Than Print Hold Job
   • Release the lock of confidential files

● Enable the data clear function:
   • Clear All Memory
   • Clear Address Book Data and Registered Data in MFP
   • Clear Document Filing Data
   • Clear All Data in Job Status Jobs Completed List

● Disable the data clear function:
   • Disable "Clear All Memory"
   • Disable "Clear Document Filing Data"
   • Disable "Power Up Auto Clear"

1.4 TOE Description

1.4.1 Physical Configuration of the TOE

Main part of the TOE is provided in two ROM boards. In implementation constraint, some of the security functions are implemented in the HDC, which is positioned as part of the TOE scope. These are shaded in Figure 2.

The physical scope of the TOE is as follows:

- Controller firmware: the firmware that controls the controller board, which is contained in the two ROM boards on the controller board. It is provided as an optional product sold separately for the MFD.

- HDC: an integrated circuit part that is mounted on the controller board. It operates under control of the controller firmware.

The above controller firmware is included in "Data Security Kit MX-FRX8 (DSK)" which is a product to enhance security of MFDs made by Sharp

Figure 2: TOE and physical configuration of the MFD

Corporation. The DSK is an optional product sold separately for Sharp Corporation MFDs and needs to be installed in the MFD to function. Although the standard firmware and the HDC are incorporated in an MFD when it is manufactured, the standard firmware does not invoke the security functions in the HDC and therefore the HDC functions simply as an interface to the HDD. The security functions in the HDC can be invoked by replacing the standard firmware with the DSK firmware in the MFD.

1.4.2 Logical Configuration of the TOE

Figure 3 shows the logical configuration of the TOE. The thick-lined frame indicates the logical scope of the TOE. Rounded boxes indicate hardware devices that are out of the TOE. Rectangles indicate functions of the TOE; and ones shaded indicate security functions. Among the data in the volatile memory, HDD, Flash memory and EEPROM, the data that security functions handle (i.e. user data and TSF data) are also shaded.

Arrows in the figure indicate data flows. Functions of the TOE usually put data in the volatile memory temporarily to pass the data to each other. However, the figure omits every such detail except security significance.
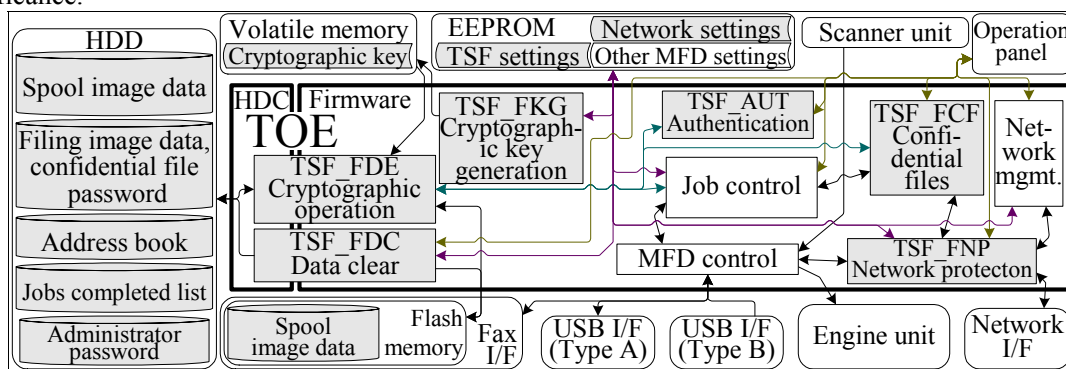
Figure 3: Logical configuration of the TOE

The large part of the TOE is firmware for the MFD. It provides security functions, while controlling the entire MFD. A small part of the TOE security functions (TSF) is implemented in the HDC and invoked by the TSF in the firmware.

The logical scope of the TOE includes the following functions:

a) Cryptographic operation function (TSF_FDE): encrypts user data and TSF data to be stored in the MSD and decrypts user data and TSF data retrieved from the MSD. This function is invoked by job control function (each job, address book and document filing functions). A part of this function is implemented in the HDC and invoked by the main part of this function in the firmware.

b) Cryptographic key generation function (TSF_FKG): generates the cryptographic key for the cryptographic operation function. This function stores the generated key in the volatile memory. It

generates a seed of the cryptographic key once when installed. From then on, it always generates a cryptographic key from the seed for the MFD whenever powered on.

c) Data clear function (TSF_FDC): overwrites the MSD to prevent information leakage from the MSD. A part of this function is implemented in HDC and invoked by the main part of this function in the firmware. This function consists of data clear programs (Auto Clear at Job End, Clear All Memory, Clear Address Book Data and Registered Data in MFP, Clear Document Filing Data, Clear All Data in Job Status Jobs Completed List and Power up Auto Clear) and setting function for them (Data Clearance Settings). "Auto Clear at Job End" is invoked by job control function (each job and document filing function).

d) Authentication function (TSF_AUT): identifies and authenticates an administrator by means of the administrator password. This function includes a management function that changes the administrator password.

e) Confidential files function (TSF_FCF): provides password protection when a user saves image data to the MFD using the document filing function (Section 1.3.5.2) and requires authentication by means of that confidential file password to reuse (such as to print or to transmit) the data. If incorrect passwords for a confidential file are entered three times in a row, this function locks that file. Only the administrator can release the locked file.

f) Network protection function (TSF_FNP): consists of the following three functions:

- Filter function: restricts the other party to communicate by the terms of IP address or MAC address.
- Communication data protection: protects the communication data by SSL. This function is not available when the user uses a client and/or a protocol not supporting SSL.
- Network settings protection: provides the network management functions (see below) only to the administrator and do not allow other users to use it.

g) Job control function: provides the UI and control the action for each MFD function; in other words each job, address book function and document filing function. This also manages the jobs by means of queues and stores the jobs completed list in the HDD.

h) MFD control function: controls MFD hardware. This also converts the data format between the data to receive or transmit and the image data in the MFD for the jobs that require the communication.

i) Network management functions: are for the administrator to query and modify the IP address to be allocated for the MFD, the IP address of DNS servers that the TOE shall refer, port control (modifying the port number or disabling for each network service) and other network settings for using the network function. This function is invoked by the network protection function (TSF_FNP).

1.4.3 Guidance Documents

Guidance documents shown in the Table 1.1 accompany the firmware as part of the TOE. Unique identifiers for the guidance documents and their versions are shown in brackets.

Table 1.1: Guidance Documents

Destination Objective	For Japan	For outside Japan
Setup	MX-FRX8 Installation Manual (in Japanese) [TCADZ1969FCZZ]	MX-FRX8 Installation Manual (in English) [TCADZ1970FCZZ]
User operation	MX-FRX8 Data Security Kit Operation Manual (in Japanese) [CINSJ4234FC51]	MX-FRX8 Data Security Kit Operation Manual (in English) [CINSE4235FC51]
	MX-FRX8 Data Security Kit Notice (in Japanese) [TCADZ1967FCZZ]	MX-FRX8 Data Security Kit Notice (in English) [TCADZ1968FCZZ]

1.4.4 Assets Protected by the TOE

The following user data are assets that are protected by the TOE.

- Image data that the MFD functions spool to process jobs
- Image data that users save as confidential files
- Address book data
- Jobs completed list data

● Network settings data

● Data transmission over the network

Specifics of each clause above are described in the following each section.

1.4.4.1 Image data that the MFD functions spool to process jobs

The assets protected by the TOE include the image data that the TOE itself temporarily spools to the HDD or the Flash memory in the MFD for processing the jobs (mentioned in this chapter) without intent of the user to save when the user uses the MFD functions of the TOE. These data possibly contain the users' sensitive information, such as the user's own information and the information of the customers of the user.

These data are deleted when the jobs are finished or cancelled, but this deletion deletes them logically and image data area remains physically in the HDD or Flash memory. Thus, the assets protected by the TOE include the image data that is logically deleted but remains physically.

1.4.4.2 Image data that users save as a confidential files

The assets protected by the TOE include the image data that the user saves to the HDD as a confidential file. As well as in the previous section, these data possibly contain the users' sensitive information.

The user can delete these data, but this deletion deletes them logically and image data area remains physically in the HDD. Thus, the assets protected by the TOE include the image data that is logically deleted but remains physically.

1.4.4.3 Address book data

The assets protected by the TOE include the address book data that the users store by the address book function and is stored in the HDD. This data is the personal data (destination name, mail address, fax number and others) that proper users share and possibly contain the organisation's sensitive information.

There is not necessarily a threat to counter if there is no method for the improper user to read or modify the address book data without standing in front of the operation panel and accessing every record in this data one by one by seeing and operating manually. However, this data shall be protected from the possibility that the improper user reads and modifies this data all at one time from the HDD directly or through the internal network.

1.4.4.4 Jobs completed list data

The assets protected by the TOE include the jobs completed list data that the job control function keeps in the HDD. This data possibly contain the organisation's sensitive information, such as user name or document name of jobs from the printer driver, destination for fax transmission or reception and others.

There is not necessarily a threat to counter if there is no method for the improper user to read the jobs completed list data without standing in front of the operation panel and accessing every record in this data one by one by seeing and operating manually. However, this data shall be protected from the possibility that the improper user read this data all at one time from the HDD directly.

1.4.4.5 Network settings data

The assets protected by the TOE include the following network settings data that the administrator stored in the EEPROM using the network management function. This data contain the organisation's sensitive information and may lead to the threat to the internal network. Moreover, it may lead the threat to other assets if tampered improperly.

● TCP/IP Settings: Enable TCP/IP, Enabling DHCP, IP Address Settings

● DNS Settings: Primary/Secondary DNS Server, Domain Name

● WINS Settings: Enable WINS, Primary/Secondary WINS Server, WINS Scope ID

● SMTP Settings: SMTP Server

● LDAP Settings: Enable LDAP, LDAP Server

● Tandem Settings: IP Address of Slave Machine, Disabling of Master Machine Mode

● Port Control: Enabling or the port number for each network service

1.4.4.6 Data transmission over the network

In this ST, the communication data being transmitted over the network to and from the MFD is assumed to be the assets in consideration of threats of wiretapping.

2 Conformance Claims

This ST satisfies the followings.

2.1 CC Conformance Claim

The versions of the CC to which this ST and the TOE claim conformance are as follows:

● Part 1: Introduction and general model
September 2006 Version 3.1 Revision 1; Japanese Translation 1.2

● Part 2: Security functional components
September 2007 Version 3.1 Revision 2; Japanese Translation 2.0

● Part 3: Security assurance components
September 2007 Version 3.1 Revision 2; Japanese Translation 2.0

The conformance of this ST to CC Part 2 is CC Part 2 conformant.

The conformance of this ST to CC Part 3 is CC Part 3 conformant.

2.2 PP Claim

This ST does not claim conformance to any PP.

2.3 Package Claim

This ST claims conformance to EAL3.

3 Security Problem Definition

This chapter defines security problems of the TOE.

3.1 Threats

Threats to the TOE are described in Table 3.1. Unless otherwise noted, each threat definition assumes the following attackers:

- Authorized MFD users or third parties.
- Someone who has the motive to obtain the assets (described in Section 1.4.4) such as image data of documents of others without authorization.
- Someone who has knowledge of the MFD and the TOE based on open information including operation manuals.

Table 3.1: Threats

Identifier	Definition
T.RECOVER	An attacker physically removes the MSD from the MFD to read the MSD. By using easily available hardware and software tools, the attacker reads and leaks the user data stored in it (include the data that is remained after deleting).
T.REMOTE	An attacker who is not allowed to access to the MFD reads and modifies the address book data in the MFD all at one time through the internal network.
T.SPOOF	An attacker who impersonates other user reads and leaks the image data from the operation panel or through the internal network that the user has saved as confidential file.
T.TAMPER	An attacker who impersonates an administrator reads or modifies the network settings data from the operation panel or through the internal network.
T.TAP	An attacker wiretaps the user data on the internal network when a proper user communicates with the MFD.

3.2 Organisational Security Policies

No organisational security policies are presumed by this ST.

Table 3.2: Organisational Security Policies

(None)

3.3 Assumptions

Use and operation of the TOE requires the environment described in Table 3.3.

Table 3.3: Assumptions

Identifier	Definition
A.NETWORK	The MFD is connected to a subnetwork in the internal network protected against attacks from any external networks, where the subnetwork for the MFD connects nothing other than devices allowed to communicate with the MFD.
A.OPERATOR	The administrator is a trustworthy person who does not take improper action with respect to the MFD and the TOE.

4 Security Objectives

This chapter describes the measures to implement the security objective policies.

4.1 Security Objectives for the TOE

The security objectives for the TOE are shown in Table 4.1.

Table 4.1: Security Objectives for the TOE

Identifier	Definition
O.FILTER	The TOE shall provide defence against network accesses from devices that are not allowed to access to the MFD.
O.MANAGE	TOE shall provide only the administrator with the security management functions to keep the secure operation.
O.REMOVE	The TOE shall encrypt the user data using a cryptographic key unique to the MFD when the TOE writes them to the MSD.
O.RESIDUAL	TOE shall overwrite the user data area in the MSD once the user data becomes unnecessary.
O.TRP	The TOE shall provide the function that prevents the user data on the internal network from wiretapping.
O.USER	The TOE shall provide the function that identifies and authenticates the proper user that stored the confidential files.

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are shown in Table 4.2.

Table 4.2: Security Objectives for the Operational Environment

Identifier	Definition
OE.CIPHER	When the user of the MFD communicates with the TOE, the administrator shall take necessary steps (examples are as follows) to protect the communication data between the MFD user and the TOE from wiretapping on the internal network where the TOE is installed. ● The SSL functions of the TOE shall be used; according to Section 1.3.2 of this ST, the administrator shall make the users use software supporting the SSL protocol as well as configuring the TOE to perform functions defined in O.TRP. ● Communication devices (such as routers and switches) with cryptographic functions shall be used. ● The administrator shall provide physical protection (such as restricted areas) to the network. ● The administrator shall make the MFD users use USB memory device to input/output the data.
OE.FIREWALL	The administrator shall connect the internal network when the TOE is installed to the external network by using the communication device having the function to protect the internal network against attacking from external networks.
OE.NOECHO	According to Section 1.3.2 of this ST, the administrator shall make the users to use software which provides a protected authentication feedback when the user of the MFD communicates with the TOE.
OE.OPERATE	Those in charge of the organisation shall understand the role of the administrator and select a suitable person with the utmost care.
OE.PC-USER	On the devices allowed to connect to the MFD on the internal network, the administrator shall run the identification and authentication function (such as logging in the OS) so that only the authorized MFD users be able to use such devices.
OE.SUBNET	The administrator shall connect only the devices that are allowed to communicate to the MFD in the subnetwork where the TOE is installed, and keep and maintain that state.
OE.USER	The administrator shall make the users of the TOE and the MFD to maintain the confidential file password securely so that it will not leak.

4.3 Security Objectives Rationale

Table 4.3 demonstrates that the policies indicated in the security objectives are effective for each of the security problems defined by the ST. Table 4.3 shows the sections of this document that provide the rationale for the respective correspondences between the security problems and the security objectives.

Table 4.3: Security Objectives Rationale

Security objective \ Security problem	T.RECOVER	T.REMOTE	T.SPOOF	T.TAMPER	T.TAP	A.NETWORK	A.OPERATOR
O.FILTER		4.3.1.2					
O.MANAGE	4.3.1.1	4.3.1.2	4.3.1.3	4.3.1.4	4.3.1.5		
O.REMOVE	4.3.1.1						
O.RESIDUAL	4.3.1.1						
O.TRP					4.3.1.5		
O.USER			4.3.1.3				
OE.CIPHER					4.3.1.5		
OE.NOECHO	4.3.1.1	4.3.1.2	4.3.1.3	4.3.1.4	4.3.1.5		
OE.FIREWALL						4.3.3.1	
OE.OPERATE							4.3.3.2
OE.PC-USER		4.3.1.2					
OE.SUBNET						4.3.3.1	
OE.USER			4.3.1.3				

4.3.1 Rationale Explaining Why Threats Are Countered

The following is the rationale explaining why all threats are countered when the security objectives are achieved.

4.3.1.1 T.RECOVER

The followings counter T.RECOVER.

- As defined in O.RESIDUAL, the TOE overwrites an area in the MSD where user data is stored when the user data becomes unnecessary. This prevents the user data in the MSD from being read out.
- The TOE encrypts the user data with MFD's own cryptographic key according to O.REMOVE when the TOE writes the user data to MSD. Therefore, a low-level attacker cannot make out the data that is stored or remained after deleting in MSD even if the attacker could read them.
- As a support of above-mentioned paragraphs, the TOE allows only the administrator to manage the security functions to ensure secure operation as defined in O.MANAGE. To support the secure operation, OE.NOECHO prevents the password from being peeped by others when the administrator types it for authentication.

When the volatile memory is removed from the MFD, all the storage data in volatile memory disappears by intercepting the power distribution. There are no interfaces to read the data directly on the memory during the run of MFD, and it requires a high level of technology like specifying the data area and under transferring the data. Therefore, it is impossible for a low-level attacker to read the data by attaching probes directly to the terminals or harness of MFD. For this reason the cryptographic key that is stored in the volatile memory cannot be read.

Therefore, it is possible to protect the information in HDD and Flash memory from the leak by following each objective above.

4.3.1.2 T.REMOTE

The followings counter T.REMOTE.

- The TOE provides the method to deny the access from devices that are not allowed to access to the MFD through the network according to O.FILTER. This denies accesses to the MFD from unauthorized devices connected to the internal network while accepts accesses to the MFD from devices (including clients and servers) connected to the internal network with the intention to be used by authorized users of the MFD (including the administrator).

- In support of the previous paragraph, as defined in O.MANAGE, the TOE allows only the administrator to manage the security functions to ensure secure operation. To support the secure operation, OE.NOECHO prevents the password from being peeped by others when the administrator types it for authentication.

- Accesses to the MFD from the devices (including clients and servers) connected to the internal network with the intention to be used by authorized users of the MFD (including the administrator) shall be permitted and are not subjected to the denial by O.FILTER. According to OE.PC-USER, an identification and authentication function (including logging in the OS) shall be required for devices allowed connections to the MFD and only authorized users shall use the devices. This prevents attackers from abusing the devices allowed connections to the MFD (those for authorized users of the MFD) to access the address book data in the MFD (by impersonating authorised users).

Thus, O.FILTER and OE.PC-USER affect mutually and supplementary, and O.MANAGE and OE.NOECHO support O.FILTER. These objectives above can prevent the attacker who is not allowed to access to the MFD from accessing through the internal network and protect the address book data in the MFD.

4.3.1.3 T.SPOOF

The followings counter T.SPOOF.

- The TOE provides the function that identifies and authenticates the proper user that stored the confidential file according to O.USER.

- In support of the previous paragraph, as defined in O.MANAGE, the TOE allows only the administrator to manage the security functions to ensure secure operation. To support the secure operation, OE.NOECHO prevents the password from being peeped by others when the administrator types it for authentication.

- The confidential file password that is required for identifying and authenticating of the proper user that stored the confidential file shall be maintained safely not to be leaked. The administrator makes the users of the TOE and the MFD to follow OE.USER. OE.NOECHO prevents the confidential file password from being peeped by others when a user types it for authentication.

These objectives above can counter the threat that caused by an attacker's impersonating other user.

4.3.1.4 T.TAMPER

To counter T.TAMPER, the TOE provides the administrator function only to the administration according to O.MANAGE. OE.NOECHO prevents the password from being peeped by others when the administrator types it for authentication. Therefore, it is possible to protect the network settings data against reading or modifying by an attacker's impersonating an administrator.

4.3.1.5 T.TAP

The followings counter T.TAP.

- The TOE provides the function that prevents the user data on the internal network from wiretapping according to O.TRP.

- In support of the previous paragraph, as defined in O.MANAGE, the TOE allows only the administrator to manage the security functions to ensure secure operation. To support the secure operation, OE.NOECHO prevents the password from being peeped by others when the administrator types it for authentication.

● In the internal network where the TOE is installed, the administrator shall exercise due care (using the SSL function of the TOE or other protective means) of the communication data between the MFD user and the TOE not to be wiretapped, according to OE.CIPHER.

These objectives above can prevent the attacker from leaking the user data floating in the internal network when the proper user communicates with the MFD.

4.3.2 Rationale for Implementation of Organisational Security Policies

No organisational security objectives are presumed for the TOE in this ST. Therefore, there are no organisational security objectives that should be implemented.

4.3.3 Rationale for Satisfaction of Assumptions

The following is the rationale explaining why all assumptions are satisfied when the security objectives are achieved.

4.3.3.1 A.NETWORK

The assumption A.NETWORK requires that the MFD that the TOE is installed to is connected to an internal network, the internal network is protected against attacking from any external networks and only the devices that are allowed to communicate to the MFD are connected to at least the same subnetwork as MFD in the internal network. This is realized by the combination of OE.FIREWALL and OE.SUBNET.

4.3.3.2 A.OPERATOR

The assumption A.OPERATOR requires that the administrator is a trustworthy person. OE.OPERATE satisfies it by enforcing strict selection of the person to be the administrator based on an understanding of the role of administrator on the part of those in charge of the organisation that owns the TOE-equipped MFD. Therefore, A.OPERATOR can be achieved.

5 Extended Components Definition

This ST does not define any extended components.

6 Security Requirements

This chapter describes the security requirements.

6.1 Requirement Operations

This section defines the operations of CC functional and assurance components.

- Iteration operation: used to cover different aspects of the same requirements.
  - Component names, component labels and element labels are used as unique identifiers, with each followed by a consecutive number in brackets.
- Assignment operation: used to assign specified values to undetermined parameters such as the length of a password in the components.
  - A value assigned to a parameter is shown in brackets. Values, even if they are a part of a list of all, are comma-delimited or itemized.
  - Information in parentheses identifying each value such as its parameter name is added to the value as necessary.
- Selection operation: used to select one or more items from those given in the components.
  - Selected items are shown in brackets, with being underlined and in italics.
- Refinement operation: used to further refine the TOE by adding details to the components.
  - Additional text is shown in **bold**.
  - If a part of the original text is deleted, the part is shown in parentheses.
  - If a part of the original text is replaced with new text, the new text in **bold** is shown immediately before the original text in parentheses.
- *Simple Italics* do not indicate requirement operations. They are only used to emphasize text throughout the ST.

6.2 Security Functional Requirements

This section describes the SFR (Security Functional Requirements) that the TOE shall satisfy, based on the classes of CC Part 2.

6.2.1 Class FCS: Cryptographic Support

●FCS_CKM.1   Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1   The TSF shall generate cryptographic keys, **every time the MFD is turned on,** in accordance with a specified cryptographic key generation algorithm [MSN-H expansion algorithm] and specified cryptographic key sizes [128 bits] that meet the following: [Sharp Standard].

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
   FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

●FCS_COP.1   Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1   The TSF shall perform [

- Encrypting the user data that will be written to the MSD
- Encrypting the TSF data that will be written to the MSD
- Decrypting the user data that has been read from the MSD
- Decrypting the TSF data that has been read from the MSD

] in accordance with a specified cryptographic algorithm [AES Rijndael algorithm] and cryptographic key sizes [128 bits] that meet the following: [FIPS PUB 197].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
                  FDP_ITC.2 Import of user data with security attributes, or
                  FCS_CKM.1 Cryptographic key generation]
                  FCS_CKM.4 Cryptographic key destruction

6.2.2 Class FDP: User Data Protection

●FDP_RIP.1   Subset residual information protection

Hierarchical to: No other components.

FDP_RIP.1.1   The TSF shall ensure that any previous information content of a resource is made
                  unavailable **by overwriting one or more times** upon the *[deallocation of the
                  resource from]* the following objects: [

                  ● The spool image data file in the HDD

                  ● The filing image data file in the HDD

                  ● The address book data file in the HDD

                  ● The jobs completed list data file in the HDD

                  ● The spool image data file in the Flash memory

                  ].

Dependencies: No dependencies.

6.2.3 Class FIA: Identification and Authentication

●FIA_AFL.1 (1)   Authentication failure handling (1)

Hierarchical to: No other components.

FIA_AFL.1.1 (1)   The TSF shall detect when *[* [3 (*positive integer number*)] *]* unsuccessful
                  authentication attempts occur related to [

                  ● the unsuccessful administrator authentication attempts following the last
                    successful authentication

                  ].

FIA_AFL.1.2 (1)   When the defined number of unsuccessful authentication attempts has been *[met]*, the
                  TSF shall [

                  ● Unsuccessful authentication reached three times: Authentication trial receptionist
                    stop for five minutes

                  ● Five minutes pass from stopping: the unsuccessful authentication number of times
                    is cleared, and it is return automatically

                  ].

Dependencies: FIA_UAU.1 Timing of authentication

●FIA_AFL.1 (2)   Authentication failure handling (2)

Hierarchical to: No other components.

FIA_AFL.1.1 (2)   The TSF shall detect when *[* [3 (*positive integer number*)] *]* unsuccessful
                  authentication attempts occur related to [

                  ● the unsuccessful authentication attempts for a confidential file following the last
                    successful authentication for that confidential file

                  ].

FIA_AFL.1.2 (2)   When the defined number of unsuccessful authentication attempts has been *[met]*, the
                  TSF shall [

                  ● Unsuccessful authentication reaches three times: Authentication trial receptionist
                    stop and lock that confidential file

                  ● Release operation of the confidential file by the administrator: the unsuccessful

> authentication number of times for a confidential file is cleared, and it is return].

Dependencies: FIA_UAU.1 Timing of authentication

●FIA_SOS.1 (1)　　Verification of secrets (1)

Hierarchical to: No other components.

FIA_SOS.1.1 (1)　The TSF shall provide a mechanism to verify that **the administrator password** (secrets) **meets** (meet) [5 to 32 alphanumeric and/or symbol characters].

Dependencies: No dependencies.

●FIA_SOS.1 (2)　　Verification of secrets (2)

Hierarchical to: No other components.

FIA_SOS.1.1 (2)　The TSF shall provide a mechanism to verify that **the confidential file password** (secrets) **meets** (meet) [5 to 8 numeric characters].

Dependencies: No dependencies.

●FIA_UAU.2 (1)　　User authentication before any action (1)

Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.2.1 (1)　The TSF shall require each **administrator** (user) to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **administrator** (user).

Dependencies: FIA_UID.1 Timing of identification

●FIA_UAU.2 (2)　　User authentication before any action (2)

Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.2.1 (2)　The TSF shall require each user **that stored a confidential file** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

●FIA_UAU.7 (1)　　Protected authentication feedback (1)

Hierarchical to: No other components.

FIA_UAU.7.1 (1)　The TSF shall provide only [the number of characters that are provided] to the **administrator** (user) while the authentication **of the administrator** is in progress.

Dependencies: FIA_UAU.1 Timing of authentication

●FIA_UAU.7 (2)　　Protected authentication feedback (2)

Hierarchical to: No other components.

FIA_UAU.7.1 (2)　The TSF shall provide only [the number of characters that are provided] to **the user that stored a confidential file** while the authentication **of the user that stored a confidential file** is in progress.

Dependencies: FIA_UAU.1 Timing of authentication

●FIA_UID.2 (1)　　User identification before any action (1)

Hierarchical to: FIA_UID.1 Timing of identification

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

Dependencies: No dependencies.

●FIA_UID.2 (2)   User identification before any action (2)

Hierarchical to: FIA_UID.1 Timing of identification

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

Dependencies: No dependencies.

6.2.4 Class FMT: Security Management

●FMT_MOF.1   Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1   The TSF shall restrict the ability to *[disable]* the functions [Clear All Memory, Clear Document Filing Data, Power Up Auto Clear] to [administrator].

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

●FMT_MTD.1 (1)   Management of TSF data (1)

Hierarchical to: No other components.

FMT_MTD.1.1 (1) The TSF shall restrict the ability to *[modify]* the [administrator password] to [administrator].

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

●FMT_MTD.1 (2)   Management of TSF data (2)

Hierarchical to: No other components.

FMT_MTD.1.1 (2) The TSF shall restrict the ability to *[modify, delete]* the [confidential file password] to [the user that stored the confidential file].

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

●FMT_MTD.1 (3)   Management of TSF data (3)

Hierarchical to: No other components.

FMT_MTD.1.1 (3) The TSF shall restrict the ability to *[query, modify]* the [

- IP address filter
- MAC address filter
- SSL Settings
- Number of Times Auto Clear at Job End Program is Repeated
- Number of Times Data Clear is Repeated
- the data areas to be cleared by Power Up Auto Clear
- Number of Times Power Up Auto Clear Program is Repeated
- Disabling of Document Filing
- Disabling of Print Jobs Other Than Print Hold Job

] to [administrator].

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

●FMT_SMF.1   Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1   The TSF shall be capable of performing the following management functions: [

MX-FRX8 Security Target

- Disable: "Clear All Memory"
- Disable: "Clear Document Filing Data"
- Disable: "Power Up Auto Clear"
- Query and Modify: "Number of Times Auto Clear at Job End Program is Repeated"
- Query and Modify: "Number of Times Data Clear is Repeated"
- Query and Modify: "the data areas to be cleared by Power Up Auto Clear"
- Query and Modify: "Number of Times Power Up Auto Clear Program is Repeated"
- Lock releasing: "confidential files"
- Modify: "the administrator password"
- Modify and Delete: "the confidential file password"
- Query and Modify: "Disabling of Document Filing"
- Query and Modify: "Disabling of Print Jobs Other Than Print Hold Job"
- Query and Modify: "IP address filter"
- Query and Modify: "MAC address filter"
- Query and Modify: "SSL settings"

].

Note: Consideration for management requirement is described in Section 6.4.1.7.

Dependencies: No dependencies.

●FMT_SMR.1 (1)   Security roles (1)
Hierarchical to: No other components.
FMT_SMR.1.1 (1) The TSF shall maintain the roles [administrator].
FMT_SMR.1.2 (1) The TSF shall be able to associate users with roles.
Dependencies: FIA_UID.1 Timing of identification

●FMT_SMR.1 (2)   Security roles (2)
Hierarchical to: No other components.
FMT_SMR.1.1 (2) The TSF shall maintain the roles [each user that stored a confidential file].
FMT_SMR.1.2 (2) The TSF shall be able to associate users with roles.
Dependencies: FIA_UID.1 Timing of identification

6.2.5 Class FTA: TOE Access

●FTA_TSE.1   TOE session establishment
Hierarchical to: No other components.
FTA_TSE.1.1   The TSF shall be able to deny session establishment based on [IP address and MAC address].
Dependencies: No dependencies.

6.2.6 Class FTP: Trusted Path/Channels

●FTP_TRP.1   Trusted path
Hierarchical to: No other components.
FTP_TRP.1.1   The TSF shall provide a communication path between itself and *[remote]* users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *[modification,*

© 2007, Sharp Corp., all rights reserved.

disclosure].

FTP_TRP.1.2   The TSF shall permit *[remote users]* to initiate communication via the trusted path.

FTP_TRP.1.3   The TSF shall require the use of the trusted path for *[* [communication services by the TOE Web, communication services for the printer driver (*other services for which trusted path is required*)] *]*.

Dependencies: No dependencies.

6.3 Security Assurance Requirements

The EAL3 TOE security assurance requirements to which this ST claims conformance are shown by assurance class of CC Part 3. This ST uses the security assurance components defined in CC Part 3 without changes as the TOE security assurance requirements.

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

6.4 Security Requirements Rationale

This section demonstrates that the security requirements are effective to meet the security objectives.

Table 6.1: TOE Security Functional Requirements Rationale

Objective Requirement	O.FILTER	O.MANAGE	O.REMOVE	O.RESIDUAL	O.TRP	O.USER
FCS_CKM.1			6.4.1.3			
FCS_COP.1			6.4.1.3			
FDP_RIP.1				6.4.1.4		
FIA_AFL.1 (1)		6.4.1.2				
FIA_AFL.1 (2)		6.4.1.2				6.4.1.6
FIA_SOS.1 (1)		6.4.1.2				
FIA_SOS.1 (2)						6.4.1.6
FIA_UAU.2 (1)		6.4.1.2				
FIA_UAU.2 (2)						6.4.1.6
FIA_UAU.7 (1)		6.4.1.2				
FIA_UAU.7 (2)						6.4.1.6
FIA_UID.2 (1)		6.4.1.2				
FIA_UID.2 (2)						6.4.1.6
FMT_MOF.1		6.4.1.2				
FMT_MTD.1 (1)		6.4.1.2				
FMT_MTD.1 (2)						6.4.1.6
FMT_MTD.1 (3)	6.4.1.1	6.4.1.2			6.4.1.5	6.4.1.6
FMT_SMF.1	6.4.1.1	6.4.1.2			6.4.1.5	6.4.1.6
FMT_SMR.1 (1)		6.4.1.2				
FMT_SMR.1 (2)						6.4.1.6
FTA_TSE.1	6.4.1.1					
FTP_TRP.1					6.4.1.5	

6.4.1 TOE Security Functional Requirements Rationale

The correspondences between TOE security functional requirements and security objectives are shown in Table 6.1.

6.4.1.1 O.FILTER

O.FILTER can be met by the combination of the functional requirements as follows.

- The TOE is able to deny session establishment based on IP address or MAC address according to FTA_TSE.1.
- The TOE provides the capacity of performing the management of the IP address filter and MAC address filter that is required for operating previous paragraph according to FMT_SMF.1.
- The ability to query or modify the IP address filter and MAC address filter described in previous paragraph is restricted to the administrator by FMT_MTD.1 (3).

Because FMT_SMF.1 and FMT_MTD.1 (3) provide the management of FTA_TSE.1 consistently, no functional requirements conflict to meet O.FILTER.

6.4.1.2 O.MANAGE

O.MANAGE can be met by the combination of the functional requirements as follows.

a) The administrator is identified and authenticated by FIA_AFL.1 (1), FIA_UAU.2 (1), FIA_UAU.7 (1) and FIA_UID.2 (1). This enables only the administrator to execute the following functions:
  - The ability to modify the administrator password that is the TSF data to achieve O.MANAGE is restricted to the administrator by FMT_MTD.1 (1).
  - Only the administrator can modify and query the set values for each TSF by FMT_MTD.1 (3).
  - By FIA_AFL.1 (2), only the administrator can release the lock of confidential files which were locked because authentication was unsuccessful for consecutive times.
  - By FMT_MOF.1, only the administrator can disable each of the Clear All Memory, Clear Document Filing Data and Power Up Auto Clear functions while they are in the process.

b) The TOE provides the capacity of performing the modification of the administrator password that is required for operating of authentication of the administrator described above according to FMT_SMF.1.

c) Proper SOF shall be ensured for the administrator password as the followings show:

• To counter brute force attacks to break the administrator password, FIA_AFL.1 (1) requires to stop the acceptance of authentication trial for a certain period after authentication trials are unsuccessful for consecutive times.

• FIA_SOS.1 (1) requires a quality verification mechanism for the administrator password.

d) The administrator is assigned the role of TOE management by FMT_MOF.1 and FMT_MTD.1 (1). Since this role is maintained by FMT_SMR.1 (1), only authorized administrators can execute management functions.

The above FIA_AFL.1 (1), FIA_UID.2 (1), FIA_UAU.2 (1), FIA_UAU.7 (1), FMT_MOF.1, FMT_MTD.1 (1), FMT_MTD.1 (3), FMT_SMF.1 and FMT_SMR.1 (1) support each other based on mutual dependencies and they do not require any functionalities which conflict mutually. No conflictive functionalities are required between these requirements and FIA_AFL.1 (2). FIA_AFL.1 (2) and FMT_SMF.1 support mutually. FMT_SMR.1 (1) supports FIA_AFL.1 (2). No conflictive functionalities are required between these requirements and FIA_SOS.1 (1). FIA_SOS.1 (1) and FIA_AFL.1 (1) support mutually. Therefore, the set of requirements for O.MANAGE are consistent and do not conflict.

6.4.1.3 O.REMOVE

The intent of O.REMOVE is to counter T.RECOVER; in other words to make the user data stored in MSD not to regenerate even if the MSD is removed from MFD. This can be met by the combination of the functional requirements as follows.

● An attacker may attempt to reproduce user data by installing the MSD in any other MFD than the very MFD that has stored the user data to the MSD. Such an attempt will fail because the TOE encrypts user data to be written to the MSD as FCS_COP.1 requires.

● FCS_CKM.1 generates the cryptographic key that satisfies FCS_COP.1.

Because FCS_CKM.1 and FCS_COP.1 depend mutually, no functional requirements conflict to meet O.REMOVE.

6.4.1.4 O.RESIDUAL

To meet O.RESIDUAL, FDP_RIP.1 requires to overwrite the following objects' area one or more times upon the deallocation of the resource from the following objects.

● The target object are the spool image data file in the HDD, filing image data file in the HDD, address book data file in the HDD, jobs completed list data file in the HDD and the spool image data file in the Flash memory.

● The resource from these objects is deallocated when the jobs are completed or cancelled, the user deletes the confidential file and the specific data clear program is invoked by the operation or settings made by the administrator.

● The programs described in previous paragraph are Clear All Memory program, Clear Address Book Data and Registered Data in MFP program, Clear Document Filing Data program, Clear All Data in Job Status Jobs Completed List program and Power Up Auto Clear program.

Since O.RESIDUAL can be met by only a single functional requirement, it cannot cause any conflicts between functional requirements.

6.4.1.5 O.TRP

O.TRP can be met by the combination of the functional requirements as follows.

● FTP_TRP.1 enables the establishment and maintenance of trusted communications between the user and the TSF.

● The ability to query or modify the TSF data related to FTP_TRP.1; in other words, SSL Settings is restricted to the administrator by FMT_MTD.1 (3)

● Capability to manage them is implemented as FMT_SMF.1 requires.

Because FMT_MTD.1 (3) and FMT_SMF.1 define the management of FTP_TRP.1 in a mutually complementary manner, conflict of a functional requirement does not occur to achieve O.TRP as above.

6.4.1.6 O.USER

O.USER can be met by the combination of the functional requirements as follows.

a) The user that stored a confidential file is identified and authenticated by FIA_AFL.1 (2), FIA_UAU.2 (2), FIA_UAU.7 (2) and FIA_UID.2 (2). Thus only the user that stored a confidential file can access to the confidential file (include the management of the confidential file password).

b) It is ensured that the confidential file password meets 5 to 8 numeric characters according to FIA_SOS.1 (2).

c) The ability to modify the confidential file password is restricted to the user that stored a confidential file by FMT_MTD.1 (2).

d) The ability to query or modify the management for improving the effect of protection by the confidential file; in other words Disabling of Document Filing and Disabling of Print Jobs Other Than Print Hold Job is restricted to the administrator by FMT_MTD.1 (3).

e) The roles of the user that stored a confidential file are maintained and the user that stored a confidential file is associated with those roles by FMT_SMR.1 (2).

f) Capability to manage the confidential password is implemented as FMT_SMF.1 requires.

a) is related to the event about the identification and authentication of the user that stored a confidential file. b), c) and f) are related to the event about the modification of the confidential file password. d) is related to the event about the management by the administrator.

These three events occur independently of each other, and do not conflict mutually.

Conflict does not occur in a) because four functional requirements in a) affect mutually and supplementary to achieve the identification and authentication of the user that stored a confidential file.

Conflict does not occur in b), c) and f) because three functional requirements in b), c) and f) affect mutually and supplementary to achieve the modification of the confidential file password.

Conflict does not occur in e) because this functional requirement is depended on by c) and supported by a).

Thus, these functional requirements do not conflict to meet O.USER.

6.4.1.7 Rationale for consistence of TOE security management functions

Some of TOE security functional requirements require the security management function. [CC_PART2] suggests the management activities foreseen to each functional component as the management requirements of each component.

Table 6.2: Management Functions of the TOE

Management Function Origin	Management Function required	Consideration for management requirement
FCS_CKM.1	—	The cryptographic key attributes are not changed.
FCS_COP.1	—	(No management requirements)
FDP_RIP.1	• Disable: "Clear All Memory" • Disable: "Clear Document Filing Data" • Disable: "Power Up Auto Clear" • Query and Modify: "Number of Times Auto Clear at Job End Program is Repeated" • Query and Modify: "Number of Times Data Clear is Repeated" • Query and Modify: "the data areas to be cleared by Power Up Auto Clear" • Query and Modify: "Number of Times Power Up Auto Clear Program is Repeated"	The timing to perform protection is fixed to the release of allocation
FIA_AFL.1 (1)	—	The threshold and action are fixed.
FIA_AFL.1 (2)	• Lock releasing: "confidential files"	The threshold and action are fixed.
FIA_SOS.1 (1)	—	The quality metric is fixed.
FIA_SOS.1 (2)	—	The quality metric is fixed.
FIA_UAU.2 (1)	• Modify: "the administrator password"	Management Function required agrees with management requirement.
FIA_UAU.2 (2)	• Modify and Delete: "the confidential file password" • Query and Modify: "Disabling of Document Filing" • Query and Modify: "Disabling of Print Jobs Other Than Print Hold Job"	Management Function required agrees with management requirement.
FIA_UAU.7 (1)	—	(No management requirements)
FIA_UAU.7 (2)	—	(No management requirements)
FIA_UID.2 (1)	—	Identification of the administrator is fixed.
FIA_UID.2 (2)	—	Identification of each user that stored a confidential file is fixed.
FMT_MOF.1	—	No role groups
FMT_MTD.1 (1)	—	No role groups
FMT_MTD.1 (2)	—	No role groups
FMT_MTD.1 (3)	—	No role groups
FMT_SMF.1	—	(No management requirements)
FMT_SMR.1 (1)	—	No user groups
FMT_SMR.1 (2)	—	No user groups
FTA_TSE.1	• Query and Modify: "IP address filter" • Query and Modify: "MAC address filter"	Management Function required agrees with management requirement.
FTP_TRP.1	• Query and Modify: "SSL settings"	Management Function required agrees with management requirement.

The management functions required by all TOE security functional requirement components are shown in Table 6.2 with the consideration for management requirement. The management functions specified by FMT_SMF.1 agree with the management functions required shown in the table.

Thus, TOE security requirements are internally consistent with security management functions.

6.4.1.8 Rationale for security functional requirement dependencies

Table 6.3 shows the dependencies that the security functional requirements must satisfy according to the CC, the dependencies that the TOE satisfies, and the dependencies that the TOE does not satisfy. The dependency that is marked with "#" in the table is satisfied by the hierarchically upper SFR. Table 6.4 shows the justification for the TOE not satisfying certain dependencies. Correspondences between the following two tables are indicated by common identifiers (such as J1).

Table 6.3: SFR Dependencies

Dependencies Requirement	Stipulated	Satisfied	Unsatisfied	Justification
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1	FCS_CKM.4	J1
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1	FCS_CKM.4	J1
FDP_RIP.1	—	—	—	—
FIA_AFL.1 (1)	FIA_UAU.1 #	FIA_UAU.2 (1)	—	—
FIA_AFL.1 (2)	FIA_UAU.1 #	FIA_UAU.2 (2)	—	—
FIA_SOS.1 (1)	—	—	—	—
FIA_SOS.1 (2)	—	—	—	—
FIA_UAU.2 (1)	FIA_UID.1 #	FIA_UID.2 (1)	—	—
FIA_UAU.2 (2)	FIA_UID.1 #	FIA_UID.2 (2)	—	—
FIA_UAU.7 (1)	FIA_UAU.1 #	FIA_UAU.2 (1)	—	—
FIA_UAU.7 (2)	FIA_UAU.1 #	FIA_UAU.2 (2)	—	—
FIA_UID.2 (1)	—	—	—	—
FIA_UID.2 (2)	—	—	—	—
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1 (1)	—	—
FMT_MTD.1 (1)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1 (1)	—	—
FMT_MTD.1 (2)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.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	—	—	—	—
FMT_SMR.1 (1)	FIA_UID.1 #	FIA_UID.2 (1)	—	—
FMT_SMR.1 (2)	FIA_UID.1 #	FIA_UID.2 (2)	—	—
FTA_TSE.1	—	—	—	—
FTP_TRP.1	—	—	—	—

Table 6.4: Justification of Unsatisfied SFR Dependencies

	Unsatisfied	Justification Rationale
J1	FCS_CKM.4	The cryptographic key is stored in volatile memory. When the power is off, electrical charge of volatile memory in which the cryptographic key is stored disappears and the cryptographic key is destructed. Therefore, there is no necessity to implement the TSF that performs the standard key destruction method, and FCS_CKM.4 is not required to specify standards.

6.4.2 TOE security Assurance Requirements Rationale

The TOE is a part of MFD and optional product for MFD that is sold separately; in other words commercial product. The threat is that a low-level attacker may use a device other than the MFD to physically, and read and leak information in the MSD of the MFD. To assure in the commercial product the reliability of the security functions countering such threats, EAL3 is selected, which includes analyses of security objectives taken during the TOE development and of guidance to use the security functions safely is included.

Since the assurance requirements conform to EAL3, all assurance requirements meet the dependencies.

7 TOE Summary Specification

By describing a summary specification of the TOE security function (TSF), this chapter shows that the TOE security functional requirements are satisfied. Table 7.1 shows the correspondences between the TOE security functional requirements and the TOE security functions. The section number where each correspondence is described is shown in the table.

Table 7.1: Security Functional Requirements and TOE Security Specifications

Function Requirement	TSF_FKG	TSF_FDE	TSF_FDC	TSF_AUT	TSF_FCF	TSF_FNP
FCS_CKM.1	7.1					
FCS_COP.1		7.2				
FDP_RIP.1			7.3			
FIA_AFL.1 (1)			7.3	7.4		7.6
FIA_AFL.1 (2)					7.5	
FIA_SOS.1 (1)				7.4		
FIA_SOS.1 (2)					7.5	
FIA_UAU.2 (1)			7.3	7.4		7.6
FIA_UAU.2 (2)					7.5	
FIA_UAU.7 (1)			7.3	7.4		7.6
FIA_UAU.7 (2)					7.5	
FIA_UID.2 (1)			7.3	7.4		7.6
FIA_UID.2 (2)					7.5	
FMT_MOF.1			7.3			
FMT_MTD.1 (1)				7.4		
FMT_MTD.1 (2)					7.5	
FMT_MTD.1 (3)			7.3		7.5	7.6
FMT_SMF.1			7.3	7.4	7.5	7.6
FMT_SMR.1 (1)				7.4		
FMT_SMR.1 (2)					7.5	
FTA_TSE.1						7.6
FTP_TRP.1						7.6

7.1 Cryptographic Key Generation (TSF_FKG)

According to FCS_CKM.1, this TSF generates a cryptographic key (common key) to support the encryption function of the user data and the TSF data.

The TSF automatically generates the secure seed when the TOE is installed. With the seed, the TSF generates a 128-bit key using the MSN-H expansion algorithm every time the MFD is turned on. The MSN-H expansion algorithm is a cryptographic key generation algorithm which meets the Sharp standard and generates a 128-bit key. Therefore, the TOE satisfies FCS_CKM.1.

The TOE in each MFD generates a cryptographic key always using the same seed and algorithm. The key generated is stored to the volatile memory to use them in the AES Rijndael and is destructed when the MFD is turned off.

7.2 Cryptographic Operation (TSF_FDE)

As defined in FCS_COP.1, this TSF always encrypts and writes the user data and the TSF data when it is necessary to write them to the MSD. In addition, this function reads them from the MFD and decrypts when these data are required. The AES Rijndael algorithm that is based on FIPS PUBS 197 and the 128 bits cryptographic key that is generated by cryptographic key generation function (TSF_FKG) are used for encryption and decryption.

The following user data below are the target of cryptographic operation:

- Image data that are spooled to the HDD
- Image data that are spooled to the Flash memory
- Image data that are stored to the HDD
- Address book data in the HDD
- Jobs completed list data in the HDD

The following TSF data below are the target of cryptographic operation:

- Confidential file password in the HDD
- Administrator password in the HDD

Therefore, the TOE satisfies FCS_COP.1.

7.3 Data Clear (TSF_FDC)

In the following, first the TSF overview and then each component are described.

7.3.1 Overview of the Data Clear Function

The whole picture of this TSF and its correspondences between SFRs are described.

The TOE provides the data clear function that clears image data files that are spooled and stored, the address book data file and the jobs completed list data file. The following each program is contained in this function:

a) Auto Clear at Job End program

b) Clear All Memory program

c) Clear Address Book Data and Registered Data in MFP program

d) Clear Document Filing Data program

e) Clear All Data in Job Status Jobs Completed List program

f) Power Up Auto Clear program

Every program above and their settings functions make up the TSF. The programs correspond to the SFRs as follows:

- Each program overwrites the HDD one or more times with a random value, and the Flash memory once with a fixed value (a line of 0-bit value or a line of 1-bit value). Each program overwrites assigned objects (such as image data files) to disable regeneration of the information stored in the objects (such as image data). Thus, the TOE satisfies FDP_RIP.1.

- The above b), d) and f) have the cancel operation (Section 7.3.3) to stop in accordance with FMT_SMF.1 and satisfy FIA_AFL.1 (1), FIA_UAU.2 (1), FIA_UAU.7 (1) and FIA_UID.2 (1) in cooperation with TSF_AUT and TSF_FNP which are later discussed. The cancel operation requires the administrator to be identified and authenticated according to FIA_UID.2 (1) and FIA_UAU.2 (1). For authentication, the protected feedback by FIA_UAU.7 (1) and the failure handling by FIA_AFL.1 (1) are provided. This allows only the administrator to stop the data clear function in process as defined in FMT_MOF.1.

- This TSF allows the administrator who is identified and authenticated according to TSF_AUT to use settings functions (Section 7.3.8) according to FMT_SMF.1. This allows the TSF to satisfy FMT_MTD.1 (3) in cooperation with TSF_FCF and TSF_FNP.

The following sections elaborate upon each program and settings.

7.3.2 Auto Clear at Job End program

This program overwrites the image data that has been:

- Spooled to the HDD or the Flash memory in order to process a job, when the job is completed or cancelled, and
- Saved to the HDD using the document filing function (include the confidential files function), when the user deletes the data.

This program is always invoked at the specified timing in both case and the method to disable this program is not provided.

7.3.3 Clear All Memory program

This program is invoked from the operation panel by the administrator who is identified and authenticated by TSF_AUT and overwrites the following data:

- All of the spool image data in the HDD
- All of the filing image data in the HDD
- The jobs completed list data in the HDD
- All of the spool image data in the Flash memory

This program does not clear the address book data.

This program accepts the cancel operation. Before allowing cancelling this program while running, this TSF always requires the administrator who calls this program to enter the administrator password whenever a cancel operation is taken. The cancel operation serves as identification of the administrator defined in FIA_UID.2 (1) and entering the administrator password serves as authentication of the administrator defined in FIA_UAU.2 (1). While entering for authentication, the TOE shows as many asterisk characters as characters entered according to FIA_UAU.7 (1), however does not show the characters entered. The overwrite operation is only cancelled if entering for authentication is successful.

If an incorrect administrator password is entered three times in a row while entering for authentication of cancel operation, this program stops accepting further authentication attempts as defined in FIA_AFL.1 (1); that is to lock the administrator password. When five minutes passed from locking, this program unlocks automatically; that is to clear the unsuccessful authentication number of times and return from locking state automatically.

7.3.4 Clear Address Book Data and Registered Data in MFP program

This program is invoked by the operation of the administrator who is identified and authenticated by TSF_AUT and overwrites the address book data in the HDD. This program does not accept the cancel operation for the relatively short time required.

7.3.5 Clear Document Filing Data program

This program is invoked by the operation of the administrator who is identified and authenticated by TSF_AUT and overwrites the image data in the HDD. The data to be cleared by this program is specified one or more from the following choices by the administrator when this program is invoked.

- All of the spool image data in the HDD
- All of the filing image data in the HDD

This program accepts the cancel operation as well as Clear All Memory program.

7.3.6 Clear All Data in Job Status Jobs Completed List program

This program is invoked from the operation panel by the administrator who is identified and authenticated by TSF_AUT and overwrites the jobs completed list data in the HDD. This program does not accept cancel operation for the relatively short time required.

7.3.7 Power Up Auto Clear program

This program overwrites and clears the data when the TOE is turned on, unless the TOE has any reserved transmission jobs or any Fax/Internet fax reception jobs not yet printed out.

This program is enabled or disabled; in other words, this program is run or not when the TOE is powered on, according to the settings that are configured beforehand. The target data of this program is also according to those settings.

This program clears every data as well as the Clear All Memory program above, or the specified data in the HDD. The data in the HDD can be specified among the spool image data, filing image data or jobs completed list data.

This program accepts cancel operation as well as Clear All Memory program.

7.3.8 Data Clearance Settings

This TSF provides the following configuration functions below for the every program above:

- Number of Times Auto Clear at Job End Program is Repeated:
  accepts any integer between 1 and 7 inclusive as the number of times overwriting the data on the HDD for the Auto Clear at Job End program. The default is 1.

- Number of Times Data Clear is Repeated:
  accepts any integer between 1 and 7 inclusive as the number of times overwriting the data on the HDD for the Clear All Memory program, Clear Address Book Data and Registered Data in MFP program, the Clear Document Filing Data program and the Clear All Data in Job Status Jobs Completed List program. The default is 1.

- Power Up Auto Clear:
  accepts settings to specify data areas to be cleared for which Power Up Auto Clear program is valid. The default is that Power Up Auto Clear program is disabled for every data (no data is specified).

- Number of Times Power Up Auto Clear Program is Repeated:
  accepts any integer between 1 and 7 inclusive as the number of times overwriting the data on the HDD for the Power Up Auto Clear program. The default is 1.

Only the administrator identified and authenticated by TSF_AUT is allowed to query and modify each setting above.

7.4 Authentication (TSF_AUT)

This TSF enforces the identification and authentication of the administrator by the administrator password. According to FMT_SMF.1 and FMT_MTD.1 (1), the TSF allows only the administrator who is identified and authenticated by the TSF to modify the administrator password. According to FIA_SOS.1 (1), the TSF only accepts a password consisting of 5 to 32 alphanumeric and symbolic characters.

The functions not for the administrator are available without identification and authentication of the administrator.

In cooperation with TSF_FDC and TSF_FNP, this TSF satisfies FIA_AFL.1 (1), FIA_UAU.2 (1), FIA_UAU.7 (1) and FIA_UID.2 (1).

This function provides the interfaces of the function for the administrator when the administrator is identified by the running operation of the management functions or the login operation of the administrator according to FIA_UID.2 (1), and the authentication of the administrator is successful by the correct administrator password according to FIA_UAU.2 (1),. The login operation of the administrator includes both identification of administrator and authentication of the administrator password from the operation panel or via the TOE Web.

When the administrator password is entered from the operation panel, this TSF, according to FIA_UAU.7 (1), shows as many asterisk characters as characters entered, however does not show the characters entered.

When the administrator password is entered via the TOE Web, this TSF specifies the input type as a password to the client. This requires the client to hide the character that the user entered such as a substitute character.

If an incorrect administrator password is entered three times in a row while entering for authentication of the administrator password, this program stops accepting further authentication attempts according to FIA_AFL.1 (1); that is to lock the administrator password. When five minutes passed from locking, this program unlocks automatically; that is to clear the unsuccessful authentication number of times and return from locking state automatically.

The TSF identifies the administrator by the authentication function and relates him/her to the role. By providing only the administrator with the management function to change (modify) the administrator password, the secure maintenance of the role is achieved. Thus, the TOE satisfies FMT_SMR.1 (1).

7.5 Confidential files (TSF_FCF)

When a user saves image data in the MFD as a confidential file, the data is protected by a password and authentication is required before calling it up and using it.

This TSF provides the interface for creating the confidential file to the each Copier, Printer driver, PC-Fax and Scan to HDD and, according to FIA_SOS.1 (2), verifies that the confidential file password meets the quality metric, 5 to 8 numeric characters.

This TSF provides functionalities of the operations on saved confidential files on the operation panel and the TOE Web. According to FIA_UID.2 (2), the TSF identifies the user that stored a confidential file when the user selects the confidential file and, according to FIA_UAU.2 (2), provides the interface for file manipulation only when authentication is successful with the correct confidential file password. During the authentication, the TSF does not disclose information other than the number of characters typed according to FIA_UAU.7 (2).

Whenever a user attempts some operation on a saved confidential file on the operation panel, this TSF requests the user to enter the confidential file password. This TSF shows as many asterisk characters as characters entered, however does not show the characters entered. In case a user attempts some operation on a saved confidential file via the operation panel, this TSF allows the operations described in Section 1.3.5.2 except Preview, only when a confidential file password is given and it is identical to the confidential file password during the saving of the file.

In case a user attempts some operation on a saved confidential file via the TOE Web, this TSF allows all operations including Preview, only when a confidential file password is given and it is identical to the confidential file password during the saving of the file. This TSF specifies the input type as a password to the client when the confidential file password is entered. This requires the client to hide the character that the user entered such as a substitute character.

If an incorrect confidential file password is entered three times in a row during the authentication before an operation on a saved confidential file, this TSF stops accepting further authentication attempts and locks the file to prohibit any operations according to FIA_AFL.1 (2). The number of authentication failures is counted for each file. When authentication is successful, the authentication failure count of the file is reset to zero. The lock can be released by only the administrator identified and authenticated by TSF_AUT.

According to FMT_MTD.1 (2) and FMT_SMF.1, this TSF allows to change the confidential file password as one of the operations on a saved confidential file and verifies the new confidential password meets the quality metric, 5 to 8 numeric characters.

This TSF identifies the user that stored a confidential file by identification and authentication of the user prior to file manipulation and relates him/her to the role. By providing only the user that stored a confidential file with the function to change (modify) the confidential file password, the secure maintenance of the role is achieved. Thus, the TOE satisfies FMT_SMR.1 (2)

This TSF allows changing the property, as one of the operations on a saved confidential file. The password is deleted when the property is changed to other than Confidential. In the other direction, to change the property to Confidential, the TSF requires the user to specify a confidential file password which meets the quality metric, 5 to 8 numeric characters, according to FIA_SOS.1 (2).

This TSF exports the encrypted data to the Web browser of the client. This TSF also imports both encrypted and not encrypted data from the Web browser of the client.

According to FMT_SMF.1 and FMT_MTD.1 (3), this TSF provides the following management functions for the document filing function and allows the administrator whom TSF_AUT has identified and authenticated to execute them:

- Management functions for improving the effect of protection by the confidential file:
  - Disabling of Document Filing: disables each mode of saving for each job type. The default and recommended value is that the non-confidential mode (where files are saved without password protection) is disabled for all job types.
  - Disabling of Print Jobs Other Than Print Hold Job: disables the job to print out on the spot from the printer driver. This function denies the job without Holding and holds the Hold job by ignoring that the job is printed out or not. This function is recommended to use in the environment that has the high risk that the third person takes away the output paper.
- Management function for locking the confidential files:
  - Release the lock of confidential files: releases locked confidential files by the failure of the authentication for the confidential file password. This management function is provides as "*Release the Lock on File/Folder Manipulation*".

7.6 Network Protection Function (TSF_FNP)

In the following, first the TSF overview and then each component are as follows.

7.6.1 Overview of Network Protection

Components of this TSF and their correspondences between SFRs are as follows. This TSF consists of the following functions:

  a) Filter function

  b) Communication data protection function

  c) Network settings protection

The above a) satisfies FTA_TSE.1. The above b) satisfies FTP_TRP.1. In cooperation with TSF_FDC and TSF_AUT, the above c) satisfies FIA_AFL.1 (1), FIA_UAU.2 (1), FIA_UAU.7 (1) and FIA_UID.2 (1). In cooperation with TSF_FDC and TSF_FCF, the a) and b) above satisfy FMT_MTD.1 (3) and FMT_SMF.1. The following sections elaborate upon each function.

7.6.2 Filter Function

This function denies the communication with the other party not to be intended according to the settings that the administrator configured beforehand. The settings can be configured the terms of IP address and MAC address. This TSF always cancels the network packet from the other party that does not match the terms, does not respond to and manage it.

The terms of IP address are specified as the range up to 4 and selected whether these terms are allowed or not. The terms of MAC address are specified as the allowed MAC address up to 10.

This TSF satisfies FTA_TSE.1 because it rejects communication to and from an unintended third party based on the IP address and the MAC address. According to FMT_MTD.1 (3), the TSF allows only the administrator who is identified and authenticated by TSF_AUT to query and modify the filtered values of the IP address and the MAC address which are TSF data.

7.6.3 Communication Data Protection Function

This function provides the HTTPS communication function to prevent wiretapping of communication data between the client and the TOE Web. This function also provides the IPP-SSL communication function to prevent wiretapping of print data that is sent from the printer driver of the client.

HTTPS communication begins by the connection from the Web browser of the client and keeps communication until it is disconnected. IPP-SSL communication also begins by the connection from the printer driver of the client and keeps communication until it is disconnected.

The cryptographic algorithms used in HTTPS communication and IPP-SSL communication are RSA, DES, Triple-DES, AES and SHA-1. The server private key and public key are installed by configuring of the administrator.

According to FMT_MTD.1 (3), the TSF allows only the administrator who is identified and authenticated by TSF_AUT to query and modify SSL settings which are a collection of the set values relating to HTTPS communication and IPP-SSL communication (TSF data).

7.6.4 Network Settings Protection

This function provides the interfaces to manage the network settings data described in Section 1.4.4.5 at the operation panel and the TOE Web. These interfaces are provided only to the administrator to prevent other users from accessing. So this TSF enforces the identification and authentication same as TSF AUT before providing the interfaces to manage the network settings data. The identification and authentication is executed according to FIA_UID.2 (1), FIA_UAU.2 (1), FIA_UAU.7 (1) and FIA_AFL.1 (1) in the same way as TSF_AUT.

8 Appendix

This chapter describes the definitions of terms.

8.1 Terminology

Terminology unique to this ST is defined in Table 8.1.

Table 8.1: Terminology

Term	Definition
Auto Clear at Job End	The function that clears (by overwriting) image data of each job stored in some MSD of the MFD, invoked when a job is finished or cancelled and when a user deletes a saved data file.
Board	A printed circuit board on which components are mounted by soldering.
Clear Address Book Data and Registered Data in MFP	An operation to clear (by overwriting) address book data stored in the HDD. This function is invoked by the operation of the administrator.
Clear All Data in Job Status Jobs Completed List	The function to overwrite the jobs completed list data that is stored to the HDD. This is invoked by the operation of the administrator.
Clear All Memory	The function to overwrite the all image data and job completed list data that are stored to the MSD in the MFD. This function is invoked by the operation of the administrator.
Clear Document Filing Data	The function to overwrite the image data that are stored to the HDD. This function is invoked by the operation of the administrator. The main objective is to clear the image data that are stored, but it is also available to clear the image data that are spooled.
Confidential file	The data that the user saved with the protection of a password (confidential file password) to prevent the others from manipulating.
Confidential file password	The password to prevent the others from reusing the confidential file without permission.
Controller board	The board that controls the whole MFD. This contains the microprocessor to execute firmware of the TOE, volatile memory, HDC, HDD and others.
Controller firmware	The firmware that controls the controller board in the MFD. This is contained in the ROM board on the controller board.
Disabling of Document Filing	The management function to disable to save the image data for each job type and mode. This is used to disable to save the image data without Confidential Mode.
Disabling of Print Jobs Other Than Print Hold Job	Disables to print out the jobs from the printer driver on the spot. This function denies the jobs without Holding and only holds the jobs with Holding by ignoring the settings that is whether the jobs are printed or not.
Document filing	The function that stores image data handled by the MFD into the HDD, for users' later operations, such as a printing or a transmission. This is also called "Filing" in this document.
Engine	A device that forms print images on receiver papers, with mechanism of paper feeding/ejection. Also called as "print engine" or "engine unit".
External network	A network, not the internal network of an organisation, which the organisation does not manage.
File manipulation	An operation to manipulate image data saved as a file.
Filing	Stands for "Document filing". This is also to store the image data by document filing function.
Firmware	The software that is embedded to the machines to control the machine's hardware. In this document, firmware especially indicates the controller firmware.
Flash memory	A type of non-volatile memory that allows the entire memory to be erased at once and also allows rewriting to any part of memory.
Hold	To store the job from printer driver by filing.
Image data	Digital data, especially in this document, of two-dimensional image that each function of the MFD manages.
Internal network	The network that is inside the organisation and protected against the threat about security from any external networks.

38

Term	Definition
Job	The sequence from beginning to end of the use of an MFD function (copier, printer, scanner, fax reception, fax transmission, or PC-Fax). In addition, the instruction for a functional operation is sometimes called a job.
Jobs completed list	The record about the completed jobs, stored in the HDD of the MFD.
Lock	The function to stop accepting passwords if incorrect passwords are entered in a row.
Memory	A memory device; in particular a semiconductor memory device.
Non-volatile memory	The memory device that retains its contents even when the power is turned off.
Operation panel	The user interface unit in front of the MFD. This contains the start key, numeric key, function key and liquid crystal display with touch operation system.
Power Up Auto Clear	The function to overwrite the data in the MSD when the MFD is powered on. This function is invoked when the MFD is powered on, according to the settings that are specified by the administrator beforehand.
Scan to HDD	One of the filing functions. It scans the original to obtain image data, and does only save a file of the image data into the HDD, while neither prints nor transmits it.
Scanner unit	The device that scans the original and gets the image data. This is used for copier, scanner, fax transmission or scan to HDD.
Spool	Storing the job's image data to the MSD temporary to increase the input and output efficiency.
Standard firmware	The controller firmware that is installed to the MFD that TOE is not installed to. TOE contains the controller firmware and standard firmware is removed when the TOE is installed.
Subnetwork	A part of internal network divided by router.
Tandem copy	Tandem print in the MFD's copier function.
Tandem print	The function to print a large job twice faster than usually by halving that job among two MFDs.
Unit	A substance provided standard that can be attached to or detached from a printed circuit board; or an option that is installed and is ready for operation. This can also be a system that includes a mechanism and is ready for operation.
User that stored a confidential file	The user that saved the image data as a confidential file.
Volatile memory	A memory device, the contents of which vanish when the power is turned off.

8.2 Acronyms

Acronyms used in this ST are indicated in Table 8.2 and Table 8.3.

Table 8.2: Acronyms in the CC

Acronym	Definition
CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

Table 8.3: Other Acronyms

Acronym	Definition
AES	Advanced Encryption Standard, established by NIST (National Institute of Standards and Technology, United States of America)
DSK	Data Security Kit MX-FRX8, an optional product for the MFD providing the firmware part of the TOE.
EEPROM	Electrically Erasable Programmable ROM, a type of non-volatile memory that allows low frequency of electrical rewriting at any address.
HDC	Hard Disk Controller
HDD	Hard Disk Drive
HTTP	Hypertext Transfer Protocol, a communication protocol generally used for Web.
HTTPS	HTTP over SSL, HTTP with protection of SSL.
I/F	Interface
IPP	Internet Printing Protocol, a communication protocol for printing.
IPP-SSL	IPP over SSL, IPP with protection of SSL.
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol, a communication protocol for directory service.
MFD	Multi Function Device, a digital multifunctional device which is an office machine mainly equipped with copier, printer, scanner and fax functions.
MSD	Mass Storage Device, in this document, this especially indicates the HDD and Flash memory in MFD.
NIC	Network Interface Card, or, Network Interface Controller
PC	Personal Computer
ROM	Read Only Memory
SSL	Secure Socket Layer, a cryptographic communication protocol for computer network.
TLS	Transport Layer Security, a cryptographic communication protocol for computer network.
UI	User Interface
USB	Universal Serial Bus, a serial bus standard to connect between IT equipments.
SMTP	Simple Mail Transfer Protocol, a communication protocol to transfer E-mails.
WINS	Windows Internet Name Service, resolves a NetBIOS name into the IP address.