SHARP

MX-FRX2

Security Target

Version 0.05

This document is a translation of the security target written in Japanese, which has been evaluated and certified. The Japan Certification Body has reviewed and checked it.

SHARP CORPORATION

Revision history

Date	Ver.	Revision	Author	Reviewed	Approved
6 Feb. 2006	0.01	• Original Draft	Nakagawa	Iwasaki	Kubota
13 Mar. 2006	0.02	• Modified TOE Description and related descriptions	Nakagawa	Iwasaki	Kubota
21 June 2006	0.03	• Corrected errors: chapter 5, 6 and 8	Nakagawa	Iwasaki	Kubota
29 Aug. 2006	0.04	• Modified assumption A.NETWORK and related descriptions	Nakagawa	Iwasaki	Kubota
6 Oct. 2006	0.05	• Modified description on the cryptographic key generation function (TSF_FKG) and related descriptions, in response to Observation Report ASE001-01	Nakagawa	Iwasaki	Kubota

Table of Contents

1 Security Target Introduction 6
1.1 ST Identification 6
1.2 ST Overview 6
1.3 CC Conformance Claim 6
1.4 Reference Materials 6
1.5 Conventions, Terminology, and Acronyms 7
1.5.1 Conventions 7
1.5.2 Terminology 7
1.5.3 Acronyms 9
2 TOE Description 10
2.1 TOE Overview 10
2.1.1 TOE Type 10
2.1.2 Overview of the TOE Security Functions 10
2.2 TOE Configuration 10
2.2.1 Physical Scope and Boundaries of the TOE 10
2.2.2 Logical Scope and Boundaries of the TOE 11
2.3 Overview of the MFD Functions and Applications 12
2.3.1 Job function 12
2.3.2 Document filing function 13
2.3.3 Address book function 13
2.4 Operating/managing the TOE 14
2.5 Assets Protected by the TOE 14
2.5.1 Image data that the MFD functions spool to process jobs. 14
2.5.2 Image data that users save as a confidential files 14
2.5.3 Address book data. 15
2.5.4 Jobs completed list data 15
2.5.5 Network settings data 15
3 TOE Security Environment 16
3.1 Assumptions 16
3.2 Threats 16
3.3 Organizational Security Policies 16
4 Security Objectives 17
4.1 Security Objectives for the TOE 17
4.2 Security Objectives for the Environment 17
5 IT Security Requirements 18
5.1 TOE Security Requirements 18
5.1.1 TOE Security Functional Requirements 18
5.1.2 TOE Minimum Strength of Function 23
5.1.3 TOE Security Assurance Requirements 23
5.2 Security Requirements for the IT Environment 24
6 TOE Summary Specification 25
6.1 TOE Security Functions (TSF) 25
6.1.1 Cryptographic key generation (TSF_FKG) 25

6.1.2 Cryptographic operation (TSF_FDE) 26
6.1.3 Data clear (TSF_FDC) 26
6.1.4 Authentication (TSF_AUT) 28
6.1.5 Confidential files (TSF_FCF) 28
6.1.6 Network protection function (TSF_FNP) 29
6.2 TSF Strength of Security Functions 30
6.3 Assurance Measures 30
7 PP Claims 31
8 Rationale 32
8.1 Security Objectives Rationale 32
8.1.1 A.NETWORK 32
8.1.2 A.OPERATOR 32
8.1.3 T.RECOVER 32
8.1.4 T.REMOTE 33
8.1.5 T.SPOOF 33
8.1.6 T.TAMPER 33
8.1.7 T.TAP 33
8.1.8 P.RESIDUAL 34
8.2 Security Requirements Rationale 34
8.2.1 Security Functional Requirements Rationale 34
8.2.2 Rationale for consistence of TOE security management functions 38
8.2.3 Rationale for security functional requirement dependencies 40
8.2.4 Mutual effect of security requirements 41
8.2.5 TOE security assurance requirements Rationale 42
8.2.6 Rationale for Minimum Strength of Function 42
8.3 TOE Summary Specification Rationale 42
8.3.1 TOE Summary Specification Rationale 42
8.3.2 TOE assurance measures Rationale 48
8.3.3 Rationale for Strength of TOE Security Function 49

List of Tables

Table 1-1: Reference Materials 7
Table 1-2: Terminology 7
Table 1-3: Acronyms 9
Table 3-1: Assumptions 16
Table 3-2: Threats 16
Table 3-3: Organizational Security Policies 16
Table 4-1: TOE Security Objectives 17
Table 4-2: Environmental Security Objectives 17
Table 5-1: Assurance Requirements 24
Table 6-1: Security Functional Requirements and TOE Security Specifications 25
Table 6-2: Assurance Measures 30
Table 8-1: Security Objectives Rationale 32
Table 8-2: Security Functional Requirements Rationale 35
Table 8-3: Management Functions of the TOE 39
Table 8-4: Security Functional Requirement Dependencies 40
Table 8-5: Mutual effect of security requirements 41

List of Figures

Figure 2-1: TOE and physical configuration of the MFD 10
Figure 2-2: Logical configuration of the TOE 11
Figure 2-3: Usage environment of the MFD 12

1 Security Target Introduction

1.1 ST Identification

This section provides information needed to identify this ST and its TOE.

ST Title:	MX-FRX2 Security Target
ST Version:	0.05
Publication Date:	6 October 2006
Author:	Sharp Corporation
TOE Identification:	MX-FRX2 Version M.10
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999 — also known as ISO/IEC 15408:1999; with CCIMB Interpretations as of 01 December 2003
ST Evaluator:	Japan Electronics and Information Technology Industries Association, IT Security Center
Keywords:	SHARP, SHARP Corporation, Digital Multifunction Device, Multifunction Device, Multifunction Printer, MFP, MFD, encryption, data encryption, data clearing

1.2 ST Overview

This ST explains about MX-FRX2, which is the TOE composed of the following two parts. One of the parts that compose this TOE, MX-FRX2, is firmware provided in the form of “Data Security Kit MX-FRX2” that is the product to enhance the security of Multi Function Device made by SHARP. The other is the HDC that runs under the control of that firmware.

A Multi Function Device (hereafter referred to as “MFD”) is an office machine that has functions such as copy, printer, image scanning and fax. “Data Security Kit MX-FRX2” is an optional product for the MFD made by SHARP that is sold separately and works by installing to the MFD. The HDC of this TOE is a part of an MFD. The security functions in the HDC are enabled by the firmware in “Data Security Kit MX-FRX2.”

This TOE is intended to counter attempts to steal image data stored in non-volatile storage devices in a MFD such as HDD. Its major security functions are:

a) Encryption of the image data and related data
b) Erasure of the image data and related data by overwriting when these data be deleted
c) Password protection of the image data and related data that are stored to the HDD by user

1.3 CC Conformance Claim

This ST is claiming the following conformance:

a) CC Version 2.1, ISO/IEC 15408:1999
b) With CCIMB Interpretations as of 01 December 2003
c) Part 2 Conformant
d) Part 3 Conformant
e) EAL3 Augmented with ADV_SPM.1
f) Conformant to no PP

1.4 Reference Materials

The materials listed in Table 1-1 have been referred to prepare this ST. Hereafter references to [CC_PART1], [CC_PART2] and [CC_PART3] shall be interpreted as being modified by [INTPR_01DEC2003], unless otherwise noted.

Table 1-1: Reference Materials

Identifier	Title
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1, CCIMB-99-031.
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1, CCIMB-99-032.
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1, CCIMB-99-033.
[INTPR_01DEC2003]	CCIMB Interpretations-0407 (as of 01 December 2003)

1.5 Conventions, Terminology, and Acronyms

This section identifies the conventions and defines the terminology and acronyms used in this ST.

1.5.1 Conventions

This section describes the conventions used in this ST.

The following conventions are used to distinguish text with special meaning.

a) *Plain italicized text* is used to emphasize text.

The following conventions are used to express the use of operations that are allowed for the CC functions and assurance components.

b) The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password.
   - One or more assignment values are shown in brackets [ ]. When a value or part of a value indicates a list, breaks between elements are indicated by commas or itemization.
   - When values are assigned to a list of parameters, the parameter name is indicated in parentheses ( ) next to each value unless the name is self-evident.
   - When multiple values are assigned to a single parameter, information to distinguish each value is provided in parentheses ( ) next to the value unless the information is self-evident.

c) The refinement operation is used to add detail to a component, and thus further restricts the TOE.
   - Additional text is indicated in **bold**.
   - When one section of text is replaced by another, such as the replacement of a general term with a more specialized term, the original text is shown in parentheses ( ) and the new text is shown immediately before it in **bold**.
   - A list value is indicated in the same way as an assignment operation.
   - When text is deleted as an editorial refinement, the deleted text is indicated in parentheses ( ).

d) The selection operation is used to select one or more options when multiple options are provided in a component.
   - Selections are denoted in slant brackets *[ ]* by *[underlined italicized text]*.

e) Iteration is used to cover different aspects of the same requirement.
   - An iteration number inside parentheses ( ) is appended to the component name, short name, and element name as a unique identifier.

1.5.2 Terminology

Terminology unique to this document is defined in Table 1-2.

Table 1-2: 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.

Term	Definition
Clear Address Book Data and Registered Data in MFP	An operation to clear (by overwriting) address book data stored in the HDD.
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 record 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 manipulation.
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. This is stored to 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 ST.
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 organization, which the organization 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 ST, 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 ST, of two-dimensional image that each function of the MFD manages.
Internal network	The network that is inside the organization and protected against the threat about security from any external networks.
Job	The sequence from beginning to end of the use of an MFD function (copy, print, scan send, 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.
Paper feed tray	The device that holds the paper to print and feed it to the engine unit at printing.

Term	Definition
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 copy, scan send, 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 TOE is installed.
Subnetwork	A monolithic network that does not contain routers inside.
Tandem copy	Tandem print in the MFD's copy 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.

1.5.3 Acronyms

Acronyms used in this ST are indicated in Table 1-3.

Table 1-3: Acronyms

Acronym	Definition
AES	Advanced Encryption Standard, established by NIST (National Institute of Standards and Technology, United States of America)
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.
LDAP	Lightweight Directory Access Protocol, the name of the communication protocol for directory service.
MSD	Mass Storage Device, in this ST, this especially indicates the HDD and Flash memory in MFD.
NIC	Network Interface Card, or, Network Interface Controller
OS	Operating System
ROM	Read Only Memory
SSL	Secure Socket Layer, 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.

2 TOE Description

2.1 TOE Overview

2.1.1 TOE Type

The TOE is an IT product.

The main part of the TOE is the firmware for the MFD that is stored to the ROM. By replacing the MFD standard firmware, it offers the security function and controls the entire MFD.

The HDC that is a hardware part in the MFD is also a part of the TOE and controlled by the firmware.

2.1.2 Overview of the TOE Security Functions

The main security functions of the TOE are the cryptographic operation function, the data clear function and the confidential files function. These functions are intended to counter attempts to steal image data in the MFD in which the TOE is installed.

The cryptographic operation function encrypts the image data and others that MFD manages before it is stored to the HDD or Flash memory in the MFD.

The data clear function writes random values or a fixed value over encrypted data area in the HDD or Flash memory in the MFD.

The confidential files functions make it possible that user stores the image data to the HDD with password to prevent the others from reusing it without permission.

2.2 TOE Configuration

This section describes the physical and logical configuration of the TOE.

2.2.1 Physical Scope and Boundaries of the TOE

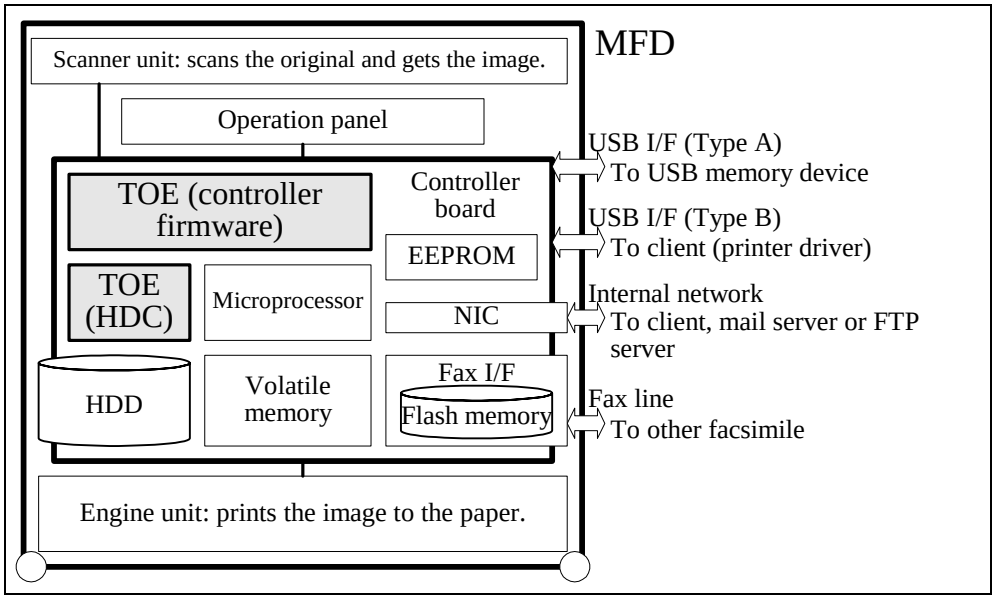

Figure 2-1: TOE and physical configuration of the MFD

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 2-1.

The TOE runs on the following SHARP MFDs: MX-3500FN, MX-3500N, MX-3500NJ, MX-3501FN, MX-3501N, MX-3501NJ, MX-4500FN, MX-4500N, MX-4500NJ, MX-4501FN, MX-4501N and MX-4501NJ.

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.
- HDC: an integrated circuit part that is mounted on the controller board.

2.2.2 Logical Scope and Boundaries of the TOE

Figure 2-2 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.

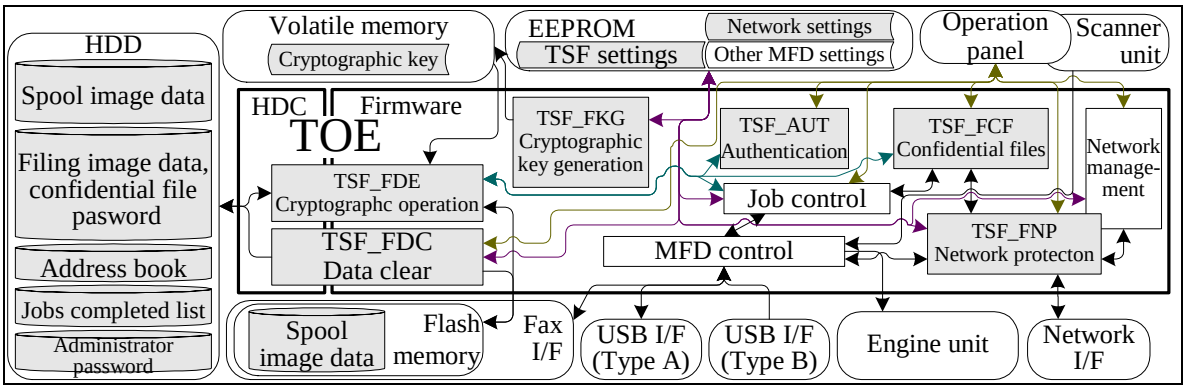

Figure 2-2: Logical configuration of the TOE

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 2.3.2) 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).

2.3 Overview of the MFD Functions and Applications

As well as the standard MFD firmware, the TOE has the following MFD functions: copy, printer, network scanner, fax transmission, fax reception, and PC-Fax. The TOE executes a part of the TOE security functions (TSF) automatically while each of these MFD functions is being executed. This property of the TOE protects even a user with no knowledge or awareness about the TOE security functions. The usage environment of the MFD that the TOE is installed to is shown in Figure 2-3.

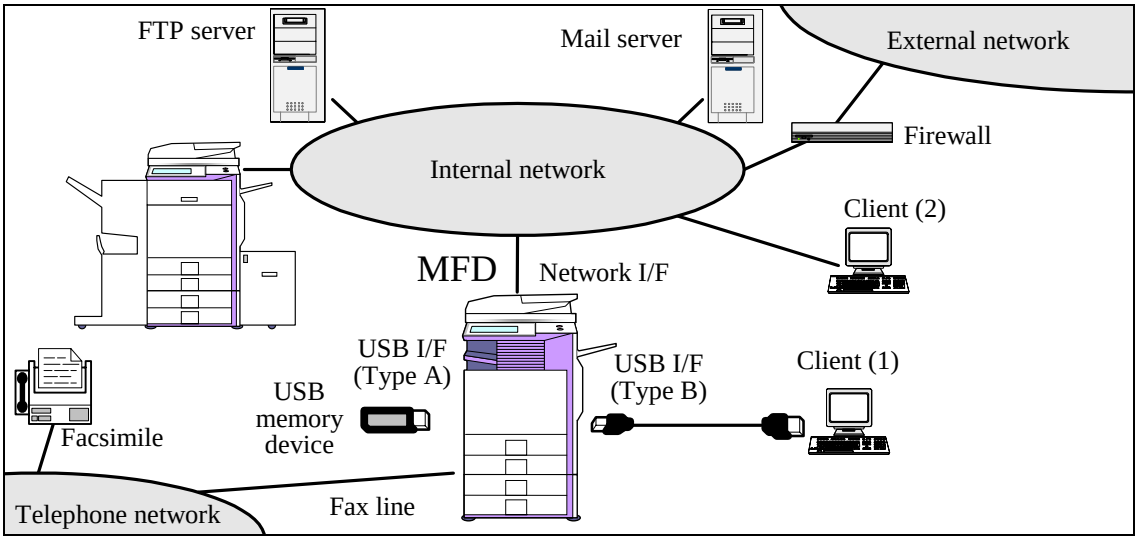

Figure 2-3: Usage environment of the MFD

Each MFD function that 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.

2.3.1 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) Copy: 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. A tandem print request from another MFD is printed in the same manner.
   - Pull print: acquires the print data in an FTP server or a USB memory device through 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 is 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 MFD's software tool.
   - 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 MFD's software tool.
   - Internet Fax: transmits it 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.

2.3.2 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.
- 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 by any medium available for the network scanner function or facsimile.
  - Preview: displays the rough outline of the saved image data.
  - Property change: removes the password from a file with a password, or vice versa.
  - 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 a binary data that is possible to restore (import) 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.

2.3.3 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 to 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.

2.4 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 Program
  - 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”

2.5 Assets Protected by the TOE

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

a) Image data that the MFD functions spool to process jobs

b) Image data that users save as confidential files

c) Address book data

d) Jobs completed list data

e) Network settings data

Specific for each clause above is described in the following each section.

2.5.1 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.

2.5.2 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.

2.5.3 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 to the HDD. This data is the personal data (destination name, mail address, fax number and others) that proper users use in cooperation and possibly contain the organization's sensitive information.

There is no threat to have to cope with always 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. Although this data shall be protected from the possibility that the improper user reads and modifies this data from the HDD directly or through the internal network together.

2.5.4 Jobs completed list data

The assets protected by the TOE include the jobs completed list data that the job control function keeps to the HDD. This data possibly contain the organization'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 no threat to have to cope with always 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. Although this data shall be protected from the possibility that the improper user read this data from the HDD directly together.

2.5.5 Network settings data

The assets protected by the TOE include the following network settings data that the administrator stored to the EEPROM using the network management function. This data contain the organization's sensitive information and is possibly the threat for the internal network. In addition, it is possibly the threat for other assets to be modified dishonesty.

a) TCP/IP Settings: Enable TCP/IP, Enable DHCP, IP Address Settings
b) DNS Settings: Primary/Secondary DNS Server, Domain Name
c) WINS Settings: Enable WINS, Primary/Secondary WINS Server, WINS Scope ID
d) SMTP Settings: SMTP Server
e) LDAP Settings: Enable LDAP, LDAP Server
f) Tandem Settings: IP Address of Slave Machine, Disabling of Master Machine Mode
g) Port Control: Enabling or the port number for each network service

3 TOE Security Environment

3.1 Assumptions

Use and operation of the TOE requires the environment described in Table 3-1.

Table 3-1: 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 TOE.

3.2 Threats

Threats to the TOE are described in Table 3-2. Each threat supposes the attacker who possesses the low attack potential.

Table 3-2: Threats

Identifier	Definition
T.RECOVER	An attacker removes the MSD from the MFD to read the MSD, reads and leaks the user data stored in it (include the data that is remained after deleting).
T.REMOTE	An attacker who are not allowed to access to the MFD reads and modifies the address book data in the MFD through the internal network together.
T.SPOOF	An attacker impersonates other user reads and leaks the image data that the user has saved as confidential file from the operation panel or through the internal network.
T.TAMPER	An attacker 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.

3.3 Organizational Security Policies

Organizational security policies are described in Table 3-3.

Table 3-3: Organizational Security Policies

Identifier	Definition
P.RESIDUAL	Upon completion or interruption of a job, the user data area spooled to the MSD shall be overwritten one or more times. The user data area in the MSD that is deleted by user shall be overwritten one or more times. When the MFD is disposed of or its ownership changes, all user data areas in the MSD shall be overwritten one or more times.

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE are shown in Table 4-1.

Table 4-1: TOE Security Objectives

Identifier	Definition
O.FILTER	The TOE shall provide defence against network accesses from devices that those who are not allowed to access to the MFD.
O.MANAGE	The TOE shall provide the function that identifies and authenticates the proper administrator.
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	The TOE shall overwrite the user data area spooled to the MSD one or more times when a job is finished or cancelled. The TOE shall overwrite the user data area in the MSD that is specified by the user's delete operation one or more times. The TOE shall provide the function to overwrite all user data areas in the MSD one or more times by the administrator's operation.
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 real user that stored the confidential file.

4.2 Security Objectives for the Environment

The security objectives for the environment are shown in Table 4-2.

Table 4-2: Environmental Security Objectives

Identifier	Definition
OE.CIPHER (1)	The administrator shall configure the TOE to enable its communication data protection when the user of the MFD communicates with the TOE, so that the communication data will not be wiretapped.
OE.CIPHER (2)	In the internal network where the TOE is installed, the administrator shall exercise due care (such as using network switches with encryption, or making the MFD user use USB memory device to input/output the data) of the communication data between the MFD user and the TOE not to be wiretapped.
OE.ERASEALL	When the MFD is disposed of or its ownership changes, the administrator shall overwrite all user data areas in the MSD one or more times by using the TOE's function.
OE.FIREWALL	The administrator shall enforce to connect the internal network that the TOE is installed to with external network by using the communication device that implements the function to protect the internal network against attacking from any external networks.
OE.OPERATE	Those in charge of the organization 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 with the MFD on the internal network, the administrator shall run the identification and authentication function 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 that 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.

5 IT Security Requirements

5.1 TOE Security Requirements

5.1.1 TOE Security Functional Requirements

This section describes the Security Functional Requirements that the TOE shall satisfy, based on the classes of [CC_PART2]. The minimum strength of function for the TOE is defined in section 5.1.2.

5.1.1.1 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 in accordance with a specified cryptographic key generation algorithm [MSN-R expansion algorithm] and a specified cryptographic key size [128 bits] that meet the following [Data Security Kit Encryption Standard].
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

●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 was read from the MSD ● Decrypting the TSF data that was read from the MSD] in accordance with a specified cryptographic algorithm [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 FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

5.1.1.2 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

5.1.1.3 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 or surpassed, 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 or surpassed, the TSF shall [● Unsuccessful authentication reached 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 identify itself 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 identify itself before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies

5.1.1.4 Class FMT: Security management

●FMT_MOF.1 (1)	Management of security functions behaviour (1)
Hierarchical to:	No other components.
FMT_MOF.1.1 (1)	The TSF shall restrict the ability to ***[enable]*** the functions [Clear All Memory, Clear Document Filing Data, Power Up Auto Clear, Clear Address Book Data and Registered Data in MFP, Clear All Data in Job Status Jobs Completed List] to [administrator].
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

●FMT_MOF.1 (2) Management of security functions behaviour (2)

Hierarchical to: No other components.

FMT_MOF.1.1 (2) 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_MOF.1 (3) Management of security functions behaviour (3)

Hierarchical to: No other components.

FMT_MOF.1.1 (3) The TSF shall restrict the ability to *[modify the behaviour of]* the functions [Clear Document Filing Data, Power Up Auto Clear, document filing function, network protection function] to [administrator].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

●FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Dependencies: ADV_SPM.1 Informal TOE security policy model
[FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
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 (3) The TSF shall restrict the ability to *[modify, [create (other operations)]]* 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 Program
- 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 security management functions: [

- Enable or Disable “Clear All Memory”
- Enable or Disable “Clear Document Filing Data”
- Disable “Power Up Auto Clear”
- Enable “Clear Address Book Data and Registered Data in MFP”
- Enable “Clear All Data in Job Status Jobs Completed List”
- 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 Program”
- Query and Modify “Number of Times Power Up Auto Clear Program is Repeated”
- Release the lock of confidential files
- Modify the administrator password
- Modify the confidential file password
- Query and Modify “Disabling of Document Filing”
- Query and Modify ”Disabling of Print Jobs Other Than Print Hold Job”
- Manage “IP address filter” and “MAC address filter”
- Manage the services protected by SSL

].

Note: Consideration for management requirement is described in section 0.

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

5.1.1.5 Class FPT: Protection of the TSF

●FPT_RVM.1	Non-bypassability of the TSP
Hierarchical to:	No other components.
FPT_RVM.1.1	The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
Dependencies:	No dependencies

5.1.1.6 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

5.1.1.7 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 or 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 service by TOE Web and for the printer driver (*other services for which trusted path is required*)] *]*.
Dependencies:	No other components.

5.1.2 TOE Minimum Strength of Function

The overall security minimum strength of function for the TOE is *SOF-basic.*

Among the functional requirements that this TOE satisfies, only FIA_AFL.1 (1), FIA_AFL.1 (2), FIA_SOS.1 (1), FIA_SOS.1 (2), FIA_UAU.2 (1), FIA_UAU.2 (2), FIA_UAU.7 (1) and FIA_UAU.7 (2) use a probabilistic or permutational mechanism, and the explicitly stated functional strength is SOF-basic. FCS_COP.1 is a functional requirement that uses a cryptographic algorithm, and thus does not apply to this SOF level.

5.1.3 TOE Security Assurance Requirements

Assurance components for the assurance level selected by this document are shown in Table 5-1. Table 5-1 shows the assurance requirements that must be satisfied to claim EAL3+ADV_SPM.1 compliance.

Table 5-1: Assurance Requirements

Component	Component Name	Dependencies:
ACM_CAP.3	Authorization controls	ACM_SCP.1, ALC_DVS.1
ACM_SCP.1	TOE CM coverage	ACM_CAP.3
ADO_DEL.1	Delivery procedures	No dependencies
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1
ADV_FSP.1	Informal functional specification	ADV_RCR.1
ADV_HLD.2	Security enforcing high-level design	ADV_FSP.1, ADV_RCR.1
ADV_RCR.1	Informal correspondence demonstration	No dependencies
ADV_SPM.1	Informal TOE security policy model	ADV_FSP.1
AGD_ADM.1	Administrator guidance	ADV_FSP.1
AGD_USR.1	User guidance	ADV_FSP.1
ALC_DVS.1	Identification of security measures	No dependencies
ATE_COV.2	Analysis of coverage	ADV_FSP.1, ATE_FUN.1
ATE_DPT.1	Testing: high-level design	ADV_HLD.1, ATE_FUN.I
ATE_FUN.1	Functional testing	No dependencies
ATE_IND.2	Independent testing - sample	ADV_FSP.1, AGD_ADM.1, AGD_USR.1
AVA_MSU.1	Examination of guidance	ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, AGD_USR.1
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1, ADV_HLD.1
AVA_VLA.1	Developer vulnerability analysis	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1

5.2 Security Requirements for the IT Environment

The security objectives for the environment do not require any security requirements for the IT environment of the TOE.

6 TOE Summary Specification

This chapter describes the security functions and assurance measures performed by the TOE to meet the security requirements.

6.1 TOE Security Functions (TSF)

Table 6-1 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 6-1: Security Functional Requirements and TOE Security Specifications

Function Requirement	TSF_FKG	TSF_FDE	TSF_FDC	TSF_AUT	TSF_FCF	TSF_FNP
FCS_CKM.1	6.1.1					
FCS_COP.1		6.1.2				
FDP_RIP.1			6.1.3			
FIA_AFL.1 (1)			6.1.3	6.1.4		6.1.6
FIA_AFL.1 (2)					6.1.5	
FIA_SOS.1 (1)				6.1.4		
FIA_SOS.1 (2)					6.1.5	
FIA_UAU.2 (1)			6.1.3	6.1.4		6.1.6
FIA_UAU.2 (2)					6.1.5	
FIA_UAU.7 (1)			6.1.3	6.1.4		6.1.6
FIA_UAU.7 (2)					6.1.5	
FIA_UID.2 (1)			6.1.3	6.1.4		6.1.6
FIA_UID.2 (2)					6.1.5	
FMT_MOF.1 (1)			6.1.3			
FMT_MOF.1 (2)			6.1.3			
FMT_MOF.1 (3)			6.1.3		6.1.5	6.1.6
FMT_MSA.2	6.1.1					
FMT_MTD.1 (1)				6.1.4		
FMT_MTD.1 (2)					6.1.5	
FMT_MTD.1 (3)			6.1.3		6.1.5	6.1.6
FMT_SMF.1			6.1.3	6.1.4	6.1.5	6.1.6
FMT_SMR.1 (1)				6.1.4		
FMT_SMR.1 (2)					6.1.5	
FPT_RVM.1	6.1.1	6.1.2	6.1.3	6.1.4	6.1.5	6.1.6
FTA_TSE.1						6.1.6
FTP_TRP.1						6.1.6

6.1.1 Cryptographic key generation (TSF_FKG)

The TOE generates a cryptographic key (common key) to support the encryption function of the user data and the TSF data. When the MFD is powered on, a cryptographic key (common key) is always generated.

The TOE generates the cryptographic key as a 128-bit of secure key from the secure seed by using MSN-R expansion algorithm and stores it to the volatile memory to use it in the AES Rijndael, that is the cryptographic algorithm. The MSN-R expansion algorithm is the cryptographic key generation algorithm and is satisfied the Data Security Kit Encryption Standard.

The seed that is the security attribute of the cryptographic key is generated from the secure method following the TSP model by the TOE. The assurance measure of the TOE security assurance requirements

ADV_SPM.1 (Table 6-2) provides the TSP model. When installed, in accordance with the TSP model, the TOE generates a seed that differs from an MFD to another. Thus, each TOE instance in each MFD always generates its cryptographic key from its own constant seed using the same algorithm.

6.1.2 Cryptographic operation (TSF_FDE)

This function always encrypts and writes the user data and the TSF data when it is necessity to write them to the MSD. In addition, this function reads them from the MFD and decrypts when these data are required.

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

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.

6.1.3 Data clear (TSF_FDC)

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:

- Auto Clear at Job End program
- 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
- Power Up Auto Clear program

Every program above overwrites the HDD one or more times with random values. In addition, these programs overwrite the Flash memory once with a fixed value. The repeat count of overwriting the data on the HDD is specified by this TSF.

The following sections elaborate upon each program and settings:

6.1.3.1 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 ends, 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.

6.1.3.2 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 authentication of the administrator who calls this program whenever a cancel operation is taken. While entering for authentication, the TOE shows as many asterisk "＊" characters as characters entered, however does not show the characters entered. The clearing 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; 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.

6.1.3.3 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 do not accepts the cancel operation for the relatively short time required.

6.1.3.4 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.

6.1.3.5 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 do not accepts cancel operation for the relatively short time required.

6.1.3.6 Power Up Auto Clear program

This program overwrites and clears the data when the TOE is powered 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.

6.1.3.7 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 enable or disable *Power Up Auto Clear* program for each data. 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.

6.1.4 Authentication (TSF_AUT)

This TSF enforces the identification and authentication of the administrator by the administrator password. Only the administrator identified and authenticated by this TSF is allowed to change the administrator password. The administrator password is allowed to use only 5 to 32 alphanumeric and/or symbol characters.

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

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, and the authentication of the administrator is successful by the correct administrator password. The login operation of the administrator includes both identification of administrator and authentication of the administrator password in the operation panel or the TOE Web.

When the administrator password is entered from the operation panel, this TSF 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; 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.

6.1.5 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 Copy, Printer driver, PC-Fax and Scan to HDD and 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.

Whenever a user attempts some operation on a saved confidential file, 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 2.3.2 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. 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.

This TSF allows changing the password, as one of the operations on a saved confidential file. This TSF verifies the new confidential password meets the quality metric, 5 to 8 numeric characters.

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, a confidential file password must be set, and then this TSF verifies that the confidential file password meets the quality metric, 5 to 8 numeric characters.

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.

This TSF provides the following management functions for the document filing function:

Only the administrator identified and authenticated by TSF_AUT is allowed to execute these functions.

- Management functions for improving the effect of protection by the confidential file:
  - Disabling of Document Filing: enables to disable the each saving mode for each job type. The setting that all non-confidential modes (without password) are disabled is default and recommended.
  - 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 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*".

6.1.6 Network protection function (TSF_FNP)

This TSF consists of the following functions.

- Filter function
- Communication data protection function
- Network settings protection

The following sections elaborate upon each function.

6.1.6.1 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. Only the administrator identified and authenticated by TSF_AUT is allowed to configure this function's settings.

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.

6.1.6.2 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 is also begins by the connection from the printer driver of the client and keeps communication until it is disconnected.

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

Only the administrator identified and authenticated by TSF_AUT is allowed to configure the SSL settings that is the management function of HTTPS communication and IPP-SSL communication and modify the behaviour of the network protection function by selecting that each of HTTPS communication and IPP-SSL communication is used or not (disable).

If HTTPS communication and IPP-SSL communication are selected not to use, the network protection function runs with each communication function is disabled.

6.1.6.3 Network settings protection

This function provides the interfaces to manage the network settings data described in section 2.5.5 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.

6.2 TSF Strength of Security Functions

The following security functions are based on a probabilistic or permutational mechanism:

- The administrator password: corresponded to FIA_AFL.1 (1), FIA_SOS.1 (1), FIA_UAU.2 (1) and FIA_UAU.7 (1) and implemented by authentication function (TSF_AUT), data clear function (TSF_FDC) and network protection function (TSF_FNP).
- The confidential file password: corresponded to FIA_AFL.1 (2), FIA_SOS.1 (2), FIA_UAU.2 (2) and FIA_UAU.7 (2) and implemented by confidential files function (TSF_FCF).

The strength of these security functions is SOF-basic.

6.3 Assurance Measures

The documents that serve as the assurance measure for each component of the security assurance requirements in this ST are shown in Table 6-2.

Table 6-2: Assurance Measures

Component	Assurance Measures
ACM_CAP.3 ACM_SCP.1	Color Renaissance series Configuration Management MX-FRX2 Version M.10 Configuration List
ADO_DEL.1	Color Renaissance series Delivery Procedures
ADO_IGS.1	MX-FRX2 Installation Manual MX-FRX2 Installation Manual (English, German, French, Spanish)
ADV_FSP.1	Color Renaissance series Security Functional Specifications
ADV_HLD.2	Color Renaissance series High-level Design
ADV_RCR.1	Color Renaissance series Representation Correspondence Analysis
ADV_SPM.1	Color Renaissance series Security Policy Model Specifications
AGD_ADM.1 AGD_USR.1 AVA_MSU.1	MX-FRX1 MX-FRX2 Data Security Kit Operation Manual MX-FRX2 Data Security Kit Notice
ALC_DVS.1	Color Renaissance series Development Security Specifications
ATE_COV.2	Color Renaissance series Coverage Analysis
ATE_DPT.1	Color Renaissance series High-level Design Testing Analysis
ATE_FUN.1	MX-FRX2 Functional Testing Specifications Color Renaissance series Testing Environment and Tools Manual
ATE_IND.2	TOE
AVA_SOF.1	Color Renaissance series Strength of Security Function Analysis
AVA_VLA.1	Color Renaissance series Vulnerability Analysis

7 PP Claims

The TOE does not claim conformance to any PP.

8 Rationale

This chapter demonstrates the completeness and consistency of this ST.

8.1 Security Objectives Rationale

Table 8-1 demonstrates that the policies indicated in the security objectives are effective for the assumptions, threats and organizational security policies indicated in the TOE security environment. Table 8-1 shows the section of this document that provides the rationale for the correspondence between the security objectives and the assumptions, threats and organizational security policies.

Table 8-1: Security Objectives Rationale

TOE security environment / Security Objective	A.NETWORK	A.OPERATOR	T.RECOVER	T.REMOTE	T.SPOOF	T.TAMPER	T.TAP	P.RESIDUAL
O.FILTER				8.1.4				
O.MANAGE				8.1.4	8.1.5	8.1.6	8.1.7	8.1.8
O.REMOVE			8.1.3					
O.RESIDUAL								8.1.8
O.TRP							8.1.7	
O.USER					8.1.5			
OE.CIPHER (1)							8.1.7	
OE.CIPHER (2)							8.1.7	
OE.ERASEALL								8.1.8
OE.FIREWALL	8.1.1							
OE.OPERATE		8.1.2						
OE.PC-USER				8.1.4				
OE.SUBNET	8.1.1							
OE.USER					8.1.5			

8.1.1 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 the sub network that the MFD is connected to at least in the internal network. This is realized by the combination of OE.FIREWALL and OE.SUBNET.

8.1.2 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 who will be the administrator based on an understanding of the role of administrator on the part of those in charge of the organization that owns the TOE-equipped MFD. Therefore, A.OPERATOR can be achieved.

8.1.3 T.RECOVER

The TOE encrypts the user data with MFD's own cryptographic key according to O.REMOVE that is against from T.RECOVER when the TOE writes the user data to MSD. Therefore, the attacker possessing a low-level technical potential cannot make out the data that is stored or remained after deleting in MSD even if the attacker could read them.

When the volatile memory will be removed from the MFD, the data will be lost because loosing power supply will destroy any data in volatile memory. There are no interface 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 data to read the data by attaching probes directly to the terminals or harness of MFD. Therefore, it is impossible for attacker possessing a low-level technical potential. 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.

8.1.4 T.REMOTE

The following objective below opposes against T.REMOTE.

- The TOE provides the method to deny the access from the device that the user who are not allowed to access to the MFD use through the network according to O.FILTER.
- As a support for the previous paragraph, the TOE provides the function that identifies and authenticates the administrator who configures the settings that is required for operating previous paragraph according to O.MANAGE.
- To make that only the proper users of the MFD are able to use the MFD, the administrator runs the function that identifies and authenticates the allowed user at the devices that are allowed to connect to the MFD without denying by the above way in an internal network according to OE.PC-USER.

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.

8.1.5 T.SPOOF

The following objective below opposes against T.SPOOF.

- The TOE provides the function that identifies and authenticates the proper user that stored the confidential file according to O.USER.
- As a support for the previous paragraph, the TOE provides the function that identifies and authenticates the administrator who configures the settings that is required for operating previous paragraph according to O.MANAGE.
- 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 do it according to OE.USER.

These objectives above can oppose against the threat that occurred by an attacker’s impersonating other user.

8.1.6 T.TAMPER

The TOE provides the function that identifies and authenticates the proper administrator according to O.MANAGE that is against from T.TAMPER. Therefore, it is possible to protect the network settings data against reading or modifying by an attacker’s impersonating an administrator.

8.1.7 T.TAP

The following objective below opposes against T.TAP.

- The TOE provides the function that prevents the user data on the internal network from wiretapping according to O.TRP.
- As a support for the previous paragraph, the TOE provides the function that identifies and authenticates the administrator who configures the settings that is required for operating previous paragraph according to O.MANAGE.
- The administrator prevents the communication data from wiretapping by configuring the TOE to enable the TOE’s communication data protection function when the user of MFD communicates to the TOE according to OE.CIPHER (1).
- In the internal network where the TOE is installed, the administrator shall exercise due care (such as using network switches with encryption, or making the MFD user use USB memory device to

input/output the data) of the communication data between the MFD user and the TOE not to be wiretapped, according to OE.CIPHER (2). This is required when the TOE's communication data protection cannot use for the reasons that the client or protocol does not support using the TOE's communication data protection function and others.

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.

8.1.8 P.RESIDUAL

P.RESIDUAL can be achieved by the following objective below.

- Upon completion or interruption of a job, the TOE overwrites the user data area spooled to the MSD one or more times according to O.RESIDUAL.
- The TOE overwrites the user data area in the MSD that is specified by the user's delete operation one or more times according to O.RESIDUAL.
- When the MFD is disposed of or its ownership changes, the administrator overwrites all user data areas in the MSD one or more times by using the function of the TOE according to OE.ERASEALL. This requires the support of the TOE and the function described in next paragraph is available.
- The TOE provides the function to overwrite all user data areas in the MSD one or more times by the administrator's operation according to O.RESIDUAL.
- As a support for the previous paragraph, the TOE provides the function that identifies and authenticates the administrator who configures the settings that is required for operating previous paragraph according to O.MANAGE.

These objectives above can achieve P.RESIDUAL.

8.2 Security Requirements Rationale

In the following, it is demonstrated that the IT security requirements attain the security objectives.

8.2.1 Security Functional Requirements Rationale

The correspondence between security functional requirements and security objectives is shown in Table 8-2. Table 8-2 shows the section that provides the rationale for the correspondence between the security functional requirements and the security objectives.

Table 8-2: Security Functional Requirements Rationale

Objective Requirement	O.FILTER	O.MANAGE	O.REMOVE	O.RESIDUAL	O.TRP	O.USER
FCS_CKM.1			8.2.1.3			
FCS_COP.1			8.2.1.3			
FDP_RIP.1				8.2.1.4		
FIA_AFL.1 (1)		8.2.1.2				
FIA_AFL.1 (2)						8.2.1.6
FIA_SOS.1 (1)		8.2.1.2				
FIA_SOS.1 (2)						8.2.1.6
FIA_UAU.2 (1)		8.2.1.2				
FIA_UAU.2 (2)						8.2.1.6
FIA_UAU.7 (1)		8.2.1.2				
FIA_UAU.7 (2)						8.2.1.6
FIA_UID.2 (1)		8.2.1.2				
FIA_UID.2 (2)						8.2.1.6
FMT_MOF.1 (1)				8.2.1.4		
FMT_MOF.1 (2)				8.2.1.4		
FMT_MOF.1 (3)				8.2.1.4	8.2.1.5	8.2.1.6
FMT_MSA.2			8.2.1.3			
FMT_MTD.1 (1)		8.2.1.2				
FMT_MTD.1 (2)						8.2.1.6
FMT_MTD.1 (3)	8.2.1.1			8.2.1.4	8.2.1.5	8.2.1.6
FMT_SMF.1	8.2.1.1	8.2.1.2			8.2.1.5	8.2.1.6
FMT_SMR.1 (1)		8.2.1.2				
FMT_SMR.1 (2)						8.2.1.6
FPT_RVM.1	8.2.1.1	8.2.1.2	8.2.1.3	8.2.1.4	8.2.1.5	8.2.1.6
FTA_TSE.1	8.2.1.1					
FTP_TRP.1					8.2.1.5	

8.2.1.1 O.FILTER

O.FILTER can be achieved by the combination of the following functional requirements.

- 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).
- It is ensured that the inspection of the IP address and MAC address is invoked and succeeds before session establishment is allowed according to FPT_RVM.1. FPT_RVM.1 also supports not to be able to bypass FMT_MTD.1 (3).

FMT_SMF.1 and FMT_MTD.1 (3) provide the management of FTA_TSE.1 consistently and do not compete among them.

In addition, contention does not occur in FPT_RVM being a requirement for use in a mutual support.

Contention of a functional requirement does not occur to achieve O.FILTER as above.

8.2.1.2 O.MANAGE

O.MANAGE can be achieved by the combination of the following functional requirements.

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).

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) It is ensured that the administrator password meets 5 to 32 alphanumeric and/or symbol characters when the administrator password is modified according to FIA_SOS.1 (1).

d) 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).

e) The roles of administrator are maintained and the administrator is associated with those roles by FMT_SMR.1 (1).

f) FTP_RVM.1 supports not to be able to bypass functional requirements to achieve O.MANAGE.

a) is related to the phenomenon about the identification and authentication of the administrator. b), c) and d) are related to the phenomenon about the modification of the administrator password.

Each phenomenon does not need to compete in being a stand-alone phenomenon about these two phenomena.

Contention does not occur in a) because four functional requirements in a) affect mutually and supplementary to achieve the identification and authentication of the administrator.

Contention does not occur in b), c) and d) because three functional requirements in b), c) and d) affect mutually and supplementary to achieve the modification of the administrator password.

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

Contention does not occur in f) being a requirement for use in a mutual support.

Contention of a functional requirement does not occur to achieve O.MANAGE as above.

8.2.1.3 O.REMOVE

The intent of O.REMOVE is to oppose against T.RECOVER; in other words to make the data stored in MSD not to regenerate even if the MSD is removed from MFD. This can be achieved by the combination of the following functional requirements.

a) FCS_COP.1 protects the data stored in MSD 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 the user data stored as FCS_COP.1 requires.
- Same as user data, the administrator password and confidential file password included in the TSF data are also encrypted by FCS_COP.1 when these data are stored to the HDD. Therefore reading the user data indirectly by an attacker's trying to read these passwords and impersonate is also prevented.

b) FCS_CKM.1 generates the cryptographic key to achieve FCS_COP.1.

c) The seed of the cryptographic key is generated by TOE itself and accepted as security attribute according to FMT_MSA.2.

d) FTP_RVM.1 supports not to be able to bypass functional requirements to achieve O.REMOVE.

Contention does not occur in FCS_CKM.1 and FMT_MSA.2 above because these functional requirements are depended on by FCS_COP.1.

Contention does not occur in FPT_RVM being a requirement for use in a mutual support.

Contention of a functional requirement does not occur to achieve O.REMOVE as above.

8.2.1.4 O.RESIDUAL

O.RESIDUAL can be achieved by the combination of the following functional requirements.

a) FDP_RIP.1 overwrites 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 deallocation of the resource from these objects is occurred when the jobs are finished or cancelled, the user deletes the confidential file and the specific data clear program is invoked by the administrator's operation.

- 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.

b) The ability to manage about FDP _RIP.1 is restricted to the administrator by the following functional requirements.

- The ability to enable the each function *Clear All memory*, *Clear Document Filing Data*, *Clear Address Book Data and Registered Data in MFP*, *Clear All Data in Job Status Jobs Completed List* and *Power Up Auto Clear* that are TSF related to FDP_RIP.1 is restricted to the administrator by FMT_MOF.1 (1).
- The ability to disable the each function *Clear All memory*, *Clear Document Filing Data* and *Power Up Auto Clear* that are the TSF related to FDP_RIP.1 is restricted to the administrator by FMT_MOF.1 (2).
- The ability to modify the behaviour of the function *Clear Document Filing Data* and *Power UP Auto Clear* that are the TSF related to FDP_RIP.1 is restricted to the administrator by FMT_MOF.1 (3).
- The ability to query or modify the TSF data related to FDP_RIP.1; in other words *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* Program and N*umber of Times Power Up Auto Clear Program is Repeated* is restricted to the administrator by FMT_MTD.1 (3).

c) FTP_RVM.1 supports not to be able to bypass functional requirements to achieve O.RESIDUAL.

Each phenomenon in a) and b) does not need to compete in being a stand-alone phenomenon in b) about these four phenomena and a) manages them.

Contention does not occur in each phenomenon in a) and b) because stand-alone phenomenon in a) and b) corresponds a functional requirement.

Contention does not occur in c) being a requirement for use in a mutual support.

Contention of a functional requirement does not occur to achieve O.RESIDUAL as above.

8.2.1.5 O.TRP

O.TRP can be achieved by the combination of the following functional requirements.

- The trusted communication can be provided between users and TSF and kept it by FTP_TRP.1.
- The ability to modify the behaviour of network protection function that are the TSF related to FTP_TRP.1 is restricted to the administrator by FMT_MOF.1 (3).
- 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.
- FTP_RVM.1 supports not to be able to bypass functional requirements to achieve O.TRP.

Contention does not occur in FMT_MOF.1 (3), FMT_MTD.1 (3) and FMT_SMF.1 because three functional requirements provides the management of FTP_TRP.1 mutually and supplementary.

Contention does not occur in FPT_RVM.1 being a requirement for use in a mutual support.

Contention of a functional requirement does not occur to achieve O.TRP as above.

8.2.1.6 O.USER

O.USER can be achieved by the combination of the following functional requirements.

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 behaviour of document filing function that provides O.USER (include the confidential files function) is restricted to the administrator by FMT_MOF.1 (3).

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

e) 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).

f) 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).

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

h) FTP_RVM.1 supports not to be able to bypass functional requirements to achieve O.USER.

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

Each phenomenon does not need to compete in being a stand-alone phenomenon about these three phenomena.

Contention 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.

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

Contention does not occur in c) and e) because two functional requirements in c) and e) affect mutually and supplementary to achieve the management by the administrator.

Contention does not occur in f) because this functional requirement is depended on by d) and supported by a).

Contention does not occur in h) being a requirement for use in a mutual support.

Contention of a functional requirement does not occur to achieve O.USER as above.

8.2.2 Rationale for consistence of TOE security management functions

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

The management functions required by all TOE security functional requirement components are shown in Table 8-3 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.

Table 8-3: Management Functions of the TOE

Management Function Origin	Management Function required	Consideration for management requirement
FCS_CKM.1	—	The attributes of the encryption key is not changed.
FCS_COP.1	—	(no management requirements)
FDP_RIP.1	• Enable or Disable “Clear All Memory” • Enable or Disable “Clear Document Filing Data” • Disable “Power Up Auto Clear” • Enable “Clear Address Book Data and Registered Data in MFP” • Enable “Clear All Data in Job Status Jobs Completed List” • 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 Program” • 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)	• Release the lock of 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 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 (1)	—	No role groups
FMT_MOF.1 (2)	—	No role groups
FMT_MOF.1 (3)	—	No role groups
FMT_MSA.2	—	(no management requirements)
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
FPT_RVM.1	—	(no management requirements)
FTA_TSE.1	• Manage “IP address filter” and “MAC address filter”	Management Function required agrees with management requirement.
FTP_TRP.1	• Manage the services protected by SSL	Management Function required agrees with management requirement.

8.2.3 Rationale for security functional requirement dependencies

Security functional requirement dependencies are shown in Table 8-4. Table 8-4 shows the dependencies that the security functional requirements must satisfy according to the CC, the dependencies that the TOE satisfies, and the section that provides the rationale for dependencies that are not satisfied. The dependency that is marked with "*" in the table is satisfied with the component that is hierarchically upper.

Table 8-4: Security Functional Requirement Dependencies

Dependencies Requirement	Stipulated	Satisfied	Unsatisfied	Justification
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	FCS_COP.1, FMT_MSA.2	FCS_CKM.4	8.2.3.1
FCS_COP.1	[FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1, FMT_MSA.2	FCS_CKM.4	8.2.3.1
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 (1)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1 (1)	—	—
FMT_MOF.1 (2)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1 (1)	—	—
FMT_MOF.1 (3)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1 (1)	—	—
FMT_MSA.2	ADV_SPM.1, [FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	ADV_SPM.1	FDP_ACC.1, FDP_IFC.1, FMT_MSA.1, FMT_SMR.1	8.2.3.2
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)	—	—
FPT_RVM.1	—	—	—	—
FTA_TSE.1	—	—	—	—
FTP_TRP.1	—	—	—	—

8.2.3.1 Justification for no satisfaction on 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 use a key destruction method that meets standards, and FCS_CKM.4 is not required to specify standards.

8.2.3.2 Justification for no satisfaction of dependencies on FMT_MSA.2

The seed of cryptographic key is a security attribute related to cryptographic operation that is managed by the TOE. Even the administrator is not allowed to change the seed of cryptographic key, and thus FMT_MSA.1 and FMT_SMR.1 are not required. Similarly, the cryptographic key and seed of cryptographic key are not accessed by the user or administrator and not accepted from the outside of TOE, and thus either FDP_ACC.1 or MDP_IFC.1 is not required.

8.2.4 Mutual effect of security requirements

Table 8-5 shows the mutual effect of security requirements.

Table 8-5: Mutual effect of security requirements

Defence Requirement	Bypass	Disabling
FCS_CKM.1	FPT_RVM.1	—
FCS_COP.1	FPT_RVM.1	—
FDP_RIP.1	FPT_RVM.1	FMT_MOF.1 (2), FMT_MTD.1 (3)
FIA_AFL.1 (1)	FPT_RVM.1	—
FIA_AFL.1 (2)	FPT_RVM.1	FMT_MOF.1 (3)
FIA_SOS.1 (1)	FPT_RVM.1	—
FIA_SOS.1 (2)	FPT_RVM.1	FMT_MOF.1 (3)
FIA_UAU.2 (1)	FPT_RVM.1	—
FIA_UAU.2 (2)	FPT_RVM.1	FMT_MOF.1 (3)
FIA_UAU.7 (1)	FPT_RVM.1	—
FIA_UAU.7 (2)	FPT_RVM.1	FMT_MOF.1 (3)
FIA_UID.2 (1)	FPT_RVM.1	—
FIA_UID.2 (2)	FPT_RVM.1	FMT_MOF.1 (3)
FMT_MOF.1 (1)	FPT_RVM.1	—
FMT_MOF.1 (2)	FPT_RVM.1	—
FMT_MOF.1 (3)	FPT_RVM.1	—
FMT_MSA.2	—	—
FMT_MTD.1 (1)	FPT_RVM.1	—
FMT_MTD.1 (2)	FPT_RVM.1	—
FMT_MTD.1 (3)	FPT_RVM.1	—
FMT_SMF.1	—	—
FMT_SMR.1 (1)	—	—
FMT_SMR.1 (2)	—	—
FPT_RVM.1	—	—
FTA_TSE.1	FPT_RVM.1	—
FTP_TRP.1	FPT_RVM.1	FMT_MOF.1 (3)

8.2.4.1 Bypassing

Bypassing of the functional requirements in Table 8-5 is discussed below.

a) Cryptographic key generation FCS_CKM.1 is always invoked when the power is turned on and thus bypassing is not possible.

b) Cryptographic operation FCS_COP.1 always encrypts the user data and TSF data before these data are stored and decryption is enforced only when these data are read, and thus bypassing is not possible.

c) Sub-set residual information protection FDP_RIP.1 is always invoked during *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 thus bypassing is not possible.

d) FIA_AFL.1 (1), FIA_UAU.2 (1), FIA_UAU.7 (1) and FIA_UID.2 (1) related to administrator identification and authentication are always invoked during identification and authentication of administrator, and thus bypassing is not possible.

e) FIA_AFL.1 (2), FIA_UAU.2 (2), FIA_UAU.7 (2) and FIA_UID.2 (2) related to identification and authentication of the user that stored the confidential file is always invoked during identification and authentication of the user that stored the confidential file, and thus bypassing is not possible.

f) Verification of secrets FIA_SOS.1 (1) is always invoked without fail when the administrator password is changed (modified), and thus bypassing is not possible.

g) Verification of secrets FIA_SOS.1 (2) is always invoked without fail when the confidential file is stored, the confidential file password is changed (modified) and the property of the file that is not confidential is changed to confidential, and thus bypassing is not possible.

h) Management of security functions behaviour FMT_MOF.1 (1) always requires administrator authentication FIA_UAU.2 (1) before operation for enabling data clear, and thus bypassing is not possible.

i) Management of security functions behaviour FMT_MOF.1 (2) always invokes administrator authentication FIA_UAU.2 (1) before operation for disabling data clear, and thus bypassing is not possible.

j) Management of security functions behaviour FMT_MOF.1 (3) always requires administrator authentication FIA_UAU.2 (1) before operation for modifying the behaviour of *Clear Document Filing Data*, *Power Up Auto Clear*, document filing function and network protection function, and thus bypassing is not possible.

k) Management of TSF data FMT_MTD.1 (1) always requires administrator authentication FIA_UAU.2 (1), and thus bypassing is not possible.

l) Management of TSF data FMT_MTD.1 (2) always requires the authentication of the user that stored the confidential file FIA_UAU.2 (2), and thus bypassing is not possible.

m) Management of TSF data FMT_MTD.1 (3) always requires administrator authentication FIA_UAU.2 (1), and thus bypassing is not possible.

n) TOE session establishment FTA_TSE.1 is always invoked when network I/F detects the network packet, and thus bypassing is not possible.

o) Trusted path FTP_TRP.1 is always invoked when the remote user requires the use of trusted path, and thus bypassing is not possible.

8.2.4.2 Disabling

Disabling of the functional requirements in Table 8-5 is discussed below.

a) FDP_RIP.1 is protected against the disabling as follows.

- Disabling *Clear All Memory* program and *Clear Document Filing Data* program is restricted only to the administrator by FMT_MOF.1 (2).
- Configuring for disabling *Power Up Auto Clear* program and disabling *Power Up Auto Clear* program is restricted only to the administrator by FMT_MTD.1 (3) and FMT_MOF.1 (2).

b) FIA_AFL.1 (2), FIA_SOS.1 (2), FIA_UAU.2 (2), FIA_UAU.7 (2) and FIA_UID.2 (2) are protected against the disabling as follows.

- Modifying the behaviour of document filing function is restricted only to the administrator by FMT_MOF.1 (3).

c) FTP_TRP.1 is protected against the disabling as follows.

- Modifying the behaviour of network protection function is restricted only to the administrator by FMT_MOF.1 (3).

8.2.4.3 Tampering

This TOE has only permitted the behaviour management of the security function only to the administrator. Thus, improper subjects do not exist, the access control is not required, and TSF is not tampered.

8.2.5 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. For this reason, the quality assurance level selected for the TOE is EAL3 + ADV_SPM.1, a sufficient level for commercial use. ADV_SPM.1 is selected due to the dependency on ADV_SPM.1 that is indicated in the functional requirement FMT_MSA.2. All dependencies are satisfied as Table 5-1.

Each matter does not need to compete in assurance requirements aside from ADV_SPM.1 applying a package of EAL3 mutually. Competition with other matters does not occur in ADV_SPM.1 being assurance requirements of individual specifications named a TSP model.

8.2.6 Rationale for Minimum Strength of Function

It is expected that this TOE will be used in general commercial systems, and thus malicious acts will be attacks that make use of public information. For this reason, the attack potential of attacker is “low-level”. The minimum strength of function level of this TOE is SOF-basic, and it can cope with the malicious acts that make use of public information by attackers possessing a low-level attack potential. Explicit strength of function of each FIA_AFL.1 (1), FIA_AFL.1 (2), FIA_SOS.1 (1), FIA_SOS.1 (2), FIA_UAU.2 (1), FIA_UAU.2 (2), FIA_UAU.7 (1) and FIA_UAU.7 (2) is SOF-basic and they do not conflict the minimum strength of function.

8.3 TOE Summary Specification Rationale

This section demonstrates that the TOE security functions and their assurance measures meet the IT security requirements.

8.3.1 TOE Summary Specification Rationale

As for the correspondence between the security functional requirements and the TOE security specifications at Table 6-1, the rationale is shown below.

8.3.1.1 FCS_CKM.1

When the MFD is powered on, TSF_FKG generates a 128 bits cryptographic key (common key) using the MSN-R expansion algorithm. The MSN-R expansion algorithm is based on the SHARP Corporation Encryption Standards for MFD Data Security Kits, and thus FCS_CKM.1 is satisfied.

8.3.1.2 FCS_COP.1

The user data and TSF data that are stored to the MSD are encrypted and decrypted by TSF_FDE according to the AES Rijndael algorithm standardized in FIPS PUB 197, and thus FCS_COP.1 is satisfied.

8.3.1.3 FDP_RIP.1

TSF_FDC disables the regeneration of image data stored in an image data file in the MSD (either HDD or Flash memory) by overwriting the file at least once when the *Auto Clear at Job End* program runs.

TSF_FDC disables the regeneration of image data stored in all image data files in the MSD (both HDD and Flash memory) by overwriting all the files at least once when the *Clear All Memory* program runs. It is possible to configure that this program runs when the *Power Up Auto Clear* program runs.

TSF_FDC disables the regeneration of image data stored in all image data files in the MSD area specified by the administrator by overwriting all the files at least once when the *Clear Document Filing Data* program runs. It is possible to configure that this program runs when the *Power Up Auto Clear* program runs.

TSF_FDC disables the regeneration of jobs completed list data stored in jobs completed list data file by overwriting the file at least once when the *Clear All Data in Job Status Jobs Completed List* program runs. It is possible to configure that this program runs when the *Power Up Auto Clear* program runs.

TSF_FDC disables the regeneration of address book data stored in address book data file by overwriting the file at least once when the *Clear Address Book Data and Registered Data in MFP* program runs.

Thus, FDP_RIP.1 is satisfied.

8.3.1.4 FIA_AFL.1 (1)

Both TSF_AUT and TSF_FNP identify and authenticate the administrator. The cancel operation of TSF_FDC authenticates the administrator. These support the authentication failure handling as defined by FIA_AFL.1 (1). Thus, FIA_AFL.1 (1) is satisfied.

8.3.1.5 FIA_AFL.1 (2)

When TSF_FCF authenticates each user that saved a confidential file before allowing an operation to the file, TSF_FCF counts the number of failed authentication attempts for each confidential file. TSF_FCF stops accepting further authentication attempts and locks a confidential file when authentication failures repeated 3 times in a row on the file. The lock can be released only with *Release the lock on document filing output operation* function by TSF_FCF that only the administrator who TSF_AUT has successfully authenticated allows to invoke. Thus, FIA_AFL.1 (2) is satisfied.

8.3.1.6 FIA_SOS.1 (1)

When the administrator password is changed by TSF_AUT, TSF_AUT verifies that the administrator password meets 5 to 32 alphanumeric and/or symbol characters and does not accept the administrator password that does not satisfy that quality metric, and thus FIA_SOS.1 (1) is satisfied.

8.3.1.7 FIA_SOS.1 (2)

When the confidential file is stored, the confidential file password is changed and the property of the file that is not confidential is changed to confidential by TSF_FCF, TSF_FCF verifies that the confidential file password meets 5 to 8 numeric characters and does not accept the confidential file password that does not satisfy that quality metric, and thus FIA_SOS.1 (2) is satisfied.

8.3.1.8 FIA_UAU.2 (1)

TSF_AUT enforces the authentication by entering the administrator password before the operation of the function for the administrator. TSF_FNP enforces the authentication by entering the administrator

password before providing the interface that operates the network settings data. TSF_FDC enforces the authentication by entering the administrator password when *Clear All Memory*, *Clear Document Filing Data* and *Power Up Auto Clear* are cancelled. Thus, FIA_UAU.2 (1) is satisfied.

8.3.1.9 FIA_UAU.2 (2)

TSF_FCF enforces the authentication by entering the confidential file password when the user attempts some operation on a confidential file, and thus FIA_UAU.2 (2) is satisfied.

8.3.1.10 FIA_UAU.7 (1)

TSF_AUT and TSF_FNP only indicate as many substitute characters as characters entered for the protected feedback while authentication of the administrator. This is same while authentication of the administrator by the cancel operation of TSF_FDC, and thus FIA_UAU.7 (1) is satisfied.

8.3.1.11 FIA_UAU.7 (2)

TSF_FCF only indicates as many substitute characters as characters entered for the protected feedback while authentication of the confidential file password, and thus FIA_UAU.7 (2) is satisfied.

8.3.1.12 FIA_UID.2 (1)

TSF_AUT requires the operation for the identification of the administrator before the operation of the function for the administrator. TSF_FNP requires the operation for the identification of the administrator before providing the interface that operates the network settings data. The cancel operation of *Clear All Memory*, *Clear Document Filing Data* and *Power Up Auto Clear* by TSF_FDC corresponds to the identification of the administrator. Thus, FIA_UID.2 (1) is satisfied.

8.3.1.13 FIA_UID.2 (2)

When the user attempts some operation on a confidential file by TSF_FCF, the operation for the selection of the confidential file is required. This corresponds to the identification of the user that stored a confidential file, and thus FIA_UID.2 (2) is satisfied.

8.3.1.14 FMT_MOF.1 (1)

TSF_FDC provides the interface to enable *Clear All Memory*, *Clear Document Filing Data*, *Clear Address Book Data and Registered Data in MFP* and *Clear All Data in Job Status Jobs Completed List* only to the administrator. Configuring for enabling *Power Up Auto Clear* is same as this. Thus, FMT_MOF.1 (1) is satisfied.

8.3.1.15 FMT_MOF.1 (2)

TSF_FDC provides the interface to disable *Clear All Memory*, *Clear Document Filing Data* and *Power Up Auto Clear* only to the administrator. Configuring for disabling *Power Up Auto Clear* is same as this. Thus, FMT_MOF.1 (2) is satisfied.

8.3.1.16 FMT_MOF.1 (3)

TSF_FDC provides the interface to modify the behaviour of *Clear Document Filing Data*; in other words the interface to choose the data to be cleared only to the administrator when *Clear Document Filing Data* is enforced.

TSF_FDC provides the configuration function "*Power Up Auto Clear*" that is the interface to modify the behaviour of *Power Up Auto Clear* and described as Data Clearance Settings (section 6.1.3.7) only to the administrator.

TSF_FCF provides the function "*Disabling of Document Filing*" and "*Disabling of Print Jobs Other Than Print Hold Job*" that are the interface to modify the behaviour of document filing function only to the administrator.

TSF_FNP provides the function "*SSL settings*" that is the interface to modify the behaviour of network protection function only to the administrator.

Thus, FMT_MOF.1 (3) is satisfied.

8.3.1.17 FMT_MSA.2

It is explained that a cryptographic key is sure to be generated based on the secure seed for ADV_SPM.1, and FMT_MSA.2 is satisfied by cryptographic key generation TSF_FKG.

8.3.1.18 FMT_MTD.1 (1)

The administrator identified and authenticated by TSF_AUT is able to modify the administrator password by TSF_AUT, and thus FMT_MTD.1 (1) is satisfied.

8.3.1.19 FMT_MTD.1 (2)

The interface to modify the confidential file password by TSF_FCF is provided only to the user that stored a confidential file identified and authenticated by TSF_FCF and not provided to others.

The interface to create the confidential file password by TSF_FCF is provided when the confidential file is stored and the property of the file is changed to confidential by the user that stored a confidential file identified and authenticated by TSF_FCF and not provided when others.

Thus, FMT_MTD.1 (2) is satisfied.

8.3.1.20 FMT_MTD.1 (3)

The interface to query and modify "*IP address filter*" is provided by TSF_FNP.

The interface to query and modify "*MAC address filter*" is provided by TSF_FNP.

The interface to query and modify "*SSL Settings*" is provided by TSF_FNP.

The interface to query and modify "*Number of Times Auto Clear at Job End Program is Repeated*" is provided by TSF_FDC.

The interface to query and modify "*Number of Times Data Clear is Repeated*" is provided by TSF_FDC.

The interface to query and modify "*the data areas to be cleared by Power Up Auto Clear Program*" is provided by TSF_FDC.

The interface to query and modify "*Number of Times Power Up Auto Clear Program is Repeated*" is provided by TSF_FDC.

The interface to query and modify "*Disabling of Document Filing*" is provided by TSF_FCF.

The interface to query and modify "*Disabling of Print Jobs Other Than Print Hold Job*" is provided by TSF_FCF.

Each interface above is provided only to the administrator identified and authenticated by TSF_AUT, and thus FMT_MTD.1 (3) is satisfied.

8.3.1.21 FMT_SMF.1

TSF_FDC contains the ability to enable or disable "*Clear All Memory*".

TSF_FDC contains the ability to enable or disable "*Clear Document Filing Data*".

TSF_FDC contains the ability to disable "*Power Up Auto Clear*".

TSF_FDC contains the ability to enable "*Clear Address Book Data and Registered Data in MFP*".

TSF_FDC contains the ability to enable "*Clear All Data in Job Status Jobs Completed List*".

TSF_FDC contains the ability to query and modify "*Number of Times Auto Clear at Job End Program is Repeated*".

TSF_FDC contains the ability to query and modify "*Number of Times Data Clear is Repeated*".

TSF_FDC contains the ability to query and modify "*the data areas to be cleared by Power Up Auto Clear Program*".

TSF_FDC contains the ability to query and modify "*Number of Times Power Up Auto Clear Program is Repeated*".

TSF_FCF contains the ability to release the lock of confidential files.

TSF_AUT contains the ability to modify the administrator password.

TSF_FCF contains the ability to modify the confidential file password.

TSF_FCF contains the ability to query and modify "*Disabling of Document Filing*".

TSF_FCF contains the ability to query and modify "*Disabling of Print Jobs Other Than Print Hold Job*".

TSF_FNP contains the ability to manage "*IP address filter*" and "*MAC address filter*".

TSF_FNP contains the ability manage the services protected by SSL.

Thus, FMT_SMF.1 is satisfied.

8.3.1.22 FMT_SMR.1 (1)

Identification and authentication of administrator by TSF_AUT specifies the administrator. This associates the user with the role. In addition, even if the administrator password is changed (modified), association and maintenance of the role continues, and thus FMT_SMR.1 (1) is satisfied.

8.3.1.23 FMT_SMR.1 (2)

Identification and authentication of the user that stored the confidential file by TSF_FCF specifies the user that stored the confidential file. This associates the user with the role. In addition, even if the confidential file password is changed (modified), association and maintenance of the role continues, and thus FMT_SMR.1 (2) is satisfied.

8.3.1.24 FPT_RVM.1

The supports by FPT_RVM.1, mentioned in section 8.2.4.1, are implemented by the TSFs as follows:

a) TSF_FKG always generates the cryptographic key according to FCS_CKM.1 when the power is turned on.

b) TSF_FDE always encrypts the user data and TSF data when these data are stored to the MSD and decrypts only the user data and TSF data that have been read according to FDC_COP.1.

c) TSF_FDC always overwrites according to FDP_RIP.1 when the jobs are finished or canceled, the user deletes the confidential file and the data clear program by the operation of the administrator is called. If the administrator configured that *Power Up Auto Clear* is enabled, TSF_FDC always overwrites according to FDP_RIP.1 when the power is turned on.

d) TSF_FDC, TSF_AUT and TSF_FNP always enforces the identification operation of the administrator according to FIA_UID.2 (1), authentication of the administrator password according to FIA_UAU.2 (1), protection of the feedback of the administrator password according to FIA_UAU.7 (1) and locking the administrator password according to FIA_AFL.1 (1) when the administrator is identified and authenticated.
TSF_FDC allows the cancellation of *Clear All Memory*, *Clear Document Filing Data* and *Power Up Auto Clear* only when the identification and authentication of the administrator by TSF_FDC is invoked and successful.
TSF_FDC, TSF_FCF and TSF_FNP provide the interface of the function for the administrator only when the identification and authentication of the administrator by TSF_AUT is invoked and successful.
TSF_FNP provides the interface to manage the network settings data only when the identification and authentication of the administrator by TSF_FNP is invoked and successful.

e) TSF_FCF always enforces the select operation of the confidential file according to FIA_UID.2 (2), authentication of the confidential file password according to FIA_UAU.2 (2), protection of the feedback of the confidential file password according to FIA_UAU.7 (2) and locking the confidential file according to FIA_AFL.1 (2) when a user attempts some operation on a confidential file.

f) TSF_AUT always verifies that the administrator password meets the quality metric, 5 to 32 alphanumeric and/or symbol characters according to FIA_SOS.1 (1) when the administrator password is changed.

g) TSF_FCF always verifies that the confidential file password meets the quality metric, 5 to 8 numeric characters according to FIA_SOS.1 (2) when the confidential file is stored, the confidential file password is changed and the property of the file that is not confidential is changed to confidential.

h) TSF_FDC provides the interface to enable *Clear All Memory*, *Clear Document Filing Data*, *Clear Address Book Data and Registered Data in MFP* and *Clear All Data in Job Status Jobs Completed List* and the interface to configure for enabling *Power Up Auto Clear* according to FMT_MOF.1 (1) only when the authentication of the administrator by TSF_AUT is invoked and successful.

i) TSF_FDC allows disabling *Clear All Memory*, *Clear Document Filing Data* and *Power Up Auto Clear* according to FMT_MOF.1 (2) only when the authentication of the administrator by TSF_FDC is invoked and successful.
TSF_FDC also provides the interface to configure for disabling *Power Up Auto Clear* according to FMT_MOF.1 (2) only when the authentication of the administrator by TSF_AUT is invoked and successful.

j) TSF_FDC provides the interface to modify the behaviour of *Clear Document Filing Data* function and *Power Up Auto Clear* function according to FMT_MOF.1 (3) only when the authentication of the administrator by TSF_AUT is invoked and successful.
TSF_FCF provides the interface to modify the behaviour of document filing function according to FMT_MOF.1 (3) only when the authentication of the administrator by TSF_AUT is invoked and successful.
TSF_FNP provides the interface to modify the behaviour of network protection function according to FMT_MOF.1 (3) only when the authentication of the administrator by TSF_AUT is invoked and successful.

k) TSF_AUT provides the interface to modify the administrator password according to FMT_MTD.1 (1) only when the authentication of the administrator by TSF_AUT is invoked and successful.

l) TSF_FCF provides the interface to modify the confidential file password according to FMT_MTD.1 (2) only when the authentication of the administrator by TSF_FCF is invoked and successful.

m) TSF_FNP provides the interface to query and modify *SSL Settings* according to FMT_MTD.1 (3) only when the authentication of the administrator by TSF_AUT is called and successful.
TSF_FDC provides the interface to query and modify *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 Program* and *Number of Times Power Up Auto Clear Program is Repeated* according to FMT_MTD.1 (3) only when the authentication of the administrator by TSF_AUT is invoked and successful.
TSF_FCF provides the interface to query and modify *Disabling of Document Filing* and *Disabling of Print Jobs Other Than Print Hold Job* according to FMT_MTD.1 (3) only when the authentication of the administrator by TSF_AUT is invoked and successful.

n) TSF_FNP requires that the network packet detected by network I/F is always verified in terms of IP address and MAC address, compared with the settings and judged that this packet is accepted or not according to FTA_TSE.1 before the response and management.

o) TSF_FNP requires that the protected communication path be always established according to FTP_TRP.1 before receive or transmit communication data that shall be protected when the remote user requires the use of trusted path.

8.3.1.25 FTA_TSE.1

The filter function provided by TSF_FNP cancels the network packet from the other party not to be intended and denies every session establishment according to the IP address and MAC address settings that the administrator specified beforehand, and thus FTA_TSE.1 is satisfied.

8.3.1.26 FTP_TRP.1

The communication data protection function provided by TSF_FNP provides the communication path that is protected by SSL; in other words the communication path with HTTPS and IPP-SSL between remote user at the client and MFD that TOE is installed to. These communication paths are logically distinct from other communication paths and contain the ability to provide assured identification of its end points and protection of the communicated data from modification or disclosure.

This function contains the ability to permit to initiate communication via the trusted path protected by SSL for the remote user .at the client's request; in other words for the connection from the Web browser or printer driver that is installed to the client.

This function contains the ability to require the use of the trusted path protected by SSL for communication service for TOE Web and printer driver.

Thus, FTP_TRP.1 is satisfied.

8.3.2 TOE assurance measures Rationale

The assurance measures in section 6.3 satisfy TOE security assurance requirements by means of the following contents of each assurance measures (referred as A.m. in this section).

a) ACM_CAP.3, ACM_SCP.1

A.m.: Colour Renaissance series Configuration Management

MX-FRX2 Version M.10 Configuration List

Contents: It specifies the measures and procedures to distinguish every configuration item uniquely and to assure that users can be aware of which instance of the TOE they are using.

It specifies that changes only for the items that are under control of this assurance measure can be managed and that evaluation evidences that TOE implementation and the other assurance components of ST requires are modified by the managed way with appropriate authorization.

b) ADO_DEL.1

A.m.: Colour Renaissance series Delivery Procedures

Contents: It specifies the measures and procedures to maintain the security of TOE when TOE is delivered from the developer to the users.

c) ADO_IGS.1

A.m.: MX-FRX2 Installation Manual

MX-FRX2 Installation Manual (English, German, French, Spanish)

Contents: It specifies the measures and procedures of installation of TOE.

d) ADV_FSP.1

A.m.: Colour Renaissance series Security Functional Specifications

Contents: It specifies the behaviour of TSF and the interfaces that user-visible interfaces.

e) ADV_HLD.2

A.m.: Colour Renaissance series High-level Design

Contents: It specifies the assurance that TOE provides the architecture that is suitable for the implementation of TOE functional requirements, from the view point of main structural units (subsystems) of TOE and the view point of associating these units with the functions that they provides.

f) ADV_RCR.1

A.m.: Colour Renaissance series Representation Correspondence Analysis

Contents: It specifies the correspondence among TOE Summary Specifications, Functional Specifications and High-level Design.

g) ADV_SPM.1

A.m.: Colour Renaissance series Security Policy Model Specifications

Contents: It specifies the correspondence among Function Specifications, Security Policy Model and these policies of the TSP. It provides the assurance that only the secure value can be accepted as the security attributes.

h) AGD_ADM.1

A.m.: MX-FRX2 MX-FRX2 Data Security Kit Operation Manual

MX-FRX2 Data Security Kit Notice

Contents: They are the documents (operation manuals) that are written for the sake of maintaining and administering of TOE properly by TOE administrators.

i) AGD_USR.1

A.m.: MX-FRX2 MX-FRX2 Data Security Kit Operation Manual
MX-FRX2 Data Security Kit Notice

Contents: They are the documents (operation manuals) that are written for the secure use of TOE for TOE users.

j) ALC_DVS.1

A.m.: Colour Renaissance series Development Security Specifications

Contents: It specifies the physical, procedural and personnel security measures used in the development environment of TOE.

k) ATE_COV.2

A.m.: Colour Renaissance series Coverage Analysis

Contents: It is the document that describes that it is enough to demonstrate that TSF operates as stated in the Functional Specifications, in the tests described in the Functional Testing Specifications.

l) ATE_DPT.1

A.m.: Color Renaissance series High-level Design Testing Analysis

Contents: It is the document that describes that it is enough to demonstrate that TSF operates as stated in the High-level Design Specifications, in the tests described in the Functional Testing Specifications.

m) ATE_FUN.1

A.m.: MX-FRX2 Functional Testing Specifications

Color Renaissance series Testing Environment and Tools Manual

Contents: They are the documents that describe about the tests to establish that all the execution of the security function is as stated in the specifications.

n) ATE_IND.2

A.m.: TOE

Contents: TOE suitable for testing

o) AVA_MSU.1

A.m.: MX-FRX1 MX-FRX2 Data Security Kit Operation Manual
MX-FRX2 Data Security Kit Notice

Contents: They are the documents (operation manuals) that are written about the maintenance and administration method for the proper use of TOE for the TOE administrators and the secure use of TOE for the TOE users.

p) AVA_SOF.1

A.m.: Color Renaissance series Strength of Security Function Analysis

Contents: It is what strength of function analysis for probabilistic and permutational mechanism is performed.

q) AVA_VLA.1

A.m.: Colour Renaissance series Vulnerability Analysis

Contents: It is what describes the existence of obvious security vulnerability of TOE security and the analysis that they can not be abused in the intended environment for the TOE.

8.3.3 Rationale for Strength of TOE Security Function

The TSFs that are implemented using a probabilistic or permutational mechanisms are authentication (TSF_AUT), data clear (TSF_FDC), network protection (TSF_FNP) and confidential files (TSF_FCF). These functions have security strength of function of SOF-basic.

Thus, the minimum value of these security strengths of function is SOF-basic and the TOE security strength of function and the minimum strength of function described in section 5.1.2 are consistent.