SHARP

MX-FR10

Security Target

Version 0.07

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

SHARP CORPORATION

Revision history

Date	Ver.	Revision	Author	Reviewed	Approved
2008-09-02	0.01	• Original Draft	Nakagawa	Sakamoto	Kodaka
2008-11-17	0.02	• Rewrote some portion of ST Introduction, functional requirements and security functions.	Sakamoto	Nakagawa	Kodaka
2008-11-27	0.03	• Modified ST Introduction and security requirements.	Nakagawa	Sakamoto	Kodaka
2009-02-02	0.04	• Modified TOE Identification and functional requirements. • In response to the Observation Reports ASE001-01 and ASE002-01	Nakagawa	Sakamoto	Kodaka
2009-03-24	0.05	• In response to the Observation Report ASE002-01	Nakagawa	Sakamoto	Kodaka
2009-03-31	0.06	• In response to the Observation Report ASE002-01	Nakagawa	Sakamoto	Kodaka
2009-04-24	0.07	• Added identifiers of the guidance documents.	Nakagawa	Sakamoto	Yamaguchi

Table of Contents

1 ST Introduction 6
1.1 ST Reference 6
1.2 TOE Reference 6
1.3 TOE Overview 6
1.3.1 TOE Type 6
1.3.2 Required non-TOE hardware/software/firmware 6
1.3.3 Main Security Functions 6
1.3.4 TOE Usage 7
1.3.5 Overview of the MFD Functions and Applications 7
1.4 TOE Description 9
1.4.1 Physical Configuration of the TOE 9
1.4.2 Logical Configuration of the TOE 9
1.4.3 Guidance Documents 11
1.4.4 Assets Protected by the TOE 11
1.4.5 Related parties of the TOE 12
2 Conformance Claims 13
2.1 CC Conformance Claim 13
2.2 PP Claim 13
2.3 Package Claim 13
3 Security Problem Definition 14
3.1 Threats 14
3.2 Organisational Security Policies 14
3.3 Assumptions 14
4 Security Objectives 15
4.1 Security Objectives for the TOE 15
4.2 Security Objectives for the Operational Environment 15
4.3 Security Objectives Rationale 16
4.3.1 Rationale Explaining Why Threats Are Countered 16
4.3.2 Rationale for Implementation of Organisational Security Policies 18
4.3.3 Rationale for Satisfaction of Assumptions 18
5 Extended Components Definition 19
6 Security Requirements 20
6.1 Requirement Operations 20
6.2 Security Functional Requirements 20
6.2.1 Class FCS: Cryptographic Support 20
6.2.2 Class FDP: User Data Protection 21
6.2.3 Class FIA: Identification and Authentication 22
6.2.4 Class FMT: Security Management 23
6.2.5 Class FTA: TOE Access 25
6.2.6 Class FTP: Trusted Path/Channels 25
6.3 Security Assurance Requirements 26
6.4 Security Requirements Rationale 27
6.4.1 Security Functional Requirements Rationale 27
6.4.2 Security Assurance Requirements Rationale 33

7 TOE Summary Specification 34
7.1 Cryptographic Key Generation (TSF_FKG) 34
7.2 Cryptographic Operation (TSF_FDE) 34
7.3 Data Clear (TSF_FDC) 35
7.3.1 Overview of the Data Clear Function 35
7.3.2 Auto Clear at Job End program 35
7.3.3 Clear All Memory program 36
7.3.4 Clear Address Book Data and Registered Data in MFP program 36
7.3.5 Clear Document Filing Data program 36
7.3.6 Clear All Data in Job Status Jobs Completed List program 36
7.3.7 Power Up Auto Clear program 36
7.3.8 Data Clearance Settings 37
7.4 Authentication (TSF_AUT) 37
7.5 Confidential files (TSF_FCF) 38
7.6 Network Protection Function (TSF_FNP) 39
7.6.1 Overview of Network Protection 39
7.6.2 Filter Function 39
7.6.3 Communication Data Protection Function 39
7.6.4 Network Settings Protection 40
7.7 Fax Flow Control (TSF_FFL) 40
8 Appendix 41
8.1 Terminology 41
8.2 Acronyms 43

List of Tables

Table 1.1: Guidance Documents 11
Table 3.1: Threats 14
Table 3.2: Organisational Security Policies 14
Table 3.3: Assumptions 14
Table 4.1: Security Objectives for the TOE 15
Table 4.2: Security Objectives for the Environment 15
Table 4.3: Security Objectives Rationale 16
Table 6.1: Security Functional Requirements Rationale 27
Table 6.2: Management Functions of the TOE 31
Table 6.3: Security Functional Requirement Dependencies 32
Table 6.4: Justification of Unsatisfied SFR Dependencies 32
Table 7.1: Security Functional Requirements and TOE Security Specifications 34
Table 8.1: Terminology 41
Table 8.2: Acronyms in the CC 43
Table 8.3: Other Acronyms 44

List of Figures

Figure 1: Usage environment of the MFD 8
Figure 2: TOE and physical configuration of the MFD 9
Figure 3: Logical Configuration of the TOE 10

1 ST Introduction

In accordance with the Common Criteria (CC) identified in Section 2.1, this chapter identifies this Security Target (ST) and the Target of Evaluation (TOE) claiming conformance to this ST. For that, this chapter presents ST reference, TOE reference, TOE overview and TOE description. See Sections 8.1 and 8.2 for terminology used in this ST.

1.1 ST Reference

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

Title: MX-FR10 Security Target

Version: 0.07

Publication Date: 2009-04-24

Author: Sharp Corporation

1.2 TOE Reference

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

Name: MX-FR10

Version: C.10

Developer: Sharp Corporation

1.3 TOE Overview

1.3.1 TOE Type

The TOE is an IT product to protect data in a Multi Function Device (MFD).

The main part of the TOE is the firmware in ROMs and HDD for the MFD. By replacing the MFD standard firmware, it offers the security function and controls the entire MFD.

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

MFDs, Multi Function Devices, are office machines mainly with copier, printer, scanner and fax functions.

1.3.2 Required non-TOE hardware/software/firmware

The TOE operates on the MFD (hardware) made by Sharp Corporation, namely, MX-2600FG, MX-2600FN, MX-2600G, MX-2600N, MX-2600NJ, MX-3100FG, MX-3100FN, MX-3100G, MX-3100N and MX-3100NJ.

1.3.3 Main Security Functions

The TOE security feature mainly provides the following functions aiming to counter unauthorized attempts to steal image data in the MFD where the TOE is installed.

a) Cryptographic operation function: encrypts image data and other data that the MFD handles before it is written to the HDD or Flash memory in the MFD.

b) Data clear function: overwrites an area where encrypted data is stored into the HDD or Flash memory in the MFD with a random or fixed value.

c) Confidential file function: provides password protection for image data on the HDD stored by the user to protect them from being reused by others.

d) Network protection function: prevents unauthorized accesses over the network, wiretapping of communication data and unauthorized modification of the network settings.

e) Fax flow control function: prevents accesses through the telephone line connected to the MFD's fax I/F from accessing the internal network through the MFD's network I/F.

1.3.4 TOE Usage

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

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

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

- When users enter a job such as copy into the MFD, they select to save the image data and specify a password. This allows the TOE to save the image data of the job into the HDD along with the password after job completion.
- Users set an original on the MFD, select "Scan to HDD" on the operation panel of the MFD and specify a password. This allows the TOE to scan the original and obtain its image data from the MFD scanner unit, and save the image data into the HDD along with the password.
- Users select a confidential file saved into the HDD, enter the password and specify a file manipulation (including print, send, preview and delete) on the operation panel of the MFD or from a client connected to the network. The TOE checks the password entered and, when the password is verified, performs the file manipulation. The TOE disables the file manipulation if an incorrect password is entered three times in a row.

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

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

e) When users communicate with the MFD from a client over the network, the SSL, IPsec and SNMP v3 functions of the TOE can be used. When a print job is sent from a client, the print image data is protected using the IPP-SSL protocol from being wiretapped during transmission. When users access the Web page provided by the MFD (TOE) for remote operation such as reusing a confidential file, the SSL (HTTPS) protocol can be used to protect information including the password from being wiretapped during transmission. In addition, IPsec is used for IP-based communication between clients and the MFD to protect data from being wiretapped during transmission. SNMP v3 is used for SNMP-based communication to protect data sent and received to control the MFD remotely based on the MIB from being wiretapped during transmission.

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

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

1.3.5 Overview of the MFD Functions and Applications

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

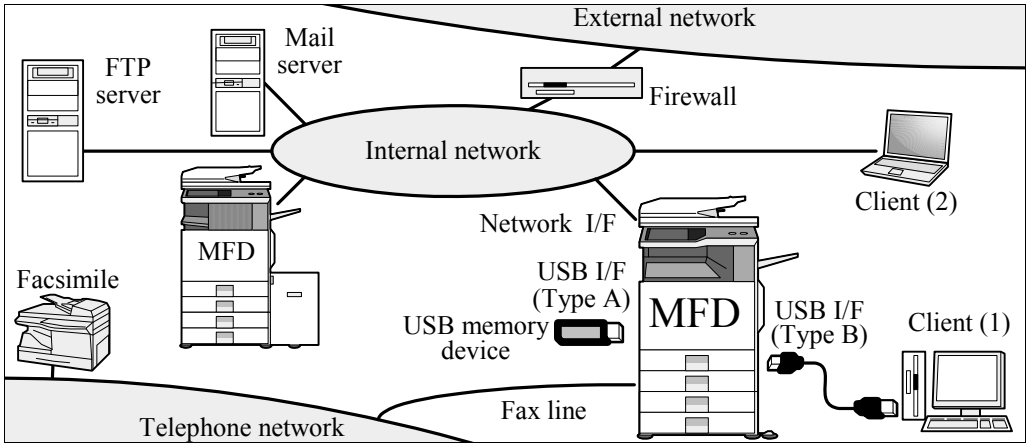

Figure 1: Usage environment of the MFD

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

1.3.5.1 Job function

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

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

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

- Printer driver: generates print data at a client and sends it 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 the Web. Received data by the internet fax and tandem print requests from another MFD are printed in the same manner.
- Pull print: acquires print data in an FTP server, a network folder or a USB memory device by operations on the operation panel.

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

- E-mail: transmits it as an attachment to an E-mail.
- File server: transmits it to an FTP server.
- Desktop: transmits it via FTP to a client running the software tool delivered together with the MFD or provided separately.
- Network folder: transmits it into a shared folder of Microsoft Windows over the network.
- USB memory: puts it into a USB memory device plugged into the MFD.
- PC scan: transmits it via TWAIN to a client running the software tool delivered together with the MFD.
- Internet Fax: transmits it as an attachment to an E-mail according to the Internet Fax standard specification.

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

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

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

1.3.5.2 Document filing function

The document filing function provides the following functions that allow users to save image data into the HDD in the MFD and operate it from the operation panel or the client via the 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 saved image data for the following operations.
  - Print: prints saved image data to the paper. If Tandem Print mode is selected, this function sends image data to the MFD that the administrator specified beforehand.
  - Send: transmits saved image data either by any medium available for the network scanner function or by facsimile.
  - Preview: displays the rough outline of saved image data.
  - Property change: removes the password from a file with a password, or vice versa.
  - Password change: changes confidential file passwords.
  - Delete: removes a saved image data that the user no longer needs, and overwrites it.
  - Backup (export): transfers the saved image data to the client as a binary data, from which the user can restore (import) the image data later.

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

1.3.5.3 Address book function

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

1.4 TOE Description

1.4.1 Physical Configuration of the TOE

The physical scope of the TOE is shaded in Figure 2. Main part of the TOE is in the MFD's controller firmware and provided as "Data Security Kit MX-FR10 (DSK)", an optional product for Sharp MFDs to enhance security coming with two ROM boards and a USB memory device. Part of the security function is included in the MFD's HDC, which is also within the scope of the TOE.

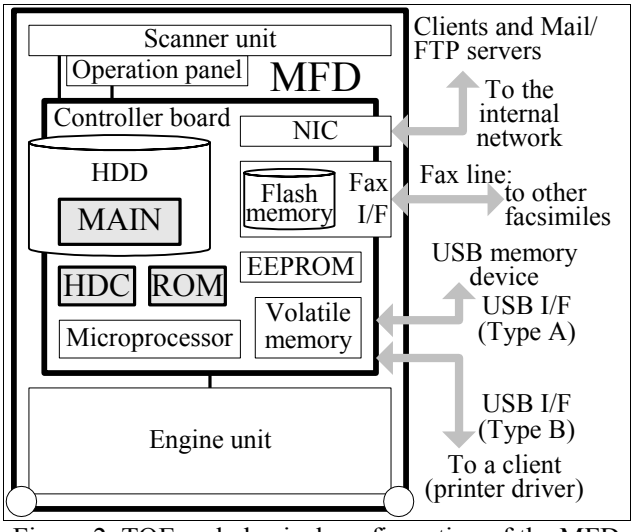

Figure 2: TOE and physical configuration of the MFD

- ROM: contains part of the controller firmware. When the TOE is installed to the MFD, two ROMs of the standard firmware are removed from the controller board and replaced with two ROMs of the DSK.
- MAIN: is part of the controller firmware and installed from the USB memory device of the DSK to the HDD in the MFD.
- HDC: is an integrated circuit part that is mounted on the controller board in the MFD beforehand.

1.4.2 Logical Configuration of the TOE

Figure 3 shows the logical configuration of the TOE. The thick-lined frame indicates the logical scope of the TOE. Rounded boxes indicate hardware devices that are out of the TOE. Rectangles indicate functions

of the TOE; and ones shaded indicate security functions. Among the data in the volatile memory, HDD, Flash memory and EEPROM, the data that security functions handle (i.e. user data and TSF data) are also shaded.

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

The large part of the TOE is the firmware for the MFD, providing security functions as well as control of the entire MFD. Part of the TOE security functions (TSFs) is implemented in the HDC and invoked by the TSFs 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 into 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 and stores the key into the volatile memory.

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 file function (TSF_FCF): provides password protection when a user saves image data into the MFD using the document filing function (Section 1.3.5.2) and requires authentication by means of that confidential file password to reuse (such as to print or to transmit) the data. If an incorrect password for a confidential file is 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 function: protects the communication data by SSL, IPsec and SNMP v3. This function is not available when the user uses a client and/or a protocol not supporting SSL, IPsec and SNMP v3.
- Network settings protection: provides the network management functions (see below) only to the administrator and do not allow other users to use it.

g) Fax flow control function (TSF_FFL): prevents accesses through the telephone line connected to the MFD's fax I/F from accessing the internal network through the MFD's network I/F.

h) 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 into the HDD.

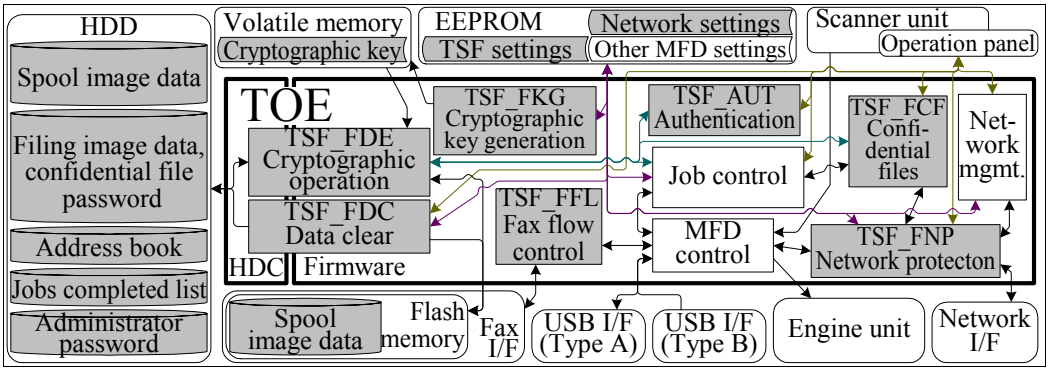

Figure 3: Logical Configuration of the TOE

i) 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.

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

1.4.3 Guidance Documents

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

Table 1.1: Guidance Documents

For Japan	MX-FR10 Data Security Kit Operation Manual (in Japanese) [CINSJ4568FC51]	MX-FR10 Data Security Kit Notice (in Japanese) [TCADJ2011FCZZ]
For outside Japan	MX-FR10 Data Security Kit Operation Manual (in English) [CINSZ4569FC51]	MX-FR10 Data Security Kit Notice (in English) [TCADZ2012FCZZ]

1.4.4 Assets Protected by the TOE

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

- Image data that the MFD functions spool to process jobs
- Image data that users save as confidential files
- Address book data
- Jobs completed list data
- Network settings data
- Data transmission over the network

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

1.4.4.1 Image data that the MFD functions spool to process jobs

The assets protected by the TOE include the image data that the TOE itself temporarily spools into 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.

MFDs "delete" these image data when the jobs are finished or cancelled to deallocate resources. To "delete" here means just to make the storage area "unused" by marking it "deleted" in the allocation table. This is to "delete" the image data that occupied the storage area, in the same way as data files on the hard disk connected to a general personal computer are deleted; the deleted image data can remain in the cleared area until the area is reused by other jobs. Thus, this ST includes into the assets the deleted image data remaining on the HDD or the Flash memory in the MFD.

1.4.4.2 Image data that users save as confidential files

The assets protected by the TOE include the image data that the user saves into 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, in the same way as the previous section, the image data can remain on the HDD after this deletion. Thus, the deleted image data remaining on the HDD is also included in the assets.

1.4.4.3 Address book data

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

There is not necessarily a threat to counter if there is no method for the improper user to read or modify the address book data without standing in front of the operation panel and accessing every record in this data

one by one by seeing and operating manually. However, this data shall be protected from the possibility that the improper user reads and modifies this data all at one time from the HDD directly or through the internal network.

1.4.4.4 Jobs completed list data

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

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

1.4.4.5 Network settings data

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

- TCP/IP Settings: Enable TCP/IP, Enable DHCP, IP Address Settings
- DNS Settings: Primary/Secondary DNS Server, Domain Name
- WINS Settings: Enable WINS, Primary/Secondary WINS Server, WINS Scope ID
- SMTP Settings: SMTP Server
- LDAP Settings: Enable LDAP, LDAP Server
- Tandem Connection Settings: IP Address of Slave Machine, Disabling of Master Machine Mode
- Port Control: Enabling or the port number for each network service

1.4.4.6 Data transmission over the network

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

1.4.5 Related parties of the TOE

This section describes those related to the TOE and the TOE-equipped MFD.

- Owner: an organisation which possesses the TOE and MFD and is in control of them.
- Those in charge of the organisation: belongs to the owner and is in charge of management of the MFD.
- Administrator: is assigned operation and management of the TOE and MFD by those in charge of the organisation.
- User: uses the MFD functions (Section 1.3.5) of the TOE and MFD.

2 Conformance Claims

This ST satisfies the followings.

2.1 CC Conformance Claim

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

- Part 1: Introduction and general model
  September 2006 Version 3.1 Revision 1; Japanese Translation 1.2
- Part 2: Security functional components
  September 2007 Version 3.1 Revision 2; Japanese Translation 2.0
- Part 3: Security assurance components
  September 2007 Version 3.1 Revision 2; Japanese Translation 2.0

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

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

2.2 PP Claim

This ST does not claim conformance to any PP.

2.3 Package Claim

This ST claims conformance to EAL3.

3 Security Problem Definition

This chapter defines security problems of the TOE.

3.1 Threats

Threats to the TOE are described in Table 3.1. Each of them assumes attackers who possess the basic attack potential.

Table 3.1: 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 is not allowed to access the MFD reads or modifies the address book data in the MFD all at one time through the internal network.
T.SPOOF	An attacker who impersonates other user reads and leaks the image data that the user has saved as confidential file from the operation panel or through the internal network.
T.TAMPER	An attacker who impersonates an administrator reads or modifies the network settings data from the operation panel or through the internal network.
T.TAP	An attacker wiretaps user data on the internal network when a proper user communicates with the MFD.

3.2 Organisational Security Policies

Organisational security policies are described in Table 3.2.

Table 3.2: Organisational Security Policies

Identifier	Definition
P.RESIDUAL	Upon completion or cancellation of a job, the area in the MSD where the user data has been spooled shall be overwritten one or more times. When a user deletes a job or file, the area in the MSD which stores the user data shall be overwritten one or more times. When the MFD is disposed of or its ownership changes, all the user data areas in the MSD shall be overwritten one or more times.
P.FAXTONET	Accesses through the telephone line connected to the MFD's fax I/F shall be prevented from accessing the internal network through the MFD's network I/F.

3.3 Assumptions

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

Table 3.3: Assumptions

Identifier	Definition
A.NETWORK	The TOE-installed 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.

4 Security Objectives

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

4.1 Security Objectives for the TOE

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

Table 4.1: Security Objectives for the TOE

Identifier	Definition
O.FILTER	The TOE shall provide means for rejecting attempts to access the MFD from any devices that unauthorized users use via the network.
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 into the MSD.
O.RESIDUAL	The TOE shall overwrite the user data area spooled into the MSD one or more times when a job is finished or cancelled. The TOE shall overwrite a specific user data area in the MSD one or more times when the user deletes a file. The TOE shall provide the function to overwrite all the user data areas in the MSD one or more times when the administrator operates to overwrite.
O.TRP	The TOE shall provide the function that protects the user data on the internal network from being wiretapped.
O.USER	The TOE shall provide the function that identifies and authenticates the proper user that stored the confidential file.
O.FAXTONET	The TOE shall prevent accesses through the telephone line connected to the MFD's fax I/F from accessing the internal network through the MFD's network I/F.

4.2 Security Objectives for the Operational Environment

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

Table 4.2: Security Objectives for the Environment

Identifier	Definition
OE.CIPHER	When the user of the MFD communicates with the TOE, the administrator shall take necessary steps (examples are as follows.) to protect the communication data between the MFD user and the TOE from wiretapping on the internal network where the TOE is installed. ● The SSL, IPsec and SNMP v3 functions of the TOE shall be used; the administrator shall make sure that the users of the TOE and MFD use software supporting the function. The administrator shall also configure the TOE to perform the functions defined in O.TRP. ● Communication devices (such as routers and switches) with cryptographic functions shall be used. ● The administrator shall provide physical protection (such as restricted areas) to the network. ● The administrator shall make the MFD users use USB memory device to input/output the data.
OE.ERASEALL	When the MFD is disposed of or its ownership changes, the administrator shall overwrite all the user data areas in the MSD one or more times using the TOE's function.
OE.FIREWALL	The administrator shall connect the internal network when the TOE is installed to the external network by using the communication device having the function to protect the internal network against attacking from external networks.
OE.OPERATE	Those in charge of the organisation shall understand the role of the administrator and select a suitable person with the utmost care.

Identifier	Definition
OE.PC-USER	On the devices allowed to connect to the MFD on the internal network, the administrator shall run the identification and authentication function (such as logging in the OS) so that only the proper MFD users be able to use such devices.
OE.SUBNET	The administrator shall connect only the devices that are allowed to communicate to the MFD in the subnetwork where the TOE is installed, and keep and maintain that state.
OE.USER	The administrator shall make the users of the TOE and the MFD maintain their confidential file password securely so that it will not leak.

4.3 Security Objectives Rationale

Table 4.3 demonstrates that the policies indicated in the security objectives are effective for the threats, organisational security policies and assumptions indicated in the security problem definition. Table 4.3 shows the sections of this document that provide the rationale for the correspondences of threats, organisational security policies and the assumptions.

Table 4.3: Security Objectives Rationale

Security problem / Security objective	T.RECOVER	T.REMOTE	T.SPOOF	T.TAMPER	T.TAP	P.RESIDUAL	P.FAXTONET	A.NETWORK	A.OPERATOR
O.FILTER		4.3.1.2							
O.MANAGE		4.3.1.2	4.3.1.3	4.3.1.4	4.3.1.5	4.3.2.1			
O.REMOVE	4.3.1.1								
O.RESIDUAL						4.3.2.1			
O.TRP					4.3.1.5				
O.USER			4.3.1.3						
O.FAXTONET							4.3.2.2		
OE.CIPHER					4.3.1.5				
OE.ERASEALL						4.3.2.1			
OE.FIREWALL								4.3.3.1	
OE.OPERATE									4.3.3.2
OE.PC-USER		4.3.1.2							
OE.SUBNET								4.3.3.1	
OE.USER			4.3.1.3						

4.3.1 Rationale Explaining Why Threats Are Countered

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

4.3.1.1 T.RECOVER

To counter T.RECOVER, the TOE encrypts user data using a unique cryptographic key for MFD before the data is written to the MSD, as defined in O.REMOVE. Therefore, the attacker possessing the basic attack potential cannot make out the data that is stored or remained after deleting in the MSD even if the attacker could read it out.

When the volatile memory is removed from the MFD, all the storage data in volatile memory disappears by intercepting the power distribution. There are no interfaces to read the data directly on the memory during the run of MFD, and it requires a high level of technology like specifying the data area and under transferring the data. Therefore, it is impossible for attacker possessing the basic attack potential to read

the data by attacking probes directly to the terminals or harness of MFD. For this reason the cryptographic key that is stored into the volatile memory cannot be read.

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

4.3.1.2 T.REMOTE

The followings counter T.REMOTE.

- According to O.FILTER, the TOE provides the method to deny accesses to the MFD from any devices that unauthorized users use via the network. This denies accesses to the MFD from unauthorized devices connected to the internal network while accepts accesses to the MFD from devices (including clients and servers) connected to the internal network with the intention to be used by proper users of the MFD (including the administrator).
- In support of the previous paragraph, as defined in O.MANAGE, the TOE provides the function to identify and authenticate the administrator who configures settings required for the operation of the TOE.
- Accesses to the MFD from the devices (including clients and servers) connected to the internal network with the intention to be used by proper users of the MFD (including the administrator) shall be permitted and are not subjected to the denial by O.FILTER. According to OE.PC-USER, an identification and authentication function (including logging in the OS) shall be required for devices allowed connections to the MFD and only authorized users shall use the devices. This prevents attackers from abusing the devices allowed connections to the MFD (those for proper users of the MFD) to access the address book data in the MFD (by impersonating proper users).

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

4.3.1.3 T.SPOOF

The followings counter T.SPOOF.

- The TOE provides the function that identifies and authenticates the proper user that stored the confidential file according to O.USER.
- In support of the previous paragraph, as defined in O.MANAGE, the TOE provides the function to identify and authenticate the administrator who configures settings required for the operation of the TOE.
- The confidential file password that is required for identifying and authenticating of the proper user that stored the confidential file shall be maintained safely not to be leaked. The administrator makes the users of the TOE and the MFD to follow OE.USER.

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

4.3.1.4 T.TAMPER

To counter T.TAMPER, the TOE provides the function to identify and authenticate the proper administrator according to O.MANAGE. Therefore, it is possible to protect the network settings data against reading or modifying from the operation panel or through the internal network by an attacker impersonating the administrator.

4.3.1.5 T.TAP

The followings counter T.TAP.

- The TOE provides the function that protects the user data on the internal network from being wiretapped according to O.TRP.
- In support of the previous paragraph, as defined in O.MANAGE, the TOE provides the function to identify and authenticate the administrator who configures settings required for the operation of the TOE.
- In the internal network where the TOE is installed, the administrator shall exercise due care (using the TSF according to O.TRP, or other protective means when the MFD is in an environment where the use

of the TSF is not suitable) of the communication data between the MFD user and the TOE not to be wiretapped, according to OE.CIPHER.

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

4.3.2 Rationale for Implementation of Organisational Security Policies

The following shows the rationale for all the organisational security policies to be implemented by achieving all the security objectives.

4.3.2.1 P.RESIDUAL

P.RESIDUAL can be achieved by the following objectives.

- Upon completion or cancellation of a job, the TOE overwrites the area in the MSD where the user data spooled one or more times according to O.RESIDUAL.
- According to O.RESIDUAL, the TOE overwrites a specific user data area in the MSD one or more times when the user deletes a file.
- When the MFD is disposed of or its ownership changes, the administrator overwrites all the 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 the user data areas in the MSD one or more times by the administrator's operation according to O.RESIDUAL.
- In support of the previous paragraph, as defined in O.MANAGE, the TOE provides the function to identify and authenticate the administrator who configures settings required for the operation of the TOE.

These objectives above can achieve P.RESIDUAL.

4.3.2.2 P.FAXTONET

To implement P.FAXTONET, as defined in O.FAXTONET, the TOE shall prevent accesses through the telephone line connected to the MFD's fax I/F from accessing the internal network through the MFD's network I/F. Thus, P.FAXTONET can be achieved.

4.3.3 Rationale for Satisfaction of Assumptions

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

4.3.3.1 A.NETWORK

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

4.3.3.2 A.OPERATOR

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

5 Extended Components Definition

This ST does not define any extended components.

6 Security Requirements

This chapter describes the security requirements.

6.1 Requirement Operations

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

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

6.2 Security Functional Requirements

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

6.2.1 Class FCS: Cryptographic Support

FCS_CKM.1a Cryptographic key generation a

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1a The TSF shall generate the cryptographic key in accordance with a specified cryptographic key generation algorithm [MSN-R2 expansion algorithm] and specified cryptographic key size [128 bits] that meet the following: [Data Security Kit Encryption Standard].

FCS_CKM.1b Cryptographic key generation b

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1b The TSF shall generate the cryptographic key in accordance with a specified cryptographic key generation algorithm [MSN-R2 expansion algorithm] and specified cryptographic key size [256 bits] that meet the following: [Data Security Kit Encryption Standard].

FCS_COP.1a Cryptographic operation a

Hierarchical to: No other components.

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

FCS_COP.1.1a The TSF shall perform [

- Encrypting the user data that will be written to the Flash memory
- Decrypting the user data that was read from the Flash memory

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

FCS_COP.1b Cryptographic operation b

Hierarchical to: No other components.

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

FCS_COP.1.1b The TSF shall perform [

- Encrypting the user data that will be written to the HDD
- Encrypting the TFS data that will be written to the HDD
- Decrypting the user data that was read from the HDD
- Decrypting the TFS data that was read from the HDD

] in accordance with a specified cryptographic algorithm [Rijndael Algorithm] and cryptographic key size [256 bits] that meet the following: [FIPS PUB 197].

6.2.2 Class FDP: User Data Protection

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [fax information flow control SFP] on [

- Subject: reception at the fax I/F from the fax line and transmission from the network I/F to the internal network
- Information: data received at the fax I/F from the fax line
- Operation: relay from the fax I/F to the network I/F

].

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attributes initialization

FDP_IFF.1.1 The TSF shall enforce the [fax information flow control SFP] based on the following types of subjects and information security attributes: [

- Reception at the fax I/F from the fax line (subject): No security attributes
- Transmission from the network I/F to the internal network (subject): No security attributes
- Communication data received from the fax line (information): No security attributes

]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [Never permits].

FDP_IFF.1.3 The TSF shall enforce the [None (additional information flow control SFP rules)].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [None].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [None].

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

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 on the HDD
- The filing image data file on the HDD
- The address book data file on the HDD
- The jobs completed list data file on the HDD
- The spool image data file in the Flash memory

].

6.2.3 Class FIA: Identification and Authentication

FIA_AFL.1a Authentication failure handling a

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1a 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.1.2a When the defined number of unsuccessful authentication attempts has been *[met]*, the TSF shall [

- Unsuccessful authentication reached three times: Reception of authentication trials stops for five minutes.
- Five minutes later after stopping: the number of times authentication was unsuccessful is cleared, and the reception of authentication trials is recovered

].

FIA_AFL.1b Authentication failure handling b

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1b 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 the confidential file].

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

- Unsuccessful authentication reached three times: Reception of authentication trials stops and the confidential file is locked
- Release operation of the confidential file by the administrator: the number of times authentication was unsuccessful is cleared, and the reception of authentication trials is recovered

].

FIA_SOS.1a Verification of secrets a

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1a The TSF shall provide a mechanism to verify that **the administrator password** (secrets) **meets** (meet) [5 to 32 alphanumeric and/or symbol characters, i.e., all the 95 characters of

No. 32 through No.126 specified by ISO/IEC 646 coded character set for information interchange].

FIA_SOS.1b Verification of secrets b

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FIA_UAU.2a User authentication before any action a

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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

FIA_UAU.2b User authentication before any action b

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1b 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.

FIA_UAU.7a Protected authentication feedback a

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1a 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.

FIA_UAU.7b Protected authentication feedback b

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1b 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** is in progress.

FIA_UID.2a User identification before any action a

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

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

FIA_UID.2b User identification before any action b

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

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

6.2.4 Class FMT: Security Management

FMT_MOF.1a Management of security functions behaviour a

Hierarchical to: No other components.

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

FMT_MOF.1.1a 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 and Clear All Data in Job Status Jobs Completed List] to [administrator].

FMT_MOF.1b Management of security functions behaviour b

Hierarchical to: No other components.

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

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

FMT_MOF.1c Management of security functions behaviour c

Hierarchical to: No other components.

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

FMT_MOF.1.1c The TSF shall restrict the ability to *[modify the behaviour of]* the functions [Clear Document Filing Data, Power Up Auto Clear, Document Filing and Network Protection] to [administrator].

FMT_MTD.1a Management of TSF data a

Hierarchical to: No other components.

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

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

FMT_MTD.1b Management of TSF data b

Hierarchical to: No other components.

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

FMT_MTD.1.1b The TSF shall restrict the ability to *[modify,* [create (*other operations*)]*]* the [confidential file password] to [the user that stored the confidential file].

FMT_MTD.1c Management of TSF data c

Hierarchical to: No other components.

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

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

- IP address filter
- MAC address filter
- SSL Settings
- IPsec Settings
- SNMP 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].

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [
- Enable and Disable “Clear All Memory”
- Enable and 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”
- Lock releasing “confidential files”
- Modify “the administrator password”
- Modify “confidential file passwords”
- 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 SSL-protected services
- Query and Modify “IPsec Settings”
- Query and Modify “SNMP Settings”

]

Note: Consideration for management requirement is described in Section 6.4.1.9.

FMT_SMR.1a Security roles a

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1a The TSF shall maintain the roles [administrator].

FMT_SMR.1.2a The TSF shall be able to associate users with roles.

FMT_SMR.1b Security roles b

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1b The TSF shall maintain the roles [each user that stored a confidential file].

FMT_SMR.1.2b The TSF shall be able to associate users with roles.

6.2.5 Class FTA: TOE Access

FTA_TSE.1 TOE session establishment

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [IP address and MAC address].

6.2.6 Class FTP: Trusted Path/Channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured

identification of its end points and protection of the channel data from **disclosure** (modification or disclosure).

FTP_ITC.1.2 The TSF shall permit *[the TSF]* to initiate communication via **IPsec** (the trusted channel).

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [
- Pull print function of the printer function
- Scanner function

].

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

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 *[disclosure]*.

FTP_TRP.1.2 The TSF shall permit *[remote users]* to initiate communication via **HTTPS, IPP-SSL, IPsec and SNMPv3** (the trusted path).

FTP_TRP.1.3 The TSF shall require the use of the trusted path for *[*[
- Administrator authentication, manipulation of confidential files, reading out the address book data, modification of the address book, filter setting and network settings via the TOE Web
- Image data reception from the printer driver in the printer function
- Image data reception for push print of the printer function
- MFD remote management based on the MIB

(*other services for which a trusted path is required*)]*]*.

6.3 Security Assurance Requirements

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

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

  - ASE_TSS.1 — TOE summary specification
- Class ATE: Tests
  - ATE_COV.2 — Analysis of coverage
  - ATE_DPT.1 — Testing: basic design
  - ATE_FUN.1 — Functional testing
  - ATE_IND.2 — Independent testing - sample
- Class AVA: Vulnerability assessment
  - AVA_VAN.2 — Vulnerability analysis

6.4 Security Requirements Rationale

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

6.4.1 Security Functional Requirements Rationale

The correspondences between security functional requirements and security objectives are shown in Table 6.1. Table 6.1 shows the sections that provide the rationale for the correspondences between the security functional requirements and the security objectives.

Table 6.1: Security Functional Requirements Rationale

Objective / Requirement	O.FILTER	O.MANAGE	O.REMOVE	O.RESIDUAL	O.TRP	O.USER	O.FAXTONET
FCS_CKM.1a			6.4.1.3				
FCS_CKM.1b			6.4.1.3				
FCS_COP.1a			6.4.1.3				
FCS_COP.1b			6.4.1.3				
FDP_IFC.1							6.4.1.7
FDP_IFF.1							6.4.1.7
FDP_RIP.1				6.4.1.4			
FIA_AFL.1a		6.4.1.2					
FIA_AFL.1b						6.4.1.6	
FIA_SOS.1a		6.4.1.2					
FIA_SOS.1b						6.4.1.6	
FIA_UAU.2a		6.4.1.2					
FIA_UAU.2b						6.4.1.6	
FIA_UAU.7a		6.4.1.2					
FIA_UAU.7b						6.4.1.6	
FIA_UID.2a		6.4.1.2					
FIA_UID.2b						6.4.1.6	
FMT_MOF.1a				6.4.1.4			
FMT_MOF.1b				6.4.1.4			
FMT_MOF.1c				6.4.1.4	6.4.1.5	6.4.1.6	
FMT_MTD.1a		6.4.1.2					
FMT_MTD.1b						6.4.1.6	
FMT_MTD.1c	6.4.1.1			6.4.1.4	6.4.1.5	6.4.1.6	
FMT_SMF.1	6.4.1.1	6.4.1.2		6.4.1.4	6.4.1.5	6.4.1.6	
FMT_SMR.1a		6.4.1.2					
FMT_SMR.1b						6.4.1.6	
FTA_TSE.1	6.4.1.1						
FTP_ITC.1					6.4.1.5		
FTP_TRP.1					6.4.1.5		

6.4.1.1 O.FILTER

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

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

FMT_SMF.1 and FMT_MTD.1c provide the management of FTA_TSE.1 consistently and do not conflict among them.

As explained above, functional requirements do not conflict to meet O.FILTER.

6.4.1.2 O.MANAGE

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

a) The administrator is identified and authenticated by FIA_AFL.1a, FIA_UAU.2a, FIA_UAU.7a and FIA_UID.2a.

b) The TOE provides the capability to modify the administrator password that is required for authentication of the administrator described above according to FMT_SMF.1.

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

d) The capability to modify the administrator password that is the TSF data to achive O.MANAGE is restricted to the administrator by FMT_MTD.1a.

e) The role of the administrator is maintained and the administrator is associated with the roles by FMT_SMR.1a.

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

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

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

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

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

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

6.4.1.3 O.REMOVE

The intent of O.REMOVE is to counter T.RECOVER; to prevent the user data stored into the MSD from being regenerated even if the MSD is removed from the MFD. This can be met by the combination of the functional requirements as follows.

- According to FCS_COP.1a and FCS_COP.1b, the user data to be written to the MSD is encrypted. Therefore, even if the MSD is connected to a device which is not the MFD having originally stored the data into the MSD, the encryption protects the data from being regenerated.
- FCS_CKM.1a and FCS_CKM.1b generate the cryptographic key that satisfy each of FCS_COP.1a and FCS_COP.1b.

FCS_COP.1a and FCS_CKM.1a depend mutually in cryptographic operation for the Flash memory. FCS_COP.1b and FCS_CKM.1b depend mutually in cryptographic operation for the HDD. Between the Flash memory and the HDD, there are no causes of conflicts. Thus, functional requirement do not conflict to meet O.REMOVE as above.

6.4.1.4 O.RESIDUAL

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

a) FDP_RIP.1 requires overwriting the following objects' area one or more times upon the deallocation of the resource from the following objects.
   - The target objects are the spool image data file on the HDD, filing image data file on the HDD, address book data file on the HDD, jobs completed list data file on the HDD and the spool image data file in the Flash memory.
   - The resource from these objects is deallocated when the jobs are completed or cancelled, the user deletes the confidential file and the specific data clear program is invoked by the operation made by the administrator.
   - Specific data clear programs described in the previous paragraph include 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.

b) According to FMT_SMF.1, the management capability defined in FDP_RIP.1 is provided.

c) In each of the following functional requirements, the management capability defined in FDP_RIP.1 is restricted to the administrator.
   - According to FMT_MOF.1a, the capability is restricted to the administrator to enable each of the functions of 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 included in the TSF relating to FDP_RIP.1.
   - According to FMT_MOF.1b, the capability is restricted to the administrator to disable each of the functions of Clear All Memory, Clear Document Filing Data and Power Up Auto Clear included in the TSF relating to FDP_RIP.1.
   - According to FMT_MOF.1c, the capability is restricted to the administrator to modify the behaviour of each of the functions of Clear Document Filing Data and Power Up Auto Clear included in the TSF relating to FDP_RIP.1.
   - According to FMT_MTD.1c, the capability is restricted to the administrator to query or modify the TSF data relating to FDP_RIP.1: 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.

Conflict does not occur in c) because each functional requirement in c) is independent. Conflict does not occur in b) and c) because b) and c) defines the management of a) mutually and supplementary.

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

6.4.1.5 O.TRP

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

- The combination of FTP_ITC.1 and FTP_TRP.1 provides the function to protect user data over the internal network from wiretapping.
- The capability to modify the behaviour of the TSF defined by FTP_ITC.1 and FTP_TRP.1, that is, Network Protection function is restricted to the administrator by FMT_MOF.1c.
- The capability to query or modify the TSF data relating to FTP_ ITC.1 and FTP _TRP.1, that is, the SSL Settings, IPsec Settings and SNMP Settings is restricted to the administrator by FMT_MTD.1c.
- Operation and management can be implemented as FMT_SMF.1 requires.

Conflict does not occur between the above FMT_MOF.1c, FMT_MTD.1c and FMT_SMF.1 because they define the management of FTP_ITC.1 and FTP_TRP.1 mutually and complementary. FTP_TRP.1 defines requirements for the communication service provided by the TOE for remote users. FTP_ITC.1 defines requirements for the communication function provided by the TOE between remote trusted IT products and local users. These two are independent and does not conflict with each other. Thus, these functional requirements do not conflict to meet O.TRP.

6.4.1.6 O.USER

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

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

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

c) The capability to modify the behaviour of the Document Filing function (including the confidential file function) which implements O.USER is restricted to the administrator by FMT_MOF.1c.

d) The capability to modify a confidential file password is restricted to the user that stored the confidential file by FMT_MTD.1b.

e) The capability to manage the behaviour of TSF for improving the effectiveness of protection obtained by using the confidential file, that is , to query or modify Disabling of Documetn Filing and Disabling of Print Jobs other Than Print Hold Job is restricted to the adinistrator by FMT_MTD.1c.

f) The role of the user that stored a confidential file is maintained and the user that stored a confidential file is associated with the role by FMT_SMR.1b.

g) Management and operation of confidential passwords are implemented as FMT_SMF.1 requires.

h) The capability to release the lock of confidential files is restricted to the administrator by FIA_AFL.1b.

a) is related to the event about the identification and authentication of the user that stored a confidential file. b), d) and g) are related to the event about the modification of confidential file passwords. c), e) and h) are related to the event about the management by the administrator. These three events occur independently of each other, and do not conflict mutually.

Conflict does not occur in a) because the four functional requirements in a) affect mutually and supplementary to achieve the identification and authentication of the user that stored a confidential file. Conflict does not occur in b), d) and g) because the three functional requirements in b), d) and g) affect mutually and supplementary to achieve the modification of confidential file passwords. Conflict does not occur in c), e) and h) because the three functional requirements in a), e) and h) affect mutually and supplementary to achieve management by the administrator. Conflict does not occur in f) because this functional requirement is depended on by d) and supported by a).

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

6.4.1.7 O.FAXTONET

O.FAXTONET can be met by the combination of functional requirements of FDP_IFC.1 and FDP_IFF.1

These two functional requirements implements a data flow control that never allows the data received from the fax line to be relayed to the internal network. This prevents accesses from the telephone line connected to the MFD's fax I/F from being relayed to the internal network through the MFD's networkI/F.

Conflict does not occur in the two functional requirements which meet O.FAXTONET, because they depend on each other.

6.4.1.8 Rationale for consistency of the entire security functional requirements

As described in Sections 6.4.1.1 through 6.4.1.7, conflict does not occur between each of the security functional requirements which implement the TOE security objectives, eliminating any inconsistency. Furthermore, as shown in Table 4.1, each of the TOE security objectives is independent and does not conflict with each other; no conflict occurs between the TOE security objectives and they are consistent.

Thus, no conflict occurs among the whole security functional requirements which meet the TOE security objectives and the entire security functional requirements are consistent.

6.4.1.9 Rationale for consistency of the TOE security management function

Some of the TOE security functional requirements require the security management function. CC Part 2 suggests the management activities foreseen to each functional component as the management requirements of each component.

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

Thus, the TOE security requirements are internally consistent in terms of security management functions.

Table 6.2: Management Functions of the TOE

Management Function Origin	Management Function required	Consideration for management requirement
FCS_CKM.1a	—	(No management requirements)
FCS_CKM.1b	—	(No management requirements)
FCS_COP.1a	—	(No management requirements)
FCS_COP.1b	—	(No management requirements)
FDP_IFC.1	—	(No management requirements)
FDP_IFF.1	—	No attributes.
FDP_RIP.1	• Enable and Disable “Clear All Memory” • Enable and 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 deallocation.
FIA_AFL.1a	—	The threshold and action are fixed.
FIA_AFL.1b	• Lock releasing “confidential files”	The threshold and action are fixed.
FIA_SOS.1a	—	The quality metric is fixed.
FIA_SOS.1b	—	The quality metric is fixed.
FIA_UAU.2a	• Modify “the administrator password”	Management Function required agrees with management requirement.
FIA_UAU.2b	• Modify “confidential file passwords” • 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.7a	—	(No management requirements)
FIA_UAU.7b	—	(No management requirements)
FIA_UID.2a	—	Identification of the administrator is fixed.
FIA_UID.2b	—	Identification of each user that stored a confidential file is fixed.
FMT_MOF.1a	—	No role groups
FMT_MOF.1b	—	No role groups
FMT_MOF.1c	—	No role groups
FMT_MTD.1a	—	No role groups
FMT_MTD.1b	—	No role groups
FMT_MTD.1c	—	No role groups
FMT_SMF.1	—	(No management requirements)
FMT_SMR.1a	—	No user groups
FMT_SMR.1b	—	No user groups
FTA_TSE.1	• Manage “IP address filter” and “MAC address filter”	Management Function required agrees with management requirement.
FTP_ITC.1	• Query and Modify “IPsec Settings”	Management Function required agrees with management requirement.
FTP_TRP.1	• Manage SSL-protected services • Query and Modify “IPsec Settings” • Query and Modify “SNMP Settings”	Management Function required agrees with management requirement.

6.4.1.10 Rationale for security functional requirement dependencies

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

Table 6.3: Security Functional Requirement Dependencies

Dependencies Requirement	Stipulated	Satisfied	Unsatisfied	Justification
FCS_CKM.1a	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1a	FCS_CKM.4	J1
FCS_CKM.1b	The same as the above	FCS_COP.1b	FCS_CKM.4	J1
FCS_COP.1a	[FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1a	FCS_CKM.4	J1
FCS_COP.1b	The same as the above	FCS_CKM.1b	FCS_CKM.4	J1
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1	—	—
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1	FMT_MSA.3	J2
FDP_RIP.1	—	—	—	—
FIA_AFL.1a	FIA_UAU.1 *	FIA_UAU.2a	—	—
FIA_AFL.1b	FIA_UAU.1 *	FIA_UAU.2b	—	—
FIA_SOS.1a	—	—	—	—
FIA_SOS.1b	—	—	—	—
FIA_UAU.2a	FIA_UID.1 *	FIA_UID.2a	—	—
FIA_UAU.2b	FIA_UID.1 *	FIA_UID.2b	—	—
FIA_UAU.7a	FIA_UAU.1 *	FIA_UAU.2a	—	—
FIA_UAU.7b	FIA_UAU.1 *	FIA_UAU.2b	—	—
FIA_UID.2a	—	—	—	—
FIA_UID.2b	—	—	—	—
FMT_MOF.1a	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1a	—	—
FMT_MOF.1b	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1a	—	—
FMT_MOF.1c	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1a	—	—
FMT_MTD.1a	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1a	—	—
FMT_MTD.1b	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1b	—	—
FMT_MTD.1c	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1a	—	—
FMT_SMF.1	—	—	—	—
FMT_SMR.1a	FIA_UID.1 *	FIA_UID.2a	—	—
FMT_SMR.1b	FIA_UID.1 *	FIA_UID.2b	—	—
FTA_TSE.1	—	—	—	—
FTP_ITC.1	—	—	—	—
FTP_TRP.1	—	—	—	—

Table 6.4: Justification of Unsatisfied SFR Dependencies

	Unsatisfied	Justification Rationale
J1	FCS_CKM.4	The cryptographic key is stored into 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 need to implement the TSF that performs the standard key destruction method, and FCS_CKM.4 is not required to specify standards.
J2	FMT_MSA.3	Fax information flow control SFP never permits the target information flow. Therefore, security attributes need not to be dealt with in implementing SFP; FMT_MSA.3 is not required which defines the default values of the security attributes.

6.4.2 Security Assurance Requirements Rationale

The TOE is a part of the MFD and an optional product for the MFD that is sold separately, which is a commercial product. The major threat is an attacker with the basic attack potential who may read and leak the information in the MSD of the MFD by a physical means such as using a device other than the MFD. Therefore, the Evaluation Assurance Level of the TOE is EAL 3 which is sufficient for commercial products.

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

7 TOE Summary Specification

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

Table 7.1: Security Functional Requirements and TOE Security Specifications

Function / Functional Requirement	TSF_FKG	TSF_FDE	TSF_FDC	TSF_AUT	TSF_FCF	TSF_FNP	TSF_FFL
FCS_CKM.1a	7.1						
FCS_CKM.1b	7.1						
FCS_COP.1a		7.2					
FCS_COP.1b		7.2					
FDP_IFC.1							7.7
FDP_IFF.1							7.7
FDP_RIP.1			7.3				
FIA_AFL.1a			7.3	7.4		7.6	
FIA_AFL.1b					7.5		
FIA_SOS.1a				7.4			
FIA_SOS.1b					7.5		
FIA_UAU.2a			7.3	7.4		7.6	
FIA_UAU.2b					7.5		
FIA_UAU.7a			7.3	7.4		7.6	
FIA_UAU.7b					7.5		
FIA_UID.2a			7.3	7.4		7.6	
FIA_UID.2b					7.5		
FMT_MOF.1a			7.3				
FMT_MOF.1b			7.3				
FMT_MOF.1c			7.3		7.5	7.6	
FMT_MTD.1a				7.4			
FMT_MTD.1b					7.5		
FMT_MTD.1c			7.3		7.5	7.6	
FMT_SMF.1			7.3	7.4	7.5	7.6	
FMT_SMR.1a				7.4			
FMT_SMR.1b					7.5		
FTA_TSE.1						7.6	
FTP_ITC.1						7.6	
FTP_TRP.1						7.6	

7.1 Cryptographic Key Generation (TSF_FKG)

This TOE generates cryptographic keys (common key) to support the cryptographic operation function for user data and TSF data. The cryptographic keys (common key) are generated every time the MFD is powered on.

The TOE generates 128-bit and 256-bit secure keys using the MSN-R2 expansion algorithm and stores the keys into the volatile memory to use them for the AES Rijndael, a cryptographic algorithm. The MSN-R2 expansion algorithm is an algorithm for generating cryptographic keys which conform to the Data Security Kit Encryption Standard. Therefore, the TOE satisfies FCS_CKM.1and FCS_CKM.1b.

7.2 Cryptographic Operation (TSF_FDE)

The TSF always encrypts user data and TSF data before writing them to the MSD. When necessary, the TSF reads the data from the MSD and decrypts them for further use.

The following user data are the targets of cryptographic operation:

- Image data spooled into the HDD
- Image data spooled into the Flash memory
- Image data stored into the HDD
- Address book data on the HDD
- Jobs completed list data on the HDD

The following TSF data are the target of cryptographic operation:

- Confidential file passwords on the HDD
- Administrator password on the HDD

For encryption and decryption of the user data in the Flash memory above, 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. Therefore, the TOE satisfies FCS_COP.1a.

For encryption and decryption of the user data and the TSF data on the HDD above, the 256 bits cryptographic key is used. Therefore, this TOE satisfies FCS_COP.1b.

7.3 Data Clear (TSF_FDC)

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

7.3.1 Overview of the Data Clear Function

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

The TOE provides data clear functions that clear image data files that are spooled or stored, the address book data file and the jobs completed list data file. Each of the following programs is contained in this function:

a) Auto Clear at Job End program

b) Clear All Memory program

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

d) Clear Document Filing Data program

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

f) Power Up Auto Clear program

Each of the above programs and their settings functions make up the TSF and correspond to the SFRs as follows.

- Each program overwrites the HDD one or more times with a random value and the Flash memory once with a fixed value. Each program disables regeneration of the information (such as image data) stored in the objects (such as image data files) by overwriting the objects. Thus, the TOE satisfies FDP_RIP.1.
- The TSF allows the administrator who has been identified and authenticated according to TSF_AUT to invoke the above b), c), d), e) and f) according to FMT_SMF.1 and FMT_MOF.1a.
- The above b), d) and f) have the cancel operation (Section 7.3.3) to stop in accordance with FMT_SMF.1 and satisfy FIA_AFL.1a, FIA_UAU.2a, FIA_UAU.7a and FIA_UID.2a in cooperation with TSF_AUT and TSF_FNP which are later discussed. The cancel operation requires the administrator to be identified and authenticated according to FIA_UID.2a and FIA_UAU.2a. For authentication, the protected feedback by FIA_UAU.7a and the failure handling by FIA_AFL.1a are provided. This allows only the administrator to cancel ongoing data clear programs as defined in FMT_MOF.1b.
- The TSF allows the administrator who has been identified and authenticated according to TSF_AUT to use settings functions (Section 7.3.8) according to FMT_SMF.1. This allows the TSF to satisfy FMT_MOF.1c and FMT_MTD.1c in cooperation with TSF_FCF and TSF_FNP.

The following sections elaborate upon each program and settings.

7.3.2 Auto Clear at Job End program

This program overwrites the image data that has been:

- spooled into the HDD or the Flash memory in order to process a job, when the job is completed, and
- stored into the HDD using the document filing function (including the confidential file function) when the user deletes the data.

This program is always invoked at the specified timing in both cases and no means to disable this program is provided.

7.3.3 Clear All Memory program

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

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

This program does not clear the address book data.

This program can be cancelled. To cancel this program, the administrator is required to select a cancellation and then the TSF requires the administrator who has invoked the program to enter the administrator password. The cancel operation serves as identification of the administrator defined in FIA_UID.2a and entering the administrator password serves as authentication of the administrator defined in FIA_UAU.2a. While entering for authentication, the TOE shows as many asterisks as characters entered according to FIA_UAU.7a, however does not show the characters entered. The overwrite operation is only cancelled if entering for authentication is successful.

If an incorrect password is entered three times in a row in an authentication process required for cancelling the program, reception of further authentication attempts stops as defined in FIA_AFL.1a; the administrator password is locked. In five minutes after the locking, the program unlocks the administrator password automatically; the number of times authentication was unsuccessful is cleared, and the reception of authentication trials is recovered.

7.3.4 Clear Address Book Data and Registered Data in MFP program

This program is invoked by the administrator who has been identified and authenticated by TSF_AUT and overwrites the address book data on the HDD.

This program can not be cancelled because the program completes in a relatively short time.

7.3.5 Clear Document Filing Data program

This program is invoked by the administrator who has been identified and authenticated by TSF_AUT and overwrites image data on 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 on the HDD
- All of the filing image data on the HDD

This program can be cancelled the same way the Clear All Memory program can.

7.3.6 Clear All Data in Job Status Jobs Completed List program

This program is invoked from the operation panel by the administrator who has been identified and authenticated by TSF_AUT and overwrites the jobs completed list data on the HDD.

This program can not be cancelled because the program completes in a relatively short time.

7.3.7 Power Up Auto Clear program

This program overwrites data when the TOE is powered on, unless the TOE has any reserved scan jobs or fax send jobs or any fax/Internet fax receive jobs which are not yet printed out.

Whether this program is enabled or disabled, or this program is invoked or not, when the TOE is turned on varies depending on the settings set beforehand. The data to be cleared by this program also varies depending on the setting; either all the data that the Clear All Memory program covers or specified data on

the HDD. One or more kinds of data can be specified as the target, namely, spool image data, filing image data or jobs completed list data.

This program can be cancelled the same way the Clear All Memory program can.

7.3.8 Data Clearance Settings

This TSF provides the following configuration functions below for 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 is repeated using 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 is repeated using each of the Clear All Memory program, Clear Address Book Data and Registered Data in MFP program, Clear Document Filing Data program and Clear All Data in Job Status Jobs Completed List program. The default is 1.
- Power Up Auto Clear:
  accepts settings to specify data areas to be cleared using the Power Up Auto Clear program. The default is that Power Up Auto Clear program is disabled for every data (no data is specified).
  This program is the same as “the data areas to be cleared by Power Up Auto Clear” in FMT_MTD.1.1c.
- 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 is repeated using the Power Up Auto Clear program. The default is 1.

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

7.4 Authentication (TSF_AUT)

This TSF enforces the identification and authentication of the administrator by the administrator password. According to FMT_SMF.1 and FMT_MTD.1a, the TSF allows only the administrator who has been identified and authenticated by the TSF to modify the administrator password. According to FIA_SOS.1a, the TSF only accepts a password which is 5 to 32 characters consisting of any of the 95 characters of No. 32 through No.126 specified by ISO/IEC 646 coded character set for information interchange. An example is as follows. Note that the shape of each character depends on the environment:

- 52 alphabetic characters: `A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z`
- 10 numeric characters: `0 1 2 3 4 5 6 7 8 9`
- 33 symbolic characters: `! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ¥ ] ^ _ ` { | }` ~ and space.

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

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

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

When the administrator password is entered from the operation panel, this TSF, according to FIA_UAU.7a, shows as many asterisks 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 password is entered three times in a row in an authentication process of the administrator password, reception of further authentication attempts stops as defined in FIA_AFL.1a; the administrator password is locked. In five minutes after the locking, the function unlocks the administrator password automatically; the number of times authentication was unsuccessful is cleared, and the reception of authentication trials is recovered.

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

7.5 Confidential files (TSF_FCF)

When a user saves image data into 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 an interface for creating confidential files to each of the copier, printer driver, PC-fax and Scan to HDD and, according to FIA_SOS.1b, verifies that confidential file passwords meet the quality metric of 5 to 8 numeric characters.

This TSF provides functions to operate saved confidential files from the operation panel or via the TOE Web. According to FIA_UID.2b, the TSF identifies the user that stored a confidential file when the user selects his/her confidential file and, according to FIA_UAU.2b, provides the interface for file manipulation only when authentication is successful with the correct confidential file password. During the authentication, the TSF does not disclose any information other than the number of characters typed according to FIA_UAU.7b.

Whenever a user attempts some operation on his/her saved confidential file from the operation panel, the TSF requests the user to enter the confidential file password. This TSF shows as many asterisks as the characters entered, however does not show the characters themselves.

When a user attempts some operation on his/her saved confidential file via the TOE Web, this TSF specifies the input type as a password to the client when the confidential file password is entered. This requires the browser of the client to hide the characters that the user entered by replacing them with substitute characters.

If an incorrect confidential file password is entered three times in a row during the authentication before reusing a saved confidential file, the TSF stops accepting further authentication attempts and locks the file to prohibit any operations according to FIA_AFL.1b. 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 who has been identified and authenticated by TSF_AUT.

According to FMT_MTD.1b and FMT_SMF.1, this TSF allows only the user that stored a confidential file who has been identified and authenticated by the TSF to change the password, as one of the operations on a saved confidential file. According to FIA_SOS.1b, this TSF verifies the new confidential password meets the quality metric of 5 to 8 numeric characters.

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

This TSF provides the function to change 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. On the other hand, to change the property to Confidential, the TSF requires the user to set a confidential file password which meets the quality metric of 5 to 8 numeric characters, according to FIA_SOS.1b.

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

According to FMT_SMF.1, FMT_MOF.1c, FMT_MTD.1c and FIA_AFL.1b, this TSF provides the following management functions for the document filing function and allows the administrator whom TFS_AUT has identified and authenticated to execute them:

- Management functions for improving the effectiveness of protection obtained by using the confidential file:

- Disabling of Document Filing: disables each mode of saving for each job type. The default and recommended value is that the non-confidential mode (where files are saved without password protection) is disabled for all job types.
- Disabling of Print Jobs Other Than Print Hold Job: disables the job to print out on the spot from the printer driver. This function denies the job without Holding and holds the Hold job regardless the job is printed out or not. This function is recommended to use in the environment that has the high risk that the third person takes away the output paper.

- Management function for locking confidential files:
  - Release the lock of confidential files: releases the lock of confidential files which have been locked by the failure of the authentication for the confidential file password. This management function is provided as "*Release the Lock on File/Folder Manipulation*".

7.6 Network Protection Function (TSF_FNP)

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

7.6.1 Overview of Network Protection

Components of this TSF and their correspondences between SFRs are as follows.

This TSF consists of the following functions.

a) Filter function

b) Communication data protection function

c) Network settings protection

Each of the above components satisfies the SFRs as follows:

- The above a) satisfies FTA_TSE.1
- The above b) satisfies FTP_ITC.1 and FTP_TRP.1. In cooperation with TSF_FDC and TSF_FCF, it also satisfies FMT_MOF.1c.
- In cooperation with TSF_FDC and TFS_AUT, c) satisfies FIA_AFL.1a, FIA_UAU.2a, FIA_UAU.7a and FIA_UID.2a
- a), b), TSF_FDC and TSF_FCF cooperate to satisfy FMT_MTD.1c and FMT_SMF.1.

The following sections elaborate upon each function.

7.6.2 Filter Function

This function rejects attempts to communicate from parties who are not expected to do so according to the settings that the administrator configured beforehand based on IP addresses and MAC addresses. The TSF always cancels network packets from parties that do not meet the conditions and does not respond to or process them.

Up to 4 ranges of IP addresses can be specified and it can be set whether to allow or deny the ranges.

Up to 10 MAC addresses to allow communication can be specified.

The TSF satisfies FTA_TSE.1 because it rejects communication to and from an unintended third party based on the IP address and the MAC address. According to FMT_MTD.1c, the TSF allows only the administrator who has been identified and authenticated by TSF_AUT to query and modify TSF data i.e. the settings for the IP and MAC address filtering.

7.6.3 Communication Data Protection Function

This TSF provides the following communication data protection function.

- According to FTP_TRP.1, this function provides the HTTPS communication function to prevent wiretapping of communication data between the client and the TOE Web. HTTPS communication starts when the remote user accesses the TOE Web from the client browser and the communication is kept until disconnected.
- According to FTP_TRP.1, 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. IPP-SSL communication starts

when the remote user accesses the MFD by sending a print job by the printer driver from applications on the client and the communication is kept until disconnected.

- According to FTP_TRP.1, this function provides the SNMP v3 function to prevent wiretapping of the SNMP-based communication (MFD remote management based on the MIB) between the client and the TOE. The remote user sends a request from the SNMP manager on the client and the TOE responds to the request.
- According to FTP_ITC.1 and FTP_TRP.1, this function provides the IPsec function to prevent wiretapping of all the IP-based communication between the client and the TOE. This provides protection to the following communication in addition to those for the Web, printer driver and SNMP described above.
  - Communication for the local user to obtain image data in the FTP server or a shared folder using Pull-print function of the MFD. This is defined in FTP_ITC.1.
  - Communication for the local user to send image data using the scanner function of the MFD. This is defined in FTP_ITC.1.
  - Communication for the remote user to send image data to the MFD to use the Push-print function of the MFD. This is defined in FTP_TRP.1.

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

According to FMT_MTD.1c, the TSF allows only the administrator who has been identified and authenticated by TSF_AUT to query and modify the SSL Settings which are a collection of the settings relating to HTTPS communication and IPP-SSL communication (TSF data), the IPsec Settings which are the settings relating to IPsec communication and the SNMP Settings which are the settings relating to SNMP v3 communication.

By enabling or disabling each of HTTPS, IPP-SSL, IPsec and SNMP v3 communications, the behaviour of the network protection function can be changed. When any of HTTPS, IPP-SSL, IPsec or SNMP v3 communications is disabled, the network protection function behaves with those communications disabled. The TSF only allows the administrator who has been identified and authenticated by TSF_AUT to change the behaviour according to FMT_MOF.1c.

7.6.4 Network Settings Protection

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

7.7 Fax Flow Control (TSF_FFL)

According to FDP_IFC.1 and FDP_IFF.1, this TSF performs a data flow control that never allows data received from the fax line to be relayed to the internal network. This prevents accesses from the telephone line connected to the MFD's fax I/F from being relayed to the internal network through the MFD's network I/F.

8 Appendix

This chapter describes the definitions of terms.

8.1 Terminology

Terminology used in this ST is defined in Table 8.1.

Table 8.1: Terminology

Term	Definition
Administrator password	A password to protect special functions for the administrator including the security management functions which are important in operation and management of the TOE and MFD from being used by those other than the administrator.
Auto Clear at Job End	The function to overwrite image data of each job stored into some MSD of the MFD, invoked when a job is finished or cancelled and when a user deletes a saved data file.
Board	A printed circuit board on which components are mounted by soldering.
Clear Address Book Data and Registered Data in MFP	The function to overwrite address book data stored into the HDD. This function is invoked by the operation of the administrator.
Clear All Data in Job Status Jobs Completed List	The function to overwrite the jobs completed list data that is stored into the HDD. This function is invoked by the operation of the administrator.
Clear All Memory	The function to overwrite the all image data and job completed list data that are stored into 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 into 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 password protection (confidential file password) to prevent others from manipulating.
Confidential file password	The password to prevent others from reusing the confidential file without permission.
Controller board	The board that controls the whole MFD. This contains the microprocessor to execute firmware of the TOE, volatile memory, HDC, HDD and others.
Controller firmware	The firmware that controls the controller board in the MFD; It is contained in the ROM board and the HDD, which are implemented on the controller board.
Data file	In this document, objects consisting of allocated MSD resources to store information (including image data).
Data Security Kit Encryption Standard	Sharp Corporation's documentation intended for in-house use which defines the standards for an algorithm for cryptographic operation and generation of cryptographic keys used in the cryptographic operation for MFD's Data Security Kit.
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 jobs sent from a printer driver on the spot. Print jobs are denied and only hold jobs and print hold jobs are accepted; print hold jobs are only held without being printed out.
Document filing	The function that stores image data that the MFD handles into the HDD for users' later operations such as printing and transmission. This is also called "Filing" in this document.
Engine	A device that forms print images on receiver papers, with mechanism of paper feeding/ejection. Also called as "print engine" or "engine unit".
External network	A network, not the internal network of an organisation, which the organisation does not manage.
File manipulation	An operation to manipulate image data saved as a file.
Filing	Stands for "Document filing". This is also to store the image data by document filing function.
Firmware	The software that is embedded to the machines to control the machine's hardware. In this document, firmware especially indicates the controller firmware.

Term	Definition
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 a job sent from a printer driver using the document filing function.
Image data	Digital data, especially in this document, of two-dimensional image that each function of the MFD manages.
Internal network	The network that is inside the organisation and protected against the threat about security from any external networks.
IP address	A call sign, used for IP, to identify devices for communication.
IP address filter	A function to restrict devices for communication by determining to accept or not communication based on their IP addresses.
Job	The sequence from beginning to end of the use of an MFD function (copier, printer, scanner, fax reception, fax transmission, or PC-Fax). In addition, the instruction for a functional operation is sometimes called a job.
Jobs completed list	The record about the completed jobs, stored into the HDD of the MFD.
Lock	The function to stop accepting passwords if wrong passwords are entered in a row.
MAC address	A call sign, used for MAC, to identify devices of communication media.
MAC address filter	A function to restrict devices for communication by determining to accept or not communication based on their MAC addresses.
Memory	A memory device; in particular a semiconductor memory device.
MSN-R2 expansion algorithm	Sharp Corporation's original algorithm for generating cryptographic keys which is defined in Data Security Kit Encryption Standard.
Non-volatile memory	The memory device that retains its contents even when the power is turned off.
Operation panel	The user interface unit in front of the MFD. This contains the start key, numeric key, function key and liquid crystal display with touch operation system.
Power Up Auto Clear	The function to overwrite the data in the MSD when the MFD is powered on. This function is invoked when the MFD is powered on, according to the settings that are specified by the administrator beforehand.
Scan to HDD	One of the filing functions. It scans the original to obtain image data, and does only save a file of the image data into the HDD, while neither prints nor transmits it.
Scanner unit	The device that scans the original and gets the image data. This is used for copier, scanner, fax transmission or scan to HDD.
Spool	Storing the job's image data into 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 replaced with the TOE's controller firmware when TOE is installed.
Subnetwork	A part of internal network divided by router.
Tandem copy	Tandem print in the MFD's copier function.
Tandem print	The function to print a large job twice faster than usually by halving that job among two MFDs.
TWAIN	A technical standard for PC to be input image data from devices such as scanners.
Unit	A substance provided standard that can be attached to or detached from a printed circuit board; or an option that is installed and is ready for operation. This can also be a system that includes a mechanism and is ready for operation.
User that stored a confidential file	The user that saved the image data as a confidential file.
Volatile memory	A memory device, the contents of which vanish when the power is turned off.

8.2 Acronyms

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

Table 8.2: Acronyms in the CC

Acronym	Definition
CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

Table 8.3: Other Acronyms

Acronym	Definition
AES	Advanced Encryption Standard: established by NIST (National Institute of Standards and Technology, United States of America)
DSK	Data Security Kit MX-FR10: an optional product sold separately for the MFD, including the firmware part of the TOE.
EEPROM	Electrically Erasable Programmable ROM: a type of non-volatile memory that allows low frequency of electrical rewriting at any address.
HDC	Hard Disk Controller: the HDC in the MFD includes part of the TOE hardware.
HDD	Hard Disk Drive
HTTP	Hypertext Transfer Protocol: a communication protocol generally used for the Web.
HTTPS	HTTP over SSL: HTTP with protection of SSL.
I/F	Interface
IP	Internet Protocol: a communication protocol to divide data in packets to deliver it to the destination.
IPP	Internet Printing Protocol: a communication protocol for printing.
IPP-SSL	IPP over SSL: IPP with protection of SSL.
IPsec	Security Architecture for Internet Protocol: a communication protocol consisting of ensuring integrity and providing authentication mechanism using the AH (Authentication Header), data encryption using the ESP (Encapsulated Security Payload) and key exchange using the IKE (Internet Key Exchange protocol), protecting data from being tampered and maintaining confidentiality of data by the IP packet.
IT	Information Technology
LDAP	Lightweight Directory Access Protocol: a communication protocol for directory service.
MAC	Media Access Control: communication protocols to allow a number of communication devices to share a single communication medium by identifying devices and mediating communication to avoid collision.
MFD	Multi Function Device: a digital multifunctional device which is an office machine mainly equipped with copier, printer, scanner and fax functions. In this document, only models listed in Section 1.3.2.
MIB	Management Information Base: a virtual database used for managing information in controlling network devices remotely, required for the SNMP.
MSD	Mass Storage Device: in this document, this especially indicates the HDD and Flash memory in MFD.
NIC	Network Interface Card or Network Interface Controller
OS	Operating System
PC	Personal Computer
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.
SNMP	Simple Network Management Protocol: a communication protocol which manages network devices.
SNMP v3	SNMP version 3: the SNMP which performs functions for protecting SNMP packets transmitted on a network by authenticating and encrypting them from being wiretapped, spoofed, tampered or replayed.
WINS	Windows Internet Name Service: resolves a NetBIOS name into the IP address.