



Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2010-03-01 (ITC-0295)
Certification No.	C0281
Sponsor	Sharp Corporation
Name of TOE	MX-FR22
Version of TOE	C.10
PP Conformance	None
Assurance Package	EAL3
Developer	Sharp Corporation
Evaluation Facility	Information Technology Security Center Evaluation Department

This is to report that the evaluation result for the above TOE is certified as follows.

2011-01-28

Takumi Yamasato, Technical Manager
Information Security Certification Office
IT Security Center

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following criteria prescribed in the "IT Security Evaluation and Certification Scheme".

- Common Criteria for Information Technology Security Evaluation
Version 3.1 Release 3
- Common Methodology for Information Technology Security Evaluation
Version 3.1 Release 3

Evaluation Result: Pass

"MX-FR22 C.10" has been evaluated in accordance with the provision of the "IT Security Certification Procedure" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:

This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1. Executive Summary.....	5
1.1 Product Overview	5
1.1.1 Assurance Package	5
1.1.2 TOE and Security Functionality.....	5
1.1.2.1 Threats and Security Objectives	5
1.1.2.2 Configuration and Assumptions.....	6
1.1.3 Disclaimers	6
1.2 Conduct of Evaluation	6
1.3 Certification	6
2. Identification	7
3. Security Policy.....	8
3.1 Security Function Policies.....	8
3.1.1 Threats and Security Function Policies.....	8
3.1.1.1 Threats	8
3.1.1.2 Security Function Policies against Threats	9
3.1.2 Organisational Security Policies and Security Function Policies	11
3.1.2.1 Organisational Security Policies.....	11
3.1.2.2 Security Function Policies to Organisational Security Policies	12
4. Assumptions and Clarification of Scope	14
4.1 Usage Assumptions	14
4.2 Environment Assumptions.....	14
4.3 Clarification of scope	15
5. Architectural Information	16
5.1 TOE boundary and component	16
5.2 IT Environment	17
6. Documentation	18
7. Evaluation conducted by Evaluation Facility and results	19
7.1 Evaluation Approach	19
7.2 Overview of Evaluation Activity	19
7.3 IT Product Testing	20
7.3.1 Developer Testing.....	20
7.3.2 Evaluator Independent Testing.....	23
7.3.3 Evaluator Penetration Testing.....	25
7.4 Evaluated Configuration	28
7.5 Evaluation Results.....	28
7.6 Evaluator Comments/Recommendations	29
8. Certification.....	30
8.1 Certification Result.....	30

8.2 Recommendations 30

9. Annexes 31

10. Security Target 31

11. Glossary 32

12. Bibliography 35

1. Executive Summary

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "MX-FR22 C.10" (hereinafter referred to as "the TOE") developed by Sharp Corporation, and evaluation of the TOE was finished on 2011-01 by Information Technology Security Center Evaluation Department (hereinafter referred to as "Evaluation Facility"). It reports to the sponsor, Sharp Corporation and provides information to the users and system operators who are interested in this TOE.

The reader of the Certification Report is advised to read the Security Target (hereinafter referred to as "the ST") that is the appendix of this report together. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in ST.

This certification report assumes "the general consumers who purchase this TOE" to be a reader. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee individual IT product itself.

1.1 Product Overview

Overview of the TOE functions and operational conditions are as follows. Refer to and after Chapter 2 for details.

1.1.1 Assurance Package

Assurance Package of the TOE is EAL3.

1.1.2 TOE and Security Functionality

The TOE is an IT Product to protect data in a Multi Function Device (hereinafter referred to as "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.

The main security functions of the TOE are cryptographic operation function, data clear function, confidential files function, network protection function and fax flow control function, which are aiming to counter unauthorized attempts to steal image data in the MFD where the TOE is installed.

About these security functionalities, the validity of the design policy and the accuracy of the implementation were evaluated within the scope of the assurance package. The threats and the assumptions that this TOE assumes are described in the next section.

1.1.2.1 Threats and Security Objectives

This TOE assumes the following threats and provides the Security Functions to counter them.

Assets protected by the TOE: user data, such as image data stored into the MFD, address book and others, are assumed to be disclosed or altered illegally by the following threats: unauthorized operation of the TOE, direct data read-out from storage device, access to the communication data on the network or others.

To counter these threats, encryption of the data when it is stored into the HDD or the flash memory in the MFD prevents it from being read directly. The TOE also provides protection function using password when storing image data to prevent unauthorized user from accessing to it. In addition, the TOE provides protection function using encryption of network communication to prevent communication data from being wiretapped.

Regarding settings for security functions, identification and authentication function of the administrator prevents the settings from being altered and the security functions from being disabled.

1.1.2.2 Configuration and Assumptions

The evaluated product is assumed to be operated under the following configuration and assumptions.

This TOE runs on MFDs that Sharp Corporation provides.

The MFD that this TOE is installed assumes to be connected to the clients and the various servers and used in the internal network

When the internal network is connected to the external network, firewall is connected to deny access to the MFD from the external network.

1.1.3 Disclaimers

In the operation environment that the security function for protecting communication between the TOE and a client does not work, operator shall be responsible for performing an objective for protecting communication. For details, see Chapter 4.3.

1.2 Conduct of Evaluation

Evaluation Facility conducted IT security evaluation, and completed on 2011-01 based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme"[1], "IT Security Certification Procedure"[2], "Evaluation Facility Approval Procedure"[3] provided by Certification Body.

1.3 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Reports prepared by Evaluation Facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification oversight reviews are also prepared for those concerns found in the certification process. Those concerns pointed out by the Certification Body are fully resolved, and the Certification Body confirmed that the TOE evaluation is appropriately conducted in accordance with CC ([4][5][6] or [7][8][9]) and CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by Evaluation Facility and concluded fully certification activities.

2. Identification

The TOE is identified as follows:

Name of TOE	MX-FR22
Version of TOE	C.10
Developer	Sharp Corporation

The above TOE title is for an optional product to enhance the security functions of MFDs made by Sharp Corporation.

Users can confirm by taking the following steps whether a TOE product has been evaluated and certified.

Users can confirm that the installed product is the certified TOE by comparing the title and version displayed on the MFD with those in the guidance documents, following the instructions in the documents.

3. Security Policy

This chapter describes security function policies and organisational security policies.

The TOE provides the Security Functions to counter the unauthorised access to the image data in the MFD and to protect the communication data on the network.

For meeting the organisational security policies, the TOE provides the functions to overwrite data stored into the MFD and to prevent the unauthorised access through telephone lines via fax interface.

And for each setting that is relevant to the above mentioned Security Functions, only administrators are permitted to set configurations in order to prevent the deactivation and unauthorised use of the Security Functions.

3.1 Security Function Policies

The TOE possesses the security functions to counter the threats shown in Chapter 3.1.1 and to meet the organisational security policies shown in Chapter 3.1.2.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The TOE assumes the threats shown in Table 3-1 and provides the functions as countermeasures against them.

Table 3-1 Assumed Threats

Identifier	Threat
T.RECOVER	An attacker removes the MSD from the MFD and installs it in other devices (than the MFD where the MSD is originally installed) to read and leak the user data in the MSD.
T.REMOTE	An attacker who is not allowed to access to 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 communication data on the internal network when a proper user communicates with the MFD.
-------	---

3.1.1.2 Security Function Policies against Threats

The TOE counters the threats shown in Table 3-1 in accordance with the following security functional policies:

(1) Counter against the threat of "T.RECOVER"

This threat assumes that the residual data in the MSD might be leaked when the MSD is removed from the MFD. The security functions counter this threat as follows:

1. Cryptographic key generation function (TSF_FKG):

The function to generate cryptographic keys (common key) to support the cryptographic operation function (TSF_FDE). The TOE generates 128-bit and 256-bit secure keys every time the MFD is turned on and stores them into the volatile memory.

2. Cryptographic operation function (TSF_FDE)

This TSF always encrypts user data and TSF data before writing them to the MSD. When necessary, this TSF reads the data from the MSD and decrypts them for further use. For encryption and decryption, the AES algorithm based on FIPS PUB 197 and the cryptographic key that is generated by the cryptographic key generation function (TSF_FKG) are used.

The target user data is spool image data in the HDD and Flash memory, filing image data on the HDD and the address book data on the HDD. The target TSF data is confidential file passwords and the administrator password in the HDD.

(2) Counter against the threats of "T.REMOTE" and "T.TAP"

These threats assume that the address book data that the TOE manages might be accessed without authorization via the internal network and that the data transmitted to and from the client might be wiretapped and leaked. The security functions counter these threats as follows:

1. Network protection function (TSF_FNP):

This TSF provides the following three functions for the network protection.

a) 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 rejects 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.

b) Communication data protection function:

This TSF provides the following communication data protection function.

- The HTTPS communication function to prevent wiretapping of communication data between the client and the TOE Web.
- The IPP-SSL communication function to prevent wiretapping of print data that is

sent from the printer driver of the client.

The TSF allows only the administrator who has been identified and authenticated by the authentication function (TSF_AUT) to query and modify the settings above. By enabling or disabling each of the above communications, the behaviour of the network protection function can be changed.

c) Network Settings Protection Function

This function provides the interfaces to manage the network settings data on the operation panel and the TOE Web. These interfaces are provided only to the administrator to prevent other users from accessing.

(3) Counter against the threat of "T.TAMPER"

This threat assumes that the network settings data that the TOE manages might be accessed without authorization from the operation panel or via the internal network. The following security function counters the threat. Data transmitted from the client is protected by the communication data protection function of the network protection function (TSF_FNP).

1. Authentication (TSF_AUT):

This TSF enforces the identification and authentication of the administrator by the administrator password. The administrator password shall be 5 to 32 characters; 95 kinds of characters (52 alphabets, 10 numbers and 33 symbols) can be used. This function provides the interfaces of the function for the administrator when the authentication of the administrator is successful by the correct administrator password. When the administrator password is entered from the operation panel, the TSF shows as many asterisks as characters entered, however does not show the characters entered. When the administrator password is entered via the TOE Web, the TSF 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; 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.

By providing only the administrator with the management function to change (modify) the administrator password, the secure maintenance of the role is achieved.

(4) Counter against the threat of "T.SPOOF"

This threat assumes that image data stored as confidential files in the TOE might be accessed without authorization from the operation panel or via the internal network. The following security function (confidential file function) counters the threat by identifying and authenticating the authorized user that stored the confidential file. Confidential file passwords required for identification and authentication are protected by the communication data protection function of the network protection function (TSF_FNP) and the cryptographic operation function (TSF_FDE).

1. Confidential files function (TSF_FCF):

This TSF provides password protection to image data that a user stored as a confidential file in the MFD and allows operations (such as printing) after password authentication on the operation panel or via the web. The confidential file password shall be 5 to 8 numeric characters.

During the authentication before reusing a confidential file, the TSF hides the typed

characters. If an incorrect confidential file password is entered three times in a row, the TSF locks the file. 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 Authentication (TSF_AUT).

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

This TSF provides the following management functions for the document filing function. Only the administrator who has been identified and authenticated by Authentication (TSF_AUT) is allowed to execute these functions.

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

b) 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.

3.1.2 Organisational Security Policies and Security Function Policies

3.1.2.1 Organisational Security Policies

Organisational security policies required in use of the TOE are shown in Table 3-2.

Table 3-2 Organisational Security Policies

Identifier	Organisational Security Policy
P.RESIDUAL	<p>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.</p> <p>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.</p>

	When the MFD is disposed of or its ownership changes, all the user 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.

3.1.2.2 Security Function Policies to Organisational Security Policies

The TOE meets the organisational security policies shown in Table 3-2 by implementing the following security functions.

- (1) Enforcement of the organisational security policy of "P.RESIDUAL"
 "P.RESIDUAL" requires that the data stored in the MFD's HDD and Flash memory should be overwritten. This organisational security policy is enforced by the following security functions.

1. Data clear function (TSF_FDC)

The TOE provides data clear functions that clear image data files that are spooled or stored and the address book data file. These functions consist of the following functions. Each function disables regeneration of the image data by overwriting the HDD with a random value and the flash memory with a fixed value.

a) Auto Clear at Job End:

This TSF consist of the following functions of:

- When the job is completed or cancelled, overwriting image data that has been spooled into the HDD or the flash memory in order to process a job.
- When the user deletes the data, overwriting image data stored into the HDD using the document filing function (including the confidential file function).

b) Clear All Memory

This function is invoked from the operation panel by the administrator who has been identified and authenticated by the authentication function (TSF_AUT). The function overwrites all spool image data in the HDD and the flash memory.

This function can be cancelled. When the administrator selects a cancellation, the TSF requires the administrator to be identified and authenticated. Only when the authentication is successful, the function is cancelled. During an authentication, the TOE shows as many asterisks as characters entered in stead of the entered characters itself. If an incorrect password is entered three times in a row, reception of further authentication attempts stops; 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.

c) Clear Address Book Data and Registered Data in MFP

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

d) Clear Document Filing Data

This function 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 function is specified one or more from the following choices by the administrator when this function is invoked.

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

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

(2) Implementation of the organisational security policy of "P.FAXTONET"

"P.FAXTONET" requires that the TOE prevents accesses through the telephone line connected to the MFD's fax interface from accessing the internal network through the MFD's network interface. This organisational security policy is implemented by the following security functions.

1. Fax Flow Control (TSF_FDC)

This function 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 interface from being relayed to the internal network through the MFD's network interface.

4. Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environment to operate the TOE as useful information for the judgment before the assumed reader uses the TOE.

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE.

The effective performance of the TOE security functions is not assured unless these assumptions are satisfied.

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumptions
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 MFP 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.

4.2 Environment Assumptions

The TOE operates on MFD manufactured by Sharp Corporation, namely MX-M623, MX-M623N, MX-M623U, MX-M623UJ, MX-M753, MX-M753N, MX-M753U and MX-M753UJ.

The TOE-installed MFD shall be connected to an internal network where the clients and the servers are also connected and shall be connected to a telephone line required for fax. Figure 4-1 shows the general operational environment as assumptions of the TOE.

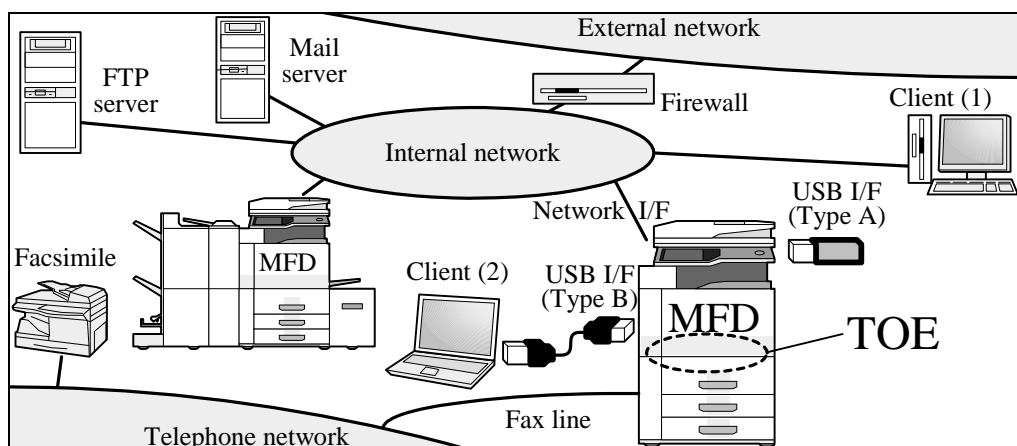


Figure 4-1 Usage Environment of the TOE

As shown in Figure 4-1, the TOE-installed MFD is connected to an internal network and a telephone line. The internal network connects the client and servers such as the FTP server and mail server as appropriate, allowing them to communicate with the TOE including sending print data.

The internal network can be connected to external networks through a firewall; the necessary settings shall be made to screen accesses to the MFD from external networks.

4.3 Clarification of scope

The TOE provides the security function (communication data protection function) to protect data transmitted to and from the client. However, when the function is disabled by the administrator or when a client on the network does not support the function, the manager of MFD's operation shall be responsible for taking measures such as installing an encryption device to protect the data to and from the client.

5. Architectural Information

This chapter explains the TOE's physical scope and logical configuration in term of their objectives and association.

5.1 TOE boundary and component

The physical scope of the TOE is shaded in Figure 5-1. Main part of the TOE is in the MFD's controller firmware and provided as "Data Security Kit MX-FR22 (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.

- 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 replace with two ROMs of the DSK.
- MAIN: is part of the controller firmware and installed from the USB memory device of DSK to the HDD in the MFD.
- HDC: is an integrated circuit part that is mounted on the controller board in the MFD beforehand.

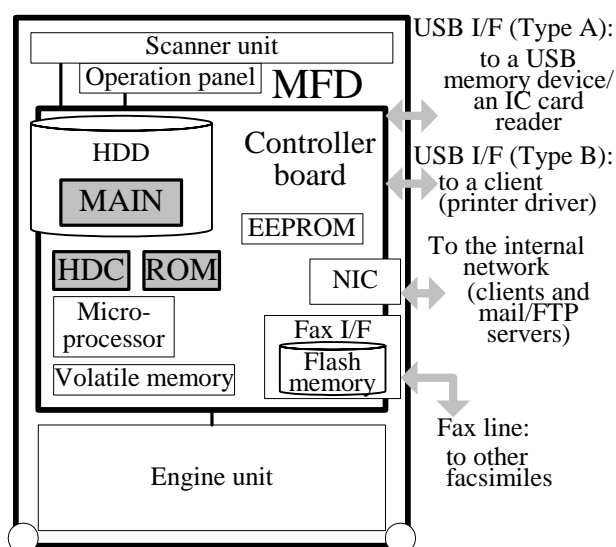


Figure 5-1 TOE boundary

Figure 5-2 shows the logical configuration of the TOE. The thick-lined frame indicates the logical scope of the TOE. Rounded boxes indicate hardware devices that are out of the TOE. Rectangles indicate functions of the TOE and ones shaded indicate security functions. Among the data in the volatile memory, HDD, Flash memory and EEPROM, the data that security functions handle (i.e. user data and TSF data) are also shaded. Arrows in the figure indicate data flows.

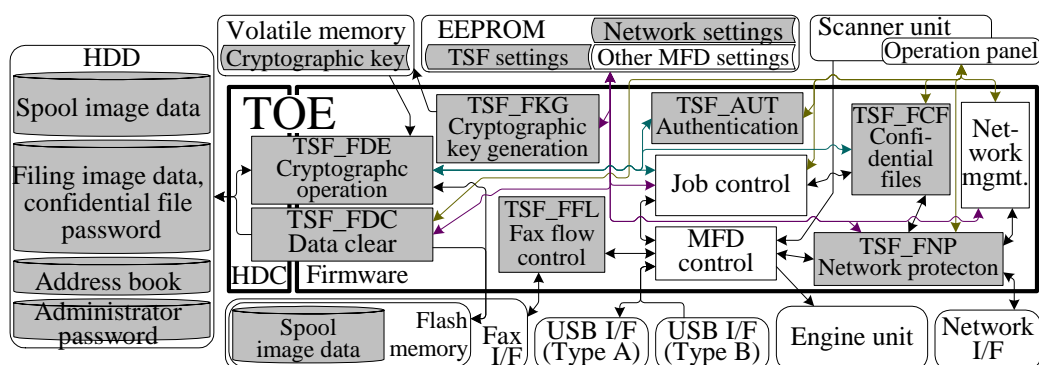


Figure 5-2 Logical configuration of the TOE

The main 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 (TSF) is implemented in the HDC and invoked by the TSF in the firmware. The security functions are as follows:

- a) Cryptographic operation function:
encrypts user data and TSF data to be stored into the MSD and decrypts user data and TSF data retrieved from the MSD.
- b) Cryptographic key generation function:
generates the cryptographic key for the cryptographic operation function.
- c) Data clear function:
overwrites the MSD to prevent information leakage from the MSD.
- d) Authentication function:
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:
provides password protection for image data in the MFD stored by the user to protect them from being reused by others.
- f) Network protection function:
prevents unauthorized accesses over the network, wiretapping of communication data and unauthorized of the network settings.
- g) 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.

5.2 IT Environment

The TOE is connected to the internal network and communicates with servers including the FTP server and the mail server and the client. It also communicates with clients connected through a USB port and fax machines connected through a fax line.

The clients on the internal network or connected through a USB port use the TOE via a printer driver or a web browser. The clients can operate via a web browser including making settings for the security functions.

6. Documentation

The identification of documents attached to the TOE is listed below.

TOE users are required fully understanding and complying with the following documents in order to satisfy the assumptions.

The version of each document is shown with [].

- MX-FR22 Data Security Kit Operation Manual [1.0]
(Japanese version and English version)

Operational manual that described usage and configuration of security functions.

- MX-FR22 Data Security Kit Notice [1.0]
(Japanese version and English version)

Notice that described requirement on secure operation and TOE installation guidance.

7. Evaluation conducted by Evaluation Facility and results

7.1 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance components in CC Part 3. Details for evaluation activities are reported in the Evaluation Technical Report. In the Evaluation Technical Report, it explains the summary of the TOE, the content of evaluation and verdict of each work unit.

7.2 Overview of Evaluation Activity

The history of evaluation conducted was present in the Evaluation Technical Report as follows.

Evaluation has started on 2010-03 and concluded by completion the Evaluation Technical Report dated 2011-01. The evaluator received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidences in relation to a series of evaluation conducted.

Additionally, the evaluator directly visited the development and manufacturing sites on 2010-10 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff interview.

Further, the evaluator executed the sampling check of the developer testing and the evaluator testing by using developer testing environment at developer site on 2010-10.

Concerns found in evaluation activities for each work unit were all issued as Observation Report and were reported to the developer. These concerns were reviewed by the developer and all concerns were solved eventually.

7.3 IT Product Testing

The evaluator confirmed the validity of the testing that the developer had executed. Based on the evidence shown by the process of the evaluation and those confirmed validity, the evaluator executed the reappearance testing, additional testing and penetration testing based on vulnerability assessments judged to be necessary.

7.3.1 Developer Testing

The evaluator evaluated the integrity of the developer testing that the developer executed and the testing documentation of actual testing results. A summary of the evaluated developer testing is as follows:

(1) Developer Testing Environment

Test configuration of the testing performed by the developer is showed in Figure 7-1 and Table 7-1.

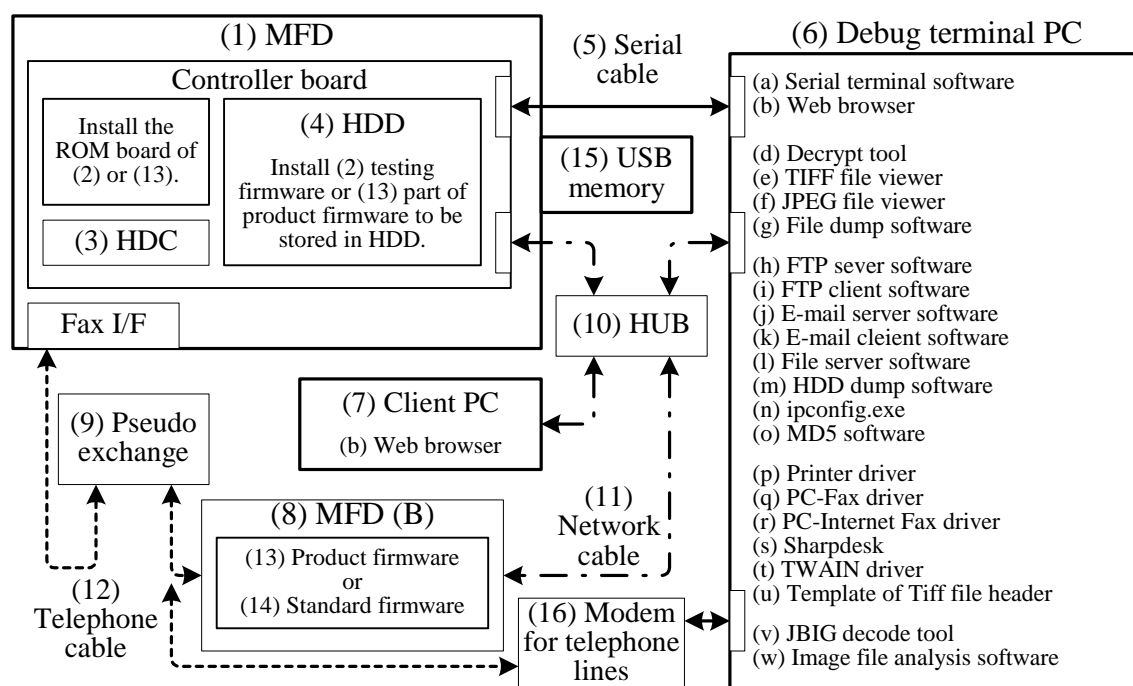


Figure 7-1 Configuration of the Developer Testing

Table 7-1 Main components

Name of Component	Description(Purpose of use)
MFD	An MFD where the TOE is installed.
Debug terminal PC	A computer where all the software used for the testing is installed.
Client PC	A computer used to test the filter function.

Pseudo exchange	A device to simulate a fax line (public line).
MFD(B)	An MFD used for tests that require two MFDs including fax and tandem printing.
Modem for telephone lines	A device that performs data communication via the public line.

The MFD used in the developer testing is one of the several MFDs identified in the ST, namely the MX-M753N. While the MFDs on which the TOE runs have different processing capabilities, the same TOE is used. Thus, the configuration of the testing environment is considered equivalent to that identified in the ST.

(2) Summary of Developer Testing

Summary of the developer testing is as follows.

(a) Developer Testing Outline

Outline of the developer testing is as follows.

<Developer Testing Approach>

Under the environment shown in Figure 7-1, either of the following two types of ROMs, the product ROM or the testing ROM, was used in compliance with the characteristics of each test. To confirm test results, the testing ROM was provided with the capability of outputting from a serial port, of outputting the cryptographic seed and keys, of enabling and disabling the cryptographic operation and of specifying data to be overwritten. However, the security functions to be tested were not affected.

The testing was conducted by stimulating interfaces including turning on/off the MFD, manual operations from the operation panel and those from the client as well as observing responses on the operation panel and on the debug terminal.

<Developer testing tools>

Tools used in the developer testing are shown in Table 7-2.

Table 7-2 Developer Testing Tools

	Name of Tool	Description
(a)	Serial terminal software	Terminal emulator software to operate the MFD via serial communication.
(b)	Web browser	HTTP-based client software to access the MFD's web server, enabling the user to operate the MFD and send print data to the MFD using the web print function (print function) of the MFD.
(d)	Decode tool	Software to decode data files encrypted by the MFD with any key.
(e)	TIFF file viewer	Image display software to display on a computer screen compressed images (JBIG and MMR) generated by the MFD.
(f)	JPEG file viewer	Image display software to display on a computer screen compressed images (JPEG) generated by the MFD.
(g)	File dump software	Software to display computer files in hex notation. It is also called binary editor.

	Name of Tool	Description
(h)	FTP server software	FTP server software which performs the Scan-to-FTP function (scan and send function) of the MFD and transfers data for debugging from the MFD over a network.
(i)	FTP client software	FTP client software to receive data transferred to the FTP server using the Scan-to-FTP function (scan and send function) of the MFD and to send print data to the MFD using the FTP Push-print function (print function).
(j)	E-mail server software	E-mail server software which performs the Scan-to-Email function and the InternetFax function (both are scan and send functions) of the MFD.
(k)	E-mail client software	E-mail client software to receive data transferred to the mail server using the Scan-to-Email function (scan and send function) of the MFD and to send print data to the MFD using the E-mail-print function (print function) of the MFD.
(l)	File server software	File server software which performs the Scan-to-SMB function (scan and send function) of the MFD. Used is the standard file sharing function of the OS installed in the debug terminal PC.
(m)	Disk dump software	Software to read any given sectors of the HDD, enabling displaying and editing them.
(n)	ipconfig.exe	Software to query or modify IP addresses and MAC addresses of the network interfaces of the clients through the command prompt.
(o)	MD5 software	Software to obtain a MD5 value of files or character strings through the command prompt.
(p)	Printer driver	Printer driver software which enables the client to send print data from client's applications and print it on the MFD. Used is the printer driver stored on the CD-ROM attached to the MFD or the printer expansion kit.
(q)	PC-Fax driver	PC-Fax driver software which performs PC-Fax, enabling the client to send fax data from client's applications and send it from the MFD. Used is the PC-Fax driver stored on the CD-ROM attached to the MFD or the printer expansion kit.
(r)	PC-InternetFax driver	PC-InternetFax driver software which performs PC-InternetFax, enabling the client to send fax data from client's applications and send it from the MFD. Used is the PC-InternetFax driver stored on the CD-ROM attached to the InternetFax expansion kit.
(s)	Sharpdesk (network scanner tool)	Client software to receive data transferred to the client using the Scan-to-DeskTop function (scan and send function) of the MFD. Used is the software stored on the CD-ROM attached to the MFD or the network scanner expansion kit.
(t)	TWAIN driver	TWAIN driver software which performs the PC scan function (scan and send function) of the MFD. Used is the TWAIN driver stored on the CD-ROM attached to the MFD or the printer expansion kit.
(u)	Template of TIFF file header	A TIFF file header for image data conversion used for the testing.
(v)	JBIG decode tool	Image data conversion software to display compressed image files generated by the MFD on a debug tool.
(w)	Image file analysis software	Software to extract and display binary files generated by the MFD on the debug terminal PC.

<Conduct of the developer testing>

As ways to stimulate interfaces, the following approaches were taken: turning on/off the MFD, manual operations from the operation panel and from the client via a web browser, data transmission via a network cable from another MFD and dial-up connection using the pseudo exchange.

To confirm responses to the above, behaviour was observed in terms of: results displayed on the web browser or operation screen of the client, those displayed on the MFD's operation panel, those on the debug terminal PC via a serial communication cable, visual inspection of printout results of the MFD and behaviour when a fax message is received.

(b) Scope of Execution of the Developer Testing

The developer testing is executed about 53 items by the developer.

By the coverage analysis, it was verified that all of the TSFIs described in the functional specification had been tested.

By the depth analysis, it was verified that the behaviour of TSF subsystems described in the TOE design had been tested enough.

(c) Result

The evaluator confirmed that the actual test results were consistent with the expected test results. The evaluator confirmed an approach of the executing developer testing and legitimacy of tested items, and confirmed that both the approaches and the results matched the test plans.

7.3.2 Evaluator Independent Testing

The evaluator executed the sample testing to reconfirm the execution of the security function by the test items extracted from the developer testing. And the evaluator executed the evaluator independent testing to reconfirm that security functions are certainly implemented from the evidence shown by the process of the evaluation.

It explains the independent testing executed by the evaluator as follows.

(1) Independent Testing Environment

The configuration of the testing conducted by the evaluator is shown in Figure 7-2. It is the same as that of the developer testing except that an external telephone is connected to the MFD in the independent testing.

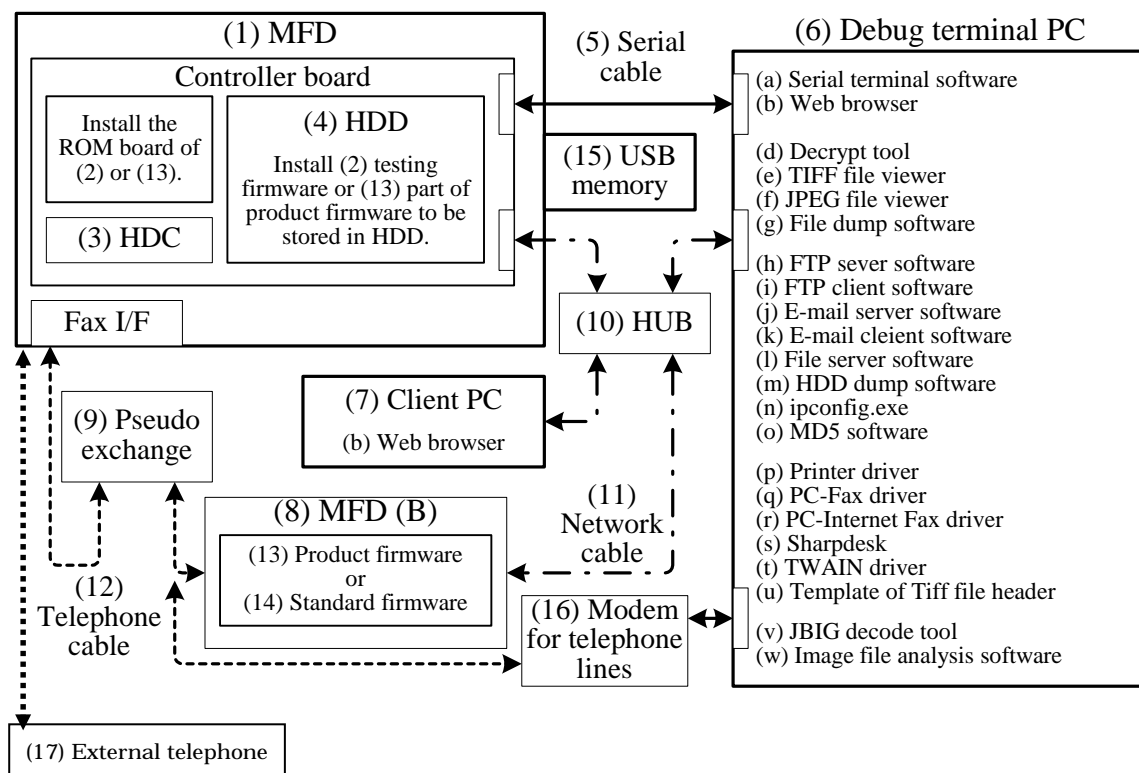


Figure 7-2 Configuration of the Evaluator Testing

(2) Outline of Evaluator Independent Testing

The independent testing performed by the evaluator is as follows.

(a) Independent Testing Points of View

The evaluator devised independent tests in the following viewpoints based on the developer testing and the evidential materials submitted for evaluation.

<Independent Testing Viewpoints>

1. Each of the TSFs which do not seem to have been considered in the developer testing is tested. For these TSFs, different types of parameters and their combinations are added to cover all range of parameters.
2. Tests are conducted to confirm TSF's behaviour more rigorously with additional timings and combinations of user operation.
3. Tests are conducted to confirm TSF's behaviour using different interfaces to the client from those used in the developer testing.
4. Consideration is made to cover all types of interfaces and all security functions that the TOE provides.

(b) Independent Testing Outline

An outline of the independent testing performed by the evaluator is as follows.

<Independent Testing Approach>

Test approaches similar to those of the developer testing were taken.

<Independent Testing Tools>

The tools shown in Table 7-2 used in the developer testing were used.

<Conduct of Independent Testing >

From the independent testing viewpoints, 11 independent tests and 16 sample tests were conducted. Main content of the tests conducted and corresponding viewpoints of independent testing are shown in Table 7-3.

Table 7-3 Points of view for the Independent Testing

Independent testing Viewpoints	Outline of the independent testing
2. 4.	A test to confirm that the security functions operates well even if backup data has been restored.
3. 4.	A test concerning print job operations from the client connected through a USB port.
2. 4.	A test to confirm that the data clear function operates well even if several operations such as changing a confidential file password or cancellation of a file deletion are added in addition to those performed in the developer testing.
2. 4.	A test to confirm that the security functions operates well even if a confidential file's property is changed while the MFD operates.
1. 4.	A test to confirm that the network protection function (filter function) operates well when different combinations of IP addresses or MAC addresses are added.
1. 4.	A test on the fax flow control function with an external telephone connected.

(c) Result

All the executed independent testing was correctly completed, and the evaluator confirmed the behavior of the TOE.

The evaluator confirmed consistencies between the expected behavior and all the testing results.

7.3.3 Evaluator Penetration Testing

The evaluator devised and executed the necessary evaluator penetration testing about the possibility of exploitable concern at assumed environment of use and attack level based on the evidence submitted during the evaluation process.

It explains an outline of the penetration testing executed by the evaluator as follows.

(1) Summary of the Penetration Testing

Summary of the penetration testing executed by the evaluator is as follows.

(a) Vulnerability of concern

The evaluator investigates potential vulnerability based on the submitted evidential materials and publicly-available information, and identified vulnerabilities as follows that needed penetration testing.

1. The assets protected by the TOE and the OS may be accessed without authorization via Telnet or FTP communications.
2. The TOE may be accessed from an unintended network port interface or the assets protected by the TOE may be leaked by sending unauthorized data to an open port.
3. The security functions may be bypassed by using interfaces whose use is not usually assumed or by accessing interfaces in unexpected ways.
4. More information than necessary may be output from interfaces, ending up leaking confidential information.
5. The security functions may be bypassed by unexpected timings of user operations or exceptional cases.
6. The security functions may be bypassed if there is vulnerability in dealing with passwords in the identification and authentication function.
7. The security functions may be bypassed if there is vulnerability in SSL implementation.
8. The security functions may be bypassed by entering unexpected values such as those above or below the range, or invalid.
9. An MFD without a TOE may leak the assets protected by the TOE when several MFDs process a job in collaboration.
10. The security functions may be bypassed by physically tampering the memory or the boards inside.
11. The security functions may be bypassed if there is vulnerability in accesses from the client via the Web.
12. The security functions may be bypassed by executing several functions at the same time.

(b) Penetration Testing Outline

The evaluator conducted the following penetration testing to determine whether there is a possibility that the potential vulnerabilities may be abused.

< Penetration Testing Environment >

The penetration testing was conducted in the same configuration as that of the evaluator independent testing (except that a client was added in which a penetration testing tool had been installed).

In the penetration testing, the following tools listed in Table 7-4 were used in addition to those in the developer testing listed in Table 7-2.

Table 7-4 Penetration Testing Tools

Name	Outline
FTP	FTP (File Transfer Protocol) client software.
netcat	A tool to read and write TCP or UDP packets.
nmap	A port scanner.
telnet	Telnet (remote login protocol) client software.

Wireshark	A tool to monitor and analyze communication on a LAN.
-----------	---

< Conduct of the vulnerability testing >

Table 7-5 shows descriptions of the penetration testing which corresponds to vulnerabilities identified in the investigation of potential vulnerability. The evaluator conducted 22 penetration tests to determine the possibility of abuse of potential vulnerability.

Table 7-5 Outline of Executed Penetration Testing

Vulnerability of concern	Outline of the penetration testing
1	Confirmed that the assets protected by the TOE and information on the system are not accessed directly even if the MFD is connected via FTP or Telnet communications.
2	Confirmed that unexpected network ports are not open (with the port scanner). And confirmed vulnerability to unauthorised accesses do not exist in the used ports
3	Confirmed that unauthorized use does not exist of the interfaces to service technicians. And confirmed that the security functions are not harmed by connecting devices through USB ports.
4	Confirmed that information leading to the leakage of confidential information is not output from TOE's interfaces.
5	Confirmed that the security functions are not bypassed even if the user operates in a way which is not specified in guidance documents or the network is shutdown during data transmission.
6	Confirmed that the identification and authentication function is not bypassed even if invalid passwords or values above or below the range are entered.
7	Confirmed that vulnerable protocols are not selected due to the settings for the client in SSL communication.
8	Confirmed that the security functions are not bypassed even if invalid addresses are specified for the network protection function (filter function).
9	Confirmed that an MFD without a TOE does not leak

	the assets protected by the TOE when tandem copying is performed.
10	Confirmed that vulnerability does not exist which may lead to the bypassing of the security functions caused by replacing or removing the ROM or board inside.
11	Confirmed that The security functions are not bypassed by specifying the URL when the client is connected to the MFD via a browser.
12	Confirmed that the security functions are invoked properly in response to user operations while a backup is made.

(c) Result

In the penetration testing conducted by evaluator, the evaluator could not find the vulnerability that attackers who have the assumed attack potential could exploit.

7.4 Evaluated Configuration

This evaluation was conducted in the configuration shown in "7.3.2 Evaluator Independent Testing" and Figure 7-2. IPv4 was used in the network. This TOE will not be used in the configuration which is significantly different from the above configuration components. Therefore, the evaluator determined the configuration of the above evaluation is appropriate.

7.5 Evaluation Results

The evaluator had the conclusion that the TOE satisfies all work units prescribed in CEM by submitting the Evaluation Technical Report.

In the evaluation, the following were confirmed.

- PP Conformance: None
- Security functional requirements: Common Criteria Part 2 Conformant
- Security assurance requirements: Common Criteria Part 3 Conformant

As a result of the evaluation, the verdict "PASS" was confirmed for the following assurance components.

- All assurance components of EAL3 package

The result of the evaluation is applied to the composed by corresponding TOE to the identification described in the chapter 2.

7.6 Evaluator Comments/Recommendations

There are no recommendations to be advised to consumers.

8. Certification

The certification body conducted the following certification based on each materials submitted by Evaluation Facility during evaluation process.

1. Contents pointed out in the Observation Report shall be adequate.
2. Contents pointed out in the Observation Report shall properly be reflected.
3. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.
4. Rationale of evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.
5. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

8.1 Certification Result

As a result of verification of submitted Evaluation Technical Report, Observation Reports and related evaluation deliverables, Certification Body determined that the TOE satisfies all components of the EAL3 in the CC part 3.

8.2 Recommendations

Users of the TOE are advised to refer to "4.2 Environment Assumptions" and "4.3 Clarification of scope" to make sure that user's TOE operational environment satisfies the requirements for operation in a network environment.

9. Annexes

There is no annex.

10. Security Target

Security Target [12] of the TOE is provided within a separate document of this certification report.

MX-FR22 Security Target Version 0.03 (September 13, 2010) Sharp Corporation

11. Glossary

The abbreviations relating to CC used in this report are listed below.

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

The abbreviations relating to TOE used in this report are listed below.

DSK	Data Security Kit MX-FR22, 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
HTTPS	HTTP over SSL, HTTP with protection of SSL.
IPP-SSL	IPP over SSL, IPP with protection of SSL.
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.
MSD	Mass Storage Device, in this document, this especially indicates the HDD and flash memory in the MFD.
ROM	Read Only Memory.
USB	Universal Serial Bus, a serial bus standard to connect between IT equipments.

The definition of terms used in this report is listed below.

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.
IP address:	A call sign, used for IP, to identify devices for communication.
MAC address:	A call sign, used for MAC, identify devices of communication media.
Image data:	Digital data, especially in this document, of two-dimensional image data that each function of the MFD manages.
Internet fax:	A function to send and receive fax messages via the Internet. In conformance to the standard specifications, fax data can be sent and received as an attachment by email.
Volatile memory:	A memory device, the contents of which vanish when the power is turned off.
Controller board:	The board that controls the whole MFD. This contains the microprocessor to execute the 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.
Subnetwork:	A part of internal network divided by router.
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.
Confidential file:	The data that the user saved with password protection (confidential file password) to prevent others from manipulating.
Spool:	Storing a job's image data into the MSD temporarily to increase the input and output efficiency.
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 operation system.
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.
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 replaced with the TOE's controller firmware when TOE is installed.
Non-volatile memory:	The memory device that retains its contents even when the power is turned off.

- Print function:** The function to print data received from external devices.
- Hold:** To store a job sent from a printer driver using the document filing function.
- Tandem print:** The function to print large job twice faster than usually by halving that job among two MFDs.
- Tandem copy:** Tandem print in the MFD's copier function.

12. Bibliography

- [1] IT Security Evaluation and Certification Scheme, May 2007, Information-technology Promotion Agency, Japan, CCS-01
- [2] IT Security Certification Procedure, May 2007, Information-technology Promotion Agency, Japan, CCM-02
- [3] Evaluation Facility Approval Procedure, May 2007, Information-technology Promotion Agency, Japan, CCM-03
- [4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001
- [5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002
- [6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003
- [7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001, (Japanese Version 1.0, December 2009)
- [8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002, (Japanese Version 1.0, December 2009)
- [9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003, (Japanese Version 1.0, December 2009)
- [10] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004
- [11] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004, (Japanese Version 1.0, December 2009)
- [12] MX-FR22 Security Target Version 0.03, (September 13, 2010) Sharp Corporation
- [13] MX-FR22 Evaluation Technical Report, Version 2.4, January 13, 2011 Information Technology Security Center Evaluation Department