Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2007-12-4 (ITC-7186)
Certification No.	C0188
Sponsor	Sharp Corporation
Name of TOE	MX-FRX8
Version of TOE	Version M.10
PP Conformance	None
Conformed Claim	EAL3
Developer	Sharp Corporation
Evaluation Facility	Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security

This is to report that the evaluation result for the above TOE is certified as follows.
2008-10-30

Hideji Suzuki, 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 Revision 2 (Translation Version 2.0)
- Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 2 (Translation Version 2.0)

Evaluation Result: Pass

"MX-FRX8 Version M.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

1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "MX-FRX8 Version M.10" (hereinafter referred to as the "TOE") conducted by Mizuho Information & Research Institute, Inc., Center for Evaluation of Information Security (hereinafter referred to as "Evaluation Facility"), and it reports to the sponsor, Sharp Corporation.

The reader of the Certification Report is advised to read the corresponding ST. The operational conditions, details of usage assumptions, corresponding security objectives, security functional and assurance requirements needed for its enforcement, the summary of security specifications and rationale of sufficiency are specifically described in the ST.

Note that the Certification Report presents the certification result, based on assurance requirements conformed to the TOE, and does not certify individual IT product itself.

1.1.1 EAL

Evaluation Assurance Level of the TOE defined by this ST is EAL3 conformance.

1.1.2 PP Conformance

There is no PP to be conformed.

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows;

Name of Product:	MX-FRX8
Version:	Version M.10
Developer:	Sharp Corporation

1.2.2 Product Overview

The TOE is an IT product (optional) to protect data in the following Multi Function Devices (MFD): MX-M850, MX-M860, MX-M950 and MX-M1100. The main part of the TOE is the firmware in ROMs for the MFD. The HDC (Hard Disk Controller), a hardware part in the MFD, is also a part of the TOE and is controlled by the firmware.

MFDs, namely, digital multifunctional devices, are office machines mainly with copier, printer, scanner and fax functions. When installed, the TOE replaces the MFD standard firmware ROM.

1.2.3 Scope of TOE and Security Functions

1.2.3.1 Physical Scope of TOE

The TOE is provided by the two ROM boards and the HDC. The scope of the TOE is shaded in Figure 1-1.

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

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

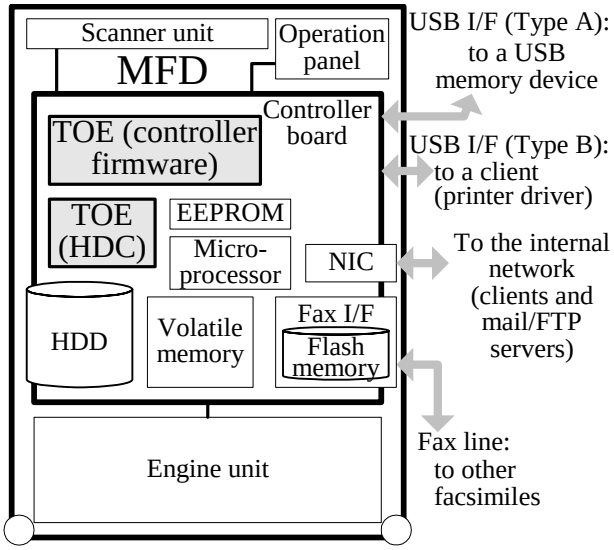

Figure 1-1: Physical configuration of the MFD and physical scope of the TOE

1.2.3.2 Logical Scope and Security Function of TOE

Figure 1-2 shows the logical configuration of the TOE. In the figure, the thick-lined frame indicates the logical scope of the TOE, and rounded boxes indicate hardware devices outside 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.

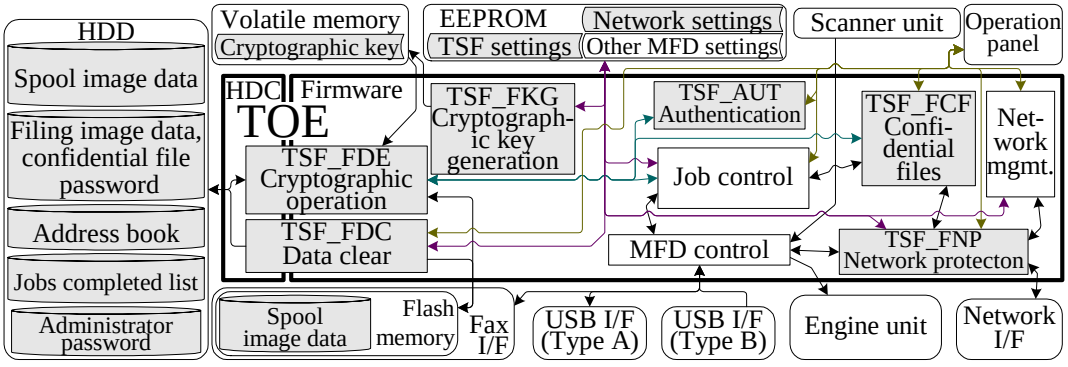

Figure 1-2: Logical configuration of the TOE

The TOE provides the following functions aiming to protect user data, including image data, etc. The purpose is to counter unauthorized attempts to obtain user data which are stored or remain in the non-volatile memory devices (such as the HDD) in the MFD. Another purpose is to counter attempts to wiretap user data when the MFD inputs and outputs the data over the network (LAN).

a) Cryptographic operation function:
When the MFD temporarily writes image data of a current job into the HDD, etc., or when users save image data of a document as a file into the HDD, it encrypts the data before being written.

b) Data clear function:
When the image data in the HDD become no longer in use, it automatically overwrites. All data are overwritten as necessary by the operation of the administrator on a daily basis or at the time of disposal of MFDs.

c) Confidential file function:
It provides password protection for files where users save image data.

d) Network protection function:
- IP/MAC address filter function
It rejects unauthorized access via network.
- SSL function
It protects data from wiretapping during transmission.

1.2.3.3 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

1.3 Conduct of Evaluation

Based on the IT Security Evaluation/Certification Program operated by the Certification Body, the functionality and assurance requirements related to the TOE are being evaluated by Evaluation Facility in accordance with those publicized documents, such as "IT Security Evaluation and Certification Scheme"[2], "IT Security Certification Application Procedure"[3], and "Evaluation Facility Approval Procedure"[4].

Scope of the evaluation is as follows;

1) Security design of the TOE shall be adequate.
2) Security functions of the TOE shall satisfy security functional requirements described in the security design.
3) The TOE shall be developed in accordance with the basic security design.
4) Above mentioned three items shall be evaluated in accordance with the provisions of CC Part 3 and CEM.

More specifically, the Evaluation Facility examined "MX-FRX8 Security Target"

(hereinafter referred to as the "ST")[1] as the basic design of security functions for the TOE, the evaluation deliverables in relation to the development of the TOE, and the development, manufacturing and shipping sites of the TOE. The Evaluation Facility evaluated if the TOE satisfies both Annex A of CC Part 1 (either of [5] or [8]) and Functional Requirements of CC Part 2 (either of [6] or [9]), and evaluated if the development, manufacturing and shipping environments for the TOE also satisfy the Assurance Requirements of CC Part 3 (either of [7] or [10]) as rationale. Such evaluation procedure and its results are presented in "MX-FRX8 Evaluation Technical Report" (hereinafter referred to as the "Evaluation Technical Report") [13]. Further, evaluation methodology shall comply with the CEM (either of [11] or [12]).

1.4 Certification

The Certification Body verifies the Evaluation Technical Report, Observation Report, prepared by the Evaluation Facility, and evaluation evidential materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification review is also prepared for those concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report dated September 2008, submitted by the Evaluation Facility, and those problems pointed out by the Certification Body are fully resolved, and it is confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body prepared this Certification Report, based on the Evaluation Technical Report submitted by the Evaluation Facility, and fully concluded the certification activities.

2. Summary of TOE

2.1 Security Problems and Assumptions

Problems to be solved by the TOE and necessary assumptions are as follows.

2.1.1 Threats

This TOE assumes such threats presented in Table 2-1 and provides functions as countermeasures against them. Possible attackers are assumed as follows;

- Threat agent
  Authorised MFD users or third parties.
- Motives
  To obtain the assets, such as image data of others' documents without authorisation.
- Attack potential
  To possess knowledge of MFDs and the TOE based on open information, including operation manuals.

Table 2-1: Assumed Threats

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

2.1.2 Organisational Security Policies

No organisational security policy is required in the use of the TOE.

2.1.3 Assumptions for Operational Environment

Assumptions required in an environment using this TOE are presented in Table 2-2. Unless these assumptions are satisfied, the effective performance of the TOE security functions is not assured.

Table 2-2: Assumptions in Use of the TOE

Identifier	Assumptions
A.NETWORK	The MFD is connected to a subnetwork in the internal network protected against attacks from any external networks, where the subnetwork for the MFD connects nothing other than devices allowed to communicate with the MFD. (Note: The above is based on the assumption that the MFD is connected to a subnetwork in the internal network protected against attacks from any external networks and that the subnetwork is only connected to devices allowed to communicate with the MFD).
A.OPERATOR	The administrator is a trustworthy person who does not take improper action with respect to the MFD and the TOE.

2.1.4 Documents Attached to Product

The identifications of the documents attached to the TOE are listed below.

Table 2-3: Documents Attached to Product

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

2.1.5 Configuration Requirements

The TOE operates on the following MFDs made by Sharp Corporation: MX-M850, MX-M860, MX-M950 and MX-M1100.

2.2 Security Objectives

The TOE counters the threats described in 2.1.1 with the implemented security functions as follows;

(1) Cryptographic key generation function (TSF_FKG):

The TSF generates a cryptographic key (common key) to support the encryption function of user data and TSF data. The TSF automatically generates the secure seed when the TOE is installed. With the seed, the TSF generates a 128-bit key every time the MFD is turned on. The TOE in each MFD generates a cryptographic key always using the same seed and same algorithm. The key generated is stored to the volatile memory and is destructed when the MFD is turned off.

(2) Cryptographic operation function (TSF_FDE):

This TSF always encrypts and writes the user data and the TSF data when it is necessary to write them to the MSD. In addition, this function reads them from the MFD and decrypts when these data are required. The cryptographic key that is generated by cryptographic key generation function (TSF_FKG) is used for encryption and decryption.

Target user data include the image data that are spooled to the HDD or Flash memory, the image data that are stored to the HDD, and address book data or job completed list data that are stored in the HDD. Target TSF data include confidential file passwords and the administrator password that are stored in the HDD.

(3) Data clear function (TSF_FDC):

The TSF provides data clear functions which clear image data files that are spooled or stored, the address book data file, and the jobs completed list data file, and it consists of the following programs. Each program overwrites HDD one or more times with a random value, and the Flash memory once with a fixed value.

a) Auto Clear at Job End program:

This program overwrites image data that has been spooled to the HDD and the Flash memory in order to process a job when the job is completed or cancelled. It also overwrites image data stored in the HDD using the document filing function (including the confidential file function) when the user deletes the data.

b) Clear All Memory program:

This program is invoked from the operation panel by the administrator who has been identified and authenticated by the authentication function (TSF_AUT), and overwrites all of the spool image data, all of the filing image data, the jobs completed list data to the HDD, and all of the spool image data in the Flash memory. This program does not clear the address book data.
In case of cancelling this program by the administrator, the TSF requires the authentication of the administrator after the cancellation was selected. The administrator is identified by the cancel operation and authenticated by inputting passwords. This TSF hides the typed password character when entering passwords. If an incorrect password is entered three times in a row, this program stops accepting further authentication attempts for five minutes.

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

This program is invoked from the operation panel by the administrator who has been identified and authenticated by the authentication function (TSF_AUT) and overwrites the address book data in the HDD. This program cannot be cancelled.

d) Clear Document Filing Data program:

This program is invoked from the operation panel by the administrator who has been identified and authenticated by the authentication function (TSF_AUT) and overwrites all spool image data and filing image data on the HDD. This program can be cancelled in the same way as the Clear All Memory program.

e) 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 the authentication function (TSF_AUT) and overwrites the jobs completed list data on the HDD. This program cannot be cancelled.

f) Power Up Auto Clear program:

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

Whether this program is executed or not when the TOE is turned on depends on the value set beforehand. The target data to be cleared by this program also depend on the value set beforehand. This program clears either all data that the Clear All Memory program covers or specified data in the HDD. One or more kind of data can be specified as a target from either spool image data, filing image data, or jobs completed list data. This program can be cancelled in the same way as the Clear All Memory program.

g) Data Clearance Settings:

In regard to each program above, this TSF provides the following functions (to query and modify) to the administrator who has been identified and authenticated by the authentication function (TSF_AUT):

- Number of Times Auto Clear at Job End Program is Repeated:
  The number of times overwriting the data on the HDD is repeated, using the Auto Clear at Job End program. Any integer between 1 and 7 inclusive are accepted. The default is 1.
- Number of Times Data Clear is Repeated:
  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. Any integer between 1 and 7 inclusive are accepted. The default is 1.
- Power Up Auto Clear Program
  It accepts settings to specify data areas to be cleared, for which the Power Up Auto Clear program is valid. The default is that Power Up Auto Clear program is disabled for every data (no data is specified).
- Number of Times Power Up Auto Clear Program is Repeated:
  The number of times overwriting the data on the HDD is repeated, using the Power Up Auto Clear program. Any integer between 1 and 7 inclusive are accepted. The default is 1.

(4) Authentication function (TSF_AUT):

This TSF enforces the identification and authentication of the administrator by the administrator password. The TSF only accepts a password consisting of 5 to 32

alphanumeric and/or symbolic characters, and it provides the interfaces of the functions for the administrator, such as the Data Clearance Setting or Change Administrator Password, when the authentication of the administrator is successful. The administrator is identified by calling administrator's functions from the operation panel or on the Web page, or by the login operation of the administrator, and is authenticated by entering the password. This TSF hides the typed password character or requires hiding the character when entering passwords. If an incorrect administrator password is entered three times in a row, this program stops accepting further authentication attempts for five minutes.

(5) Confidential files function (TSF_FCF):

This TSF provides password protection to image data which a user stored as a confidential file in the MFD and allows re-operation (print out, etc.) after the password authentication on the operation panel or via Web. The confidential file password shall be 5 to 8 numeric characters.

In the confidential file password authentication which allows re-operation of 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.

In addition, this TSF provides functions to export the encrypted data to the Web browser of the client, and also to import both encrypted and non-encrypted data from the Web browser of the client.

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.

- Disabling of Document Filing:
  It 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:
  It disables the job to print out on the spot from the printer driver. This function rejects the job without being designated as "Holding" and only holds the Hold job regardless of whether 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.

- Release the lock of confidential files:
  It releases the lock of confidential files which have been locked by the failure of the authentication for the confidential file password.

(6) Network protection function (TSF_FNP):

This TSF provides the following three functions that are related to the network protection.

a) Filter function:

This function rejects attempts to communicate from the unexpected users, according to IP address and MAC address. The administrator, who has been identified and

authenticated by TSF_AUT, specifies IP address ranges(up to 4) either to accept or reject and set MAC address (up to 10) to accept.

b) Communication data protection function:

This function provides the HTTPS communication function to protect communication between the client and the TOE via Web from wiretapping as well as the IPP-SSL communication function to protect print data sent from a client by the printer driver from wiretapping.

c) Network settings protection:

This function allows only the administrator who has been identified and authenticated by TSF_AUT to manage the network settings data from the operation panel and the Web.

3. Conduct and Results of Evaluation by Evaluation Facility

3.1 Evaluation Methods

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 overview of the TOE, the content of evaluation and verdict of each work unit in CEM.

3.2 Overview of Evaluation Conducted

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

The evaluation has started on 2007-12 and concluded by completion of the Evaluation Technical Report dated 2008-09. The Evaluation Facility 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 2008-06 and examined procedural status conducted in relation to each work unit for configuration management, delivery, and developing security by investigating records and interviewing staff. Furthermore, the evaluator executed the sampling check of the developer testing and the evaluator testing by using developer testing environment at developer site on 2008-06.

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.

Concerns that the Certification Body found in the evaluation process were described as a certification oversight review, and it was sent to Evaluation Facility. After Evaluation Facility and the developer examined it, these concerns were reflected in the evaluation report.

3.3 Product Testing

The evaluator confirmed the validity of the testing that the developer had executed. As a result of the evidence shown in 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.

3.3.1 Developer Testing

The evaluator evaluated the integrity of developer testing that the developer executed and the testing documentation of actual testing results.
The overview of evaluated tests performed by the developer is shown as follows;

1) Developer Testing Environment

Figure 3-1 shows the testing configuration executed by the developer.

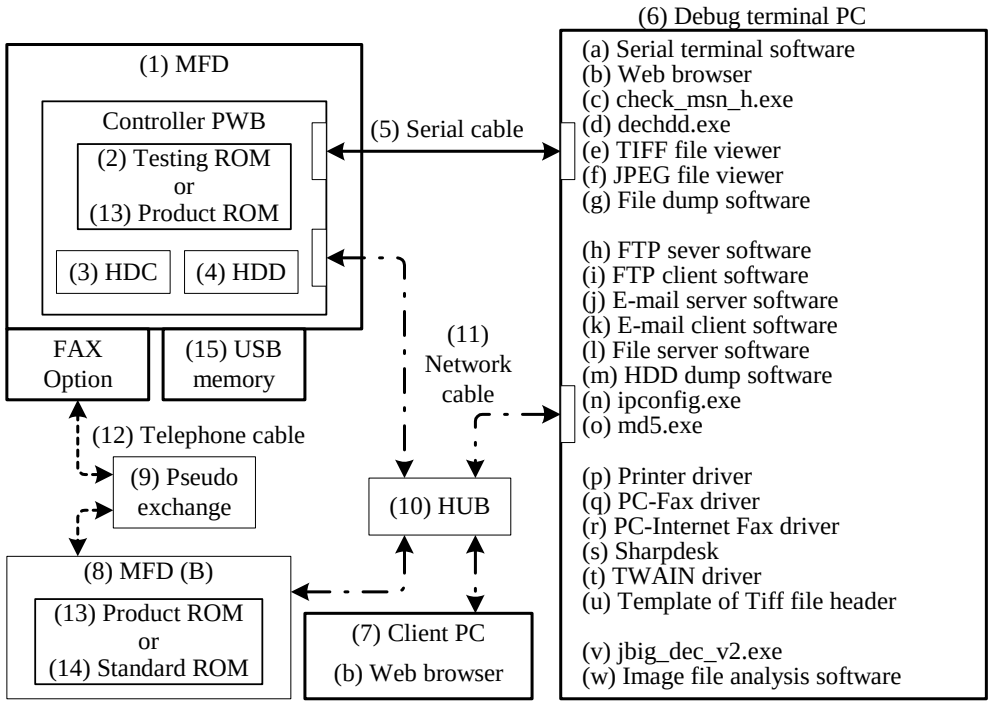

Figure 3-1: Configuration of the Developer Testing

The developer testing is executed in the same TOE testing environment as the TOE configuration identified in the ST.

2) Summary of Developer Testing

The summary of the testing performed by the developer is as follows;

a. Outline of Developer Testing

The outline of the developer testing is as follows.

Under the environment shown in Figure 3-1, either of the following two types of ROMs was used in compliance with the characteristics of each testing.

(1) Product ROM:
It is used for the testing in which security functionality can be externally observed.
(2) Testing ROM:
It is used for the testing in which security functionality, such as the cryptographic operation function and the data clear function, cannot be externally observed. The security functionality is confirmed by command operations or by outputting internal information from the debug terminal.

The developer conducted the testing by manual operation as follows: turning on/off the MFD, operations on the operation panel, operations on the TOE Web page, operations to stimulate logical external interfaces (including operations from a printer driver, a PC-Fax driver and a fax), operations on the debug terminal using the testing ROM, and special operations conducted for the testing (including pulling and returning trays, removal and installation of the HD, disconnection and connection of the fax line).

b. Scope of Testing Performed

The testing is executed on 51 items by the developer.

By the coverage analysis, it was verified that all security functions and external interfaces described in the functional specification were tested enough. By the depth analysis, it was verified that all the subsystems and the subsystem interfaces described in the TOE design were tested enough.

c. Results

The consistency between the expected test results and the actual test results provided by the developer is confirmed. The evaluator confirmed an approach of executing developer testing and the legitimacy of tested items, and confirmed consistencies between the testing approach described in the test plan and actual test results.

3.3.2 Evaluator Independent Testing

The evaluator conducted an independent testing to reconfirm that security functions are certainly implemented from the evidence shown in the process of the evaluation. The outline of the independent testing performed by the evaluator is as follows;

1) Evaluator Independent Testing Environment

Test configuration performed by the evaluator is the same configuration as the developer testing, and the testing uses the product ROM and the testing ROM.
The testing configuration performed by the evaluator is shown in Figure 3-1. The evaluator independent testing is executed in the same TOE testing environment as the TOE configuration identified in the ST.

2) Summary of Evaluator Independent Testing

Independent testing performed by the evaluator is as follows;

a. Viewpoints of Independent Testing

Referring the developer testing and the provided evaluation evidential materials, the evaluator devised the independent testing for the interfaces in order to supplement the rigorousness and sufficiency in the developer testing in terms of the following viewpoints.

(1) To test interfaces more rigorously, the evaluator conducted the same types of testing as conducted by the developer using different parameters from those used in the developer testing.
(2) To test interfaces more sufficiently, the evaluator conducted the same types of testing as conducted by the developer by stimulating the interfaces using different methods of starting from those used in the developer testing (especially logical external I/Fs).
(3) To test interfaces more sufficiently, the evaluator conducted the same types of testing as conducted by the developer in different modes from those used in the developer testing.

(4) To test interfaces more sufficiently, the evaluator conducted different types of testing from those conducted by the developer using different testing approaches from those used in the developer testing.
(5) To test interfaces more sufficiently, the evaluator conducted the same types of testing as conducted by the developer in different initial conditions from those used in the developer testing.
(6) To test interfaces more sufficiently, the evaluator used a special test tool for cases in which interfaces cannot be stimulated only by the test tool used in the developer testing, or for cases in which their behaviour cannot be observed.

b. Outline of Evaluator Independent Testing

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

In the independent testing, 31 tests were conducted. In devising the tests, the following were considered to supplement the developer testing with rigorousness and sufficiency: parameters (including the administrator password, the confidential file password and their variations), methods of starting interfaces (including print jobs via USB), modes (including the fax night mode), testing approaches (including simultaneous operations on the Web page) and initial conditions (including immediately after document filing data are restored), all of which were not used in the developer testing. Furthermore, the viewpoint of depth (behaviour of internal interfaces of subsystems) was also considered to observe behaviour of interfaces by stimulating them with tools (including OpenSSL commands and Wireshark) that were not used in the developer testing. The independent testing covered all of the security functions and 28 interfaces, which accounted for about half of all TSFI. The evaluator determined that the rest of the interfaces are not needed because the behaviours of those interfaces (including those for the data clear functions and for batch printing) were sufficiently confirmed in the developer testing.

c. Results

All the conducted evaluator independent testing was correctly completed, and the evaluator confirmed the behaviour of the TOE. The evaluator confirmed consistencies between the expected behaviour and all the testing results.

3.3.3 Evaluator Penetration Testing

Evaluator devised and conducted the necessary penetration testing for the possibility of vulnerability of concern based on the evidence submitted during the evaluation process. The outline of evaluator penetration testing is as follows;

1) Summary of Evaluator Penetration Testing

The summary of penetration testing executed by the evaluator is as follows;

a. Vulnerability of concern

The evaluator investigated potential vulnerabilities based on the provided evidence and the public domain information to identify the following vulnerabilities which require penetration testing.

The results of a well-known vulnerability search identified 7 check items for Web applications which are made public by the IPA (including checking input data by a script on the client, cross site scripting, inferring session IDs, query strings). Furthermore, vulnerabilities were identified by checking the evidence in terms of the items defined in the section of "*Generic Vulnerability Guidance*" of the CEM, which were the targets in 13 penetration tests relating to bypassing, alteration and misuse.

b. Scope of Testing Performed

Evaluator conducted the following penetration testing to determine the possibility of exploitable potential vulnerabilities.
Based on the search results above, for the check items of Web application, a test to change Web browser settings (valid/invalid of scripts) and a test in which the Web browser directly accesses the URL that requires user authentication were conducted. For bypassing, a test for unused ports using a port scan tool and a test to see if the administrator's authentication is improperly sustained after the state of the MFD is changed (including turning off the power) were conducted. For alteration and misuse, the following tests were conducted; a test for special characters of passwords, a test for the confusion of simultaneous use in the combination of accesses from the MFD's operation panel and the Web, and a test to see if the specified encrypted communication is performed using a network protocol analysis tool.

c. Results

In the penetration testing conducted by the evaluator, the evaluator could not find potential vulnerabilities that could be beyond the assumed attack potential.

3.4 Evaluation Result

3.4.1 Evaluation Result

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

3.4.2 Comments/Recommendations from Evaluator

The evaluator recommendations for users are not mentioned.

4. Conduct of Certification

The Certification Body conducted the following certification based on the materials submitted by Evaluation Facility in the 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. Submitted evidential materials were sampled, the contents were examined, and the 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.

Concerns found in the certification process were prepared as certification oversight review, and it was sent to the Evaluation Facility.

The Certification Body confirmed such concerns pointed out in Observation Report and the certification oversight review were solved in the ST and the Evaluation Technical Report, and issued this certification report.

5. Conclusion

5.1 Certification Result

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

5.2 Recommendations

None.

6. 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 the TOE used in this report are listed below.

EEPROM:	Electrically Erasable Programmable ROM; a type of non-volatile memory that allows low frequency of electrical rewriting at any part of memory.
HDC:	Hard Disk Controller
HDD:	Hard Disk Drive
HTTPS:	HTTP over SSL; HTTP with protection of SSL
IPP-SSL:	IPP over SSL; IPP with protection of SSL
LAN:	Local Area Network
MFD:	Multi Function Device; a digital multifunctional device which is an office machine equipped with copier, printer, scanner, fax and other functions.
MSD:	Mass Storage Device; referring particularly to the HDD and Flash memory in the MFD in this report.
ROM:	Read Only Memory
SSL:	Secure Socket Layer; a cryptographic communication protocol for computer network
UI:	User Interface

The definitions of terms used in this report are listed below.

Controller board:	The board that controls the whole MFD, containing a microprocessor to execute firmware of the TOE, and volatile memory, HDC, HDD and others.
Controller firmware:	The firmware that controls the controller board in the MFD; it is stored in the ROM board and implemented on the controller board.
Disabling of Print Jobs Other Than Print Hold Job:	It 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.
Document filing:	The function that stores image data handled by the MFD into the HDD inside MFD, for users' re-operations, such as a printing and a transmission.
Firmware:	The software that is embedded to the machines to control the machine's hardware; it especially indicates the controller firmware in this report.
Flash Memory:	A type of non-volatile memory that allows the entire memory to be electrically erased at once and also allows rewriting at any part of memory.
Hold:	To store a job from printer driver by filing.
Job:	The sequence from beginning to end of the use of an MFD function (copier, printer, scanner, fax transmission and reception, or PC-Fax); in addition, the instruction for a functional operation is sometimes called a job.
Subnetwork:	A part of internal network divided by a router.
Volatile memory:	A memory device, the contents of which vanish when the power is turned off.

7. Bibliography

[1] MX-FRX8 Security Target Version 0.07 (June 30, 2008) Sharp Corporation

[2] IT Security Evaluation and Certification Scheme, May 2007, Information-technology Promotion Agency, Japan CCS-01

[3] IT Security Certification Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-02

[4] Evaluation Facility Approval Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 3.1 Revision 1, September 2006, CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components Version 3.1 Revision 2, September 2007, CCMB-2007-09-002

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components Version 3.1 Revision 2, September 2007, CCMB-2007-09-003

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 3.1 Revision 1, September 2006, CCMB-2006-09-001 (Japanese Version 1.2, March 2007)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components Version 3.1 Revision 2, September 2007, CCMB-2007-09-002 (Japanese Version 2.0, March 2008)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components Version 3.1 Revision 2, September 2007, CCMB-2007-09-003 (Japanese Version 2.0, March 2008)

[11] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 3.1 Revision 2, September 2007, CCMB-2007-09-004

[12] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 3.1 Revision 2, September 2007, CCMB-2007-09-004 (Japanese Version 2.0, March 2008)

[13] MX-FRX8 Evaluation Technical Report, September 29, 2008, Mizuho Information & Research Institute, Inc., Center for Evaluation of Information Security