Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2009-09-18 (ITC-9263)
Certification No.	C0245
Sponsor	Sharp Corporation
Name of TOE	MX-FR14
Version of TOE	C.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.
2010-02-25

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 2
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 2

Evaluation Result: Pass

"MX-FR14 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

1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "MX-FR14 C.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 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 corresponding ST. The operational conditions, details of usage assumptions, corresponding security objectives, security functional and assurance requirements needed for its enforcement, their summary of security specifications and rationale of sufficiency are specifically described in 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 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-FR14
Version:	C.10
Developer:	Sharp Corporation

1.2.2 Product Overview

The TOE is an IT product (optional*1) to protect data in the following Sharp Multi Function Devices (hereinafter referred to as "MFD"): MX-M283N, MX-M283NJ, MX-M363F, MX-M363N, MX-M363NJ, MX-M363U, MX-M363UJ, MX-M423F, MX-M453N, MX-M453NJ, MX-M453U, MX-M453UJ, MX-M503F, MX-M503N, MX-M503NJ, MX-M503U and MX-M503UJ*2. The main part of the TOE is the firmware in ROMs for the MFD. The HDC (Hard Disk Controller) that is a hardware part in the MFD is also a part of the TOE and controlled by the firmware.
MFDs, digital multifunctional devices, are office machines having copier, printer, and scanner and fax functions as their primary functions.

*1. When installed, it replaces the MFD standard firmware ROM.

*2. The TOE operates only when the sharp genuine optional product including the HDD is installed in the models where the name contains "U".

1.2.3 Scope of TOE and Security Functions

1.2.3.1 Physical Scope of TOE

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

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

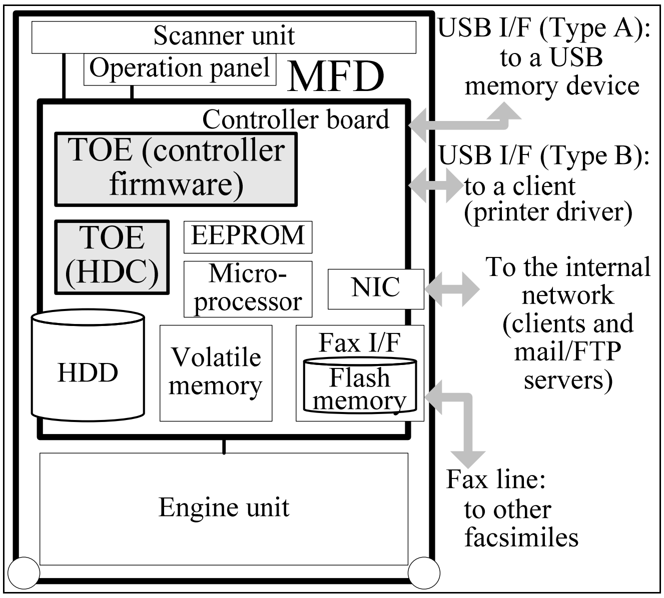
Scanner unit
Operation panel
MFD
Controller board
TOE (controller firmware)
TOE (HDC)
EEPROM
Micro-processor
NIC
HDD
Volatile memory
Fax I/F
Flash memory
Engine unit
USB I/F (Type A): to a USB memory device
USB I/F (Type B): to a client (printer driver)
To the internal network (clients and mail/FTP servers)
Fax line: to other facsimiles

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. 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.

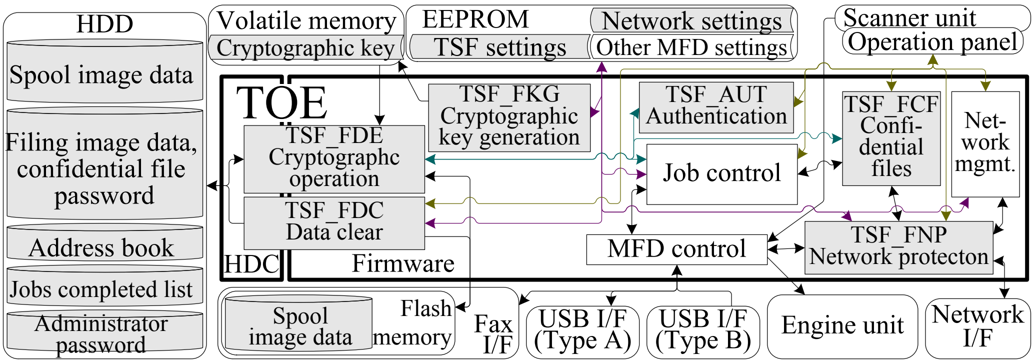

Figure 1-2: Logical configuration of the TOE

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

a) Cryptographic operation function: encrypts image data before the MFD temporarily writes image data to the HDDs while processing and before image data of a document is written in the HDD which users store.

b) Cryptographic key generation function: generates the cryptographic key for the cryptographic operation function. This function stores the generated key in the volatile memory. It generates a seed of the cryptographic key once when TOE is installed. From then on, it always generates a cryptographic key based on this seed when the power supply of MFD turns on.

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

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 files function: provides password protection for files when the user files the image data, not to be reused by others.

f) Network protection function:

- IP/MAC address filter function: rejects unauthorized accesses over the network.
- SSL function: protects the communication data from wiretapping.
- Network settings protection: provides the network management function including IP address and DNS settings exclusively to the administrator, and so as not to allow other users to use it.

1.2.3.3 Assets protected by TOE

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

- Image data that the MFD functions spool at job processing
- Image data that users save as confidential files
- Address book data

- Jobs completed data list
- Network settings data
- Communication data on network

1.3 Conduct of Evaluation

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

Scope of the evaluation is as follow;

- Security design of the TOE shall be adequate;
- Security functions of the TOE shall be satisfied with security functional requirements described in the security design;
- This TOE shall be developed in accordance with the basic security design;
- Above mentioned three items shall be evaluated in accordance with the CC Part 3 and CEM.

More specific, the Evaluation Facility examined "MX-FR14 Security Target" as the basis design of security functions for the TOE (hereinafter referred to as "the ST")[1], the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied 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 also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7] or [10]) as its rationale. Such evaluation procedure and its result are presented in "MX-FR14 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 and Observation Report prepared by the Evaluation Facility and evaluation evidence 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 2010-02 submitted by the evaluation facility and those problems pointed out by the Certification Body are fully resolved and 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 concluded fully certification activities.

2. Summary of TOE

2.1 Security Problem and assumptions

Problems should be solved by TOE and necessary assumptions are as follows;

2.1.1 Threat

This TOE assumes such threats presented in Table 2-1 and provides functions for countermeasure to them. Possible attackers are as follows:

- Threat agent: authorized MFD users or third parties.
- Motives: illegally obtaining the assets such as image data of other's documents.
- Attack ability: possesses the basic attack potential with the knowledge of MFDs and the TOE based on open information including operation manuals.

Table 2-1 Assumed Threats

Identifier	Threat
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 are 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 environment using this TOE presents in the Table 2-2.
The effective performance of the TOE security functions are not assured unless these assumptions are satisfied.

Table 2-2 Assumptions in Use of the TOE

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

2.1.4 Documents Attached to Product

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

For markets in Japan	For markets outside of Japan
"MX-FR14 Data Security Kit Operation Manual" (in Japanese) [(CINSJ4673FC51) (TINSJ4673FCZZ)]	"MX-FR14 Data Security Kit Operation Manual" (in English) [(CINSE4674FC51) (TINSE4674FCZZ)]
"MX-FR14 Data Security Kit Notice" (in Japanese) [(CINSJ4675FC51) (TINSJ4675FCZZ)]	"MX-FR14 Data Security Kit Notice" (in English) [(CINSE4676FC51) (TINSE4676FCZZ)]

2.1.5 Configuration Requirements

The TOE operates on the following MFDs made by Sharp Corporation: MX-M283N, MX-M363F, MX-M363N, MX-M363U, MX-M423F, MX-M453N, MX-M453U, MX-M503F, MX-M503N and MX-M503U. Remove the ROMs of the standard firmware from the MFD, and exchanges it to the TOE. The TOE operates only when the Sharp genuine optional product including the HDD is mounted in models whose name includes "U".

The TOE has been tested in combination with Microsoft "Internet Explorer 6.0 SP 2" as a web browser for communications to and from the MFD. Printer drivers and PC-fax drivers with required capabilities come with the MFDs listed above.

2.2 Security Objectives

TOE counters threats described in 2.1.1 as follows by implemented security functions.

(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 and a 256-bit key using the MSN-R2 expansion algorithm every time the MFD is turned on. The TOE in each MFD generates cryptographic keys always using the same seed and algorithm. The keys generated are stored to the volatile memory and are 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 keys that are generated by cryptographic key generation function (TSF_FKG) are used for encryption and decryption.

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

(3) Data clear function (TSF_FDC):

The TOE provides the data clear function that clears image data files that are spooled and stored, the address book data file and the jobs completed data list file. This function consists of the following programs. Each program overwrites the HDD one or more times with random values and overwrites 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 or the flash memory while a job is being processed, when the job is completed or cancelled. It also overwrites image data stored in the HDD using the document filing function (including the confidential files function), when the user deletes the data.

The administrator who is identified and authenticated by the authentication function (TSF_AUT) can set the number of times the Auto Clear at Job End program overwrites the HDD. The number of times is configurable any integer from 1 to 7 times and the default is 1.

b) Clear All Memory program:

This program is invoked from the operation panel by the administrator who is identified and authenticated by the authentication function (TSF_AUT) and overwrites all spool image data and filing image data, the jobs completed list data in the HDD, and all spool image data in the flash memory. The number of times the program overwrites the data is configurable any integer from 1 to 7 times and the default is 1. The address book data is not cleared. In case of "Clear All Memory program" operation is interrupted, this TSF requires authentication of the administrator who called this program, after the cancel operation is selected. The administrator is identified when the cancel operation is taken and is authenticated when the administrator password is entered. This TSF hides the typed password character. If an incorrect password is entered three times in a row, this program stops accepting further authentication attempts for five minutes (Clear All Memory program cancellation operation).

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

This program is invoked from the operation panel by the administrator who is identified and authenticated by the authentication function (TSF_AUT) and overwrites the address book data in the HDD. The number of times the program overwrites the data is configurable any integer from 1 to 7 times and the default is 1.This program does not accept the cancel operation.

d) Clear Document Filing Data program:

This program is invoked from the operation panel by the administrator who is identified and authenticated by the authentication function (TSF_AUT) and overwrites all spool image data and filing image data in the HDD. The number of times the program overwrites the data is configurable any integer from 1 to 7 times and the default is 1.This program accepts the cancel operation as well as the Clear All Memory program does.

e) Clear All Data in Job Status Jobs Completed List program:
This program is invoked from the operation panel by the administrator who is identified and authenticated by the authentication function (TSF_AUT) and overwrites the jobs completed data list in the HDD. The number of times the program overwrites the data is configurable any integer from 1 to 7 times and the default is 1. This program does not accept the cancel operation.

f) Power Up Auto Clear program:
This program overwrites and clears the data when the TOE is turned on, with the exception that the TOE has any reserved transmission jobs or any fax/Internet fax reception jobs not yet printed out.
Whether this program is run or not when the TOE is turned on is depends on the value set beforehand. The data to be cleared by this program is also depends on the value. Those values are configurable for each object and the default is "disabled" for all. This program clears either of all data that the Clear All Memory program covers or the specified data in the HDD. Among the data in the HDD, several kinds of data that can be specified are spool image data, filing image data or jobs completed data list. The number of times the Power Up Auto Clear program overwrites the HDD when the MFD is turned on is configurable any integer from 1 to 7 times and the default is 1.This program accepts the cancel operation as well as Clear All Memory program does.

(4) Authentication function (TSF_AUT):
This TSF enforces the identification and authentication of the administrator by the administrator password. The administrator password is allowed to use only 5 to 32 alphanumeric and/or symbol characters. Only this function provides the interfaces of the function for the administrator such as the Data Clearance Settings or Change Administrator Password only when succeeding in authentication of the administrator. The administrator is identified by calling administrator's functions from the operation panel or the web page, or the login operation of the administrator, and authenticated by entering the password. This TSF hides the typed password character or requires hiding the character. 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 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 is digits from 5 to 8 characters. In the confidential file password authentication which allows operations of a confidential file, this TSF hides the typed password character and, if an incorrect confidential file password is entered three times in a row, the TSF stops accepting further authentication attempts and locks the file to prohibit any operation.
The TFS also provides functions that, via the web, allow to export encrypted data to a client and to import both encrypted data and not encrypted data from a client.
This TSF provides the following management functions for the document filing function. Only the administrator identified and authenticated by TSF_AUT is allowed to execute these functions.

- Disabling of Document Filing: disables each saving mode according to the job type. The setting that prohibits all modes except the confidential mode (without password) is default and recommended value.
- 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 not specified for "Hold". And the job specified "Hold" is just held but not printed even if specified to print. This function is recommended to be used in the environment with a high risk that the third person takes away the output paper.

- Release the lock of confidential files: releases the locked confidential files by the failure of the confidential file password authentication.

(6) Network protection function (TSF_FNP):

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

a) Filter function:

This function denies the communication with the other party who is not intended based on the IP address and MAC address. The administrator identified and authenticated by TSF_AUT can set the range of IP address (up to 4 ranges) that is permitted or denied and permitted MAC addresses (up to 10).

b) Communication data protection function:

This function provides the HTTPS communication function to protect communication between a client and the TOE from wiretapping the web. This function also provides the IPP-SSL communication function to protect the data sent from the printer driver of the client from wiretapping.

c) Network settings protection:

This function provides the interfaces only to the administrator identified and authenticated by TSF_AUT to manage the network settings data from the operation panel or 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 requirements in CC Part 3. Details for evaluation activities are reported in the Evaluation Technical Report. It described the description of overview of the TOE, and the contents and verdict evaluated by each work unit prescribed in CEM.

3.2 Overview of Evaluation Conducted

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

Evaluation has started on 2009-09 and concluded by completion the Evaluation Technical Report dated 2010-02. The Evaluation Facility received a full set of evaluation deliverables necessary for evaluation provided by developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the Evaluation Facility directly visited the development and manufacturing sites on 2009-12 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff hearing. Further, the Evaluation Facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on 2009-12.

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

As for concerns indicated during evaluation process by the Certification Body, the certification review was sent to the Evaluation Facility. These were reflected to evaluation after investigation conducted by the Evaluation Facility and the developer.

3.3 Product Testing

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

3.3.1 Developer Testing

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

1) Developer Test Environment

Test configuration performed by the developer is showed in the Figure 3-1.

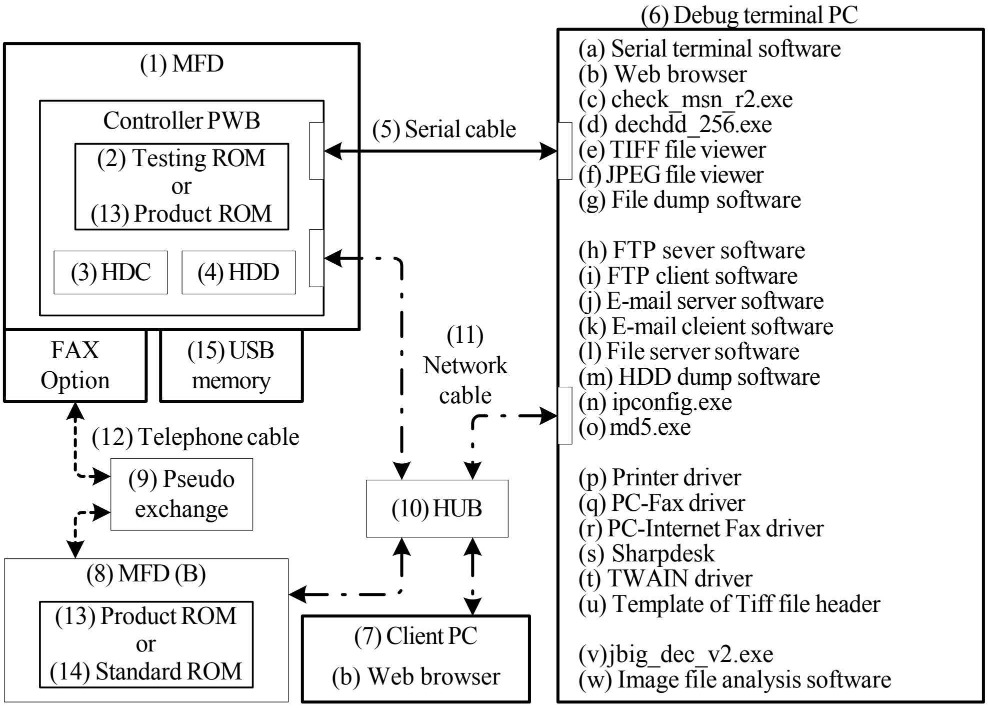

Figure 3-1: Configuration of Developer Testing

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

2) Outlining of Developer Testing

Outlining of the testing performed by the developer is as follow;

a. Test outline

Outlining of the testing performed by the developer is as follows;

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

(1) Product ROM: for the test where security functionality can be externally observed.
(2) Testing ROM: for the test where security functionality such as the cryptographic operation function and the data clear function can not be externally observed. The security functionality is confirmed through command operations and 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's 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 test of 57 items is performed by the developer.
The coverage analysis is conducted and it is verified that all security functions described in the functional specification and the external interfaces were thoroughly-tested. Then, the depth analysis is conducted and it is verified that all the subsystems described in the TOE design and the subsystem interfaces are thoroughly-tested.

c. Result

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

3.3.2 Evaluator Independent Testing

Evaluator executed the independent testing to reconfirm that Security functions are certainly implemented from the evidence shown by the process of the evaluation. Outlining of the independent testing performed by the developer is as follows;

1) Evaluator Independent Test Environment

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

2) Outlining of Evaluator Independent Testing

Independent testing performed by the evaluator is as follows;

a. In terms of Evaluator Independent Testing

Evaluator devised the independent testing for the interfaces referring the developer testing and the provided documentation to supplement the accuracy and sufficiency in the developer testing in terms of followings;

(1) To test the interfaces more rigorously, conduct the same types of tests as conducted by the developer using the parameters not used in the developer testing.
(2) To test the interfaces more sufficiently, conduct the same types of tests as conducted by the developer by stimulating the interfaces using methods of starting that were not used in the developer testing (especially logical

external interfaces).

(3) To test the interfaces more sufficiently, conduct the same types of tests as conducted by the developer in the modes that were not used in the developer testing.

(4) To test the interfaces more sufficiently, conduct different types of tests from those conducted by the developer using testing approaches that were not used in the developer testing.

(5) To test the interfaces more sufficiently, conduct the same types of tests as conducted by the developer in initial conditions that were not used in the developer testing.

(6) To test the interfaces more sufficiently, use a special test tool for cases where interfaces can not be stimulated by the test tool used in the developer testing or their behaviour can not be observed.

In tests reproducing those conducted by the developer, considering the completeness of types of TSF, TSF subsystems and interfaces, out of 57 items tested by the developer, 19 items (accounting for more than 30%) were selected for the testing.

b. Test outline

Outlining of evaluator independent testing performed by the evaluator is as follows;

Two testing approaches were used: one is observing the responses by stimulating TSFI and the other is observing the execution results made by the test tool (including confirming behaviour of subsystems that do not provide external interfaces) as same as the developer testing.
Independent testing is executed to supplement the accuracy and sufficiency in the developer testing, considerately as follows;
Parameters, method of starting interfaces (operation from USB), modes (such as the night mode), testing approaches (test on interfaces on the web page) and initial conditions (immediately after document filing data is restored), all of which were not used in the developer testing.
Furthermore, 10 tests are conducted in all from the viewpoint of depth (behaviour of internal interfaces of subsystems) and observing the followings;
exclusion control of authentication failure of the administrator and a confidential file, confirmation of encryption for SSL communication (encryption algorithm is not claimed as a security function), all of which SFR does not address, and observing behaviour of interfaces by stimulating them using a tool that was not used in the developer testing.

c. Result

All evaluator independent testing conducted is completes correctly and could confirm the behaviour of the TOE. The evaluator also confirmed that all the test results are consistent with the behaviour.

3.3.3 Evaluator Penetration Testing

Evaluator devised and conducted the necessary penetration testing about the possibility of exploitable concern from materials of evaluation process.
Outlining of Evaluator penetration testing is as follows;

1) Outlining of Evaluator Penetration Testing

Outlining of penetration testing performed by the evaluator is as follows;

a. Vulnerability of concern

Evaluator searched the potential vulnerability from information which is within the public domain and provided evidence to identify the following vulnerability that requires penetration testing.

By investigating the evidential materials from the view point of bypassing, falsification, direct attacks, monitoring and misuse, 13 candidate items for testing were identified.

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). Also, keyword retrievals conducted from each of open information held by JVN iPedia, NIST and openssl identified several candidate items for the testing.

b. Scope of Test Performed

Evaluator conducted the following penetration testing to determine the exploitable potential vulnerability.

Based on the search results above, for the web application, the following check items were tested on the browser: tests where web browser settings (valid/invalid of scripts) are changed and where the browser directly accesses the URL that requires user authentication. 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 falsification and misuse, the following tests were conducted: to see the behaviour if a password includes special characters, if simultaneous accesses in combination from the MFD's operation panel and the web will cause any confusion, and if specified encrypted communication is performed using a network protocol analysis tool.

c. Result

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

3.4 Evaluation Result

3.4.1 Evaluation Result

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

3.4.2 Evaluator comments/Recommendations

There are no recommendations to be advised to consumers.

4. Conduct of 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.

Concerns found in certification process were prepared as certification review and were sent to evaluation facility.

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

5. Conclusion

5.1 Certification Result

The Certification Body verified the Evaluation Technical Report, the Observation Report and the related evaluation evidential materials submitted and confirmed that all evaluator action elements required in CC Part 3 are conducted appropriately to the TOE. The Certification Body determined the TOE is satisfied the assurance requirements of EAL3 components 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 Functions

The abbreviations relating to 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 address.
HDC:	Hard Disk Controller.
HDD:	Hard Disk Drive.
HTTPS:	HTTP over SLL, HTTP with protection of SSL.
IPP:	Internet Printing Protocol, a communication protocol for printing.
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 equipped with copier, printer, scanner and 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 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.

MAC address: A call sign to identify devices of communication media used for MAC.

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 firmware of the TOE, volatile memory, HDC, HDD and others.

Controller firmware The firmware that controls the controller board in the MFD. This is stored in the ROM and mounted on the controller board.

Operation on saved files: Calls up the saved image data and operate it.

Subnetwork: A part of internal network divided by router.

Confidential file: The data that the user saved with the protection of a password (confidential file password) to prevent the others from manipulating.

Spool: Storing the job's image data to the MSD temporary to increase the input and output efficiency.

Clear All Memory The function that overwrites all image data and the jobs completed list data stored to the MSD in the MFD. This function is invoked by the operation of the administrator.

Document filing: The function that stores image data handled by the MFD into the HDD, for user's later operations, such as a printing or a transmission.

Hold: To store the job from printer driver by filing.

Non-volatile memory: The memory device that retains its contents even when the power is turned off.

Memory: A memory device; in particular a semiconductor memory device.

Lock The function to stop accepting passwords if incorrect passwords are entered in a row.

7. Bibliography

[1] MX-FR14 Security Target Version 0.02 (October 19, 2009) 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-FR14 Evaluation Technical Report, February 17, 2009, Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security