Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2009-03-31 (ITC-9253)
Certification No.	C0227
Sponsor	Sharp Corporation
Name of TOE	MX-FR11
Version of TOE	C.10
PP Conformance	None
Conformed Claim	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.
2009-07-27

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 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-FR11 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-FR11 C.10" (hereinafter referred to as the "TOE") conducted by Information Technology Security Center, Evaluation Department (hereinafter referred to as "Evaluation Facility"). It reports to the sponsor, Sharp Corporation, and provides information to 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, the summary of security specifications and rationale of sufficiency are specifically described in the ST.

This certification report assumes the above persons (sponsor, system operators and users of the TOE) to be a reader. 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-FR11
Version:	C.10
Developer:	Sharp Corporation

1.2.2 Product Overview

The TOE is an IT product to protect data in a Multi Function Device (MFD).
The main part of the TOE is the firmware in ROMs and HDD for the MFD. By replacing the MFD standard firmware, it offers the security function and controls the entire MFD. The HDC (Hard Disk Controller), a hardware part in the MFD, is also a part of the TOE and is controlled by the firmware.

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

The main security functions of the TOE are cryptographic operation function, data clear function, confidential file function, network protection function, and fax flow

control function, which are aiming to counter unauthorized attempts to steal image data stored in the MFD where the TOE is installed.

1.2.3 Scope of TOE and Security Functions

1.2.3.1 Physical Scope of TOE

The physical scope of the TOE is shaded in Figure 1-1. The main part of the TOE is in the MFD's controller firmware, provided by two ROM boards and a USB memory device. Part of the security functions is implemented in the HDC of the MFD, which is also included in the scope of the TOE.

- ROM:
  It contains a part of the controller firmware. When the TOE is installed to the MFD, two ROMs of the standard firmware are removed from the controller board and replaced with two ROMs of the DSK.

- MAIN:
  It is a part of the controller firmware and installed from the USB memory device of the DSK to the HDD in the MFD.

- HDC:
  It is an integrated circuit part that is mounted on the controller board in the MFD beforehand.

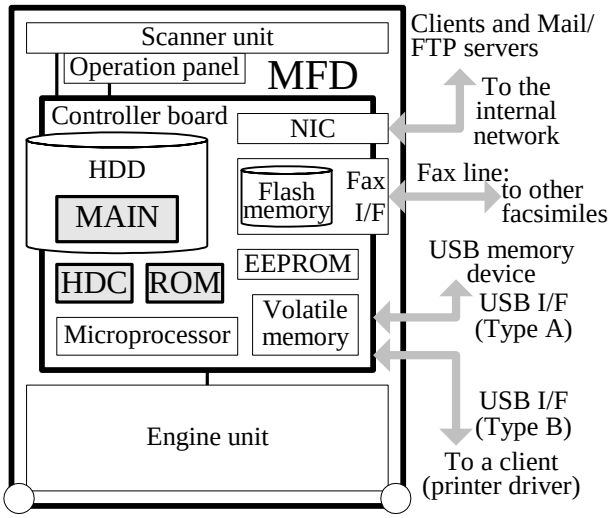

Figure 1-1: Physical configuration of the MFD and physical scope of the TOE

1.2.3.2 Logical Scope and Security Function of TOE

Figure 1-2 shows the logical configuration of the TOE. The thick-lined frame indicates the logical scope of the TOE. 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.

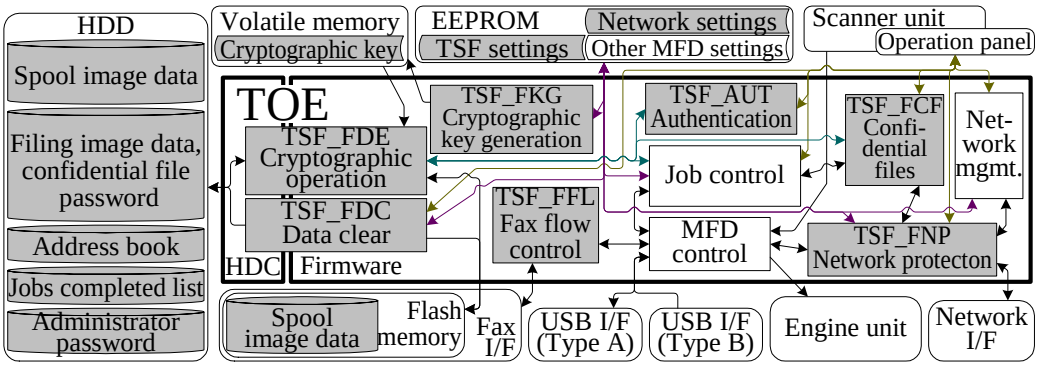

Figure 1-2: Logical configuration of the TOE

The main part of the TOE is the firmware for the MFD, providing security functions as well as controlling the entire MFD. Part of the TOE security functions (TSFs) is implemented in the HDC and invoked by the TSFs in the firmware. The security functions are as follows;

a) Cryptographic operation function:
To encrypt image data, etc., that the MFD handles before it is written to the HDD or Flash memory in the MFD.

b) Cryptographic key generation function:
To generate the cryptographic key for the cryptographic operation function.

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

d) Authentication function:
To identify and authenticate an administrator by means of the administrator password. It includes a management function that changes the administrator password.

e) Confidential file function:
To provide password protection for image data on the HDD stored by users to protect them from being reused by others.

f) Network protection function:
To prevent unauthorized accesses over the network, wiretapping of communication data and unauthorized modification of the network settings.

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

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-FR11 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-FR11 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 prepared by the Evaluation Facility and evaluation evidential materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Evaluation is completed with the Evaluation Technical Report dated July 2009, submitted by the Evaluation Facility, 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.

Table 2-1: Assumed Threats

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

2.1.2 Organisational Security Policies

Table 2-2 shows organisational security policies required in the use of the TOE.

Table 2-2: Organisational Security Policies

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

2.1.3 Assumptions for Operational Environment

Assumptions required in an environment using this TOE are presented in Table 2-3. Unless these assumptions are satisfied, the effective performance of the TOE security functions is not assured.

Table 2-3: 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 MFD connects nothing other than devices allowed to communicate with the MFD.
A.OPERATOR	The administrator is a trustworthy person who does not take improper action with respect to the TOE.

2.1.4 Documents Attached to Product

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

For Japan	MX-FR11 Data Security Kit Operation Manual (in Japanese) [CINSJ4570FC51]	MX-FR11 Data Security Kit Notice (in Japanese) [TCADJ2013FCZZ]
For outside Japan	MX-FR11 Data Security Kit Operation Manual (in English) [CINSZ4571FC51]	MX-FR11 Data Security Kit Notice (in English) [TCADZ2014FCZZ]

2.1.5 Configuration Requirements

The TOE operates on the following digital MFDs made by Sharp Corporation; MX-3600FN, MX-4100FN, MX-4100N, MX-4101FN, MX-4101N, MX-4101NJ, MX-5000FN, MX-5000N, MX-5001FN, MX-5001N and MX-5001NJ.

2.2 Security Objectives

The TOE counters the threats described in 2.1.1 with the security functions equipped, and satisfies the organisational security policies defined in Section 2.1.2. as follows;

(1) Cryptographic key generation function (TSF_FKG):

The TOE generates cryptographic keys (common key) to support the cryptographic operation function for user data and TSF data. The cryptographic keys (common key) are generated every time the MFD is powered on. The TOE generates 128-bit and 256-bit secure keys and stores the keys into the volatile memory.

(2) Cryptographic operation function (TSF_FDE):

The TSF always encrypts user data and TSF data before writing them to the MSD. When necessary, the TSF reads the data from the MSD and decrypts them for further use. For encryption and decryption, the cryptographic keys that are generated by the cryptographic key generation function (TSF_FKG) are used.

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

(3) Data clear function (TSF_FDC):

The TOE 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 is contained in 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 into the HDD or Flash memory in order to process a job when the job is completed. 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 on the HDD, and all of the spool image data in the Flash memory. This program does not clear the address book data.

To cancel this program, the administrator is required to select a cancellation, and then the TSF requires the administrator to enter the administrator password. While entering the password, the TOE shows as many asterisks as characters entered. The overwriting operation is cancelled only if the correct password is entered. If an incorrect password is entered three times in a row, the administrator password is locked. In five minutes after the locking, the program unlocks the administrator password automatically.

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

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

d) Clear Document Filing Data program:

This program is invoked by the administrator who has been identified and authenticated by the authentication function (TSF_AUT) and overwrites image data on the HDD. The data to be cleared by this program is specified one or more from the following choices by the administrator when this program is invoked: all of the spool image data on the HDD and all of the 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 data when the TOE is powered on, unless the TOE has any reserved scan jobs or fax-send jobs or any fax/Internet fax-receive jobs which are not yet printed out.

Whether this program is invoked or not when the TOE is turned on depends on the settings set beforehand. The data to be cleared by this program also depend on the settings; either all the data that the Clear All Memory program covers or specified data on the HDD. One or more kind of data can be specified as the 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 configuration functions below (to query and modify) only 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
  It is the setting to specify data areas to be cleared using the Power Up Auto Clear program. The default is that Power Up Auto Clear program is disabled for every data (no data is specified).
- 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 which is 5 to 32 characters consisting of any of the 95 kinds of characters: 52 alphabetic characters, 10 numeric characters and 33 symbolic characters. This function provides the interfaces of the functions 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, this TSF shows as many asterisks as characters entered without showing the characters entered.

If an incorrect password is entered three times in a row in the authentication process of the administrator password, the 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.

(5) Confidential files function (TSF_FCF):

It provides functions to re-operate (print out, etc.) saved confidential files; when a user saves image data into the MFD as a confidential file, the file of the data is protected by a password, and authentication is required from the operation panel or via Web before calling it up and using it. The confidential file password shall be 5 to 8 numeric characters.

During the authentication before reusing a saved 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 only by the administrator who has been identified and authenticated by authentication function (TSF_AUT).

As one of the operations, this TSF allows only the user, who stored confidential files and has been identified and authenticated by the TSF, to change the password of the confidential files. It verifies the new password shall be 5 to 8 numeric characters. It also provides the function to change the property of the confidential file; when the property is changed to other than "Confidential", the password is deleted. On the other hand, to change the property to "Confidential", the TSF requires the user to set a confidential file password of 5 to 8 numeric characters.

This TSF exports the encrypted data to the Web browser of the client. It also imports 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 administrator whom TFS_AUT has identified and authenticated to execute them.

[Management functions for improving the effectiveness of protection obtained by using the confidential file]

- Disabling of Document Filing:
  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 denies 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.

[Management function for locking confidential files]
- 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 the settings that the administrator configured beforehand based on IP addresses and MAC addresses. The TSF always cancels network packets from those users that do not meet the conditions, and it 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 functions:

- 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 printed data that are sent from the printer driver of the client
- The SNMP v3 function to prevent wiretapping of the SNMP-based communication between the client and the TOE
- The IPsec function to prevent wiretapping of all the IP-based communication between the client and the TOE

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

c) Network settings protection:

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

(7) Fax Flow Control (TSF_FFL):

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

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 2009-04 and concluded by completion of the Evaluation Technical Report dated 2009-07. 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 site on 2009-05 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 2009-05.

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.

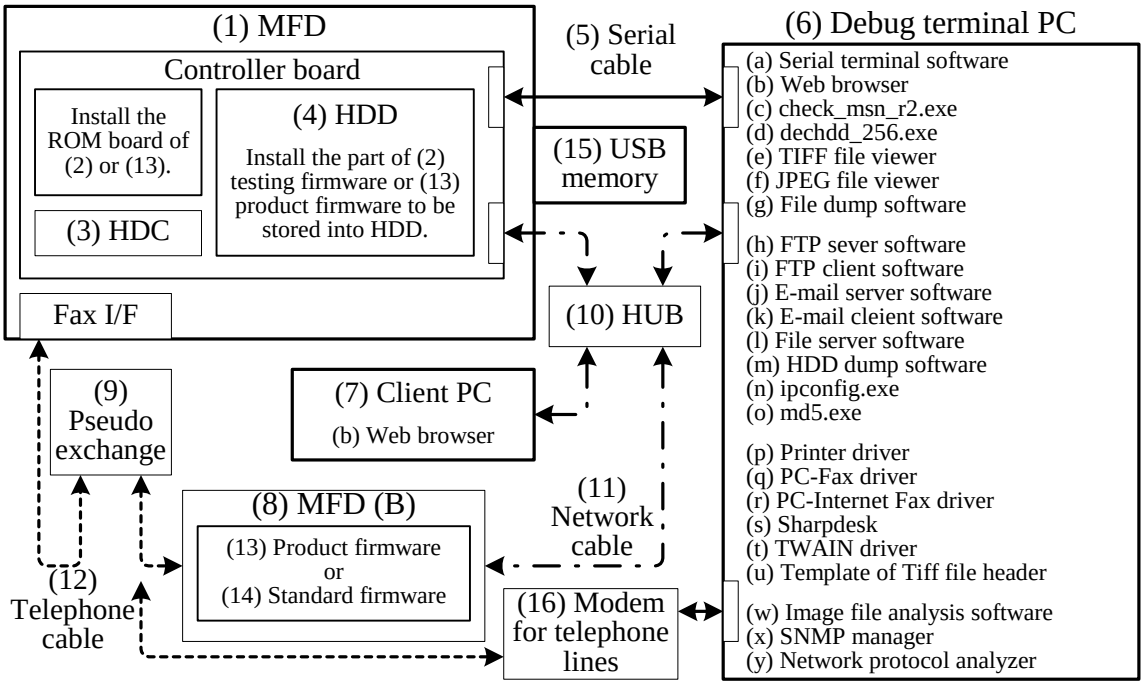

Figure 3-1: Configuration of the Developer Testing

The MFD used in the developer testing is one of the several MFDs identified in the ST; namely, MX-4101FN. 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 similar to that 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, the product ROM or the testing ROM, was used in compliance with the characteristics of each testing. To confirm the testing results, the testing ROM was provided with the capability of outputting from a serial port, of outputting the cryptographic key seed and the cryptographic key, of switching between enabling and disabling of the cryptographic operation, and of specifying data to be overwritten, without affecting the security functions to be tested.

The developer conducted the testing by stimulating interfaces (including turning on/off the MFD, manual operations from the operation panel of the MFD, manual operation from the client terminal) and by observing responses (including observation from the client terminal, from the operation panel of MFD, and from the debug terminal).

b. Scope of Testing Performed

The testing is executed on 62 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.

2) Summary of Evaluator Independent Testing

Independent testing performed by the evaluator is as follows;

a. Viewpoints of Independent Testing

The evaluator devised the independent testing based on the developer testing and the provided evaluation evidential materials in terms of the following viewpoints.

- The main TSFIs were selected so that all TSFs were covered in the testing.
- Parameters and testing approaches, which were different from those used in the developer testing, were used.
- In each interface testing, behaviour was tested in terms of timings and operations which were not likely to have been considered in the developer testing.
- It was considered that both types of interfaces; those on the operational panel and those on the Web browser, were covered.

b. Outline of Evaluator Independent Testing

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

Types of testing	Number of tested TSFs	Number of items

Evaluator devised testing	6	11
Sampling testing	(All) 7	18
Total		29

In the evaluator devised testing, 6 security functions were covered, excluding the cryptographic key generation function (TSF_FKG). 4 types of tests were conducted using external interfaces including the operation panel, Web browser, network interfaces and fax interfaces. The cryptographic key generation function (TSF_FKG) was excluded from the testing because the function only had the TSFI of turning on the MFD and the TSFI was tested in the sampling test. The evaluator devised testing included items to confirm whether the encryption would function well after restoring from PC was performed, whether the Power Up Auto Clear program would function well after Clear Document Filing Data had been cancelled, and whether the fax flow control would reject reception as expected.

In the sampling testing, all the 7 security functions were covered. It contains 5 types of external interfaces, including the operation panel, Web browser, network interfaces, fax interfaces, and turning on the MFD, so it is considered enough for sampling.

c. Results

All evaluator independent testing conducted 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 public domain information on vulnerability and attacks in general as well as the provided evidence to identify the following vulnerabilities which require penetration testing.

In the analysis of the public domain information on vulnerability (websites such as the JVN, US-CERT and CVE) based on keywords relating to the TOE's product classification and functionality which were described in the evidential materials such as the ST, no vulnerability was found to be a candidate for the evaluation penetration testing. Therefore, the following 24 vulnerabilities were identified as candidates for the evaluation penetration testing; 4 potential vulnerabilities relating to newly-added functions and networks in this TOE series, 10 potential vulnerabilities based on the public domain attacks in

general described in the *Vulnerability Analysis Guidance Ver. 1* issued on May 16, 2007 by IPA, and 10 potential vulnerabilities based on the search results of the evidential materials.

b. Scope of Test Performed

The evaluator conducted the following penetration testing to determine the exploitable potential vulnerabilities.
In the penetration testing, 24 tests based on the search results of above mentioned were conducted.
The main penetration testing includes;

(1) Tests on the potential vulnerabilities based on the public domain information to confirm that:
- The assets would not be leaked by FTP-based accesses.
- The security functions would not be disabled by unintended configuration of IPsec and SNMPv3.
- The TOE would not malfunction and leak the assets even if useless packets were sent to the SSL port.

(2) Tests on the potential vulnerabilities based on the public domain attacks in general to confirm that:
- The security would not be harmed from the interfaces for service technicians.
- The Copy Start screen appearing on the operation panel when the MFD is turned on would not leak confidential information.
- Clearing would be completed even if the network was shut down while the clearing was in progress.

(3) Tests on the potential vulnerabilities based on the search results of the evidential materials to confirm that:
- An MFD without the TOE would not leak the image data when tandem copying was performed.
- The security functions would not be disabled even if the ROMs were replaced.
- The security functions would not be disabled even if the TOE ran without the volatile memory and no cryptographic key was generated.
- Authentication via the web browser would not be bypassed.

c. Results

In the penetration testing conducted by the evaluator, the evaluator could not find the exploitable vulnerabilities that attackers could exploit who have 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 during the evaluation process.

1. Evidential materials submitted were sampled, the contents were examined, and the related work units shall be evaluated as presented in the Evaluation Technical Report.
2. Retionale of evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.
3. The Evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

5. Conclusion

5.1 Certification Result

As a result of verification of submitted Evaluation Technical 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.

DSK:	Data Security Kit MX-FR11, 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 part of memory.
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
IPsec:	Security Architecture for Internet Protocol: a communication protocol, consisting of ensuring integrity, providing authentication mechanism using the AH (Authentication Header), data encryption using the ESP (Encapsulated Security Payload), key exchange using the IKE (Internet Key Exchange protocol), protecting data from being tampered and maintaining confidentiality of data by the IP packet.
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, 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
USB:	Universal Serial Bus, a serial bus standard to connect between IT equipments.
SNMP:	Simple Network Management Protocol, a communication protocol which manages network devices.
SNMP v3:	SNMP version 3, the SNMP which implements functions for protecting against wiretapping, spoofing, tampering, and replaying, by authenticating and encrypting SNMP packets transmitted on a network.

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

Controller board:	The board that controls the whole MFD; containing a microprocessor, volatile memory, HDC, HDD, and others, to execute firmware of the TOE.
Controller firmware:	The firmware that controls the controller board in the MFD; it is stored in the ROM board and the HDD, which are implemented on the controller board.
Document filing:	The function that stores image data, which the MFD handles, into the HDD inside MFD, in order for users to re-operate (printing and transmission, etc.) afterwards; this is also called "Filing" in this report.
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 sent from a printer driver using the document filing function.
IP address:	A call sign, used for IP, to identify devices for communication.
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.
MAC address:	A call sign, used for MAC, to identify devices on communication media.
Non-volatile memory:	A memory device that retains its contents even if the power is turned off.
Subnetwork:	A part of internal network divided by router.
Volatile memory:	A memory device, the contents of which vanish when the power is turned off.

7. Bibliography

[1] MX-FR11 Security Target Version 0.03 (April 24, 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-FR11 Evaluation Technical Report, Version 2.0, July 21, 2009, Information Technology Security Center, Evaluation Department