Certification Report

Buheita Fujiwara, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	August 8, 2006 (ITC-6095)
Certification No.	C0069
Sponsor	Sharp Corporation
Name of TOE	MX-FRX3
Version of TOE	Version M.10
PP Conformance	None
Conformed Claim	EAL3 Augmented with ADV_SPM.1
TOE Developer	Sharp Corporation
Evaluation Facility	Japan Electronics and Information Technology Industries Association, Information Technology Security Center (JEITA ITSC)

This is to report that the evaluation result for the above TOE is certified as follows.
December 15, 2006

Haruki Tabuchi, Technical Manager
Information Security Certification Office
IT Security Center
Information-technology Promotion Agency, Japan

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 2.3
- Common Methodology for Information Technology Security Evaluation Version 2.3

Evaluation Result: Pass

"MX-FRX3 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-FRX3 Version M.10” (hereinafter referred to as “the TOE”) conducted by Japan Electronics and Information Technology Industries Association, Information Technology Security Center (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 and manuals (please refer to “1.5.9 Documents Attached to Product” for further details) attached to the TOE together with this report. The assumed environment, corresponding security objectives, security functional and assurance requirements needed for its implementation and their summary specifications are specifically described in ST. The operational conditions and functional specifications are also described in the document attached to the TOE.

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.

Note: In this Certification Report, IT Security Evaluation Criteria and IT Security Evaluation Method prescribed by IT Security Evaluation and Certification Scheme are named CC and CEM, respectively.

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows:

Name of Product:	MX-FRX3
Version:	Version M.10
Developer:	Sharp Corporation

1.2.2 Product Overview

The TOE consists of two parts that enhance security functions for a Multi-Function Device (hereafter referred to as “MFD”); one part is an HDC, which is a hardware part in the MFD, and the other is MFD firmware. It is provided as an optional product. It replaces the MFD standard firmware by installing to the MFD, and offers the security functions and controls the entire MFD. The TOE primarily consists of the cryptographic operation function, data clear function and confidential files function. These functions are intended to counter attempts to steal image data in a MFD.

The cryptographic operation function encrypts image and other data that the MFD handles, before storing them in the HDD or Flash memory in the MFD. The data clear function writes random values or some fixed value over the area of the encrypted data in the HDD or Flash memory in the MFD. The confidential files functions make it possible that user stores the image data to the HDD with password to prevent the others from reusing it without permission.

1.2.3 Scope of TOE and Overview of Operation

The TOE is provided by two ROM boards which are firmware upgrade kit for the MFD and its HDC. Relation between the TOE and the MFD is shown in the Figure 1-1. The TOE is shown as shaded areas in the Figure 1-1.

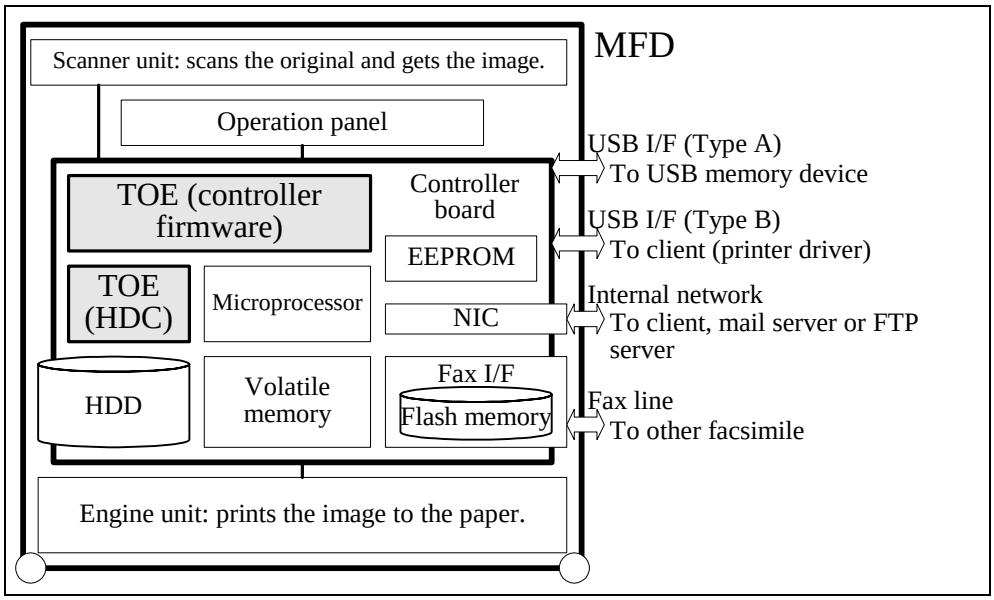

Figure 1-1: The physical configuration of the MFD and the physical scope of the TOE

The logical configuration of the TOE is shown in Figure 1-2. In the Figure 1-2, the area in the thick-lined frame indicates the TOE. The rectangles indicate the TOE's functions and the rounded boxes indicate hardware devices. Among the TOE functions, the security functions are shaded. The arrow indicates the data flow.

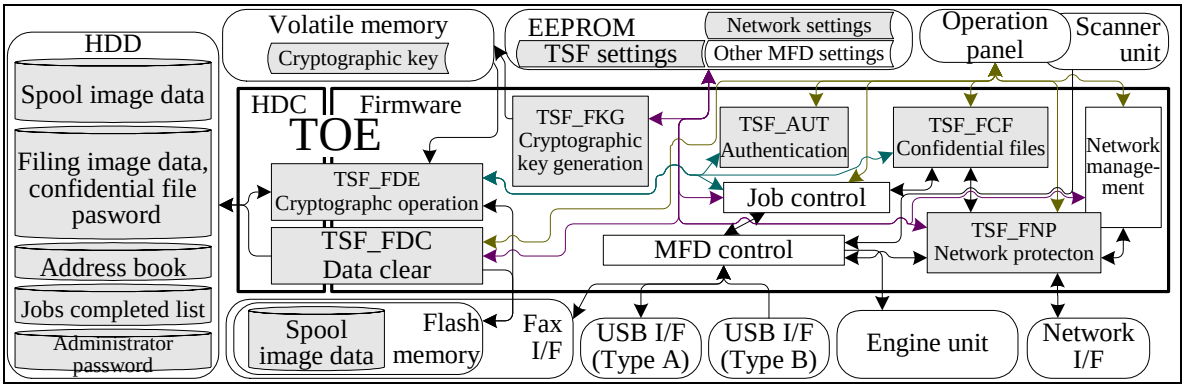

Figure 1-2: Logical configuration of the TOE

As well as the standard MFD firmware, the TOE has the MFD functions, which are copy, printer, network scanner, fax transmission, fax reception, and PC-Fax.
As well as the standard MFD firmware, the TOE has the following MFD functions: copy, printer, scan send, fax transmission, fax reception, and PC-Fax. The TOE executes security functions automatically while each of these MFD functions is being executed. Functions of the TOE and MFD functions are shown below.

1.2.3.1 TOE Functionality

The following functions are included within the logical scope of the TOE.

a) Cryptographic operation function (TSF_FDE):
encrypts the user data and TSF data that is stored to the HDD or Flash memory in the MFD and decrypts the user data and TSF data that is retrieved from the HDD or Flash memory.
b) Cryptographic key generation function (TSF_FKG):
generates the cryptographic key for the cryptographic operation function. The generated key is stored to the volatile memory in the MFD. A *seed* of the cryptographic key is generated once when the TOE is installed. From then on, a cryptographic key is always generated from the seed for the MFD whenever powered on.
c) Data clear function (TSF_FDC):
overwrites the data to prevent the leak of information from the HDD or Flash memory in the MFD. This function consists of each data clear program (*Auto Clear at Job End*, *Clear All Memory*, *Clear Address Book Data and Registered Data in MFP*, *Clear Document Filing Data*, *Clear All Data in Job Status Jobs Completed List* and *Power Up Auto Clear*) and setting function for them (Data Clearance Settings). "*Auto Clear at Job End*" is invoked by each job and document filing function in the MFD functions.
d) Authentication function (TSF_AUT):
identifies and authenticates an administrator by means of the administrator password. The administrator can manage the TSF data that contains the administrator password by this authentication.
e) Confidential files function (TSF_FCF):
requires the authentication by means of the confidential file password to print or transmit the image data (confidential file) that is stored to the MFD using the document filing function. If an incorrect password for a confidential file is entered three times in a row, this function locks that file. Only the administrator can release the locked file.
f) Network protection function (TSF_FNP):
consists of the following three functions.
    1. Filter function: restricts the other party to communicate by the terms of IP address or MAC address.
    2. Communication data protection function: protects the communication data by SSL. If the client or protocol that is not supported to use SSL is used, this function is not available.
    3. Network settings protection: provides the following network management function only to the administrator and do not allow other user to uses it.
g) Job control function:
provides the user interface and control the action for each MFD function such as job function, address book function and document filing function. This also manages the job as queue and keeps the jobs completed list to the HDD.
h) MFD control function:
controls MFD hardware. This also converts the data format between the data to receive or transfer and the image data in the MFD for the jobs that require the communication.
i) Network management function:
the function for the administrator to query and modify the address, the port and DNS for using the network functions of the MFD. This function is invoked by the network protection function (TSF_FNP).

1.2.3.2 MFD Functionality

The most MFD functions are invoked by the operation from the operation panel of the MFD. A part of them are invoked by the operation from the Web for the remote operation or receiving the data

a) Job function:
receives the image data from the MFD's scanner unit, FTP, USB memory device or fax reception, spools the image data to the HDD or Flash memory in the MFD. The spooled image data are printed or transferred to the outside through the network. This function is realized by the job control function and the MFD control function.
b) Document filing function:
stores the job's image data to the HDD in the MFD to operate it later. The confidential files function is called when deleting, backup or changing the property is specified for the management of the data.
c) Address book function:
stores the destination fax number or the E-mail address. The address book is available for entering the destination for transferring. The address book data is stored to the HDD and storing, modifying and deleting are available by the operation from the operation panel or the Web for remote operation. This function is invoked by the job control function.

1.2.3.3 Assets protected by the TOE

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

The most MFD functions are invoked by the operation from the operation panel of the MFD. A part of them are invoked by the operation from the Web for the remote operation or receiving the data

a) Image data that the MFD functions spool to process jobs:
the image data that the TOE itself temporarily spools to the HDD or the Flash memory in the MFD for processing jobs when the user uses the MFD functions. The image data that is logically deleted but remains physically in the HDD or the Flash memory when the jobs are finished or cancelled is also included in this data.
These data possibly contain the users' sensitive information.
b) Image data that users stored as a confidential files:
the image data that users stored to the HDD as a confidential file. The image data that is logically deleted but remains physically in the HDD when the user deleted is also included in this data.
These data possibly contain the users' sensitive information.
c) Address book data:
the address book data that users store by the address book function and is stored to the HDD. This data is the personal data (destination name, mail address, fax number and others) that proper users of the MFD use in cooperation. It is allowed to see every record in this data one by one from the operation panel.
d) Jobs completed list data:
the data of completed jobs as which the job control function keeps such as user name or document name of jobs from the printer driver, destination for fax transmission or reception and others to the HDD. It is allowed to see every record in this data one by one from the operation panel.
e) Network settings data:
the information about network settings that the MFD requires to connect to the network. It is possibly leaking of the assets to the network without intent or the threat for other TSF functions that this data is modified dishonesty.
The network settings data is TCP/IP settings (Enable TCP/IP, Enable DHCP, IP Address Settings), DNS Settings (Primary/Secondary DNS Server, Domain Name), WINS Settings (Enable WINS, Primary/Secondary WINS Server, WINS Scope ID), SMTP Settings (SMTP Server), LDAP Settings (Enable LDAP, LDAP Server), Tandem Settings (IP Address of Slave Machine, Disabling of Master Machine Mode), Port Control (Enabling or the port number for each network service).

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-FRX3 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 C of CC Part 1 (either of [5], [8] or [11]) and Functional Requirements of CC Part 2 (either of [6], [9] or [12]) 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], [10] or [13]) as its rationale. Such evaluation procedure and its result are presented in “MX-FRX3 Evaluation Technical Report” (hereinafter referred to as “the Evaluation Technical Report”) [17]. Further, evaluation methodology should comply with the CEM (either of [14], [15] or [16]).

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 December, 2006 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.

1.5 Overview of Report

1.5.1 PP Conformance

There is no PP to be conformed.

1.5.2 EAL

Evaluation Assurance Level of TOE defined by this ST is EAL3 Augmented with ADV_SPM.1.

1.5.3 SOF

This ST claims “SOF-basic” as its minimum strength of function.
The TOE is assumed to be used in general office environment that is protected against attacks from any external networks. Since the attack with direct access to the TOE or within the internal network is under observation of the administrator, no complicated attack should be assumed.
Therefore it is rational for the TOE to assume the attackers with low attack potential, and it is enough by the SOF-basis that minimum strength of function can be opposed to low-level.

1.5.4 Security Functions

Security functions of the TOE are as follow.

(1) Cryptographic key generation function (TSF_FKG):
The TOE generates a cryptographic key (common key) to support the encryption function of the user data and the TSF data. When the MFD is powered on, a cryptographic key (common key) is always generated from the seed that is generated from the random number. A 128-bit secure key is generated using the MSN-R Expansion algorithm for the AES Rijndael cryptogram. The MSN-R Expansion algorithm is a cryptographic key generation algorithm conformant to the Data Security Kit Encryption Standard. When installed, the TOE generates a seed that differs from an MFD to another. The key generated is held in the volatile memory.

(2) Cryptographic operation function (TSF_FDE):
This function always encrypts the user data and the TSF data when these data are written to the HDD or the Flash memory and decrypts them when these data are used.
The user data that are the target are 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 list data that are stored to the HDD. The TSF data that are the target are the confidential file password and administrator password.
The data is encrypted and decrypted by the AES Rijndael algorithm that is based on FIPS PUBS 197 with the 128 bits cryptographic key that is generated by the cryptographic key generation function (TSF_FKG).

(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 list data file. This function is invoked by the following each MFD program.

Every clear program overwrites the HDD as many times as specified in *Data Clearance Settings* with random values and the Flash memory once with a fixed value.

a) Auto Clear at Job End program:
This program overwrites the image data that has been spooled to the HDD or the Flash memory in order to process a job, when the job ends, and stored to the HDD using the document filing function (include the confidential files function), when the user deletes the data.

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 the spool image data, the filing image data, the jobs completed list data in the HDD, and the spool image data in the Flash memory. The address book data is cleared by the c) described below.
Before allowing cancelling Clear All Memory program while running, this TSF always requires authentication of the administrator who called this program whenever a cancel operation is taken.
If an incorrect administrator password is entered three times in a row while entering for authentication of cancel operation, 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 is identified and authenticated by the authentication function (TSF_AUT) and overwrites the address book data in the HDD.
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 the specified spool image data or the filing image data in the HDD.
This program accepts the cancel operation as well as *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 is identified and authenticated by the authentication function (TSF_AUT) and overwrites the jobs completed list data in the HDD.
This program does not accept the cancel operation.

f) Power Up Auto Clear program:
This program overwrites and clears the target data to be cleared automatically when the TOE is powered on, unless the TOE has any reserved transmission jobs or any Fax/Internet fax reception jobs not yet printed out. The guidance calls users' attention to this.
The settings that are configured beforehand are determined that this program is run or not when the TOE is powered on. The data to be cleared by this program is also according to those settings.
This program clears every data as well as the *Clear All Memory* program above, or the specified data in the HDD. The data in the HDD can be specified among the spool image data, filing image data or jobs completed list data.
This program accepts the cancel operation as well as *Clear All Memory* program.

g) Data Clearance Settings:
This TSF provides the following configuration functions below (querying and modifying) for the every program above only to the administrator identified and authenticated by the authentication function (TSF_AUT).

- Number of Times Auto Clear at Job End Program is repeated:
[accepts any integer between 1 and 7 inclusive. The default is 1.]
The number of times overwriting the data on the HDD for the *Auto Clear at Job End* program.

- Number of Times Data Clear is repeated:
[accepts any integer between 1 and 7 inclusive. The default is 1.]
The number of times overwriting the data on the HDD for the *Clear All Memory* program, the *Clear Address Book Data and Registered Data in MFP* program, the *Clear Document Filing Data* program and the *Clear All Data in Job Status Jobs Completed List* program.

- Power Up Auto Clear:
[enable or disable for each data. The default is that *Power Up Auto Clear* program is disabled for every data (no data is specified).]
Specify the data to be cleared by *Power Up Auto Clear* program.

- Number of Times Power Up Auto Clear Program is repeated:
[accepts any integer between 1 and 7 inclusive. The default is 1.]
The number of times overwriting the data on the HDD for the *Power Up Auto Clear* program.

(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. This function provides the interfaces of the function for the administrator such as the *Data Clearance Settings* or *Change Administrator Password* when the authentication of the administrator is successful. The administrator is authenticated by entering the password from the operation panel or the Web. The entered character is hidden when the password is entered. If an incorrect administrator password is entered three times in a row while entering for authentication of the administrator password, this program stops accepting further authentication attempts for five minutes.

(5) Confidential files function (TSF_FCF):
This TSF provides the function to protect the data that is stored by the document filing function by the password that the user who stored the data specified. The confidential file password is allowed to use only 5 to 8 numeric characters.
Whenever a user attempts some operations (preview, print and others) on a stored confidential file, this TSF requires the user to enter the confidential file password on the operation panel or the Web and allows operations only when a confidential file password is given and it is identical to the confidential file password during the storing of the file. The entered character is hidden when the password is entered. If an incorrect confidential file password is entered three times in a row during the authentication before an operation on a stored confidential file, this TSF stops accepting further authentication attempts and locks the file to prohibit any operation.
This TSF provides the following management functions. Only the administrator identified and authenticated by TSF_AUT is allowed to execute these functions.

a) Disabling of Document Filing:
disables to save the image data as the non-confidential file, which is saved with no password. The settings can be done for each job type. The default and recommended value is that all non-confidential modes are disabled.

b) Disabling of Print Jobs Other Than Print Hold Job:
disables the job to print out on the spot from the printer driver. This function denies the job without Holding and holds the Hold job by ignoring that the job is printed out or not. This function is recommended to use in the environment that has the high risk that the third person takes away the output paper.

c) Release the lock of confidential files:
releases locked confidential files by the failure of the authentication for the confidential file password.

(6) Network protection function (TSF_FNP):
This TSF consists of the following three functions that are related to the network.

a) Filter function:
This function restricts the communication according to the IP address and MAC address. The terms of address that are allowed or denied to communicate are configured by the administrator beforehand and this function allows or denies the communication with packet that has the address that coincides with the terms.

b) Communication data protection function:
This function provides the HTTPS communication function to keep the confidentiality of the Web communication between the client and the TOE. This function also provides the IPP-SSL communication function to keep the confidentiality of the data that is sent from the printer driver of the client. The confidentiality is realized by the encryption and cryptographic algorithms that are used are RSA, DES, Triple-DES, AES and SHA-1.

c) Network settings protection:
This function provides the interfaces to manage the network settings data that is required for the communication of the MFD at the (operation panel and) TOE Web. This function enforces the identification and authentication of the administrator same as TSF AUT before providing the interfaces that manage the network settings data.

.

1.5.5 Threat

This TOE assumes such threats presented in Table 1-1 and provides functions for countermeasure to them.

Table 1-1 Assumed Threats

Identifier	Threat
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 are not allowed to access to the MFD reads and modifies the address book data in the MFD through the internal network together.
T.SPOOF	An attacker 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 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.

1.5.6 Organisational Security Policy

Organisational security policy required in use of the TOE is presented in Table 1-2.

Table 1-2 Organisational Security Policy

Identifier	Organisational Security Policy
P.RESIDUAL	Upon completion or interruption of a job, the user data area spooled to the MSD shall be overwritten one or more times. The user data area in the MSD that is deleted by user shall be overwritten one or more times. When the MFD is disposed of or its ownership changes, all user data areas in the MSD shall be overwritten one or more times.

1.5.7 Configuration Requirements

MFD made by SHARP, that TOE runs on are listed below:
MX-5500N, MX-6200N, MX-7000N, MX-5500NJ, MX-6200NJ and MX-7000NJ.

1.5.8 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 1-3.
The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

Table 1-3 Assumptions in Use of the TOE

Identifier	Assumptions Definition
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.
A.OPERATOR	The administrator is a trustworthy person who does not take improper action with respect to the TOE.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

1) For Japan:

MX-FRX3 Data Security Kit Operation Manual
Version: CINSJ3814FC51
Intended reader: administrator, user
Contents: (Written in Japanese)
This document is provided as the guidance of use the TOE. The items necessary for managing and operating the TOE such as usage of security function or setting method are described.

MX-FRX3 Data Security Kit Notice
Version: TCADZ1884FCZZ
Intended reader: administrator, user
Contents: (Written in Japanese)
The items necessary for managing operating the TOE in a secure manner are described.

MX-FRX3 Version M.10 Installation Manual
Version: TCADZ1882FCZZ
Intended reader: administrator and service person (a maintenance personnel from the sales company)
Contents: (Written in Japanese)
The work procedures for installation of the TOE on the main frame of MFD and the items that service person and administrator are required to perform for the secure management and operations of TOE are described to help install TOE.

2) For markets outside Japan:

MX-FRX3 Data Security Kit Operation Manual
Version: CINSZ3815FC51
Intended reader: administrator, user
Contents: (Written in English)
This document is offered as the guidance to use the TOE. The items necessary for managing and operating the TOE such as usage of security function or setting method are described.

MX-FRX3 Data Security Kit Notice
Version: TCADZ1885FCZZ
Intended reader: administrator, user
Contents: (Written in English)
The items necessary for managing operating the TOE in a secure manner are described.

MX-FRX3 Version M.10 Installation Manual
Version: TCADZ1883FCZZ
Intended reader: administrator and service person (a maintenance personnel from the sales company)
Contents: (Written in 4 languages of English, French, German and Spanish)
The work procedures for installation of the TOE on the main frame of MFD and the items that service person and administrator are required to perform for the secure management and operations of TOE are described to help install TOE.

2. Conduct and Results of Evaluation by Evaluation Facility

2.1 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 report 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

2.2 Overview of Evaluation Conducted

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

Evaluation has started on August, 2006 and concluded by completion the Evaluation Technical Report dated December, 2006. 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 October, 2006 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 October, 2006.

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.

2.3 Product Testing

Overview of developer testing evaluated by evaluator and evaluator testing conducted by evaluator are as follows.

2.3.1 Developer Testing

1) Developer Test Environment

Test configuration performed by the developer is showed in the Figure 2-1.

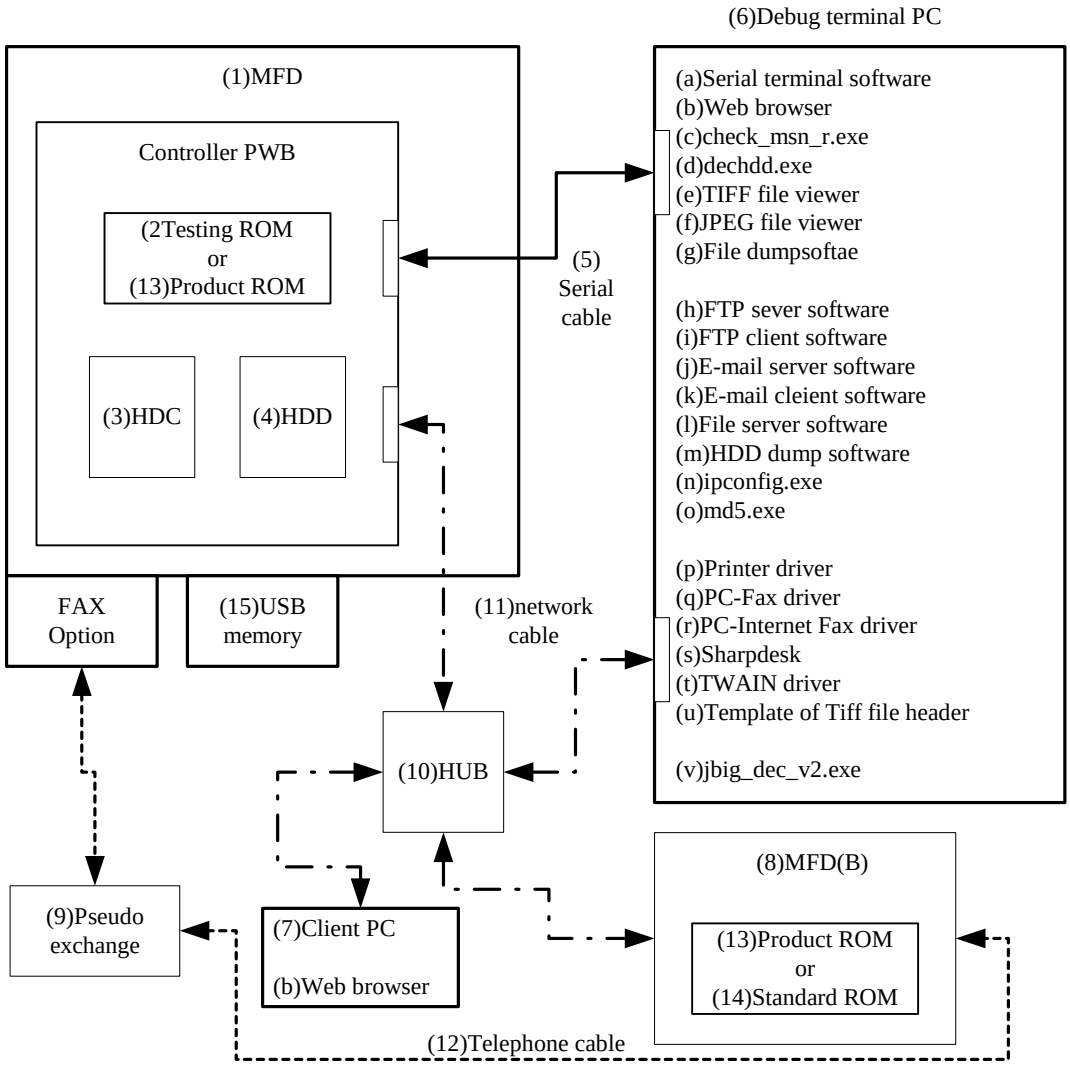

Figure 2-1 Configuration of Developer Testing

2) Outlining of Developer Testing

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

a) Test configuration

The testing configuration conducted by the developer is showed in the Figure 2-1. The developer testing had been performed in a testing environment of a hardware and software configuration equivalent to the TOE configuration identified in the ST. About the part which does not completely agree with the configuration that testing configuration is identified in ST, it is the reason to be able to consider to be equal as follows.

As for MFD of the Figure 2-1, one of MFD models (MX-6200N) that the ST identifies as environment to be used by the TOE was employed when the testing was performed. Since the HDC, a part of the TOE, is implemented in every model that the TOE works and all the HDC implemented in every model are the same parts, MFD in test configuration is equivalent to MFD that the ST

identifies as environment to be used by the TOE
Testing ROM in the Figure 2-1 is different from TOE identified in ST. Additional debug feature and modification of a security feature of part did this by reason of convenience of testing for product ROM (TOE). It employed product ROM that a security feature before it was changed worked justly, and, as for a security feature changed by reason of convenience of testing, testing was done. Therefore, what has performed the testing by employing testing ROM and product ROM can be considered equivalent to what has tested the TOE identified in the ST.

b) Testing Approach

All tests for TOE security function is performed under the circumstances of TOE testing environment configuration. For the testing, following approach was used.

1. Environment using the product ROM
   It is the same configuration that the user actually uses.
2. Environment using the testing ROM
   In contrast to the ROM use environment for product, testing ROM is used for reading the data before/ after of overwriting to clear in HDD and Flash memory out to the debug terminal through the serial cable.

The approach above is used properly in compliance with the characteristic of the test. Environment using the product ROM is used in the test which confirms with the input from and output to the standard external interface. Environment using the testing ROM is used in the test which requires the special interface to confirm the result of input and output.

c) Scope of Testing Performed

Testing is performed 63 items in Table 2-1 the developer.
The coverage analysis is conducted and examined to testing satisfactorily all of the security functions described in the functional specification and the external interface. Then, the depth analysis is conducted and examined to testing satisfactorily all the subsystems described in the high-level design and the subsystem interfaces

Table 2-1: Outlining of Developer Testing

Test classification	TSF tested mainly	Items
Pre-test	nothing	1
Administrator authentication test	TSF_AUT	4
Cryptographic key generation test	TSF_FKG	1
Storing with encryption, retrieving with decryption and clearing test in the HDD	TSF_FDE, TSF_FDC	24
Storing with encryption, retrieving with decryption and clearing test in the Flash memory	TSF_FDE, TSF_FDC	8
Disabling of cancelling the data clearance test	TSF_FDC	3
Document filing function test	TSF_FCF	17
Network protection test	TSF_FNP	5

d) Result

The evaluator confirmed the following items and the developer testing are properly enforced.

1. The TOE testing configuration in the developer testing is consistent with the TOE configuration defined in ST.
2. The developer testing approach is proper to confirm the behaviour of the TSF and TSFI.
3. The developer testing contains all the TSF, TSFI and subsystems about quantity and scope.
4. The testing approach and the actual test results are consistent with the one described in the test plan.
5. The entire test results indicate the behaviour that are expected and no problems remains.

2.3.2 Evaluator Testing

1) Evaluator Test Environment

Test configuration performed by the evaluator is the same configuration with developer testing shown in the Figure 2-1.

2) Outlining of Evaluator Testing

Outlining of the testing performed by the evaluator is as follow.

a) Test configuration

The testing configuration conducted by the evaluator is same as the developer test.

b) Testing Approach

All tests for TOE security function is performed under the same circumstances of developer testing by the evaluator. For the testing, following approach was used.

1. Environment using the product ROM
   It is the same configuration that the user actually uses.
2. Environment using the testing ROM
   In contrast to the ROM use environment for product, testing ROM is used for reading the data before/ after of overwriting to clear in HDD and Flash memory out to the debug terminal through the serial cable.

The approach above is used properly in compliance with the characteristic of the test. Environment using the product ROM is used in the test which confirms with the input from and output to the standard external interface. Environment using the testing ROM is used in the test which requires the special interface to confirm the result of input and output.

c) Scope of Testing Performed

Testing devised by the evaluator and testing from sampling of developer testing was conducted.
The security functions that are target of testing and the number of items are shown in Table 2-2.

Table 2-2: Scope of Evaluator Testing

Test classification	The number of TSF	Items
Independent testing devised by the evaluator	5	10
Testing from sampling of developer testing	6 (all)	16
Total	11	26

It is considered that main security functions should be included and all the external interfaces should be included as for the device of independent test devised by the evaluator. The testing of cryptographic key generation function (TSF_FKG) is only performed in the testing from sampling of developer testing since only the powered on is the TSFI of this function and the use of this security function while operating is infrequently.
It is considered that all the security functions and TSFI should be included as for the testing from sampling of developer testing. Representative data are extracted among the similar function. Over the 25% testing items of developer testing are performed.

d) Result

All the evaluator 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.

2.4 Evaluation Result

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

3. Conduct of Certification

The following certification was conducted 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, which 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.

4. Conclusion

4.1 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 verified the TOE is satisfied the EAL3 and ADV_SPM.1 assurance requirements prescribed in CC Part 3.

4.2 Recommendations

None

5. Glossary

The abbreviations 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
SOF:	Strength of Function
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Functions
AES:	Advanced Encryption Standard, established by NIST (National Institute of Standards and Technology, United States of America)
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
I/F:	Interface
IPP:	Internet Printing Protocol, a communication protocol for printing.
IPP-SSL:	IPP over SSL, IPP with protection of SSL.
LDAP:	Lightweight Directory Access Protocol, the name of the communication protocol for directory service.
OS:	Operating System
ROM:	Read Only Memory
SMTP:	Simple Mail Transfer Protocol
WINS:	Windows Internet Name Server WINS converts NetBIOS names to IP addresses on a LAN/WAN.

The glossaries used in this report are listed below.

Confidential file:	The file protected by password to prevent the others from reusing without permission.
Controller board:	The board that controls the whole MFD. This contains the microprocessor to execute firmware of the TOE, volatile memory, HDC, HDD and others.
Document filing:	The function that stores image data handled by the MFD into the HDD, for users' later operations, such as a printing or a transmission. This is also called "Filing" in this ST.
Engine:	A device that forms print images on receiver papers, with mechanism of paper feeding/ejection. Also called as "print engine" or "engine unit".
External network:	A network, not the internal network of an organization, which the organization does not manage.
Flash Memory:	A type of non-volatile memory that allows the entire memory to be erased at once and also allows rewriting to any part of memory.
Hold:	To store the job from printer driver by filing.
Image data:	Digital data, especially in this ST, of two-dimensional image that each function of the MFD manages.
Internal network:	The network that is inside the organization and protected against the threat about security from any external networks.
Job:	The sequence from beginning to end of the use of an MFD function (copy, print, scan send, fax reception, fax transmission, or PC-Fax). In addition, the instruction for a functional operation is sometimes called a job.
File manipulation:	An operation to manipulate image data saved as a file.
Memory:	A memory device; in particular a semiconductor memory device.
Non-volatile memory:	The memory device that retains its contents even when the power is turned off.

Operation panel:	The user interface unit in front of the MFD. This contains the start key, numeric key, function key and liquid crystal display with touch operation system.
Spool:	Storing the job's image data to the MSD temporary to increase the input and output efficiency.
Standard firmware:	The controller firmware that is installed to the MFD that TOE is not installed to. TOE contains the controller firmware and standard firmware is removed when TOE is installed.
Subnetwork:	A monolithic network that does not contain routers inside.
Tandem:	Halving a job between two MFDs for efficient printing.
Unit:	A substance provided standard that can be attached to or detached from a printed circuit board; or an option that is installed and is ready for operation. This can also be a system that includes a mechanism and is ready for operation.
Volatile memory:	A memory device, the contents of which vanish when the power is turned off.

6. Bibliography

[1] MX-FRX3 Security Target Version 0.03 (October 11, 2006) Sharp Corporation

[2] IT Security Evaluation and Certification Scheme, July 2005, Information-technology Promotion Agency, Japan EC-01

[3] IT Security Certification Procedure, July 2005, Information-technology Promotion Agency, Japan EC-03

[4] Evaluation Facility Approval Procedure, July 2005, Information-technology Promotion Agency, Japan EC-05

[5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001 (Translation Version 1.0 December 2005)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002 (Translation Version 1.0 December 2005)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003 (Translation Version 1. 0 December 2005)

[11] ISO/IEC 15408-1:2005 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004 (Translation Version 1.0 December 2005)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] MX-FRX3 Evaluation Technical Report Version 2.1, December 6, 2006, Japan

Electronics and Information Technology Industries Association, Information Technology Security Center