Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2009-10-19 (ITC-9273)
Certification No.	C0255
Sponsor	Sharp Corporation
Name of TOE	MX-FR15
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.
2010-05-26

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-FR15 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-FR15 C.10" (hereinafter referred to as "the TOE") conducted by Information Technology Security Center, Evaluation Department (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.

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 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-FR15
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 TOE is the firmware for the MFD that is stored to the ROM. By replacing the MFD standard firmware, it offers the security function and controls the entire MFD.

MFDs are office machines having copier, printer, scanner and fax functions as their primary functions.

Main security functions of the TOE are the cryptographic operation function and data clear function aiming to counter attempts to steal image data stored in the TOE-equipped MFD.

1.2.3 Scope of TOE and Security Functions

1.2.3.1 Physical Scope of TOE

The scope of the TOE is shaded in Figure 1-1. The TOE is the firmware (controller firmware) to control the controller board stored in two ROM boards mounted on the controller board of the MFD.

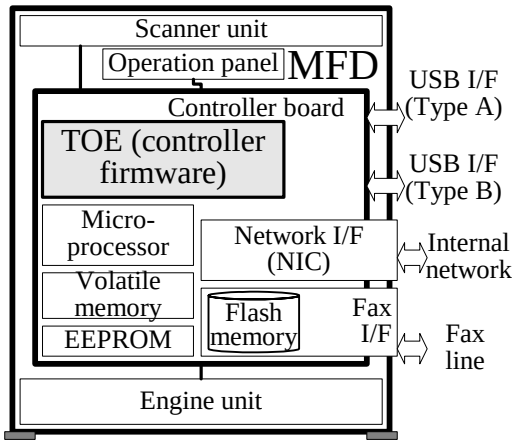

Figure 1-1: Physical configuration of the MFD and physical scope of the TOE

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 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, 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. Data exchanged between functions of TOE temporarily goes through a volatility memory. However, without the meaning on the security function, details are omitted in figure.

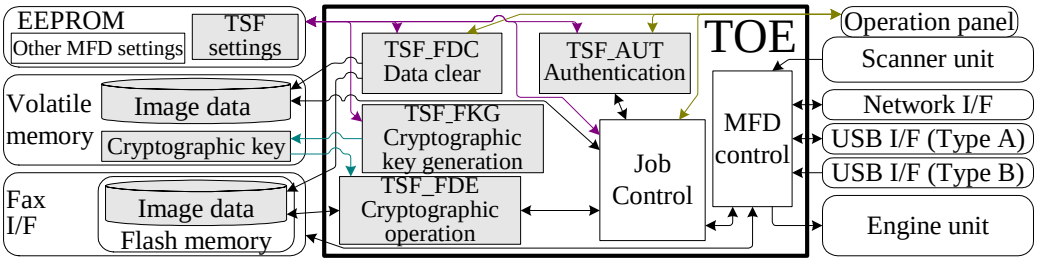

Figure 1-2: Logical configuration of the TOE

The TOE is firmware for the MFD. It offers the security functions and controls the entire MFD. The logical scope of the TOE includes the following functions:

a) Cryptographic operation function (TSF_FDE): encrypts image data to be stored in the Flash memory and decrypts image data retrieved from the Flash memory. This function is invoked by the job control function when the MFD processes a job.

b) Cryptographic key generation function (TSF_FKG): generates the cryptographic key for the cryptographic operation function and stores the key in the volatile memory.

c) Data clear function (TSF_FDC): overwrites the volatile memory and Flash memory in the MFD (hereinafter referred to as "MSD") to prevent information leakage from the MSD. This function consists of "Auto Clear at Job End" and "Clear All Memory". "Auto Clear at Job End" is activated automatically by being invoked by the job control function. "Clear All Memory" is only invoked by the administrator.

d) Authentication function (TSF_AUT): identifies and authenticates an administrator by means of the administrator password. This function includes a management function that changes the administrator password.

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-FR15 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-FR15 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 2010-05 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.

Table 2-1 Assumed Threats

Identifier	Threat
T.RECOVER	An attacker removes the Flash memory in the MFD and installs it in other devices (other than the MFD in which the memory is originally mounted) to read and leak the image data remaining in the Flash memory.

2.1.2 Organisational Security Policies

Table 2-2 shows organizational security policy required in the use of the TOE.

Table 2-1: Organizational Security Policy

Identifier	Organizational Security Policy
P.RESIDUAL	When the job is completed or is discontinued, the area in the MSD to which the image data are spooled shall be overwritten one or more times. When the MFD is disposed of or its ownership changes, all spool areas in the MSD shall be overwritten one or more times.

2.1.3 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 2-3.
The effective performance of the TOE security functions are not assured unless these assumptions are satisfied.

Table 2-3 Assumptions in Use of the TOE

Identifier	Assumptions
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 identifiers of documents attached to the TOE are listed below. Users of the TOE are required to thoroughly understand and comply with the following documents to meet the assumptions.

- MX-FR15 Data Security Kit Operation Manual [CINSE4812FC51]:
  This document is provided as the operation manual of this TOE. The items necessary for managing and operating the TOE such as usage of security function or setting method are described.
- MX-FR15 Data Security Kit Notice [CINSE4813FC51]:
  describes notes to assure secure usage of the TOE and procedures to install the TOE in the main unit of the MFD.

2.1.5 Configuration Requirements

The TOE operates on the following digital MFDs made by Sharp Corporation: MX-M363U, MX-M363UJ, MX-M453U, MX-M453UJ, MX-M503U and MX-M503UJ.

2.2 Security Objectives

TOE counters the threat defined in Section 2.1.1 by the security functions equipped, and satisfies the organizational security policies defined in Section 2.1.2 as follows:

2.2.1 Countering Threat of "T.RECOVER"

"T.RECOVER" assumes that remaining data in the Flash memory might leak when the Flash memory is removed from the MFD. This threat is countered by the following security functions:

(1) Cryptographic key generation function (TSF_FKG):

generates a cryptographic key (common key) to support the cryptographic operation function (TSF_FDE). When the MFD is powered on, the TOE always generates a 128-bit secure cryptographic key (common key) and stores it in the volatile memory.

(2) Cryptographic operation function (TSF_FDE):

On the way of the job processing, this function always encrypts the image data of the job before writing it to the Flash memory and decrypts it before reading.

To encrypt and decrypt the image data, the AES Rijndael algorithm based on FIPS PUBS 197 and the 128-bit cryptographic keys generated by the cryptographic key generation function (TSF_FKG) are used.

2.2.2 Implementation of Organizational Security Policy of "P.RESIDUAL"

"P.RESIDUAL" requires that stored data in the volatile memory and Flash memory be overwritten. This organizational security policy is implemented by the following security functions:

(1) Data clear function (TSF_FDC):

provides the function to clear image data that are spooled. This function consists of the following functions. Each function makes the reproduction of image data impossible by overwriting the volatile memory with a random value or by overwriting the Flash memory with a fixed value.

a) Auto Clear at Job End:

provides the function to clear by overwriting the image data spooled in the Volatile memory or the Flash memory to process a job when Job is completed.

b) Clear All Memory:

is invoked from the operation panel by the administrator who is identified and authenticated by authentication function (TSF_AUT) and overwrites all spooled image data in the volatile memory or the Flash memory.

This function accepts the cancel operation. Whenever a cancel operation is taken, the administrator is required to be identified and authenticated; cancelling is allowed only when the identification and authentication is successful.

(2) Authentication function (TSF_AUT):

executes the identification and authentication of the administrator by the administrator password. The TOE provides the interfaces of the function to the administrator only when the administrator is identified by the activation of the management functions and when the authentication of the administrator is successful by the correct administrator password. As a result, the administrator is specified, and the administrator's role is related to the user. When the administrator password is entered, the input character is not displayed though asterisks of the same number as the input of characters are displayed. When failing in the authentication three times in a row, this function stops accepting further authentication attempts. When five minutes passes from the authentication stop, the stop status is automatically released. That is to clear the authentication number of times for authentication failure and return to the normal state automatically.

The administrator shall be authenticated before Clear All Memory of the Data clear function (TSF_FDC) is executed and before the administrator password is modified. When the password is modified, the TOE verifies that TOE secures the quality for the password newly input from viewpoint of the length and kinds of characters of the password.

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 2009-10 and concluded by completion the Evaluation Technical Report dated 2010-05. 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 2010-2 and 2010-4 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 2010-2 and 2010-4.

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.

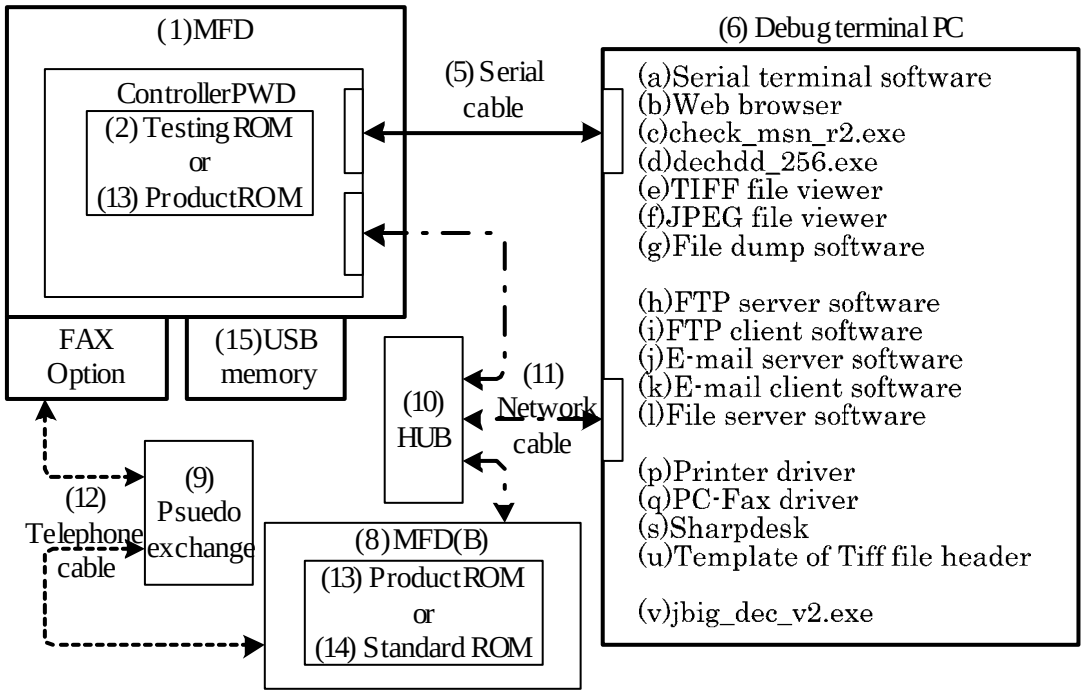

Figure 3-1: Configuration of Developer Testing

The MFD used for the test is the MX-M503U, one of the models identified in the ST.

There is a difference in the processing performance and so on in each MFD that operates TOE but TOE is common for all MFD. Therefore, the testing environment can be considered to be equivalent to that specified in the ST.

2) Outlining of Developer Testing

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

a. Test outline

Under the environment shown in Figure 3-1, the testing was conducted using two types of ROMs, a product ROM and a testing ROM, according to the characteristics of each test. To confirm the test results, the testing ROM is capable of serial port output, outputting the seed and cryptographic keys, switching between enabling and disabling of the cryptographic operation and specifying data to be overwritten, however, it does not affect the security functions which are the subject of the testing.

The developer conducted the testing by stimulating the 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 on the operation panel of the MFD or from the debug terminal).

b. Scope of Testing Performed

The test of 15 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.

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 from the developer testing and the provided evaluation documentation in the following viewpoints.

- Performing tests of each TSF by adding the type of entered parameter or the combination of entered parameter when it is judged that the developer testing is insufficient in terms of coverage of entered parameter.
- Performing tests to confirm the behaviour of TSF more strictly, by adding the timing or combination of user operation.
- Performing tests to confirm the behaviour of TSF about the connection to client, by using the interfaces that is different from the ones used for developer testing.
- Considering that all the interface types and security functions that TOE provides are covered.

b. Outlining of Evaluator Independent Testing
Considering the above points, 9 sampling test of developer testing and 5 independent testing are performed as evaluator testing. Tools and testing

technique used for independent testing performed by the evaluator are similar to ones used for 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 deliverables 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.

- The possibility that unintended network port interface exists and TOE may be accessed from the interface, or protected assets are disclosed by sending the data improperly to the open port.
- The possibility that security functions are bypassed by using the interface, such as maintenance interface or testing interface that is not used for normal operation.
- The possibility that excessive information is output from the interface and secret information is disclosed.
- The possibility that security functions are bypassed by physical operation to the memory.
- The possibility that protected assets are leaked from the MFD where TOE is not mounted when some MFDs execute processing in combination.
- The possibility that the special combination of the type of character for administrator password is not verified correctly and security functions are bypassed.

b. Scope of Test Performed

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

- Confirming by using the port scan tool that unnecessary network port is not opened.
- Confirming by transmitting an illegal packet to an open port that the vulnerability that leads to the exposure of the protected assets doesn't exist.
- Confirming by the operation from the interface for service technicians that vulnerabilities that affect security functions don't exist.
- Confirming that information to lead to the disclosure of secret information is not output from the interface of TOE.

- Confirming by replacing or by removing ROM boards, volatile memory boards or boards equipped with EEPROM, that vulnerability to lead to the bypass of security functions doesn't exist.
- Confirming that protected assets is not leaked from the MFD where TOE is not mounted when tandem printing is performed.
- Confirming that security functions are not bypassed even if the combination of the type of character for administrator password is special.

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
TSFI:	TSF Interface

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

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.
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.

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

Engine unit	A device that forms print images on receiver papers, with mechanism of paper feeding/ejection.
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.
Image data:	Digital data, especially in this document, of two-dimensional image that each function of the MFD manages.
Job	The sequence from beginning to end of the use of an MFD function (copier, printer, scanner send, fax reception, fax transmission, or

	PC-Fax). In addition, the instruction for a functional operation is sometimes called a job.
Operation panel	The user interface unit in front of the MFD. This contains the start key, numerical key, function key and liquid crystal display with touch operation system.
Scanner unit	The device that scans the original and gets the image data. This is used for copier, scanner or fax transmission.
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 replaced with the TOE's controller firmware when TOE is installed.
Tandem print	The function to print a large job twice faster than usually by halving that job among two MFDs.
Volatile memory:	A memory device, the contents of which vanish when the power is turned off.

7. Bibliography

[1] MX-FR15 Security Target Version 0.04 (March 10, 2010) 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-FR15 Evaluation Technical Report, Version 2.8, May 14, 2010, Information Technology Security Center, Evaluation Department