Certification Report

Buheita Fujiwara, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2007-03-27 (ITC-7144)
Certification No.	C0124
Sponsor	Sharp Corporation
Name of TOE	AR-FR25
Version of TOE	VERSION M.10
PP Conformance	None
Conformed Claim	EAL3 Augmented withADV_SPM.1
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.
2007-11-16

Hideji Suzuki, Technical Manager
Information Security Certification Office
IT Security Center

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following criteria prescribed in the "IT Security Evaluation and Certification Scheme".

- Common Criteria for Information Technology Security Evaluation Version 2.3
- Common Methodology for Information Technology Security Evaluation Version 2.3

Evaluation Result: Pass

"AR-FR25 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 "AR-FR25 VERSION M.10" (hereinafter referred to as "the TOE") conducted by Japan Electronics and Information Technology Industries Association, Information Technology Security Center (JEITA ITSC) (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 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:	AR-FR25
Version:	VERSION M.10
Developer:	Sharp Corporation

1.2.2 Product Overview

The TOE is the firmware to enhance security functionality of a Multi-Function Device (hereafter referred to as "MFD"). This TOE is provided as an optional product, and offers the security function and controls the entire MFD when it is installed instead of the MFD standard firmware. The TOE primarily consists of the cryptographic operation function and data clear function, aiming to prevent the information leakage of actual image data remaining in the MFD where TOE is installed.

The cryptographic operation function encrypts actual image data of each fax job before spooled to the Flash memory in MFD. The data clear is the function that random values or a fixed value overwrite the data areas where the actual image data is spooled after completing each job of the copy, print, scanning transmission and fax.

1.2.3 Scope of TOE and Security Functions

Relation between the TOE and the MFD is shown in Figure 1-1. The TOE is shown as shaded areas in Figure 1-1.
The TOE is the firmware to control the MFD stored to the ROM and is provided by the MCU_ROM on the MCU board, PCL_ROM on the PCL board, FAX_ROM on the FAX board and the IMC board.

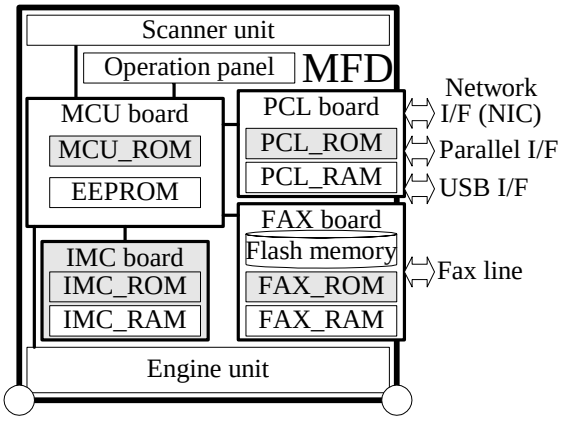

Figure 1-1: Physical configuration of the MFD and physical scope of the TOE

Figure 1-2 shows the logical configuration of the TOE. The thick-lined frame indicates the logical scope of the TOE. Rectangles indicate functions of the software. Hardware outside of the TOE is shown in the rectangle with a round corner. Among the functions of the TOE, ones shaded indicate security functions. Arrows in the figure indicate data flows.

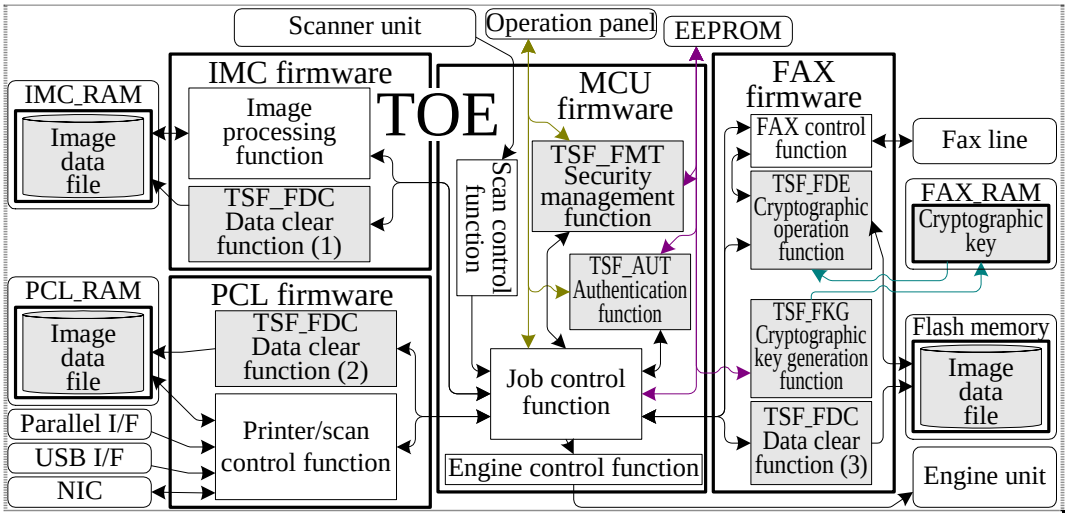

Figure 1-2: Logical configuration of the TOE

The TOE is firmware to enhance security functionality of a MFD, and controls the entire MFD.

1.2.4 TOE Functionality

Functions provided by the TOE are as follows:

a) Cryptographic operation function (TSF_FDE):
encrypts actual image data generated by the fax function, and then spools it to the Flash memory to store as image files. Moreover, to use the data, the encrypted actual image data spooled in the Flash memory is read and decoded.

b) Cryptographic key generation function (TSF_FKG):
generates the cryptographic key for encryption and decryption provided by the cryptographic operation function. This function stores the generated key in the volatile memory (FAX_RAM).

c) Data clear function(1), data clear function(2) and data clear function(3) (TSF_FDC):
overwrites the actual image data in the MSD when each of the copy, print, scan send and fax jobs is finished or cancelled (Auto Clear at Job End). This function also overwrites all actual image data in the MSD by the operation of the key operator (Clear All Memory).

d) Authentication function (TSF_AUT):
identifies and authenticates a key operator (administrator) by means of the key operator code (a password).

e) Security management function (TSF_FMT):
provides a function to change (modify) the key operator code after key operator authentication is successful.

f) Engine control function:
controls the engine unit in copy job, print job and fax reception job.

g) Scan control function:
controls the scanner unit during copy job, scan send job, and fax transmission jobs for scanning of an original.

h) Printer/scan control function:
is available when the PCL board is installed as a standard or an option in MFD that can install TOE.

- To print the received print data via networks, USB or parallel interface, the bit map image is created in the print job.
- In the scanning transmission job, after the scanned real image data is converted into the specified form, it is sent to the network through network interface.

i) Fax control function:

Controls transmission over the FAX line for a PC-Fax or fax transmission job, and reception from the FAX line for a fax reception job.

j) Image processing function:

Performs image processing for printing using feature functions of the MFD.

k) Job control function:

There are the copy job, the print job, the scanning transmission job, and fax job. This function controls the operation of the copy, print, scanning and transmission, and fax job.

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 "AR-FR25 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], [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 "AR-FR25 VERSION M.10 Evaluation Technical Report" (hereinafter referred to as "the Evaluation Technical Report") [17]. Further, evaluation methodology shall 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 2007-11 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.

This TOE assumes use in a general commercial system.
Therefore, the assumed malicious acts are attacks using public information.
For this reason, the attack potential of attacker is "low-level".
Therefore, minimum function strength is enough by "SOF-basic" that can oppose "Low-level".

1.5.4 Security Functions

This TOE provides the following security functions:

(1) Cryptographic key generation function (TSF_FKG)

The TOE generates a cryptographic key (common key) to support the actual image data encryption function. When the MFD is powered on, a cryptographic key (common key) is always generated. The cryptographic key is generated as a 128-bit of secure key using the MSN-A expansion algorithm which is the cryptographic key generation algorithm to use the AES Rijndael encryption algorithm, based on the Data Security Kit Encryption Standards. The cryptographic key is stored in FAX_RAM.

(2) Cryptographic operation function (TSF_FDE)

In the processing of a PCFAX, fax transmission, or fax reception job, the actual image data of the job is always encrypted before being spooled to Flash memory on the FAX board. When the encrypted and spooled actual image data is processed (used) actually, it is always read and used after decrypting it. The actual image data is encrypted and decrypted using the AES Rijndael algorithm based on FIPS PUBS 197 and the 128 bits cryptographic key generated by TSF_FKG cryptographic key generation.

(3) Data clear function (TSF_FDC)

The TOE provides the data clear function that clears spooled actual image data file. This function consists of the following two data clear programs:

a) Auto Clear at Job End:

Overwrites actual image data files as follows:

–When a copy job or print job ends, the actual image data file for the job that was spooled to IMC_RAM is overwritten with random values.

–When a scanning transmission job ends, the actual image data file for the job spooled to PCL_RAM is overwritten with random values.

–When a PCFAX, fax transmission, or fax reception job ends, the actual image data file for the job that was spooled to Flash memory is overwritten with fixed values.

b) Clear All Memory:

After being identified and authenticated as the key operator, all actual image data that are used for spooling to IMC_RAM and PCL_RAM are overwritten with random values by key operator's operation. Also all actual image data that are used for spooling to Flash memory on the FAX board are overwritten by fixed values.

When discontinuing this function on the way, key operator's identification and authentication by the input of the key operator code is required after the cancel operation is selected. Only when the identity authentication as a key operator succeeds, the overwriting is interrupted.
The random value used by the "overwriting" to IMC_RAM and PCL_RAM in "Clear All Memory" function is generated based on the cyclical delay Fibonacci algorithm.

(4) Authentication function (TSF_AUT)

The TOE always requires key operator identification and authentication before the key operator programs (TOE security management functions) can be used. While the key operator code is being entered, the TOE hides the entered digits and instead shows each entered digit as an asterisk "*" to indicate the number of digits entered. The key operator identification and authentication and code entry hidden feedback function are always executed, so that operation of the key operator programs is only possible when the user is identified and authenticated as a key operator.
Only when the authentication as a key operator (TSF_AUT) succeeds, the execution of "Clear All Memory" of "data clear (TSF_FDC)" and the inquiry and modification of key operator code for "security management"(TSF_FMT) are available.

(5) Security management function (TSF_FMT)

The security management (TSF_FMT) provides the functions of key operator code query and modification. The key operator code is managed by the security management (TSF_FMT). The security management (TSF_FMT) can be executed only after the key operator is identified and is authenticated (TSF_AUT). In other words, the key operator is specified and the role of the key operator is associated to the user as well as authentication (TSF_AUT). Moreover, after the key operator code is modified (changed), the role is maintained as a key operator. It is verified without fail that the main operator code newly input is 5-digit number, and it is stored in EEPROM in the MFD.

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	A low-level attacker will read the actual image

	data that remains in the flash memory in MFD by using devices other than MFD and will disclose it.

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	When each of the jobs such as copy, print, scan send or fax is completed or is discontinued, the actual image data area spooled to the MSD shall be overwritten. When the MFD is disposed of or its ownership is changed, all areas to which actual image data is spooled shall be overwritten by the key operator operation.

1.5.7 Configuration Requirements

The TOE can be used on the following Sharp MFDs: AR-317FG, AR-317FP, AR-317G, AR-317S, AR-5631, AR-M316, AR-M317, AR-M317J and AR-M318.

1.5.8 Assumptions for Operational Environment

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

Table 1-3 Assumptions in Use of the TOE

Identifier	Assumptions
A.OPERATOR	The key operator 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) Japanese version:

- AR-FR25 Data Security Kit Operation Manual
  Version: TINSJ1846QSZZ
  Intended reader: key operator, user
  Contents: 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. Written in Japanese.

- AR-FR24 AR-FR25 Data Security Kit Notice
  Version: TCADZ0501QSZZ
  Intended reader: key operator, user
  Contents: The items to which the key operator and user should pay attention in managing and operating the TOE in a secure manner are described. Written in Japanese.

(2) Overseas version:

- AR-FR25 Data Security Kit Operation Manual
  Version: TINSE1848QSZZ
  Intended reader: key operator, user
  Contents: 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. Written in English.

- AR-FR24 AR-FR25 Data Security Kit Notice
  Version: TCADZ0502QSZZ
  Intended reader: key operator, user
  Contents: The items to which the key operator and user should pay attention in managing and operating the TOE in a secure manner are described. Written in English.

To use this TOE, the key operator and user are advised to read the following documents attached to the MFD:

(1) Japanese version:

- Digital Multifunctional System Key Operator's Guide
  (TINSJ1683QSZZ)

(2) Overseas version: (Written in English)

- Digital Multifunctional System Key Operator's Guide
  (TINSE1766QSZZ)

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 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.

2.2 Overview of Evaluation Conducted

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

Evaluation has started on 2007-06 and concluded by completion the Evaluation Technical Report dated 2007-11. 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 2007-8 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 2007-08.

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.

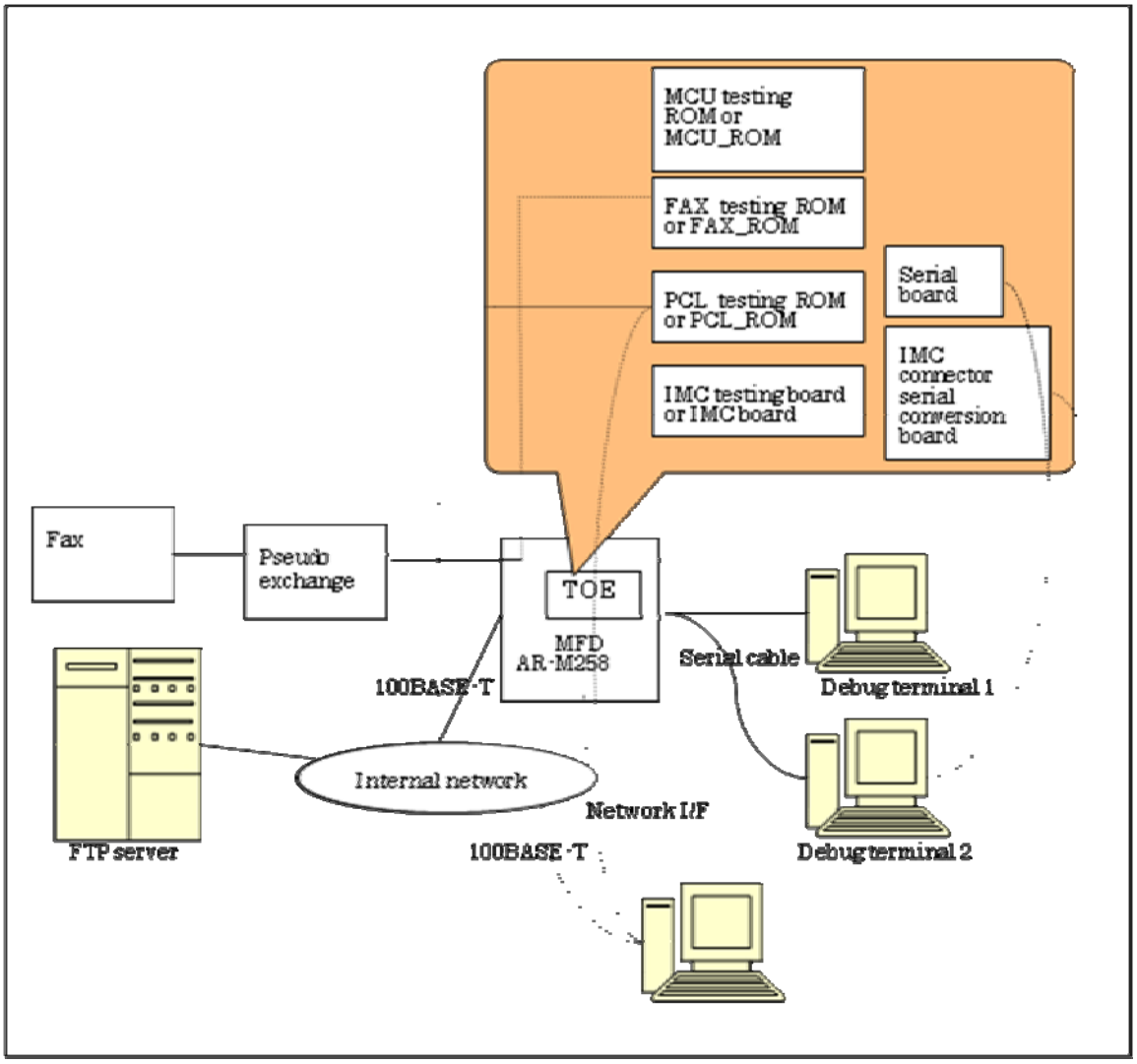

Figure 2-1: Configuration of Developer Testing

2) Outlining of Developer Testing

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

a. Test outline

The testing configuration conducted by the developer is as showed in Figure 2-1. The developer testing was performed in a testing environment of a hardware and software configuration equivalent to the TOE configuration identified in the ST. While part of the testing configuration does not completely corresponding to the configuration identified in the ST, the reasons why the testing configuration can be considered equivalent to that in the ST is as follows.

As for MFD of Figure 2-1, one (AR-317FP) of several models identified in the ST for an operating environment was used in the test.

Differences between the models identified in the ST are caused by those engine speeds (printing speed per minute) and optional functions. Because the security functions of the TOE are not affected by the model and all the

optional features are installed in the model (AR-317FP) used in this test, this test environment can be considered equivalent to the configuration with TOE identified in ST.

The testing ROMs and testing boards in Figure 2-1 are different from the TOE identified in the ST. The only difference is that in test equipment, the function for the Debug test is added to the TOE. Therefore, it can be considered equivalent to the TOE configuration.

b. Testing Approach

All tests for TOE security function are performed under the TOE testing environment configuration. The following three kinds of environments exist as a test environment of TOE.

1) Environment using the product ROM

It is the same configuration as environment that the user actually uses. The IMC connector serial conversion board and the serial board for debugging are not connected.

2) Environment using the testing ROM

In addition to the usage environment for the product ROM, following conditions are provided:

- IMC connector serial conversion board is connected to IMC board
- Serial board is connected to PCL_ROM
- IMC testing board and the PCL testing ROM are used to read out the stored or remaining data from IMC_RAM or PCL_RAM before and after overwriting to the debug terminal through the serial cable.
- In place of the FAX_ROM, the FAX testing ROM having the function to print data in the FAX_RAM or Flash memory is used.

3) Source code confirmation environment

The subsystem (IMC random number subsystem and PCL random number subsystem) that cannot be confirmed by the test and the confirmation of the activation of the interface were verified by confirming the source code.

c. Scope of Testing Performed

The test 13 items was performed by the developer.

The coverage analysis was conducted and it was verified that all security functions described in the functional specification and the external interface were thoroughly-tested. Then, the depth analysis was conducted and it was verified all the subsystems described in the high-level design and the subsystem interfaces are thoroughly-tested.

d. 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.

2.3.2 Evaluator Independent Testing

1) Evaluator Independent Test Environment

Figure 2-2 shows the configuration of the testing performed by the evaluator.

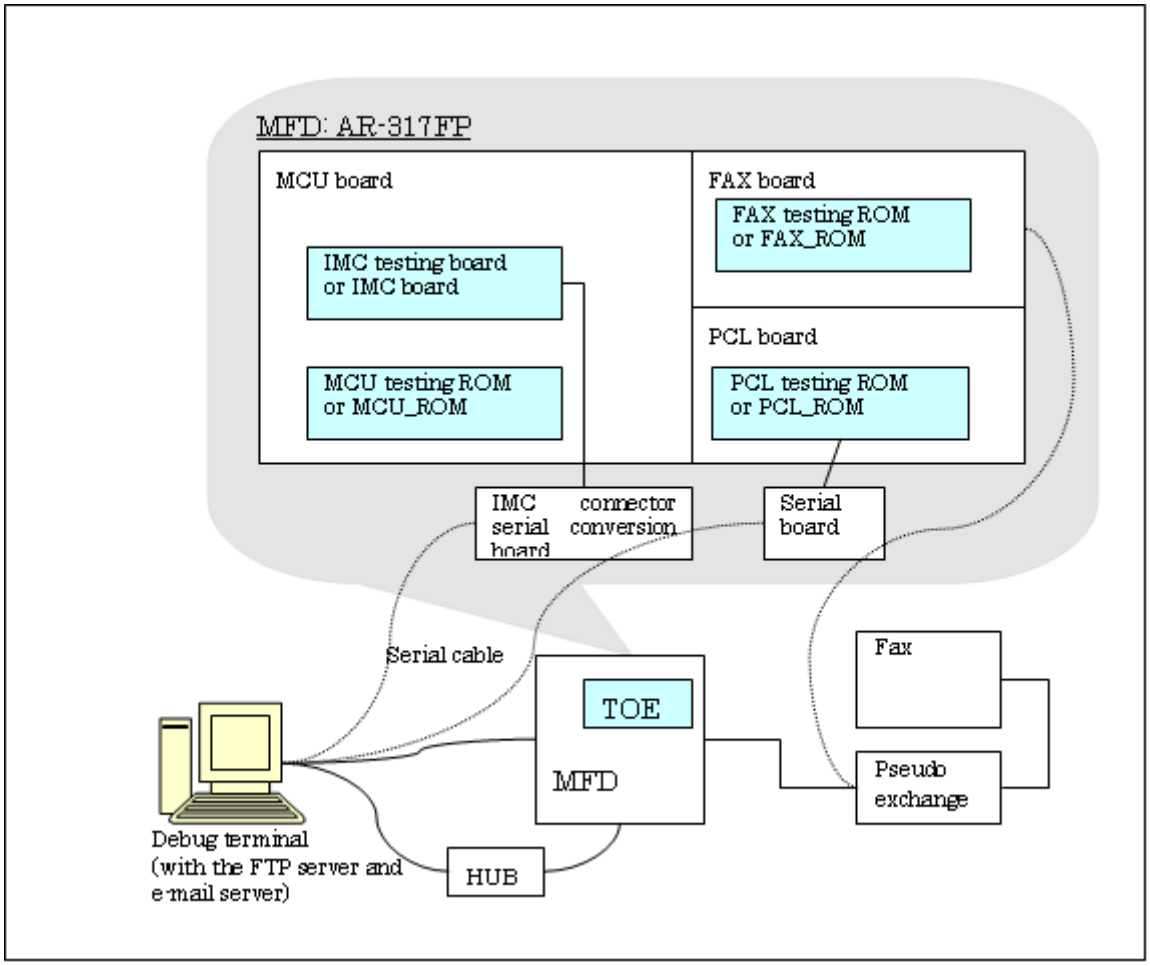

Figure 2-2: Configuration of Independent Testing

2) Outlining of Evaluator Independent Testing

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

a. Test configuration

The configuration of the testing performed by the evaluator is shown in Figure 2-2. The evaluator testing was performed in the TOE operating environment equivalent to the TOE configuration identified in the ST. Although the evaluator testing configuration was not exactly the same as the TOE configuration identified in the ST, it can be considered equivalent for the same reason described in the developer test environment.

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) Usage environment for the product ROM

It is the same configuration that the user actually uses. The IMC connector serial converter board for debugging and the serial board are not connected.

2) Usage environment for the testing ROM

In addition to the usage environment for the product ROM, following conditions are provided:

- IMC connector serial conversion board is connected to IMC board
- Serial board is connected to PCL_ROM
- IMC testing board and the PCL testing ROM are used to read out the stored or remaining data from IMC_RAM or PCL_RAM before and after overwriting to the debug terminal through the serial cable.
- In place of the FAX_ROM, the FAX testing ROM having the function to print data in the FAX_RAM or Flash memory is used.

c. Scope of testing performed

The evaluator performed the following testing including 22 items in all: tests devised originally by the evaluator, 8 items; tests reproducing those conducted by the developer, 9 items; intrusion tests, 5 items.
The following points were considered when the evaluator's original tests were devised.

1) All five security functions are included.
2) Test on the cryptographic key generation function that seems to be important from the viewpoint of the security objectives
3) Whether the TOE can operate as described in the functional specifications when it handles errors.
4) Passive tests that the developer did not perform.
5) Tests for the MFD which can install TOE other than models used in developer test

Each of the tests reproducing those conducted by the developer was chosen so that all five security functions are targeted and that the data clear function (TSF_FDC) stored in the ROMs in a dispersed manner is thoroughly tested.
For the intrusion testing, in addition to the test items targeting to three security functions (data clear, authentication and security management), items targeting the TOE and the entire TOE environment were devised to confirm whether there was any explicit vulnerability overlooked by the developer's consideration.

d. Result

All the evaluator testing conducted is completed 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 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.

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 determined the TOE is satisfied the assurance requirements of EAL3 augmented with ADV_SPM.1.components prescribed in CC Part 3.

4.2 Evaluator comments/Recommendations

There are no recommendations to be advised to consumers.

5. Glossary

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

CC:	Common Criteria for Information Technology Security Evaluation
CEM:	Common Methodology for Information Technology Security Evaluation
EAL:	Evaluation Assurance Level
PP:	Protection Profile
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Functions

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

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.
FAX board	One of the units of an MFD that can be equipped with the TOE. It provides the fax function. Support for the FAX board is the standard, optional or unavailable depending on the MFD model.
FAX_RAM	The RAM on the FAX board. A volatile memory.
FAX_ROM	The ROM on the FAX board. It is provided physically as part of the TOE.
GDI board	One of the units of an MFD that can be equipped with the TOE. It is equipped with USB and parallel I/F and provides part of the print function. It is included in a part of MFD models which do not contain the PCL board.
IMC board	One of the units of an MFD that can be equipped with the TOE. It is provided physically as part of the TOE. It provides the image processing function.
IMC_RAM	The RAM on the IMC board. A volatile memory.
IMC_ROM	The ROM on the IMC board. It is provided physically as part of the TOE.
I/F	Interface

MCU board	One of the units of an MFD that can be equipped with the TOE. It provides the control function of the entire MFD.
MCU_RAM	The RAM on the MCU board. A volatile memory.
MCU_ROM	The ROM on the MCU board. It is provided physically as part of the TOE.
MSD	Mass Storage Device, in this document, this especially indicates the IMC_RAM, PCL_RAM and Flash memory in MFD.
NIC	Network Interface Card, or, Network Interface Controller
PCL board	One of the units of an MFD that can be equipped with the TOE. It is equipped with NIC, USB and parallel I/Fs and provides the print and scan send functions. Support for the PCL board is the standard, optional or unavailable depending on the MFD model.
PCL_RAM	The RAM on the PCL board. A volatile memory.
PCL_ROM	The ROM on the PCL board. It is provided physically as part of the TOE.
RAM	Random Access Memory, memory capable of being read and written randomly.
ROM	Read Only Memory
UI	User Interface
USB	Universal Serial Bus, a serial bus standard to connect between IT equipments.
Image data	Digital data, especially in this document, of two-dimensional image that each function of the MFD manages.
Engine	A device that forms print images on receiver papers, with mechanism of paper feeding/ejection. Also called as "print engine" or "engine unit".
Auto Clear at Job End	The function that clears (by overwriting) image data of each job stored in some MSD of the MFD, invoked when a job is finished or cancelled.
Key operator	An authorized user who is allowed to access the security management function and MFD management function of the TOE.
Key operator code	A password used for authentication of the key operator.
Key operator program	The TOE security management function. It also provides the MFD management function. To access the key operator programs, identification and authentication of the key operator shall be successful.
Volatile memory	A memory device, the contents of which vanish when the power is turned off.

Board	A printed circuit board on which components are mounted by soldering.
Actual image data	Assets protected by this TOE. It is the actual image data remaining in the volatile memory or Flash memory after each processing of MFD ends.
Actual image data file	An object to be handled by the file system that manages actual image data.
Job	The flow from beginning to end of each MFD function (copy, print, scan send and fax) and sequence. In addition, the instruction of a functional operation might be called a job.
Scanner unit	The device that scans the original and gets the image data. This is used for copy, scan send or fax transmission.
Spool	Storing the job's image data to the MSD temporary to increase the input and output efficiency.
Clear All Memory	The function to overwrite the all image data that is stored to the MSD in the MFD. This function is invoked by the operation of the key operator.
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.
Firmware	The software that is embedded to the machines to control the machine's hardware.
Non-volatile memory	The memory device that retains its contents even when the power is turned off.
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.
Memory	A memory device; in particular a semiconductor memory device.
Unit	A substance provided standard that can be attached to or detached from a printed circuit board; or the option that can be installed and be operated. Moreover, the substance that can be operated by containing the mechanism.

6. Bibliography

[1] AR-FR25 Security Target Version 0.03 (September 21, 2007) 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 2.3, August 2005, CCMB-2005-08-001

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

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components Version 2.3, September 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 (Japanese Version 1.0, December 2005)

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

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components Version 2.3, August 2005, CCMB-2005-08-003 (Japanese 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 (Japanese Version 1.0, December 2005)

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

[17] AR-FR25 VERSION M.10 Evaluation Technical Report, Version2.2
November 6, 2007
Japan Electronics and Information Technology Industries Association,
Information Technology Security Center (JEITA ITSC)