Certification Report

Target of Evaluation

Application date/ID	May 17, 2004 (ITC-4028)
Certification No.	C0022
Sponsor	Sharp Corporation
Name of TOE	AR-FR12M
Version of TOE	VERSION M.2.0
PP Conformance	None
Conformed Claim	EAL3+ADV_SPM.1
TOE Developer	Sharp Corporation
Evaluation Facility	Japan Electronics and Information Technology Industries Association Information Technology Security Center

This is to report that the evaluation result for the above TOE is certified as follows.
March 9, 2004

TABUCHI Haruki, 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 "General Requirements for IT Security Evaluation Facility".

- Common Criteria for Information Technology Security Evaluation Version 2.1 (ISO/IEC 15408:1999)
- Common Methodology for Information Technology Security Evaluation Version 1.0
- CCIMB Interpretations-0210

Evaluation Result: Pass

"AR-FR12M VERSION M.20" has been evaluated in accordance with the provision of the "General Rules for IT Product Security Certification" 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-FR12M VERSION M.20” (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:	AR-FR12M
Version:	VERSION M.2.0
Developer:	Sharp Corporation

1.2.2 Product Overview

TOE is a firmware that aims to prevent disclosure of real image data stored temporarily in Mass Storage Device (hereafter referred to as MSD), which are specified for every functional unit configuration of Multi Function Device (hereafter referred to as MFD). TOE is provided as a kit of upgrading firmware of MFD.
The real image data is encrypted before it is spooled in MSD by the TOE, when the MFD functions like PCFAX, FAX sending or FAX receiving are performed. Spool data area in MSD is erased after the jobs like copying, printing, SCAN sending, PCFAX, FAX sending or FAX receiving are completed. These encryption function and data erasing function ensure the confidentiality of real image data that are stored temporarily in MSD and counter fraudulent readout of them.

1.2.3 Scope of TOE and Overview of Operation

The TOE physical configuration is shown in shaded areas in the figure 1-1.

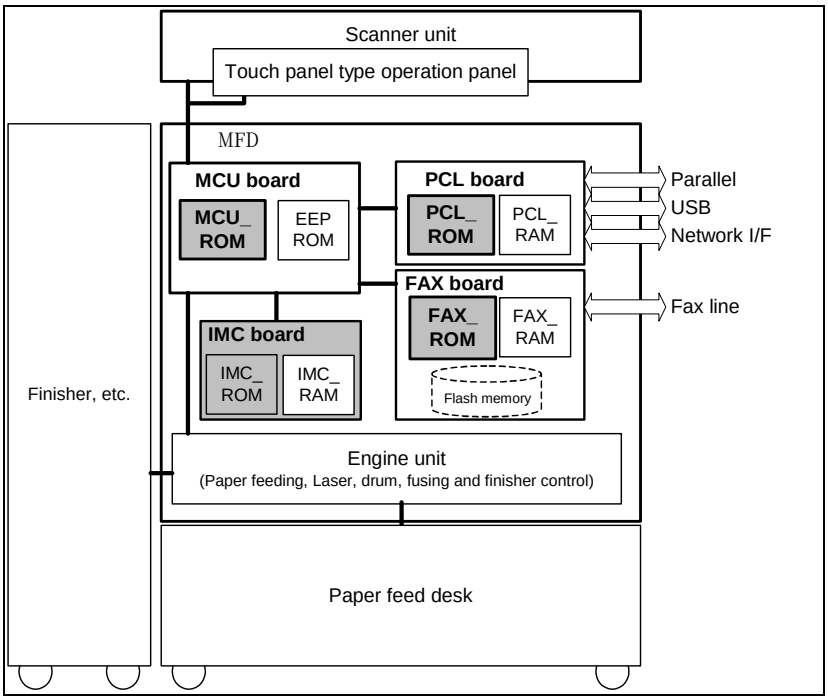

Figure 1-1: Physical configuration of MFD and TOE

The TOE of AR-FR12M consists of the following firmware stored in MCU_ROM, PCL_ROM, FAX_ROM and IMC PWB.

a) MCU firmware
   Firmware that controls the MCU board, which is contained in the MCU_ROM on the MCU board.

b) IMC firmware
   Firmware that controls the IMC board, which is contained in the ROM on the IMC board.

c) PCL firmware
   Firmware that controls the PCL board, which is contained in the PCL_ROM on the PCL board.

d) FAX firmware
   Firmware that controls the FAX board, which is contained in the FAX_ROM on the FAX board.

The logical configuration of the TOE is shown in Figure 1-2. The TOE is indicated by the thick-lined frame. The rectangles indicate firmware functions and the rectangles with rounded corners indicate hardware. Firmware functions that are security

functions are shaded. The broken line within the TOE indicates the correspondence with the physical scope of the TOE, and the name of the physical scope is indicated at the top of the broken-line frame.

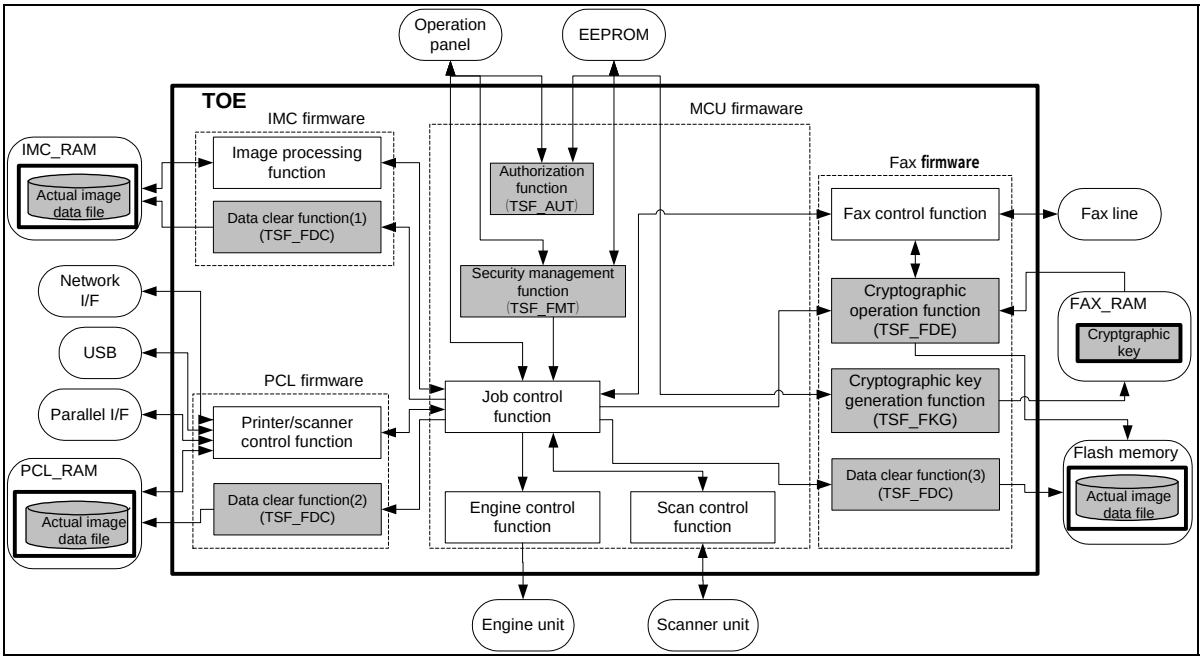

Figure 1-2: TOE logical scope

The TOE is an upgrade kit that adds security functions to the MFD. Along with providing security functions it performs control of the entire MFD. The following functions are included within the logical scope of the TOE.

a) Cryptographic operation function (TSF_FDE)
   This encrypts the actual image data of a PC FAX, fax transmission or fax reception job, spools the encrypted data to Flash memory, and manages it as an image data file. This function also reads the encrypted actual image data in Flash memory, decrypts it, and uses it.

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

c) Data clear function (1), data clear function (2), data clear function (3) (TSF_FDC)
   These functions clear actual image data, which has been spooled to the MSD and managed as an image file for a copy, print, scan send, PC FAX, fax transmission, or fax reception job, by overwriting random values or fixed values to the corresponding actual image data area. (Auto clear at job end)

This function clears all areas to which data can be spooled by writing random or fixed values over the data in those areas. (Clear all memory by key operator operation)

This consists of the following two data clear functions:

(a) Auto clear at job end

(It clears the actual image data area used by a job when the job ends.)

During the processing of job, for actual image data spooled to volatile memory, this function clears the actual image data area by overwriting it with random values. For actual image data spooled to flash memory, this function clears the actual image data area by overwriting each bit with a fixed value.

The data clear function (1) clears the volatile memory (IMC_RAM) on the IMC board. The data clear function (2) clears the volatile memory (PCL_RAM) on the PCL board. The data clear function (3) clears Flash memory on the FAX board.

(b) Clear all memory by key operator operation

(Note: This function clears the whole actual image data of any incomplete jobs or jobs that ended abnormally, and is used to prevent the leaking of information from actual image data when the MFD is disposed of or its ownership changes.)

Volatile memory on the IMC board (IMC_RAM) and volatile memory on the PCL board (PCL_RAM) are cleared by writing random values over all actual image data areas of those memories, and Flash memory on the FAX board is cleared by writing fixed values over all actual image data areas of Flash memory. This function also can cancel the clear all memory by the key operator operation.

d) Authentication function

It authenticates a key operator by means of the key operator code (password).

e) Security management function

It provides a function for changing the key operator code following authentication as a key operator.

f) Engine control function

It controls the engine unit during copy job, print job, and fax reception job.

g) Scan control function

It controls the scanner unit during copy job, scan send job, and fax transmission job for scanning of an original.

h) Printer/scanner control function

It can operate on an MFD that can be equipped with the TOE and that has the

PCL board standard or as an option.

(a) During a print job, this function creates a bitmap image for printing from the print data received through the parallel, USB or network interface.

(b) During a scan send job, this function converts the actual image data obtained by scanning into the specified format and transmits it through the network interface over the network.

Note that the MFD has neither the scanner control function nor a network interface if it can be equipped with the TOE but has the GDI board installed standard or as an option.

i) FAX control function

It 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

It performs image processing for printing using special functions of the MFD.

k) Job control function

Jobs include copy jobs, print jobs, scan send jobs, PC FAX jobs, fax transmission jobs, and fax reception jobs. The job control function controls these jobs as follows:

(a) Copy jobs:	Controls the MFD's copy operation.
(b) Print jobs:	Controls the MFD's printing operation.
(c) Scan send jobs:	Controls the MFD's scan send operation.
(d) PC FAX jobs:	Controls PC FAX jobs on the MFD.
(e) Fax transmission jobs:	Controls the MFD's fax transmission operation.
(f) Fax reception jobs:	Controls the MFD's fax reception operation.

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 "Guidance for IT Security Certification Application, etc."[2], "General Requirements for IT Security Evaluation Facility"[3] and "General Requirements for Sponsors and Registrants of IT Security Certification"[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 “Data Security Kit AR-FR12M 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], [11] or [14]) and Functional Requirements of CC Part 2 (either of [6], [9], [12] or [15]) 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], [13] or [16]) as its rationale. Such evaluation procedure and its result are presented in “Data Security Kit AR-FR12M Evaluation Technical Report” (hereinafter referred to as “the Evaluation Technical Report”)[22]. Further, evaluation methodology should comply with the CEM Part 2 (either of [17], [18] or [19]). In addition, the each part of CC and CEM shall include contents of interpretations[20] and [21].

1.4 Certificate of Evaluation

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 problems found in the certification process. Evaluation is completed with the Evaluation Technical Report dated March, 2005 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.
The augmentation component is ADV_SPM.1.

1.5.3 SOF

This ST claims “SOF-basic” as its minimum strength of function.

Since the TOE is assumed to be for use in general commercial system, possible fraudulent action is attack using public information. Therefore the SOF-basic level, which is the level to countermeasure against low-level attacks, is considered sufficient regarding attacking power by the attacker.

1.5.4 Security Functions

The TOE has the following security functions, with each of the abbreviations matching the one in the figure 1-2.

(1) Cryptographic key generation function:

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 MSN-A expansion algorithm which is the cryptographic key generation algorithm to execute the AES Rijndael encryption algorithm, based on the Data Security Kit Encryption Standards. The cryptographic key is stored in volatile memory (FAX_RAM) on the FAX board.

(2) Cryptographic operation function

During the processing of a PC FAX, 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 cryptographic key generation.

(3) Data clear function

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

a) Automatic erase after completion of each job

1) Completion of copy job/ print job

When a copy job or print job ends, the actual image data file in IMC_RAM that was spooled to volatile memory (IMC_RAM) on the IMC board is overwritten with random values.

2) Completion of scan sending job

When a scan send job ends, the actual image data file in PCL_RAM that was spooled to volatile memory (PCL_RAM) on the PCL board is overwritten with random values

3) Completion of PCFAX job, FAX sending job, FAX receiving job

The actual image data file that was spooled to Flash memory on the FAX board is overwritten with fixed values.

b) Clear all memory by key operator operation

To execute or cancel the clear all memory by key operator operation function, identification and authentication of the key operator is required.

1) Execution of all data area erase by key operator

When the key operator executes clear all memory by key operator operation after being identified and authenticated as the key operator, all actual image data that are used for spooling to volatile memory

(IMC_RAM) on the IMC board and volatile memory (PCL_RAM) on the PCL board are overwritten with random values, and all actual image data that are used for spooling to Flash memory on the FAX board are overwritten by fixed values.

2) Cancel of all data area erase by key operator

To cancel clear all memory by key operator operation, key operator identification and authentication by entry of the key operator code are required following selection of the cancel operation.

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 timing of auto clear at job end and clear all memory by key operator operation is managed so that it is executed at job end or at the instruction of clear all memory by the key operator operation. And auto clear at job end and clear all memory by key operator operation always enforced.

The random values used to overwrite volatile memory on the IMC board and on the PCL board are generated based on the cyclical delay Fibonacci algorithm.

(4) Authentication function

The TOE always requires five digits of key operator code for key operator identification and authentication before the key operator programs 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.

Clear all memory by key operator operation and query and change of the key operator code can only be used following key operator authentication.

(5) Security management function

The TOE provides the query and change of the key operator code only be executed following key operator identification

The newly inputted key operator code should be verified that it is 5-digits number and then 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 disclose information through the use of a device other than the MFD to read actual image data remained in the flash memory in 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 of a copy, print, scan send, PC FAX, fax transmission, or fax reception job, or following interruption of a job, the actual image data area spooled to the MSD shall be overwritten. When the MFD is disposed of or its ownership changes, all areas to which actual image data is spooled shall be overwritten by the key operator operation.

1.5.7 Configuration Requirements

MFD made by SHARP, that TOE run on are listed below.
AR-M236, AR-M236J, AR-M276, AR-M276J, AR-M237, Ar-M237J, AR-M277, AR-M277J, AR-266S, AR-266G, AR-266FG, AR-266FP

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
A.OPERATOR	The key operator is a trustworthy person who doesn't 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

- Operation Manual: Data Security Kit AR-FR12M
  Version: TINSJ1478QSZZ
  Intended reader: Key operator (administrator of the site)
  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.

- Notice: Data Security Kit AR-FR12M
  Version: TCADZ0427QSZZ
  Intended reader: Key operator, user
  Contents: The items necessary for managing and operating the TOE in a secure manner are described. Written in Japanese.

- AR-FR12M Installation Manual
  Version: TCADZ0409QSZZ
  Intended reader: Key operator and service person (a maintenance administrator dispatched for the sales company)
  Contents: The work procedures for installation of the TOE on the main frame of MFD and the items that service person and Key operator are required to perform for the secure management and operations of TOE are described to help install TOE. Written in Japanese.

(2) Overseas version

-AR-FR12M Data Security Kit Operation Manual
  Version: TINSE1479QSZZ
  Intended reader: Key operator (administrator of the site)
  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-FR12M Data Security Kit Notice
  Version: TCADZ0428QSZZ
  Intended reader: Key operator, user
  Contents: The items necessary for managing and operating the TOE in a secure manner are described. Written in English.

-AR-FR12M Installation Manual

Version: TCADZ0410QSZZ

Intended reader: Key operator and service person (a maintenance administrator dispatched for the sales company)

Contents: The work procedures for installation of the TOE on the main frame of MFD and the items that service person and Key operator are required to perform for the secure management and operations of TOE are described to help install TOE. Written in 4 languages of English, French, German and Spanish.

2. Conduct and Results of Evaluation by Evaluation Facility

2.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM Part 2 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 Part 2.

2.2 Overview of Evaluation Conducted

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

Evaluation has started on May, 2004 and concluded by completion the Evaluation Technical Report dated March, 2005. 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 December, 2004 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.

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

As for problem 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 Table 2-1.

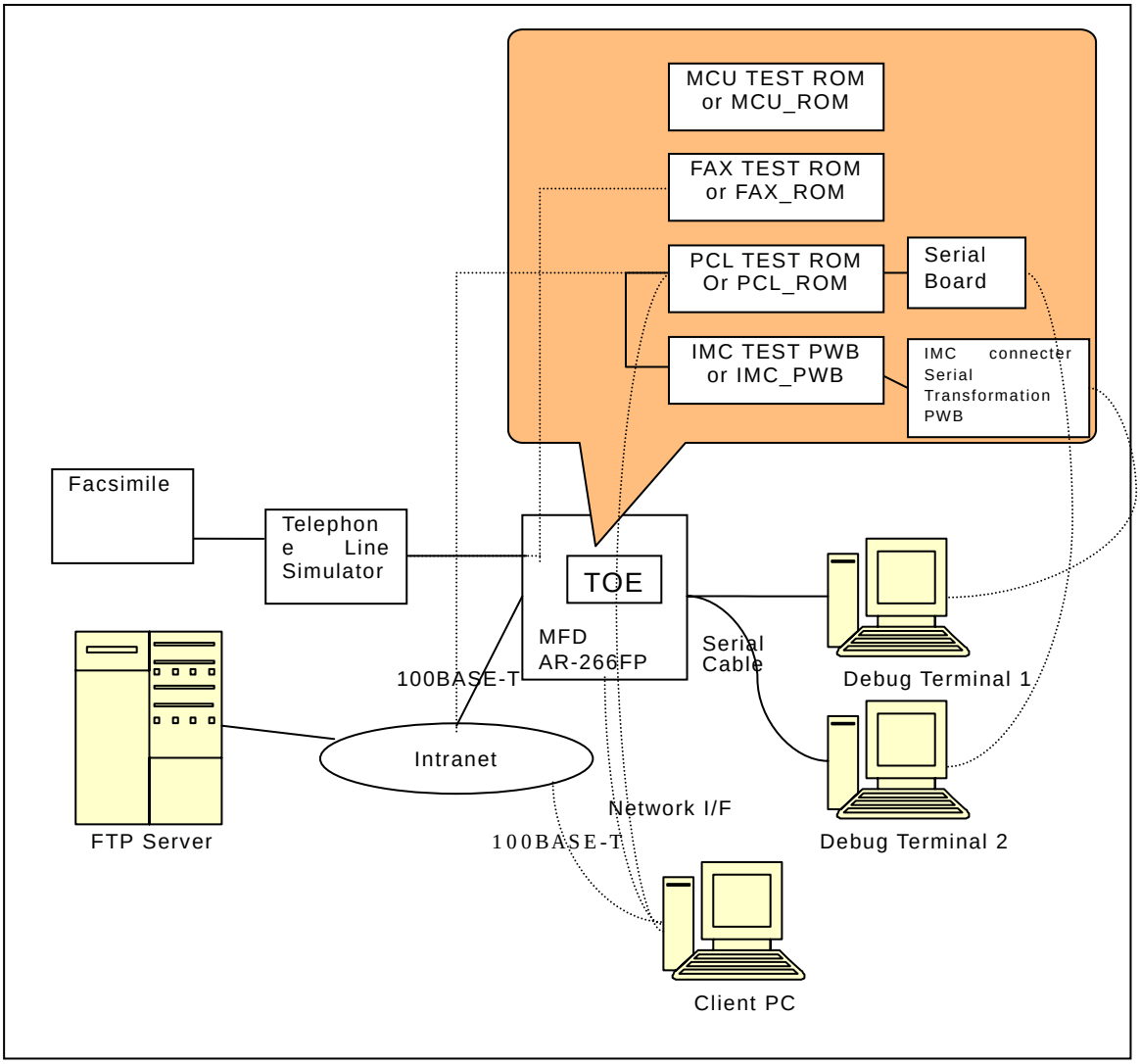

Figure 2-1 Configuration of Developer Testing

2) Outlining of Developer Testing

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

a. Test configuration

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

b. Testing Approach

All tests for TOE security function is performed under the circumstances of TOE testing environment configuration. There are 3 TOE testing environments as follows.

(1) Environment using the product ROM

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

(2) Environment using the testing ROM

As the difference of environment using the product ROM, IMC connector serial conversion PWB is connected to IMC PWB, and the serial board is connected to PCL_ROM. And in order to read the data before/after of overwriting to erase in IMC_RAM and PCL_RAM to the debug terminals through the serial cables, the IMC test PWB and the PCL test ROM are used. Moreover, FAX test ROM that has the function of printing out the data in the FAX_RAM and the Flash memory is used instead of FAX_ROM.

(3) Source code confirmation environment

Confirming the run of sub system (IMC random number sub system and PCL random number sub system) that cannot be checked by testing is demonstrated by the confirmation of the source codes.

c. Scope of Testing Performed

Items of the developer test include 5 security functions and total 13 items of tests are performed.
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.

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 Testing

1) Evaluator Test Environment

Test configuration performed by the evaluator is showed in the Table 2-2.

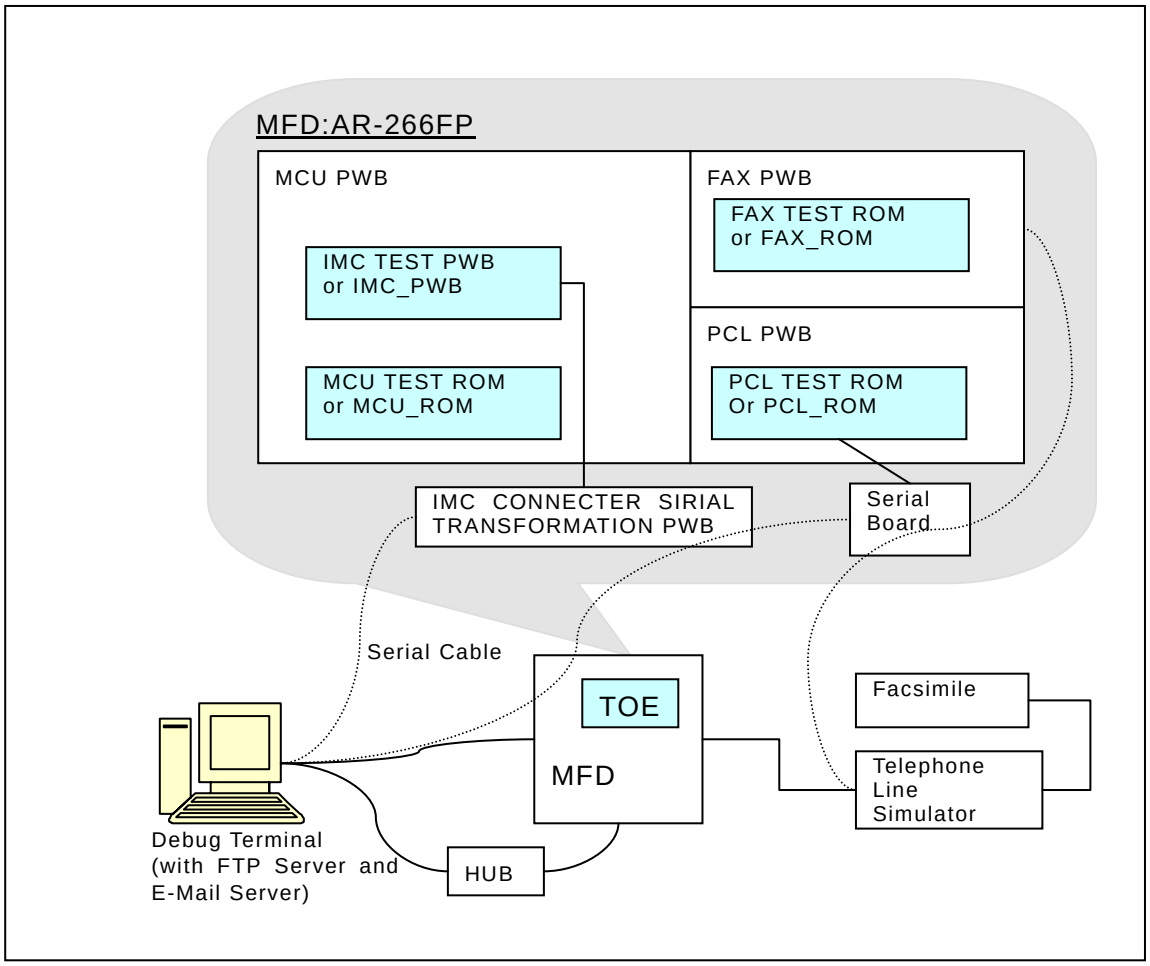

Figure 2-2 Configuration of Evaluator Testing

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

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

b. Testing Approach

All tests for TOE security function is performed under the circumstances of TOE testing environment configuration. There are 2 TOE testing environments as follows.

(1) Environment using the product ROM

It is the same configuration that the user actually uses.

IMC connector serial conversion PWB and serial PWB for debugging are not connected.

(2) Environment using the testing ROM

As the difference of environment using the product ROM, IMC connector serial conversion PWB is connected to IMC PWB, and the serial board is connected to PCL_ROM. And in order to read the data before/after of overwriting to erase in IMC_RAM and PCL_RAM to the debug terminals through the serial cables, the IMC test PWB and the PCL test ROM are used. Moreover, FAX test ROM that has the function of printing out the data in the FAX_RAM and the Flash memory is used instead of FAX_ROM. MCU test ROM to identify the test ROM is used.

c. Scope of Testing Performed

The evaluator performed total 22 items of test that include 8 items of testing that are devised by the evaluator, 9 items of sampling test of the developer test and 5 items of the penetration test.

The tests that devised by the evaluator are considered the following factors.

(1) All of 5 security functions should be included.
(2) Testing of the function that considers to be significant from the factor of the security objective (cryptographic key generation)
(3) TOE should be operated according to the function specification for the abnormal processing.
(4) Passive tests that the developer had not performed.
(5) Tests that TOE is installed on the other MFD (AR266S + Printer extended option, AR-266FG) for which TOE is available.

In the sampling of the developer test, all of 5 security functions can be selective and arranged so that all data erase functions dispersed in each ROMs can be tested thoroughly, and 9 items that correspond to 69% of 13 items that the developer had performed are selected.

In the penetration test, test items that apply to TOE and whole TOE environment are devised in addition to the 3 security functions (data erase function, authentication function, security management function), in order to confirm that the obvious vulnerability which the developer is not taking into consideration does not exist.

d. Result

All 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 Part 2 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.

Problems found in certification process were prepared as certification review, which were sent to evaluation facility.

The Certification Body confirmed such problems 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 assurance requirements with assurance component ADV_SPM.1prescribed 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

The glossaries used in this report are listed below.

AES	Advanced Encryption Standard established by NIST (National Institute of Standards and Technology)
EEPROM	Electrically Erasable Programmable ROM, a type of non-volatile memory that allows electrical rewriting to any part of memory if performed infrequently.
FAX PWB	A unit consisting of MFD that the Data Security Kit which is the TOE can be mounted and what the components are soldered to mount on the print PWB. It takes on FAX communication function.
Flash memory	A kind of volatile memory. ROM that enables electrical erasing the entire portion or rewriting the arbitrary portion.
GDI PWB	One of the constituent units that can mount the TOE and realize the print function of MFD. It equips Sharp Printer Language.
I/F	Interface
IMC PWB	A unit consisting of MFD that the Data Security Kit which is the TOE can be mounted and what the components are soldered to mount on the print PWB. A part of physical object

	provided by TOE. It takes on image processing function.
MCU PWB	A unit consisting of MFD that the Data Security Kit which is the TOE can be mounted and what the components are soldered to mount on the print PWB. It takes on control function for the entire MFD.
MSD	Mass Storage Device For this TOE, MSDs are the volatile memory on the IMC board, the volatile memory on the PCL board, and Flash memory on the FAX board. These are managed by a file system.
PCL	Printer Control Language
PCL PWB	A unit consisting of MFD that the Data Security Kit which is the TOE can be mounted and what the components are soldered to mount on the print PWB. It responds to the Sharp PCL that is positioned as a kind of PDL and takes on the printer function.
PDL	Page Description Language. This consists of the commands that control a page printer, and the language system.
RAM	Random Access Memory
ROM	Read Only Memory
Image Data	Digitalized image data of scanned original image for copying/ printing/ scanning/ FAX sending by MFD. In PCFAX, FAX sending/ receiving, data that send to the phone line or are received from the phone line are also included and data that are converted so that MFD can handle them are also called Image Data.
Engine	A device that forms printing image on the image receiving paper including the mechanism of paper feeding/ paper delivery function. It is also called Print Engine or Engine Unit.
Key Operator	An authenticated user who is permitted to access to TOE security management function / MFD management function.
Key Operator Code	Password for key operator authentication
Key Operator	TOE security management function as well as MFD management function. Identification/ authentication as the

Program	key operator is required to access to the key operator program.
Job	The flow/ sequence from the beginning through the end of each MFD function (copying/ printing/ scan sending/ PCFAX/ FAX sending/ FAX receiving). In some cases an instruction for operation is also called a job.
Data Security Kit	Upgraded kit AR-FR12M exclusively for Sharp MFD.
Memory	Storage device. Especially the storage device made of semiconductor element.
Unit	Unit that is equipped with detachable standard components or optional components on the print PWB and realized the operative conditions. Or unit that is operative including the mechanical portion.
PWB	It is referred to what components are soldered to mount on the print PWB.
Real Image Data	Real image data portion in which the control area is removed from the image data.
All data area erase	The processing of overwriting to erase all real image data area used for spooling, as for the volatile memories mounted on MFD.

6. Bibliography

[1] Data Security Kit AR-FR12M Security Target Version 0.25 February 25, 2005 SHARP Corporation

[2] Guidance for IT Security Certification Application, etc. April 2004, Information-Technology Promotion Agency, ITQM-23 (Revised on November 5, 2004)

[3] General Requirements for IT Security Evaluation Facility, April 2004, Information-Technology Promotion Agency, ITQM-07

[4] General Requirements for Sponsors and Registrants of IT Security Certification, April 2004, Information-Technology Promotion Agency, ITQM-08 (Revised on November 5, 2004)

[5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.1 August 1999 CCIMB-00-031

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031 (Translation Version 1.2 January 2001)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032 (Translation Version 1.2 January 2001)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033 (Translation Version 1.2 January 2001)

[11] ISO/IEC15408-1: 1999 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model JIS

[12] ISO/IEC 15408-2: 1999 - Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:1999 - Information technology - Security techniques – Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] JIS X 5070-1: 2000 - Security techniques - Evaluation criteria for IT security - Part 1: General Rules and general model

[15] JIS X 5070-2: 2000 - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[16] JIS X 5070-3: 2000 - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology Version 1.0 August 1999

[18] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology Version 1.0 August 1999 (Translation Version 1.0 February 2001)

[19] JIS TR X 0049: 2001 – Common Methodology for Information Technology Security Evaluation

[20] CCIMB Interpretations-0210 (February 2002)

[21] CCIMB Interpretations-0210 (February 2002) (Translation Version 1.0 October 2002)

[22] Data Security Kit AR-FR12M Evaluation Technical Report Version 3.3, March 7, 2005, Japan Electronics and Information Technology Industries Association, Information Technology Security Center