Certification Report

Buheita Fujiwara, Chairman
Information-Technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	June 14, 2005 (ITC-5046)
Certification No.	C0033
Sponsor	Sharp Corporation
Name of TOE	AR-FR22
Version of TOE	VERSION S.10
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.
October 18, 2005

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

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following criteria prescribed in the "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-0407

Evaluation Result: Pass

"AR-FR22 VERSION S.10" 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-FR22 VERSION S.10" (hereinafter referred to as "the TOE") conducted by Japan Electronics and Information Technology Industries Association, Information Technology Security Center (hereinafter referred to as "Evaluation Facility"), and it reports to the sponsor, Sharp Corporation.

The reader of the Certification Report is advised to read the corresponding ST and manuals (please refer to "1.5.9 Documents Attached to Product" for further details) attached to the TOE together with this report. The assumed environment, corresponding security objectives, security functional and assurance requirements needed for its implementation and their summary specifications are specifically described in ST. The operational conditions and functional specifications are also described in the document attached to the TOE.

Note that the Certification Report presents the certification result based on assurance requirements conformed to the TOE, and does not certify individual IT product itself.

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

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows:

Name of Product:	AR-FR22
Version:	VERSION S.10
Developer:	Sharp Corporation

1.2.2 Product Overview

The TOE is offered as a firmware up grade kit of a Multi Function Device (hereafter referred to as MFD). The TOE aims to prevent leakage of actual image data stored temporarily in Memory Device. The Memory Device that actual image data is stored temporarily is Flash memory and volatile memory (Random Access Memory). The TOE executes encryption before the actual image data are spooled in Flash memory, when the MFD functions like PCFAX, FAX sending or FAX receiving are performed. It also erases spool data area in MSD 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 secrecy of actual 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 is provided by two ROM boards which are firmware upgrade kit of the MFD. Relation between the TOE and the MFD is shown in the Figure 1-1. Physical configuration of the TOE is shown as shaded areas in the Figure 1-1.

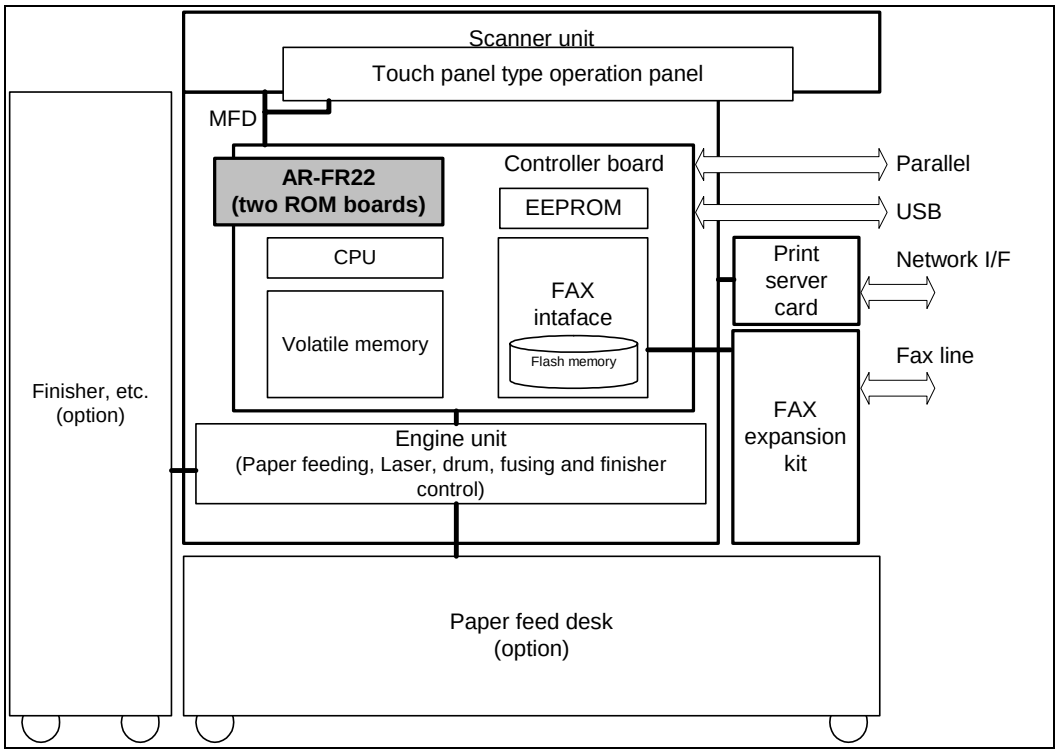

Figure1-1 : The TOE and physical configuration of the MFD

Logical configuration of the TOE is shown in the figure 1-2. In the figure 1-2, The TOE is indicated by the thick-lined frame. The rectangles indicate the TOE's functions and the rectangles with rounded corners indicate hardware. The TOE's functions that are security functions are shaded.

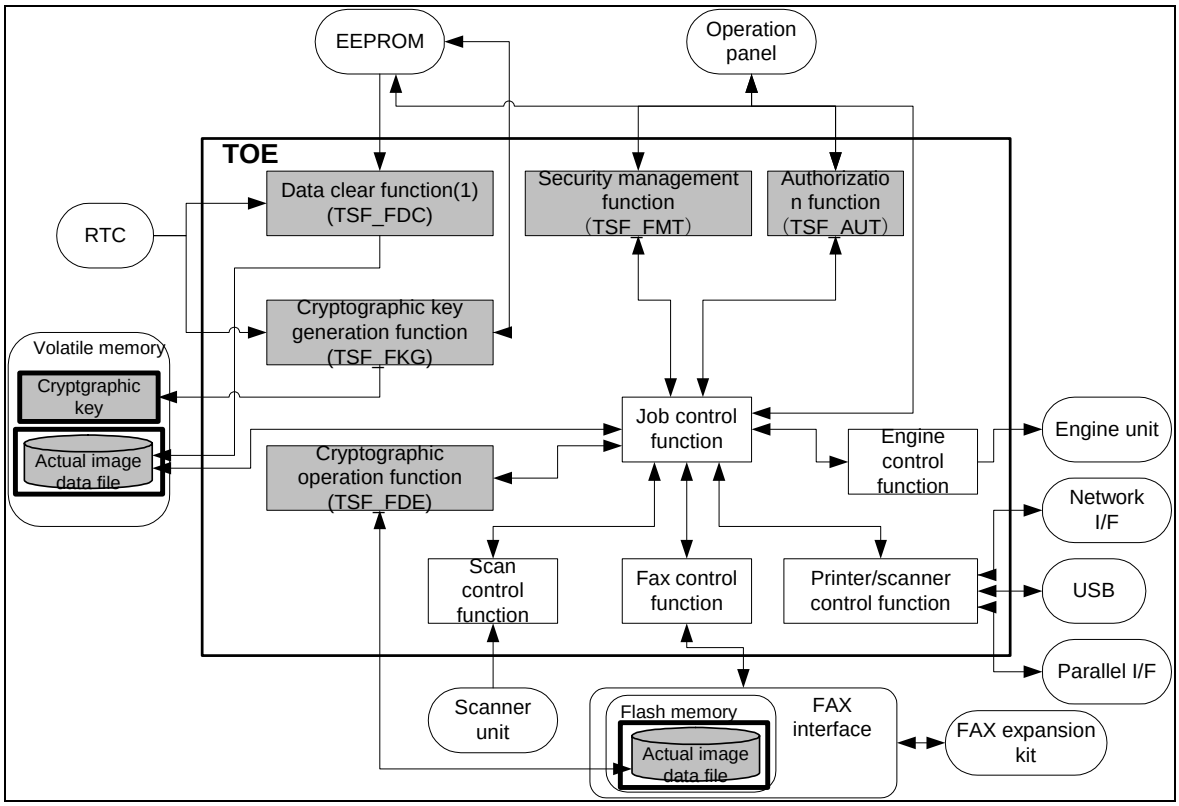

Figure 1-2 : Logical configuration of the TOE

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.

c) Data clear function (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:
· Auto clear at job end
(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.

- 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 is cleared by writing random values over all actual image data areas of those memories, and Flash memory is cleared by writing fixed values over all actual image data areas of Flash memory. This function also can cancel (interrupt) the clear all memory by the key operator operation.

d) Authentication function (TSF_AUT)
Authenticates a key operator by means of the key operator code (password).

e) Security management function (TSF_FMT)
This provides a function for changing (modifying) the key operator code following authentication as a key operator.

f) Engine control function
Controls the engine unit during 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 job for scanning of an original.

h) Printer/scanner control function
This function can operate on an MFD that can be equipped with the TOE and that has the printer board standard or as an option. In addition, the network can operate on an MFD that has the network function as an option.

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

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) 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 copy, print, scan send, PC FAX, fax transmission, and fax reception operation of the MFD.

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-FR22 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-FR22 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 (either of [20] and [21]).

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 September, 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. Because of this offensive ability

of an attack person is a low-level. Therefore, it is enough by the SOF-basis that minimum strength of function can be opposed to low-level.

1.5.4 Security Functions

Security functions of the TOE are as follow.

(1) Cryptographic key generation

The TOE generates a cryptographic key (shared key) to support the actual image data encryption function. When the MFD is powered on, a cryptographic key (shared key) is always generated. The cryptographic key is generated as a 128-bit of secure key using MSN-J 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 to generate in MSN-J expansion algorithm is used by code operation to spool in Flash memory. The cryptographic key is stored in volatile memory.

(2) Cryptographic operation

During the processing of a job, the actual image data of the job is always encrypted before being spooled to Flash memory. 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.

The cryptographic key is used in MSN-J expansion algorithm in code operation to Flash memory.

(3) Data clear

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

a) Auto clear at job end

When a copy job, print job or scan send job ends, the actual image data file in volatile memory is overwritten with random values.

When a PC FAX, fax transmission, or fax reception job ends, the actual image data file that was spooled to Flash memory 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.

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 are overwritten with random values, and all actual image data that are used for spooling to Flash memory are overwritten by fixed values. 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. In key operator authentication, when the number of times of unsuccessful authentication trial after an authentication success of the last to a key operator is authentication failure which is three continuations, an authentication input receptionist is stopped for five minutes. A normal state is returned from an authentication input stop to automatically the re-authentication input is accepted. 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 code is managed in EEPROM as authentication data for comparison

with the inputted data, and the key operator identification/authentication functions and code entry hidden feedback function are always executed, so that cancellation of clear all memory is only possible when the user is identified and authenticated as a key operator.

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 are generated based on the cyclical delay Fibonacci algorithm.

(4) Authentication

The TOE always requires key operator identification and authentication before the key operator programs (TOE security management functions) can be used. This specifies key operator and associates the role of key operator with a user. Key operator identification and authentication are enforced following selection of the key operator programs by requiring entry of the key operator code. In key operator authentication, when the number of times of unsuccessful authentication trial after an authentication success of the last to a key operator is authentication failure which is three continuations, an authentication input receptionist is stopped for five minutes. A normal state is returned from an authentication input stop to automatically the re-authentication input is accepted. 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/authentication functions 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.

Clear all memory by key operator operation, which is a data clear function (TSF_FDC), and query and change of the key operator code, which are security management functions (TSF_FMT), can only be used following key operator authentication (TSF_AUT).

(5) Security management

The key operator code is managed by the security management(TSF_FMT). The security management (TSF_FMT) can only be executed following key operator identification and authentication (TSF_AUT). Like authentication (TSF_AUT), this therefore specifies key operator and associates the role of key operator with a user and even after the key operator code is modified (changed), the role as a key operator is maintained.

· Changing (modifying) the key operator code

This function provides the functions of key operator code query and modification. The newly inputted key operator code should be verified that it is 5-digits number.

When each setting value is changed, 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 leak 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-M351U, AR-M451U, AR-355U, AR-455U, AR-355UJ, AR-455UJ, AR-311S, AR-351S, AR-451S, AR-311FP, AR-351FP, AR-451FP

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

- AR-FR22 Data Security Kit Operation Manual
  Version: CINSJ3105FC51
  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.

- AR-FR22 Data Security Kit Notice
  Version: TCADZ6053FCZZ
  Intended reader: Key operator, user
  Contents: The items necessary for managing operating the TOE in a secure manner are described. Written in Japanese.

- AR-FR22 installation manual
  Version: TCADZ6049FCZZ
  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. Described in Japanese.

(2) Overseas version

- AR-FR22 Data Security Operation manual
  Version: CINSZ3106FC51
  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-FR22 Data Security Kit Notice
  Version: TCADZ6054FCZZ
  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-FR22 installation manual
  Version: TCADZ6050FCZZ
  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. Described 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 June, 2005 and concluded by completion the Evaluation Technical Report dated September, 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 July, 2005 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 July, 2005.

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

As for concerns indicated during evaluation process by the Certification Body, the certification review was sent to the evaluation facility. These were reflected to evaluation after investigation conducted by the evaluation facility and the developer.

2.3 Product Testing

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

2.3.1 Developer Testing

1) Developer Test Environment

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

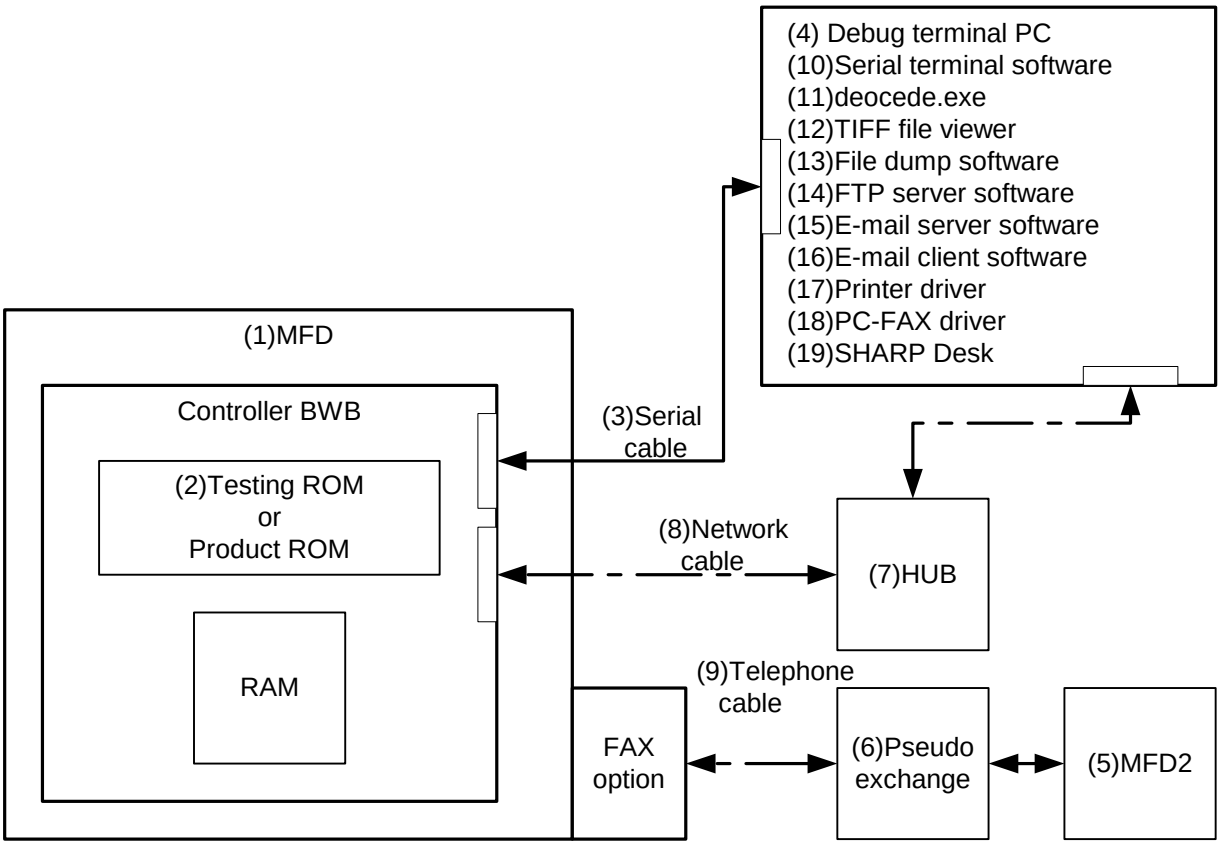

Figure 2-1 Configuration of Developer Testing

2) Outlining of Developer Testing

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

a. Test configuration

The testing configuration conducted by the developer is shown in the Figure 2-1. The developer testing has been performed in a testing environment of a hardware and software configuration equivalent to the TOE configuration identified in the ST. About the part which does not completely agree with the configuration that testing configuration is identified in ST, it is the reason to be able to consider to be equal as follows.
As for MFD of the Figure 2-1, some of models of MFD that the ST identifies as environment to be used by the TOE were employed when the testing was performed. Since these models support any function of any MFD that the ST identifies as environment to be used by the TOE, MFD in test configuration is equivalent to MFD that the ST identifies as environment to be used by the TOE.
Testing ROM in the Figure 2-1 is different from TOE identified in ST. An add of debug feature and modification of a security feature of part did this by reason of convenience of testing for product ROM (TOE). It employed product ROM that a security feature before it was changed worked justly, and, as for a security feature changed by reason of convenience of testing, testing was done. Therefore, what has performed the testing by employing testing ROM and product ROM can be considered equivalent to what has tested the TOE identified in the ST.

b. Testing Approach

All tests for TOE security function is performed under the circumstances of TOE

testing environment configuration.
For the testing, following approach was used.

1. Environment using the product ROM
   It is the same configuration that the user actually uses.
   Serial cable for debugging are not connected.
2. Environment using the testing ROM
   In contrast to the ROM use environment for product, testing ROM is used for reading the data before/ after of overwriting to clear in RAM out to the debug terminal through the serial cable. And testing ROM has function outputting cryptographic key, exogenous variable area on RAM data in a Flash memory in debug terminal.
   In convenience of testing, cryptographic key is turned into zero, and function changing random number of overwrite clearing in value expressing overwrite clearing number of times is comprised.

c. Scope of Testing Performed

Testing is performed 28 items by the developer.
The coverage analysis is conducted and examined to testing satisfactorily all of the security functions described in the functional specification and the external interface. Then, the depth analysis is conducted and examined to testing satisfactorily all the subsystems described in the high-level design and the subsystem interfaces.

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 shall be the configuration shown in figure 2-1 except the E-mail server software and the E-mail client software.

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 the configuration shown in figure 2-1 except the E-mail server software and the E-mail client software.
Because testing to use E-mail is not included in the evaluator testing, there is not influence to testing results by these software having been removed. Therefore, it is considered that the evaluator testing has been performed under equivalent configuration as the developer testing.

b. Testing Approach

For the testing, following approach was used.

1. Environment using the product ROM
   It is the same configuration that the user actually uses.
   Serial cable for debugging are not connected.
2. Environment using the testing ROM
   In contrast to the ROM use environment for product, testing ROM is used for reading the data before/ after of overwriting to clear in RAM out to the debug terminal through the serial cable. And testing ROM has function outputting cryptographic key, exogenous variable area on RAM data in a Flash memory in debug terminal.
   In convenience of testing, function turning cryptographic key into zero, and function replacing function clearing by overwriting random number with function clearing by overwriting value that is times of the overwriting is comprised.

c. Scope of Testing Performed

Total of 13 items of testing; namely 7 items from testing devised by the evaluator and 6 items from testing from sampling of developer testing was conducted. As for selection of the test subset, the following factors are considered.

1. All of 5 security functions should be included.
2. Testing of the function that seems to be important from the viewpoints of the security objectives (generation of encryption key).
3. TOE should be operated according to the function specification for the abnormal processing.
4. Functions that are newly added to AR-FR12M, which has been certified.
5. Passive tests that the developer had not performed.
6. Tests that TOE is installed on the other MFD for which TOE is available.

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.

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

The Certification Body confirmed such concerns pointed out in Observation Report and certification review were solved in the ST and the Evaluation Technical Report.

4. Conclusion

4.1 Certification Result

The Certification Body verified the Evaluation Technical Report, the Observation Report and the related evaluation evidential materials submitted and confirmed that all evaluator action elements required in CC Part 3 are conducted appropriately to the TOE. The Certification Body verified the TOE is satisfied the EAL3 and assurance component ADV_SPM.1 prescribed in CC Part 3.

4.2 Recommendations

None

5. Glossary

The abbreviations used in this report are listed below.

CC:	Common Criteria for Information Technology Security Evaluation
CEM:	Common Methodology for Information Technology Security Evaluation
EAL:	Evaluation Assurance Level
PP:	Protection Profile
SOF:	Strength of Function
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Functions
AES:	Advanced Encryption Standard, established by NIST (National Institute of Standards and Technology)
DSK:	Data Security Kit
EEPROM:	Electronically Erasable Programmable ROM, a type of non-volatile memory that allows electrical rewriting to any part of memory if performed infrequently.
I/F:	Interface
IFAX:	Internet FAX
MSD:	Mass Storage Device, For the TOE, MSDs are the volatile memory and Flash memory. These are managed by a file system.
OS:	Operating System
RAM:	Random Access Memory
ROM:	Read Only Memory
TIFF-FX:	Tag Image File Format Fax eXtended.

The glossaries used in this report are listed below.

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 Program:
TOE security management function as well as MFD management function. Identification/ authentication as the 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-FR22 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.

Actual Image Data:
Actual 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 actual image data area used for spooling, as for the volatile memories mounted on MFD.

Operation panel:
A user interface device that includes a display, buttons/keys, and buttons in a touch panel. Or the unit that includes such a device.

Non-volatile memory:
Memory that retains its contents even when the power is turned off. Non-volatile memory is often made from semiconductor elements or magnetic memory.

Flash memory: A kind of volatile memory. ROM that enables electrical erasing the entire portion or rewriting the arbitrary portion.

6. Bibliography

[1] Data Security Kit AR-FR22 Security Target Version 0.09, July 21, 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-0407 (December 2003)

[21] CCIMB Interpretations-0407 (December 2003) (Translation Version 1.0 August 2004)

[22] Data Security Kit AR-FR22 Evaluation Technical Report Version 2.2, September 9, 2005, Japan Electronics and Information Technology Industries Association, Information Technology Security Center