Certification Report

Target of Evaluation

Application date/ID	April 19, 2004 (ITC-4026)
Certification No.	C0018
Sponsor	Sharp Corporation
Name of TOE (Version of TOE)	Japan: Data Security Kit AR-FR4 version M.20 Overseas: Data Security Kit AR-FR4 version M.20 Data Security Kit AR-FR5 version E.20
PP Conformance	None
Conformed Claim	EAL4
TOE Developer	Sharp Corporation
Evaluation Facility	Fuji Research Institute Corporation Information Security Evaluation Center

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

"Data Security Kit AR-FR4 version M.20 and Data Security Kit AR-FR5 version E.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 “Japan: Data Security Kits AR-FR4 version M.20, overseas: Data Security Kits AR-FR4 version M.20 and Data Security Kits AR-FR5 version E.20 ” (hereinafter referred to as “the TOE”) conducted by Fuji Research Institute Corporation (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: Japan : Data Security Kit AR-FR4 version M.20
overseas : Data Security Kit AR-FR4 version M.20
Data Security Kit AR-FR5 version E.20

Developer: Sharp Corporation

1.2.2 Product Overview

This product called the digital multi-functional data security kit (hereafter referred to as DSK) is the firmware designed to reduce the danger of information leak, preventing the document or image data temporarily stored in a digital multi-functional device (hereafter referred to as MFD) from being opened.
An MFD, which is an office machine, is configured as a print function unit with optional copy / image scanning / fax functions. If it comes only with a print function unit (and with no other optional function), it is called MFP (Multi-Function Printer) and considered as an MFD. The DSK is offered as an upgrade kit of the MFD firmware.

1.2.3 Scope of TOE and Overview of Operation

The TOE physical configuration is the DSK. As shown in the Figure 1-1, the DSK is installed as MFD firmware ROM replacing the standard one.

The controller unit containing the DSK comes with a microprocessor; the firmware to be executed by the microprocessor; the volatile RAM to be used when the firmware is executed; and the EEPROM for storing the security settings. Spooled data, which are to be the TOE protected assets, are stored in the volatile RAM as RAM disk. An optional HDD can also be installed for the storage. As for the optional fax function, the Flash memory on the fax interface is used for spooling. The HDD, RAM and Flash memory in the MFD are generically called MSD (Mass Storage Device). All operations on MFD including the DSK security settings are performed through the operational panel.

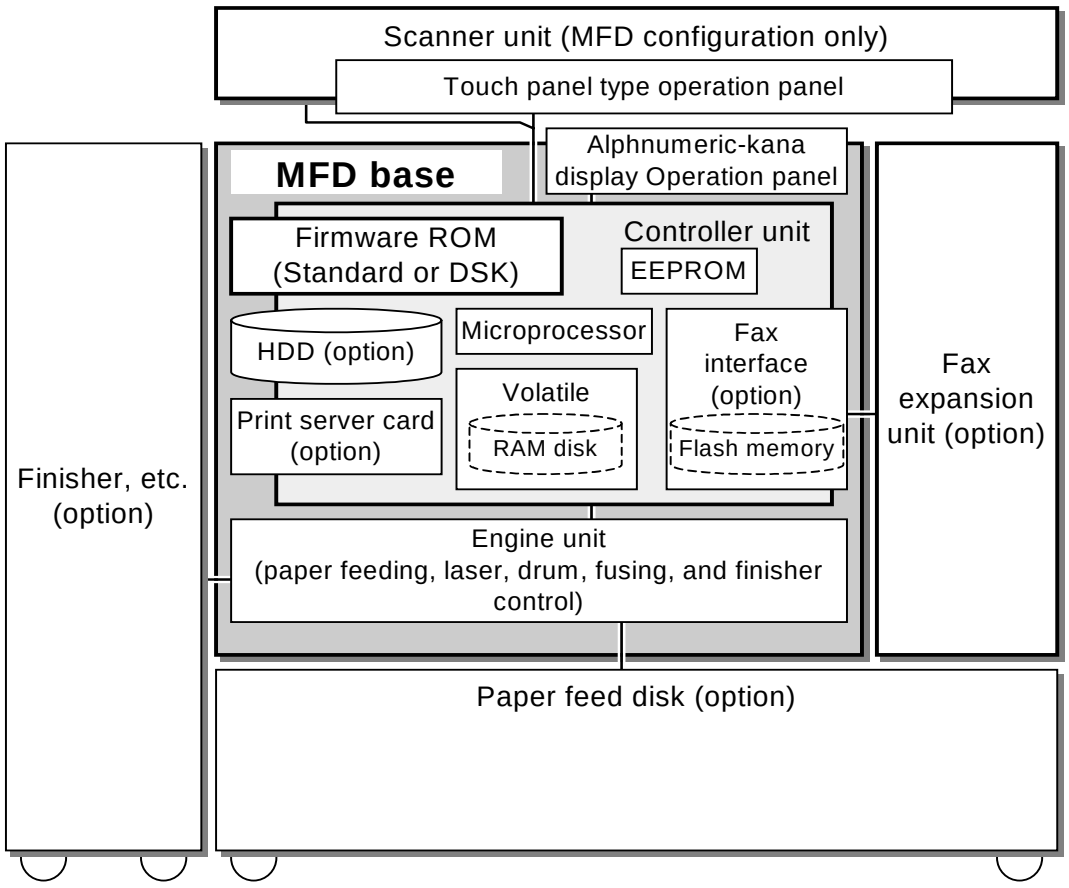

Figure 1-1: DSK in MFD

The Figure 1-2 shows the TOE logical scope. The TOE as MFD controller unit firmware intervenes the input from the operational panel for the existing MFD functions or the writing to MSD, calling the codes for executing security functions.

Abbreviations of the TOE security functions (to be detailed in the section 1.5.4) are highlighted. The parameter setups on the user interface relating to the operational panel and the message functions are screened. The others are the functions for encryption or clearance.

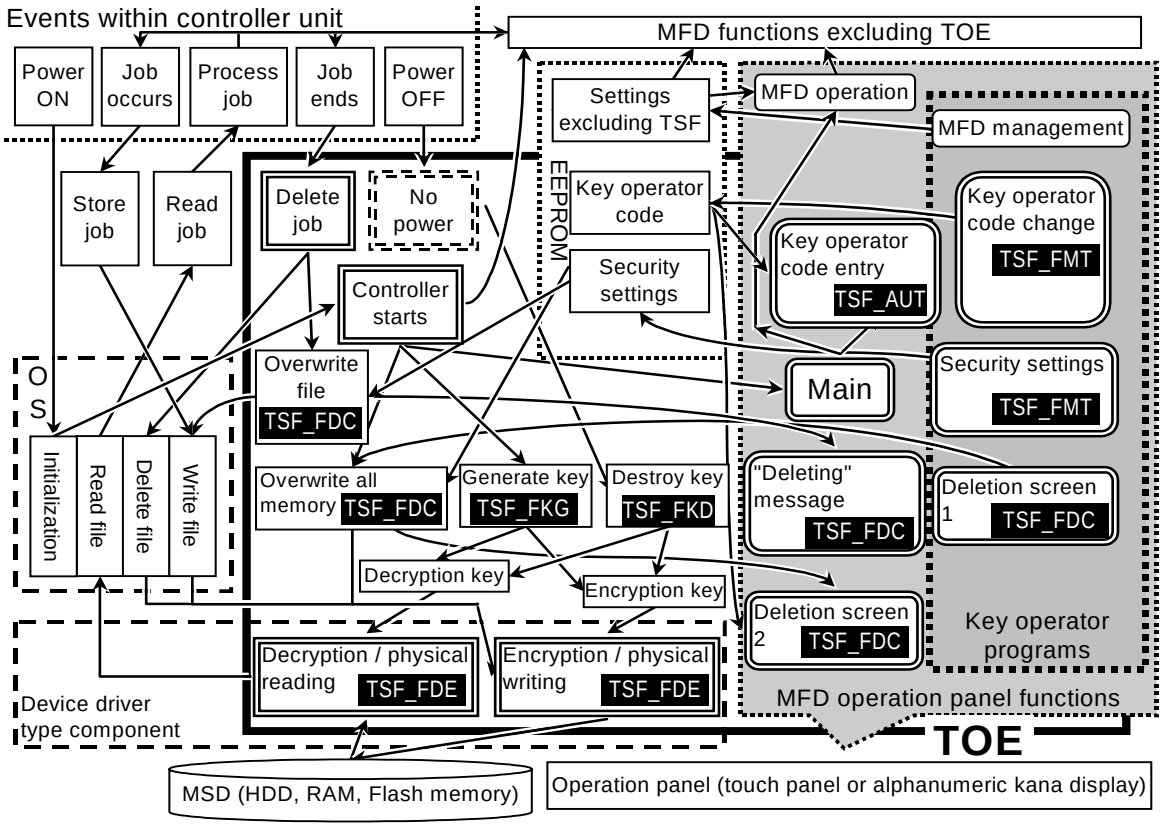

Figure 1-2: TOE logical scope

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 “Digital MFD Data Security Kit AR-FR4/AR-FR5 Security Target Version 0.04” 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 “Digital MFD Data Security Kit AR-FR4/AR-FR5 Evaluation Report Evaluation Technical Report” (hereinafter referred to as “the Evaluation Technical Report”) [21]. 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].

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 August 3 , 2004 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 EAL4 conformance.

1.5.3 SOF

This ST claims “SOF-basic” as its minimum strength of function.
This TOE is assumed to be for normal office use. Means and time of a direct attack on TOE are restricted by the environmental assumptions. Therefore the SOF-basic level, which is the level to countermeasure against low-level attacks, is considered sufficient. Even if the MSD is removed from the environment (for its usage), the data clearance and the cryptographic functions will enable a countermeasure against low-level attacks. However, the cryptographic functions are not treated as part of functional strength in this evaluation.

1.5.4 Security Functions

Security functions of the TOE are as follow.
The abbreviation of each security function corresponds to the one in the Figure 1-2.

(1) Data clearance function (TSF_FDC): The MFD spools document or image data to HDD or RAM for a printer / copy / image scanning processing; and to the Flash

memory for a fax processing. Even though these areas are freed for the memory management upon completion of a job, there are remaining data on the memory.

The TOE data clearance function clears these data left out on a spool area (HDD, RAM, Flash memory) by overwriting them. The function can perform three actions: (1) “Auto clearance upon completion of each job” for the corresponding data area, (2) “Auto clearance upon power-on” to automatically clear the entire spool area of HDD or RAM by overwrites when the TOE is powered on, and (3) “Entire data area clearance” to manually clear the entire area of HDD, RAM or Flash memory by overwrites.

The data clearance function is operated at the operational panel. A message and two screens will appear for the three actions: the clearance message for “Auto clearance upon completion of each job,” the clearance screen 1 for “Auto clearance upon power-on,” and the clearance screen 2 for “Entire data area clearance.”

(2) Cryptographic operation function (TSF_FDE): For processing data, the MFD creates the data file in MSD and reads the corresponding data for each job. The cryptographic operation function is used for the data file creation: it uses the cryptographic key produced by the cryptographic key generation function (to be described below) to encrypt data and scan them to MSD while it uses the same key to restore the data that have been retrieved for a processing.

(3) Cryptographic key generation function (TSF_FKG) and cryptographic key destruction function (TSF_FKD): The generation (destruction) function of a cryptographic key generates (destructs) the key that will be (was) used by the above cryptographic operation function. Upon start of the MFD, the cryptographic generation function generates a cryptographic key based on the date, time and tick time, and stores it to the volatile RMA. The key cannot be accessed from the operational panel or any other external interface. The cryptographic key destruction function is executed upon power-off of the volatile RAM (like when the device itself is powered off or power outage occurs). The cryptographic key generated by the cryptographic key generation function continues to be used until it is destroyed by the cryptographic key destruction function.

(4) Authentication function (TSF_AUT): The TOE has the authentication function because only the MFD administrator (called a key operator) is allowed to access the security administration function (to be described later). The key operator who enters the key operator code at the operational panel will be authenticated if the code matches the value stored in EEPROM of the MFD.

(5) Security administration function (TSF_FMT): The settings and interface that can be managed by users are offered for the TOE security function. The operational panel gives users the interface with the following security administration function.

- Data clearance setting: The function sets up the behavior of the data clearance function (TSF_FDC). You can set up the auto clearance execution/cancel upon power-on; the number of times data are auto-cleared upon completion of each job; the number of times the entire area is cleared; and the number of times data are auto-cleared upon power-on. The setup

values are stored in EEPROM.

- Key operator code setting: You can change the key operator code used for authentication. When the new key operator code is entered, the TOE checks if it is a 5-digit value. The setup value is stored in EEPROM.

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 malicious user may attempt to recover document or image data from the *residual data* in the MSD of a copy, print, scan, or fax job by physically removing the MSD from the MFD and using commercially available tools to read its contents.
T.ALTER	It is possible that a malicious user may change the settings of the security management function of the TOE.

1.5.6 Organisational Security Policy

There is no Organisational security policy required for using the TOE.

1.5.7 Configuration Requirements

The TOE, a ready-to-use upgrade kit for the MFD, is the ROM product that replaces a part of the ROM in MFD. The Table 1-2 lists the MFD models for the TOE.

Table 1-2 MFD models for TOE

DSK model / version	MFD models
AF-FR4 Version M.20	MFD models for oversea destinations: AR-M350, AR-M450, AR-M280N, AR-M350N, AR-M450N, AR-M280U, AR-M350U, AR-M450U, AR-M300U, AR-M300N, DM-3551, DM-4551 MFD models for destinations in Japan: AR-310M, AR-350M, AR-450M, AR-310S, AR-350S, AR-450S, AR-310F, AR-350F, AR-450F, DM-3551, DM-4551
AF-FR5 Version E.20	Printer models for overseas destinations: AR-P350, AR-P450, DM-3500, DM-3501, DM-4500, DM-4501

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.OFFICE	The MFD with the TOE incorporated will be installed in a normal office environment. When the office employees are all out of the office, security measures such as locking the doors are taken. In addition, if someone needs to enter the office when no employees are present, there is a means of verifying that the person is an authorized employee.
A.PROCEDURE	The key operator carefully follows these procedures: - Verifies that the TOE is installed. - Configures suitable data clear and clear repetition settings. - Regularly changes the *key operator code*. - Uses a *key operator code* that cannot be guessed easily. Does not disclose the *key operator code* to others.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

AR-FR4 Japanese version

- Document name: Instruction manual: Data Security Kit AR-FR4
- Version: 2003L DSC1 CINSJ2300FC53
- 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 in a secure manner are described. Written in Japanese.
- Document name: AR-FR4 installation manual*
- Version: TCADZ6011FCZ1(1)
- Intended reader: DSK service person (a maintenance administrator dispatched for the sales company)
- Contents: The Japanese-version AR-FR4 comes as ROMs (BOOT ROM and MAIN ROM), which this document describes how to install in MFP. Besides Japanese, the document is available in English, French, German and Spanish.
- Document name: SHARP MFP Data Security Version:M.20 E.20 Installation Check list; Instruction manual supplementary version; Models: AR-FR4 and

AR-FR5

- Version: 1.0
- Intended reader: Key operator and DSK service person
- Contents: The items that DSK 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.

AR-FR4 Overseas version

- Document name: AR-FR4 Data Security Kit Operation Manual
- Version: 2003M DSC1 CINSZ2302FC53
- Intended reader: Key operator (Administrator of the sites to be used)
- Contents: Offered as the guidance to use the TOE. The items necessary for managing and operating the TOE safely. Available in English, French, German and Spanish.
- Document name: AR-FR4 installation procedure manual*
- Version TCADZ5011FCZ1(1)
- Intended reader: DSK service person (Maintenance administrator dispatched from a sales company)
- Contents: The overseas-version AR-FR4 comes in the form of ROMs (BOOT and MAIN). The manual explains how to install these ROMs in MFP. Besides Japanese, the manual is available in English, French, German and Spanish.
- Document name: SHARP MFP Data Security Kit Version:M.20 E.20 Installation Checklist Supplemental Sheet Models:AR-FR4 AR-FR5
- Version: 1.0
- Intended reader: Key operator and DSK service person
- Contents: The items that DSK service person and Key operator are required to perform for the secure management and operations of TOE are described to help install the TOE. Available in English.

AR-FR5 Overseas version

- Document name: AR-FR5 Data Security Kit Operation Manual
- Version: 2003M DSC1 CINSZ2304FC53
- Intended reader: Key operator (Administrator of the sites to be used)
- Contents: Offered as the guidance to use the TOE. The items necessary for managing and operating the TOE safely are described. Available in English, French, German and Spanish.
- Document name: AR-FR4 installation procedure manual*
- Version: TCADZ6011FCZ1(1)
- Intended reader: DSK service person (Maintenance administrator dispatched

from a sales company)

- Contents: The overseas-version AR-FR5 comes in the form of a ROM (MAIN only). The manual describes how to install it. Besides Japanese, it is available in English, French, German and Spanish.
- Document name: SHARP MFP Data Security Kit Version:M.20 E.20 Installation Checklist Supplemental Sheet Models:AR-FR4 AR-FR5
- Version: 1.0
- Intended reader: Key operator and DSK service person
- Contents: The items that DSK service person and Key operator are required to perform for the secure management and operations are described. Available in Japanese.

* All of the Japanese-version AR-FR4 installation manual and the English-, French-, German- and Spanish-version installation manuals describe the same contents.

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 August, 2004. 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 May, 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 on May, 2004.

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

The Figure 2-1 shows the configuration of the testing system implemented by the developer. The Table 2-1 lists the devices and software tools used in the testing environment.

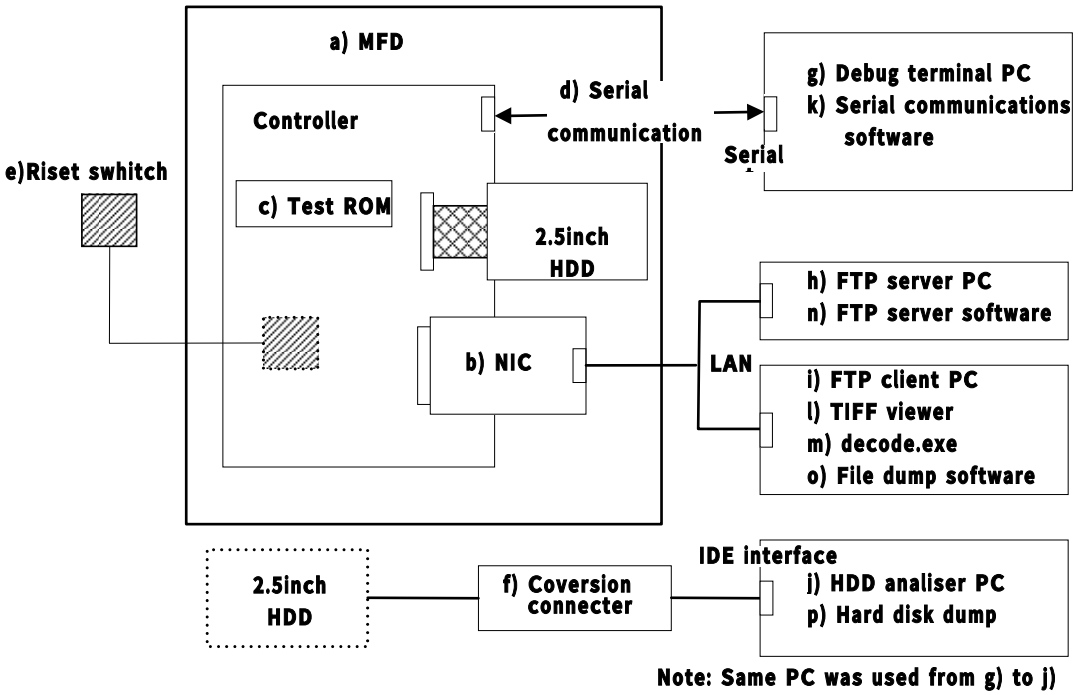

Figure 2-1 Configuration of Developer Testing

Table 2-1 Devices and tools used by the developer

Name	Overview (for each type)
Testing device	
a) MFD	MFD with TOE to be installed (AR-350S)
b) NIC	Board for connecting MFD to LAN
c) Test ROM	TOE (AR-FR4 version.M20)
d) Serial communications cable	The RS-232C compliant cable for connecting MFD and the debug terminal PC
e) Resetting switch	The switching button to be pressed for manually resetting the CPU on the MFD controller board.
f) Conversion connector	Connecter for converting the 2.5-inch IDE interface to the 3.5-inch IDE interface.
g)-j) PC	PC that enables the tools to confirm the MSD contents.

Testing tool	
k) Serial communications software	Terminal simulation software (TeraTerm Pro 2.3 19J) for the operation(s) via MFD and serial communications
l) TIFF Viewer	Image view software (IFAX VIEW version 3.0) for viewing the MFD-created compressed images on PC.
m) decode.exe	Software created by the developer for restoring the MFD-encrypted data file by using any key.
n) FTP server software	Server software (WAR-FTPD version 1.65) for forwarding the MFD-created data as a file by using FTP.
o) File dump software	Binary editor for dumping files on PC in hexadecimal numbers (Stirling version 1.31)
p) Hard disk dump software	Software that can read any specified sector in the hard disk and display/edit its contents. (DiskDump version 1.20)

2) Outlining of Developer Testing

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

a. Test configuration

The Figure 2-1 and the Table 2-1 show the configuration of the testing conducted by the developer. As for TOE, the debug ROM of AR-FR4 version M20 was used. It has the interface on which the test results can be confirmed, making the testing easy and sure. Without this interface, the ROM equals the product ROM. Therefore, the configuration meets the ST description.

b. Testing Approach

The developer used the operational panel, a job execution and/or a power-on to turn each security function (data clearance, encryption, cryptographic key generation, authentication, security control) into the completed state or into the incomplete state by the interruptions, read the results from the TOE or the MFD as direct data, and confirmed the contents on the debug PC.
The MSD contents are forwarded to the PC via LAN cable through the operations on MFD debug commands from the terminal connected by serial cable. Moreover, the HDD was physically removed from the MFD and connected to the debug PE through IDE for the confirmation of the contents. These data are confirmed by the image tools and the dump tools on the PC. The cryptographic key for the testing was used to encrypt the data. The same cryptographic key that was used for the encryption was used on the PC side for the restoration so that the data could be confirmed.

c. Scope of Testing Performed

The testing was conducted for all of the TOE security functions except for the cryptographic key destruction (data clearance, cryptographic operation, cryptographic key generation, authentication, security control). Moreover, all of the interfaces identified in the functional specifications were tested, and the correspondence between each function and external interfaces were also confirmed.
There are the total number of 28 items for testing, including the serial procedure for the encryption, restoration and data clearance for HDD/RAM and Flash memory. It was concluded that this total number is sufficient for the developer testing.
The cryptographic key destruction is due to the system characteristic causing loss of the stored contents upon power shutdown of the volatile RAM. For this reason, this function was excluded from the testing of TOE security functions.

d. Result

The evaluator confirmed that the developer conducted the testing appropriately; that the implemented items were valid; and that the methodology and results match those described by the functional test specifications.

2.3.2 Evaluator Testing

1) Evaluator Test Environment

The Figure 2-2 shows the testing system configuration of the test conducted by the evaluator. The Table 2-2 lists each device of the configuration.

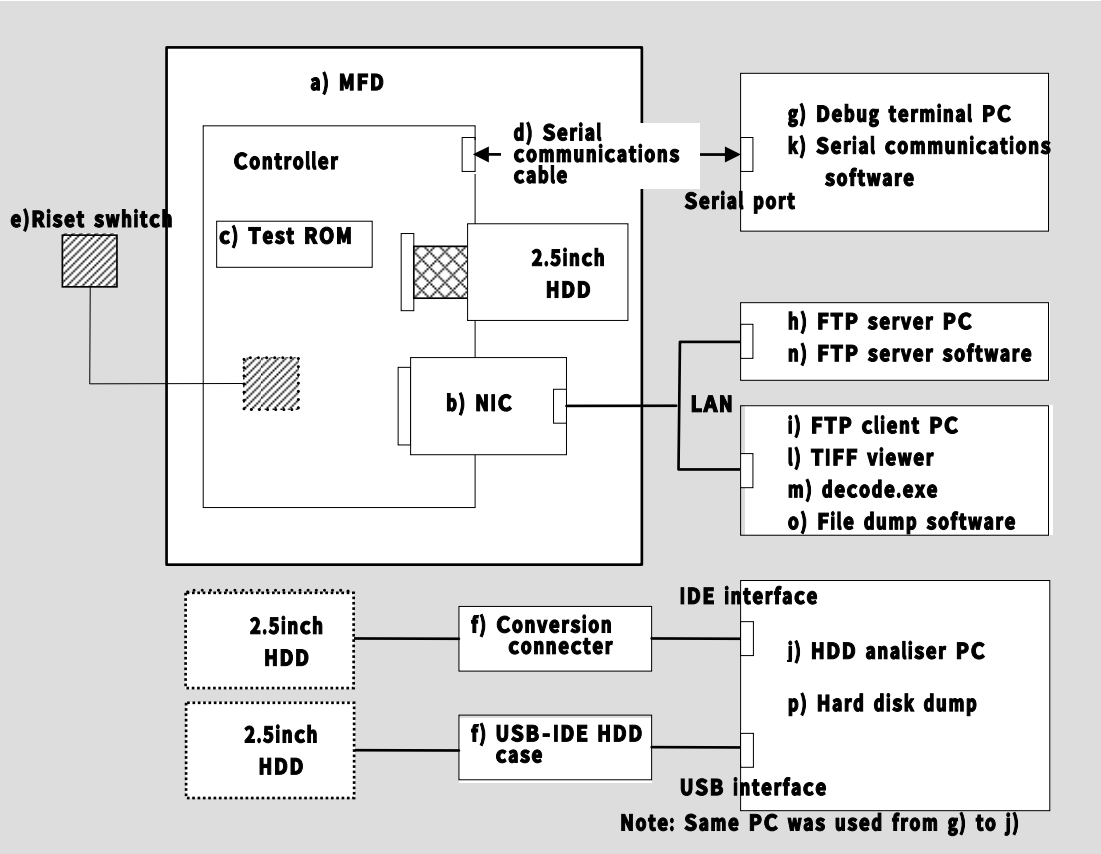

Figure 2-2 Configuration of evaluator's Testing

Table 2-2 Devices and tools used by the evaluator

Name	Overview(for each item)
Test device	
a) MFD	MFD with TOE to be installed (AR-310M)
b) NIC	Board for connecting MFD to LAN
c) Test ROM	TOE (AR-FR4 version.M20)
d) Serial communications cable	The RS-232C compliant cable for connecting MFD and the debug terminal PC
e) Reset switch	Button switch to be pressed for manually resetting the MFD controller board
f) Conversion connector	Connector for converting the 2.5-inch IDE interface to the 3.5-inch IDE interface
g) to j) PCs	PCs for activating the tools to confirm the MSD contents
Test tool	
k) Serial communications software	Terminal emulator software (TeraTerm Pro version 2.3 1.9J) for the operation(s) via MFD and serial communications
l) TIFF viewer	Image view software (IFAX VIEWER version 3.0) for displaying the MFD-created compressed images on PC
m) decode.exe	Developer software for restoring the MFD-encrypted data file with any key
n) FTP server software	Server software (WAR-FTPD version 1.65) for forwarding the MFD-created data as a file via FTP
o) File dump software	Binary editor (Stirling version 1.31) for the hexadecimal dumping of files on PC
p) Hard disk dump software	Software (DiskDump version 1.20) for reading any specified sector in the hard disk and for displaying and editing its contents

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

The Figure 2-2 and Table 2-2 show the configuration of the test conducted by the evaluator. The configuration matches the ST statements and the developer's testing environment. USB interface was used for better efficiency of testing.

b. Testing Approach

The evaluator concluded that the developer's testing methodology is appropriate for examining the expected behavior of the security functions and hence followed the developer's methodology.
The evaluator turned each security function into the completed state through the operational panel or a job or the power-on; or into the incomplete state through their suspensions, read the resulting data directly from TOE or MFD, and confirmed the contents on the debug PC.
The MSD contents are forwarded to the PC via LAN cable by operating on the MFD debug command from the terminal connected via serial cable. Moreover, the HDD was physically removed from the MFD and connected to the debug PC via IDE or USB for better efficiency of testing in order to confirm the contents. These data are confirmed on the PC through the image and dump tools. To encrypt data, a specific cryptographic key was used in this testing. The same key used for the encryption was again used for the restoration and confirmation on the PC side. (See the Figure 2-2)

c. Scope of Testing Performed

The valuator testing was conducted for all of the security functions except for the cryptographic key destruction. The typical testing patterns including normal actions and operational cancellations were implemented. The testing items counted 15 including the serial procedure related to the MSD data clearance: encryption/restoration/clearance of data.
To cover all of the security functions except for the cryptographic key destruction and all spooling (HDD, RAM disk and Flash memory), the 6 items out of the developer testing items were selected and implemented.

d. Result

The evaluator testing produced the expected results. The testing, which was sampled from the developer testing, was confirmed to have produced the results matching the functional testing specifications.

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 EAL4 assurance requirements prescribed in CC Part 3.

4.2 Recommendations

The TOE asset that needs to be protected is the MSD data removed from the MFD, whereas the opposing threat is to recover the remaining data from the MSD. Therefore, you have to remember that there is no resistance against a threat that uses legal means during the TOE operation. (For example, using an illicitly-obtained password to print the spooled data held by the job retention function) So the TOE users must understand the usage environment envisaged by the guidance in order to well manage the TOE.

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
DSK	Data Security Kit
EAL	Evaluation Assurance Level
MFD	Multi-Function Device
MFP	Multi-Function Printer
MSD	Mass Storage Device
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

6. Bibliography

[1] Digital MFD Data Security Kit AR-FR4/AR-FR5 Security Target Version 0.04: Sharp Corporation; July 30, 2004

[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 2001)

[21] Digital MFD Data Security Kit AR-FR4/AR-FR5 Evaluation Report: Fuji Research Institute Corporation; August 3, 2004; 03002795-01-R002-02

[22] JISEC Homepage Certified products list (http://www.ipa.go.jp/security/jisec/cert-list.html)