Certification Report

Buheita Fujiwara, Chairman
Information-Technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	June 1, 2005 (ITC-5045)
Certification No.	C0031
Sponsor	Sharp Corporation
Name of TOE	AR-FR21
Version of TOE	VERSION M.10
PP Conformance	None
Conformed Claim	EAL3
TOE Developer	Sharp Corporation
Evaluation Facility	Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security

This is to report that the evaluation result for the above TOE is certified as follows.
September 6, 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-FR21 VERSION M.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-FR21 VERSION M.10" (hereinafter referred to as "the TOE") conducted by Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security (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-FR21
Version:	VERSION M.10
Developer:	Sharp Corporation

1.2.2 Product Overview

This product is an upgrade kit that enhances security functions for a Multi-Function Device (hereafter referred to as "MFD"), an office machine consisting of multiple functions such as copy, printer, image scanning and fax. It is a firmware and provided as a ROM product. It replaces the MFD standard firmware, and offers enhanced functions designed in consideration of security, in addition to the functions equivalent to the MFD standard firmware.
Utilizing such security functions of this product, it is able to reduce the risk disclosing the actual image data spooled temporarily or filed in the MFD to unauthorized persons.

1.2.3 Scope of TOE and Overview of Operation

1.2.3.1 Usage environment of the MFD

Figure 1-1 shows the assumed usage environment of the MFD. Assume that sets of

the TOE are installed in both MFD (1) and MFD (2) in the diagram. Focusing on the TOE in MFD (1), MFD functions are explained below, where "MFD" refers to MFD (1).

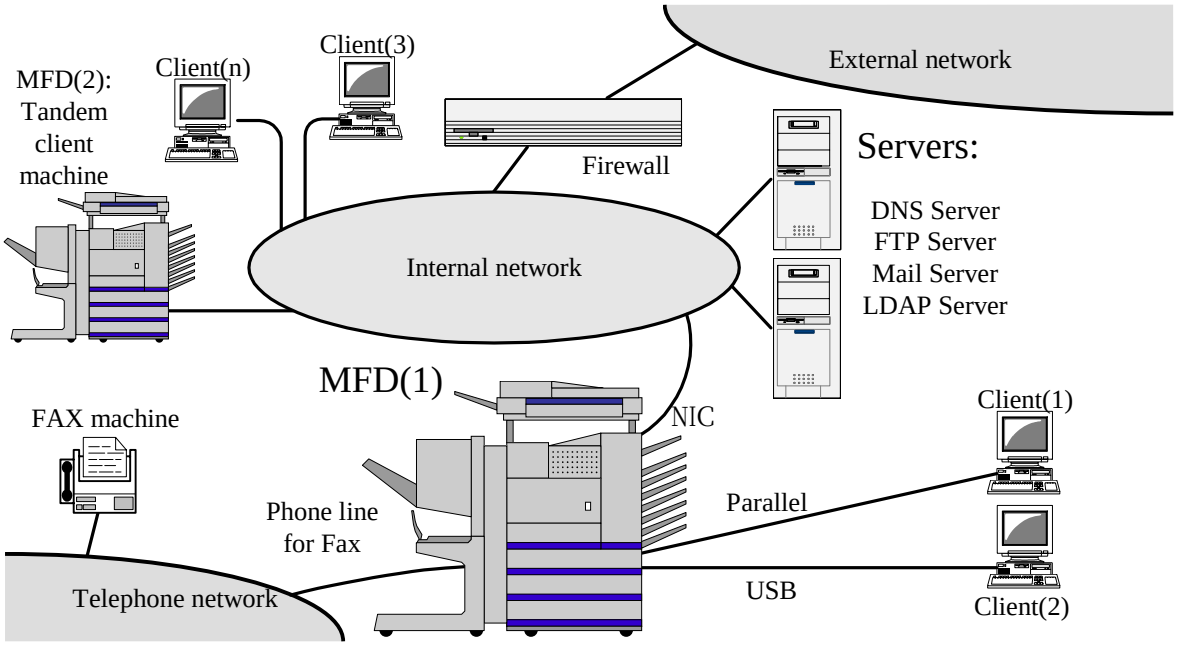

Figure 1-1: Usage environment of the MFD

In the environment shown in Figure 1-1, the TOE controls the entire MFD. Thereby the following functions are available:

(a) Copy: Prints one or more copies of the original. In tandem with MFD (2), the printing work can be shared across the network.
(b) Printer: Prints the actual image data transferred from a client via the parallel interface, USB, or the network.
(c) Direct Print: Prints the actual image data obtained using the network protocol of FTP, E-mail or Web.
(d) Network Scanning: Scans the original, and transmits the actual image data of the original to clients and/or servers via the network.
(e) Fax Transmission: Scans the original, and transmits the actual image data of the original to another fax machine via the phone line.
(f) Fax Reception: Receives actual image data from another fax machine via the phone line, and prints the actual image data.
(g) PC-FAX: Accepts actual image data transferred from a client via the parallel interface, USB, or the network. And transmits the actual image data to another fax machine via the phone line.
(h) Document Filing: Saves the actual image data of network scanning jobs, copy jobs, printer jobs and PC-FAX jobs, into the MFD. And later calls up the saved data to reuse them.
(i) Backup: Backs up the saved actual image data (by Document Filing function above) via the network into a client. And restores a backup file to the MFD.
(j) Network Management: Configures the network related settings to use the above functions via network.

1.2.3.2 TOE Configuration and Operation Overview

Figure 1-2 shows the physical configuration of the MFD. The TOE is shown as the shaded "AR-FR21" therein, and is a set of two ROM boards housing the firmware that controls the controller board of the MFD.

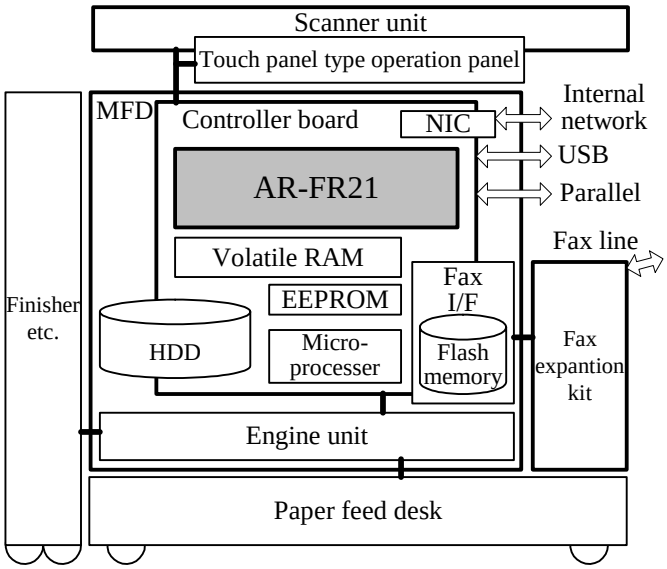

Figure 1-2: TOE and physical configuration of the MFD

The logical configuration of the TOE is shown in Figure 1-3. Each rectangle is a part of software, and each rectangle with rounded corners is a part of hardware therein. The TOE is shown as the shaded rectangle "TOE". All the TSF, the TOE Security Functions, are shown inside the shaded region. Every part of the TSF is shown as a rectangle with an identifier to which "TSF_" is prefixed.
In addition, among the user data of the TOE, the assets protected by the TOE are held in the HDD, the Flash memory and the EEPROM, each of which is outside the TOE.

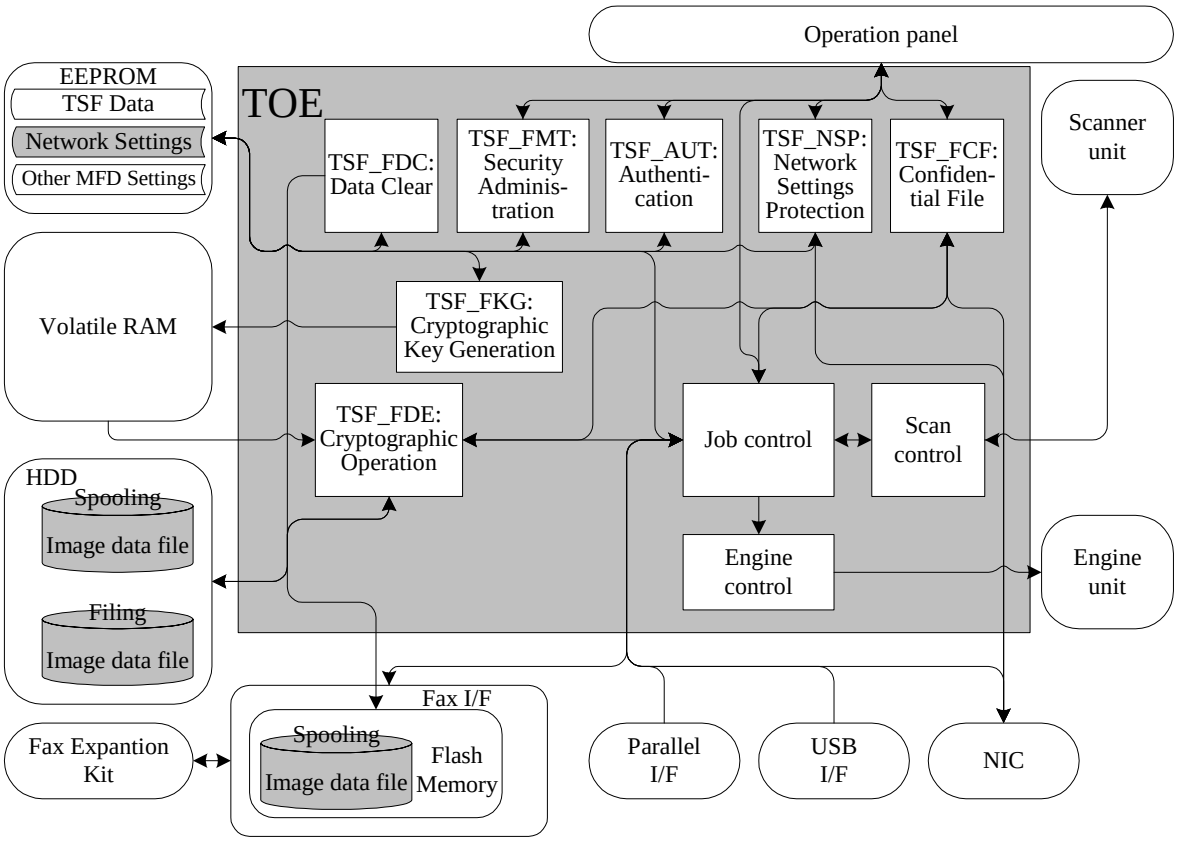

Figure 1-3: Logical configuration of the TOE

(1) During normal operations of the MFD:
The users operate the MFD either directly through the operation panel or indirectly through clients connected via parallel interface, USB or the network. With such operations by the users, actual image data are printed or sent via some of the MFD interfaces, or else, saved into or called up from the HDD for filing, as shown in the table below:

Patterns of actual image data input	Patterns of actual image data output
● Reading originals with the scanner unit ● Receiving image data through the fax interface ● Receiving image data through the parallel, USB or the NIC ● Calling up the image data saved for filing	● Printing the actual image data with the engine unit (for copy, printer, direct print or fax reception) ● Transmitting the actual image data to another fax machine (for fax transmission or PC-FAX) ● Transmitting the actual image data to clients and/or servers through the NIC (for network scanning, PC-FAX or backup) ● Saving the actual image data into the HDD (for document filing)

Here the TOE protects the actual image data, spooled temporarily in the MSD or saved in the HDD for filing, with its security functions, while the TOE offers the functions mentioned at 1.2.3.1 (a) – (i) by coordinating the functions of job control, scan control and engine control with each other.

(2) During administrative operations of the MFD:
The Key Operator administers the MFD directly through the operation panel, and the Web-Admin administers the MFD indirectly through a client connected via the network.
Here the TOE protects, with its security functions, the network settings and the TSF data (information on the security functions) against accesses of unauthorized users.

1.2.4 TOE Functionality

The details of the TOE functions are shown below:

(a) Copy:
The copy function, as well as the standard MFD firmware, is used to scan an original and print the resulting image. The major optional features are listed below:
- Tandem Copy: When two MFDs are connected to the same internal network, the MFD that scans the original (the server machine) can transfer the actual image data over the network to the other MFD (the client machine) to halve the number of copies specified by the user and share the printing work. However, the TOE does not forward the actual image data to an MFD with the standard firmware.
- Filing: This is an addition to the normal printout. The actual image data of an original can be saved in MFD. The Document Filing function prints or deletes the saved data.

(b) Printer:
The printer function, as well as the standard MFD firmware, prints print data transferred from a client, in which the printer driver for the MFD shall be installed. The print data come up via the parallel I/F, USB, or the internal network. The major optional features are listed below:
- Tandem Print: Just like the Tandem Copy function, the MFD that receives print

data plays the server machine and halves with the client machine the number of copies specified by the user.

- Hold before Print: Upon receiving a set of data, this function generates the printable actual image data from it and then saves the generated data in the MFD without printing it. It works as the *confidential print* if the data are stored with a password.
- Hold after Print: Actual image data can be printed out as usual and then saved in the MFD.
- Proof Print: This function prints out only one copy out of the designated number of prints and then retains the actual image data for the remaining number of prints, safeguarding against a large amount of misprinting.

The Document Filing function prints or deletes the data saved in the MFD.

(c) Direct Print:
The direct print function, as well as the standard MFD firmware, retrieves a file of print data from a client, an FTP server or an E-mail attachment, and prints it out, without any printer driver as opposed to the printer function. This function can be performed in either of the following ways:

- E-mail Print / Internet Fax Reception: The TOE periodically checks the mail server, receives E-mails, and prints the attached print files. E-mails sent as Internet faxes are processed in the same way.
- FTP Pull Print: Through operations on the operational panel, the TOE accesses the FTP server, retrieves a file, and then prints it out.
- FTP Push Print: This function prints print data that the clients send into the FTP server that the TOE provides.
- Web Print: This function prints print data that the clients send into the Web server that the TOE provides.

(d) Network Scanning:
The network scanning function, as well as the MFD standard firmware, scans an original to obtain image data and performs an *E-mail/FTP Transmission* or an *Internet Fax Transmission*.
Here, *FTP Transmission* (to an FTP server), *Desktop Transmission* (to a client's desktop in FTP), and *E-mail Transmission* (for a mail server) are called *E-mail/FTP Transmission* in general. To use *Desktop Transmission*, the destination client must be running the Network Scanning Tool, which is software that accompanies the MFD network scanning function.

(e) Fax Transmission:
The fax transmission function, as well as the standard MFD firmware, sends a fax to a destination fax machine that is selected on the operation panel.
The major optional features are listed below:

- Timer Transmission: The TOE holds a transmission in and starts it when the reservation time that the user has specified comes.

(f) Fax Reception:
The fax reception function, as well as the standard MFD firmware, receives a fax and prints it out.

(g) PC-FAX:
The PC-FAX (or PCFAX) function, as well as the standard MFD firmware, faxes or internet-faxes image data from a client, in which the PC-FAX driver for the MFD shall be installed. The data come up via parallel I/F, USB or the internal network.
The major optional features are listed below:

- Document Filing: Actual image data can be printed out as usual and then saved in the MFD. The data saved in the MFD may later be printed or deleted with the

Document Filing function.

(h) Document Filing:
The Document Filing function, as well as the standard MFD firmware, saves actual image data to the HDD in the MFD, and later calls them up to reuse them on the operation panel or from a client via the Web. The TOE provides *confidential mode*, a filing mode that protects the saved data by a password. A file saved in confidential mode is called a *confidential file*.
For saving data in a *confidential* file, the following four operations are available:
- *Scan Save:* Actual image data obtained by scanning is saved to the HDD without being printed or transmitted.
- Copy job (*FILE* specified): See *Copy* above.
- Printer job (*Hold before Print, Hold after Print* or *Proof Print* specified): See *Printer* above.
- PC-FAX job (*Document Filing* specified): See *PC-FAX* above.

During each saving operation above, the TOE allows the user to types in a password, and saves the password together with the actual image data into a confidential file.
For calling up a saved confidential file and using it, authentication by entry of the password is required before the operations on the file. Operations on saved files include the following:
- Print: Prints the saved file, with the settings such as number of copies to print, as well as the copy function. Tandem printing feature is also available here.
- Send: Transmits the saved file by fax, by E-mail/FTP transmission or by Internet fax.
- Preview: Displays a rough picture of the actual image data in the saved file. Available only on the Web.
- Property change: Has the saved file change from a confidential file to a file not confidential (without password), and vice versa.
- Password change.
- Delete.

(i) Backup:
The backup function, as well as the standard MFD firmware, creates a backup file in the client of a file stored in the HDD using the Document Filing function, and restores a backup file to the HDD. The former operation is called *exporting* or *backing up* the file. And the latter operation is called *importing* or *restoring* the file. These operations are instructed by the user on the clients.
A file is exported in the following sequence:
- A user accesses the TOE Web from a client and operates as needed for the options, such as selecting a file in the HDD, and specifying the password.
- The TOE confirms that the given password is correct for the selected confidential file, and then, sends the file, in its encrypted form as it has been, to the Web browser on the client.
- The Web browser on the client downloads the file and saves it.

A file is imported in the following sequence:
- A user accesses the TOE Web from a client and operates as needed for the options, such as selecting a file on the client.
- The Web browser on the client uploads the selected file onto the TOE.
- The TOE receives the file, encrypts if not yet done, and saves it.

(j) Network Management:
The network management function, as well as the standard MFD firmware, allows configuring the IP address to be allocated for the MFD, the IP address of the DNS servers that the MFD is to refer, and other network related settings. These configurations are required for utilizing MFD networking functionalities.
Some features of this function are provided via the operation panel. They are on a UI

named *Network Settings* under the Key Operator Programs UI, and include minimum settings such as IP address setting. In addition, the *Tandem Setting* is allowed only in this Network Settings UI.
The TOE provides its Web for remote operation, when set to enable TCP/IP. Some of the pages in this Web are protected by an administrative password. In the ST, the user authenticated with this administrative password is named *Web-Admin,* and the protected pages are generally named *Web-Admin Pages.*
Most features of this network management function are provided via this Web for the Web-Admin, and allow the configurations such as the settings for the MFD to refer the DNS, WINS, SMTP and LDAP servers. In the ST, the pages that contain forms for these settings and the submission target pages of the forms are generally named *Network Management Pages.* All Network Management Pages are Web-Admin Pages.

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 Multifunction Device Data Security Kit AR-FR21 Security Target" (in both English and Japanese, hereinafter referred to as "the ST")[1] as the basis design of security functions for the TOE, 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 "AR-FR21 VERSION M.10 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 problems found in the certification process. Evaluation is completed with the Evaluation Technical Report

dated August 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 conformance.

1.5.3 SOF

This ST claims "SOF-basic" as its minimum strength of function.
The internal network, in which the TOE is installed, is protected against IT security threats from any external networks. Under such an environment, limited attack should be assumed: with direct accesses to the MFD including the TOE, or within the internal network. It is not assumed to be exposed to extensive external attacks via the internet.
Therefore it is rational for the TOE to assume the attackers with low attack potential, and SOF-basic is rational to be claimed on the minimum strength of function.

1.5.4 Security Functions

Security functions of the TOE are as follow.

(1) Cryptographic operation function (TSF_FDE):
Encrypts actual image data that is being spooled or saved by the filing function and stores it in the MSD (HDD or Flash memory) by intervening with the device driver function controlling the MSDs (HDD and Flash memory) in the MFD. This function also decrypts data that was stored in the MSD by spooling or the filing function.

(2) Cryptographic key generation function (TSF_FKG):
Generates the cryptographic key for encryption and decryption by the cryptographic operation function (previous paragraph). The generated key is stored in volatile RAM.

(3) Data clear function (TSF_FDC):
When a job is completed and the image data, spooled in the HDD or the Flash memory in order to process the job, is deleted and when a user deletes an image data that the user saved in the HDD by the after-mentioned confidential file function, this function clears the actual image data area by overwriting random values or fixed values to that area *(Auto Clear at Job End).*
In addition, for uncompleted job image data and undeleted image data that a user saved, this function clears the actual image data area by overwriting random values or fixed values to that area *(Clear All Memory, Clear Document Filing Data and Power up Auto Clear).*
The following four data clear programs are provided:

- Auto Clear at Job End (for HDD and Flash memory): Clears the actual image data area used by a job after it is completed. It also clears the after-mentioned confidential file, saved by the confidential file function, when the user deletes the file.
- Clear All Memory (for HDD and Flash memory): Clears all actual image data that remain, when invoked by the operation of the administrator, the Key Operator. The administrator shall run this program when disposing of the TOE and/or the MFD or transferring ownership to another party.
- Clear Document Filing Data (for HDD): Clears the actual image data that remain in the HDD, when invoked by the operation of the administrator, the Key Operator. This program aims at batch-clearing the data saved by the users. However, this program can also clear the image data of the jobs spooled to HDD.
  The two programs, Clear All Memory and Clear Document Filing Data, are generically called *Data Clear Operations*.
- Power up Auto Clear (for HDD and Flash memory): Clears the actual image data area when the TOE is powered on, unless the TOE has any reserved transmission jobs or any Fax/Internet fax reception jobs not yet printed out. The Key Operator may enable/disable this function (whether or not executing this program at the time of power-on) and customize data area to be cleared by this program

(4) Authentication function (TSF_AUT):
Authenticates a Key Operator by means of the Key Operator Code, i.e. a password.

(5) Security administration function (TSF_FMT):
Provides following administrative functions that are essential for operating of the TOE:

- Set the number of times Auto Clear at Job End program is repeated
- Set the number of times data clear operations are repeated
- Set the data areas to be cleared by Power up Auto Clear program
- Set the number of times Power up Auto Clear program is repeated
- Change the Key Operator Code
- Release the lock of confidential files
- Reset the NIC (reset MFD network related settings, including Web-Admin password)

(6) Network settings protection function (TSF_NSP):
Protects network-related settings of MFD not to be tampered by users other than the MFD administrator.

(7) Confidential file function (TSF_FCF):
Provides password protection when a user stores image data in the MFD using the Document Filing function. The image data that is stored as a password protected file using this function is called a *confidential file*. The user establishes a password when storing the data, and the TOE then requires authentication by means of that password to reuse (print or transmit) the data.
If incorrect passwords for a confidential file are entered three times in a row, this function refuses further authentication attempts. This is called *locking*.
This function can be used for *confidential printing* of printer jobs.

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	An attacker physically removes the MSD from MFD to read the MSD and recover the actual image data stored in it.
T.SHUNT	An attacker tampers with the network-related settings of the MFD to make the MFD send the actual image data to the equipments that the attacker uses as means to attack, when a user operates the MFD to send the actual image data.
T.SPOOF	An attacker impersonates a user to print or transmit actual image data that the user has stored in the MSD.

1.5.6 Organisational Security Policy

No organizational security policies to comply with are required of the TOE utilized in organizations.

1.5.7 Configuration Requirements

The TOE runs when installed in place of the standard ROM of a Sharp MFD, the model name of which is one of the followings:
AR-311N, AR-351N, AR-451N, AR-M351N, AR-M355N, AR-M355NJ, AR-M451N, AR-M455N, AR-M455NJ, AR-M351U, AR-M355U, AR-M355UJ, AR-M451U, AR-M455U and AR-M455UJ.

1.5.8 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 1-2.
The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

Table 1-2 Assumptions in Use of the TOE

Identifier	Assumptions
A.NETWORK	The MFD, in which the TOE is installed, is connected to an internal network kept secure so as not to be wiretapped, and is protected against being accessed arbitrarily from any external networks.
A.OPERATOR	The Key Operator and the Web-Admin are trustworthy persons who will not take improper action with respect to the MFD and the TOE.
A.USER	Every user, who may be an administrator of the TOE and/or the MFD, handles the password in the following ways: ・ Every password shall be set up not easy to guess. ・ Every password shall be updated on regular basis. ・ Every password shall be maintained in safety.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

(1) Japanese version:
- AR-FR21 Data Security Kit Operation Manual
  version 0.02, CINSJ3103FC51
- AR-FR21 Data Security Kit Notice
  version 0.03, TCADZ6051FCZZ
- AR-FR21 Web Help (General), TOE built-in
- AR-FR21 Web Help (Document Filing), TOE built-in
- AR-FR21 Installation Manual
  version 0.02, TCADZ6047FCZZ

(2) English version:
- AR-FR21 Data Security Kit Operation Manual
  version 0.02, CINSZ3104FC51
- AR-FR21 Data Security Kit Notice
  version 0.03, TCADZ6052FCZZ
- AR-FR21 Web Help (General), TOE built-in
- AR-FR21 Web Help (Document Filing), TOE built-in
- AR-FR21 Installation Manual *
  version 0.02, TCADZ6048FCZZ

* German, French and Spanish versions are attached.

Following documents, attached to the MFD, shall also be read for use of the TOE:

(1) Japanese version:
- Digital Laser Copier/Printer Digital Multifunctional System
  Key Operator's Guide
  version 1 (TINSJ2818FCZZ)
- MODEL
  AR-311N
  AR-351N
  AR-451N
  Digital Laser Copier/Printer Digital Multifunctional System
  Operation Manual (for general information and copier operation)
  version 2 (TINSJ2796FCZZ)
- Digital Laser Copier/Printer Digital Multifunctional System
  Operation Manual (for printer)
  version 1 (AR311N-JP-PRINTER)
- Digital Laser Copier/Printer Digital Multifunctional System
  Operation Manual (for scanner)
  version 1 (AR351N-JP1-SCANNER)
- Digital Laser Copier/Printer Digital Multifunctional System
  Operation Manual (for facsimile)
  version 1 (TINSJ2785FCZZ)

(2) English version:
- Laser Printer Key Operator's Guide
  version 1 (TINSE2820FCZZ)
- MODEL
  AR-M351N
  AR-M451N
  Laser Printer Operation Manual (for general information and copier operation)

version 1 (TINSE2797FCZZ)
- Laser Printer Operation Manual (for printer)
version 1 (ARM451N-EX-PRINTER)
- Laser Printer Operation Manual (for network scanner)
version 1 (ARM351N-EX1-SCANNER)
- AR-FX12 Facsimile Expansion Kit Operation Manual
version 1 (TINSE2791FCZZ)

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 August, 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 June, 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 June, 2005.

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 test configuration performed by the developer is shown in the Figure 2-1.
In the Figure 2-1, *the (122) decode.exe* indicates a decryption software tool for testing. And *the (12) HDD* that connects to *the (110) PC as debug terminal* indicates that *the (12) HDD* built into *the (10) MFD* is taken out and is connected to the PC.

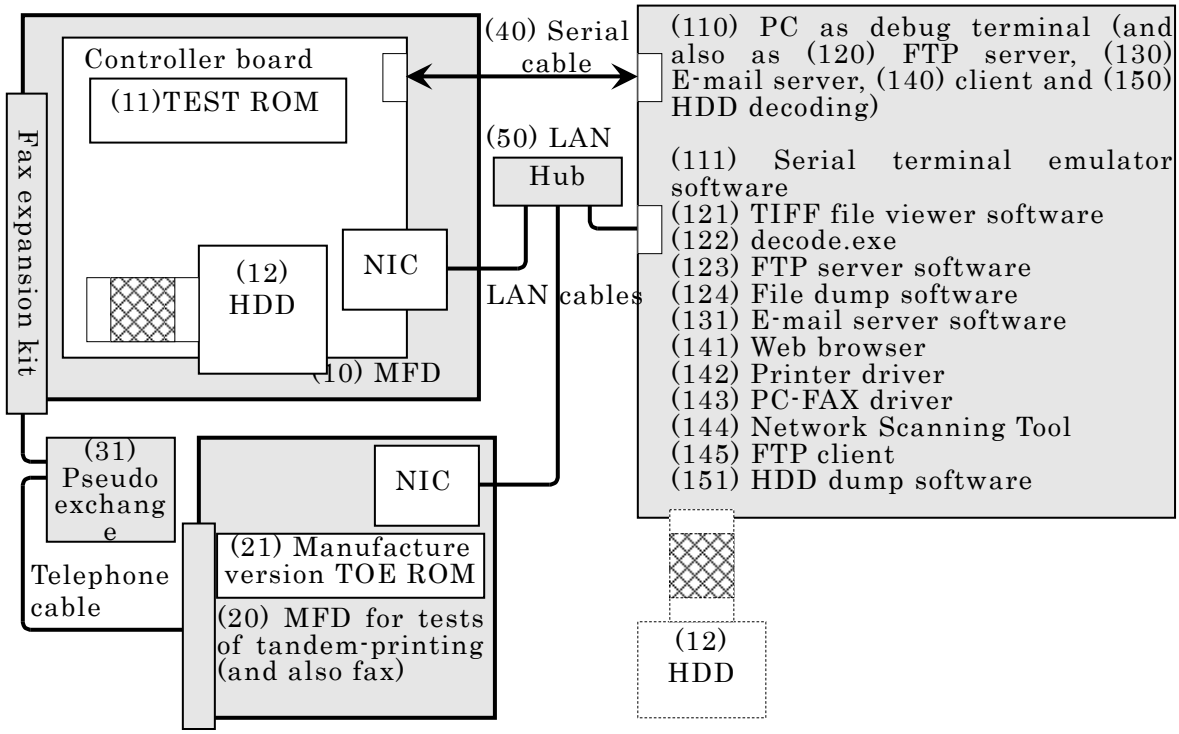

Figure 2-1: Configuration of Developer Testing

2) Outlining of Developer Testing

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

a. Test configuration

The test configuration performed 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. *The (11) TEST ROM* is similar but not identical to the TOE identified in the ST. However it is considered equivalent to the TOE because it is made of adding just debugging-functions (for testing) to the manufacture version of the TOE. Further, the testing configuration includes software tools for testing that the TOE configuration of the ST does not identify, however they do not affect behaviour of the security functions.

b. Testing Approach

The tests have been performed using the following methods:

1. Stimulate the external interfaces of the security functions by manually operating the MFD (through the operation panel, power supply etc.), and observe the output (on the operation panel, to the debug terminal and into log-files) that shows behaviour of the security functions.
2. Stimulate the external interfaces of the security functions by operating the TOE Web, and observe the output (on the operation panel, to the debug terminal, into log-files and through the TOE Web) that shows behaviour of the security functions.
3. Stimulate the external interfaces of the security functions by having the MFD scan/receive or print/transmit actual image data, and observe the output (on the operation panel, to the debug terminal, into log-files and as

dump lists of the HDD taken out from the MFD) that shows behaviour of the security functions.

c. Scope of Testing Performed

The developer performed 48 tests.
The coverage analysis is conducted and examined to testing satisfactorily all of the security functions and the external interface described in the functional specification. Then, the depth analysis is conducted and examined to testing satisfactorily all the subsystems and the subsystem interfaces described in the high-level design.

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 tests performed, and confirmed consistencies between the actual testing approach resulting in the actual test results and the test approach described in the test plan.

2.3.2 Evaluator Testing

1) Evaluator Test Environment

The test configurations for the independent testing and the penetration testing by the evaluator are shown in the Figure 2-2 and in the Figure 2-3 respectively. In the Figure 2-2, *the (122) decode.exe* indicates a decryption software tool for testing. And *the (12) HDD* that connects to *the (110) PC as debug terminal* indicates that *the (12) HDD* built into *the (10) MFD* is taken out and is connected to the PC.

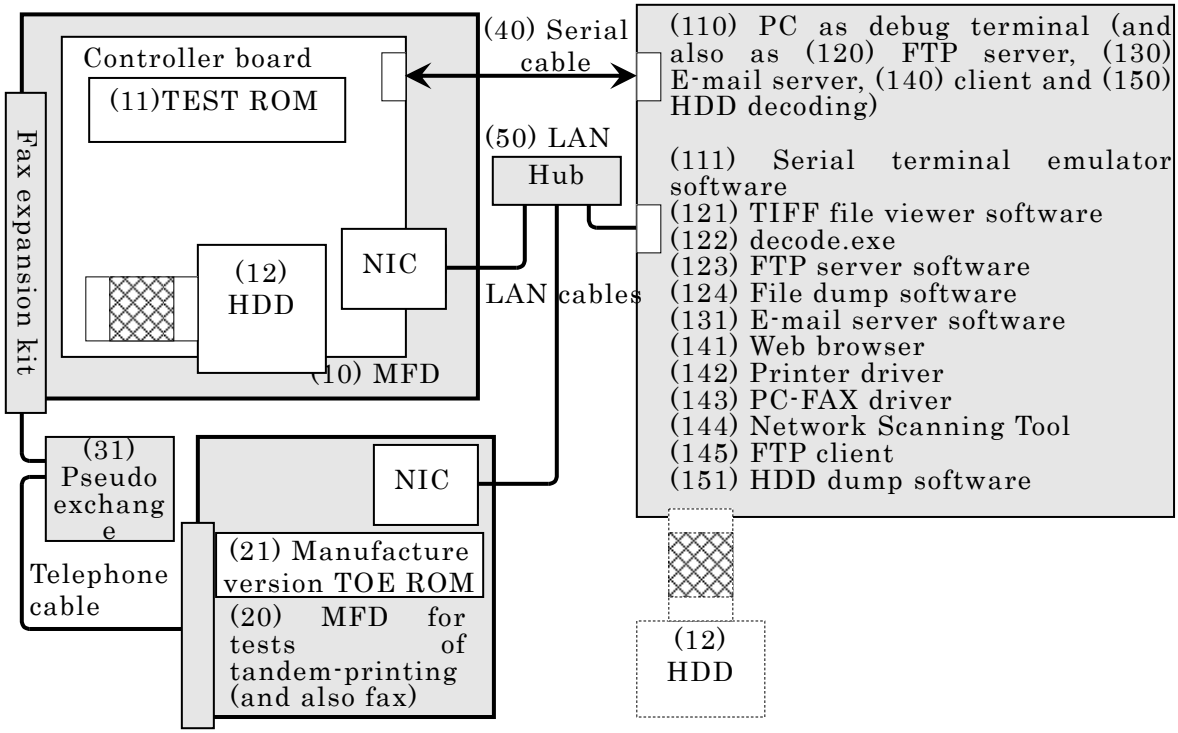

Figure 2-2: Configuration of Evaluator Independent Testing

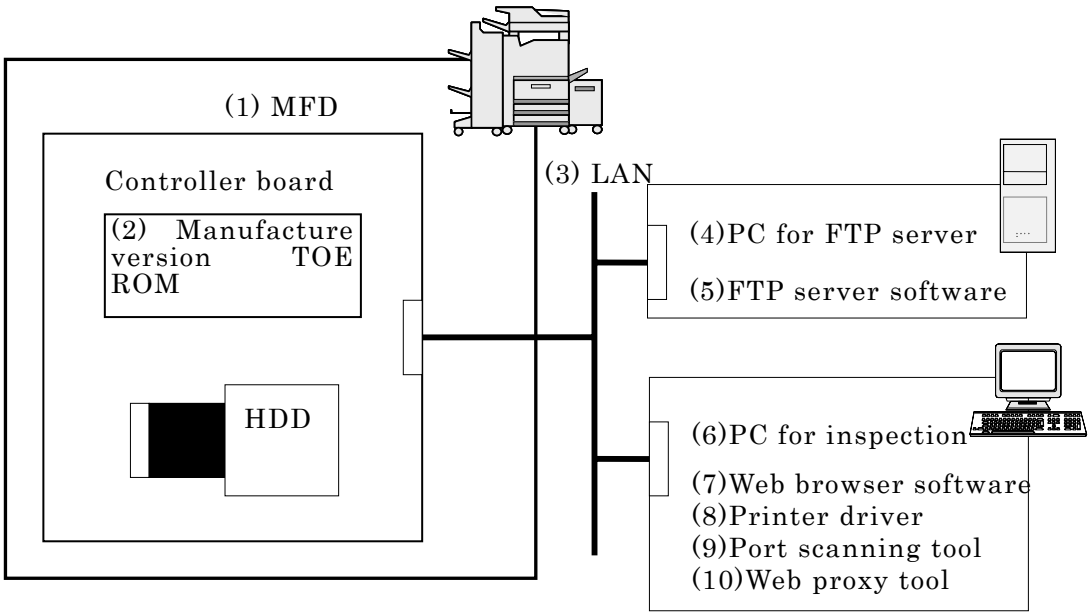

Figure 2-3: Configuration of Evaluator Penetration Testing

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

The test configuration for the independent testing performed by the evaluator, shown in the Figure 2-2, is equivalent to the developer testing. The configuration for the penetration testing is shown in the Figure 2-3. The independent testing and the penetration testing have been performed in the TOE testing environment equivalent to the TOE configuration identified in the ST. Further, the testing configuration includes tools for testing that the TOE configuration of the ST does not identify, however they do not affect behaviour of the security functions.

b. Testing Approach

The tests have been performed using the following methods:

1. Stimulate the external interfaces of the security functions by manually operating the MFD (through the operation panel, power supply etc.), and observe the output (on the operation panel, to the debug terminal and into log-files) that shows behaviour of the security functions.
2. Stimulate the external interfaces of the security functions by operating the TOE Web, and observe the output (on the operation panel, to the debug terminal, into log-files and through the TOE Web) that shows behaviour of the security functions.
3. Stimulate the external interfaces of the security functions by having the MFD scan/receive or print/transmit actual image data, and observe the output (on the operation panel, to the debug terminal and into log-files) that shows behaviour of the security functions.
4. Execute a port scan to the NIC of the MFD, and observe how it responds.

c. Scope of Testing Performed

The evaluator performed 44 tests altogether. Among them, 22 tests were designed originally as the independent testing, 14 were sampled from the developer testing and the last 8 made the penetration testing.
Each type of the evaluator testing is designed in following consideration.

[The Originally-designed Independent Testing]

(1) Shall cover all of the security functions,
(2) Shall cover all of the logical TSFI,
(3) Shall cover both user and administrator UI on the operation panel, and
(4) Shall make a different choice from the developer testing among the combinations of job type, with/without filing option and MSD type (i.e. Flash memory or HDD), for the tests of the cryptographic operation function and the data clear function.

[The Sampling Tests from the Developer Testing]

(1) Shall achieve at least 20% of the number of the tests of the developer testing,
(2) Shall cover all of the security functions,
(3) Shall cover, as regards the MSD tested, both the spool areas (of HDD and Flash memory) and the filing area, and
(4) Shall cover every class of the developer testing except “Testing by Taking HDD Out”.

[The Penetration Testing]

(1) Shall examine vulnerabilities of authenticated sessions made during accesses to the TOE Web, and
(2) Shall include on-the-spot activities to verify the rationales that public domain vulnerabilities are not exploited.

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 reviews, 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 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

The glossaries used in this report are listed below.

Actual image data:	The part of an image data file that does not include the management area.
Board:	A printed circuit board on which components are mounted by soldering.
Clear All Memory:	An operation that clears (by overwriting) all actual image data stored in all MSDs in an MFD.
Controller board:	Controls the entire MFD and is equipped with the microprocessor executing the firmware within the TOE, the volatile RAM, and the EEPROM retaining settings.
EEPROM:	Electrically Erasable Programmable ROM, a type of non-volatile memory that allows electrical rewriting to any part of memory.
Engine:	A device that prints an image on paper, including the paper feeding and paper output mechanisms. Prints out the actual image data, controlling other parts such as paper tray or finisher and is used for copy, printer, direct print, fax reception, and re-operational printout. Also called a print engine or an engine unit.
External network:	A network other than an internal network of an organization, which is not managed by the organization.
Fax expansion kit and Fax I/F:	Provide fax transmission/reception functions, equipped with the flash memory retaining the actual image data necessary for the fax transmission/reception job processing.
Filing:	A function that stores image data handled by the MFD into the HDD, for users' later operations, such as a printing or a transmission. Also called *Document Filing*.
Finisher etc.:	Optional parts available for finishing purposes such as stapling printed pages and punching holes.
Flash Memory:	A type of non-volatile memory that allows the entire memory to be erased at once and also allows rewriting to any part of memory.

HDD:	An acronym of Hard Disk Drive. Retains the actual image data necessary for job processing other than fax transmission/reception. A user can also use the Document Filing function to retain the actual image data.
I/F:	Interface
Image data:	The digital data that results from scanning an original on the MFD for a copy, print, scan, or fax transmission job. In the case of fax reception, the data received via the telephone line, or the received fax data after it has been decompressed. These types of data are also called image data when they have been compressed.
Internal network:	A network that is protected from security threats from an external network. The intranet of an organization is an "internal network".
Job:	The sequence from beginning to end of the use of an MFD function (copy, printer, direct print, network scanning, PC fax transmission, fax transmission, or fax reception). In addition, the instruction for a functional operation is sometimes called a job.
Key Operator:	A user that is authorized to access the TOE security management functions and the MFD management functions. The administrator of the MFD and the TOE.
Key Operator Code:	A password used for authentication of the Key Operator.
Key Operator Programs:	Security administrative functions of the TOE, as well as MFD administrative functions. To access the Key Operator Programs, authentication as the Key Operator is required.
LCD:	Liquid Crystal Display
Memory:	A memory device; in particular a semiconductor memory device.
MSD:	An acronym of Mass Storage Device. For the TOE, an MSD is an HDD or Flash memory.
Network settings:	A part of MFD network related setting data of which the ST claims to be a part of assets protected by the TOE.
NIC:	An acronym of Network Interface Card, or, Network Interface Controller. An Ethernet I/F for internal network connections. Some MFD models may have it as standard, and some as option.
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.
Paper tray:	Stores pages of paper for printout, sending them to the engine unit.
RAM:	Random Access Memory
ROM:	Read Only Memory
Scanner unit:	Scans an original to obtain the actual image data. Used for copy, scan transmission, fax transmission, and scan to HDD.
Touch panel type operation panel:	Has the LCD equipped with button keys and a touch panel. Provides user interfaces.
UI:	User Interface

Unit:	A module provided standard that can be attached to or detached from a printed circuit board; or an option that is installed and is ready for operation. Or a system that includes a mechanism and is ready for operation.
Web-Admin:	A user that is authenticated, as an administrator of the MFD, with an administrative password, on the Web that the TOE provides for remote operation, where Admin is an abbreviation of Administrator.

6. Bibliography

[1] Digital Multifunction Device Data Security Kit AR-FR21 Security Target – Version 0.04, 28 June 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] AR-FR21 VERSION M.10 Evaluation Technical Report Version 003, 2 August 2005, Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security