Certification Report

Target of Evaluation

Application date/ID	January 5, 2004 (ITC-4021)
Certification No.	C011
Sponsor	Konica Minolta Business Technologies, Inc.
Name of TOE	Japan: Di3510 series/Di3510f series Multi Function Peripheral Security Kit Overseas: Di3510 series/Di3510f series Multi Function Peripheral Security Kit
Version of TOE	User Interface : 4030-20G0-05-00 Network Module : 4030-A0G0-03-00
PP Conformance	None
Conformed Claim	EAL3
TOE Developer	Konica Minolta Business Technologies, Inc.
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.
July 21, 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

"Japan: Di3510 series/Di3510f series Multi Function Peripheral Security Kit, Overseas: Di3510 series/Di3510f series Multi Function Peripheral Security Kit" 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: Di3510 series/Di3510f series Multi Function Peripheral Security Kit, Overseas: Di3510 series/Di3510f series Multi Function Peripheral Security Kit” (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, Konica Minolta Business Technologies, Inc.

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: Di3510 series/Di3510f series Multi Function Peripheral Security Kit
Overseas: Di3510 series/Di3510f series Multi Function Peripheral Security Kit
Version: User Interface : 4030-20G0-05-00
Network Module: 4030-A0G0-03-00
Developer: Konica Minolta Business Technologies, Inc.

1.2.2 Product Overview

The Multi Function Peripheral (MFP) is an office IT device that is comprised by selecting and combining the functions of copying, printing, scanning and faxing. The present product (Japanese name: Di3510 series/Di3510f series Multi Function Peripheral Security Kit, English name: Di3510 series/Di3510f series Multi Function Peripheral Security Kit are identical products although the name is different) is comprised of the “User Interface,” which is a software component that carries out operational control processes from the operations panel of the MFP body, and the “Network Module,” which is a software component that carries out operational control processes from the client PC, from among the built-in control software in the Di3510 Series/Di3510f Series MFP for monochrome printing, which is provided by Konica Minolta Business Technologies, Inc. The security functions of this product provide a protective function for the exposure of document data with high confidentiality that is spooled in the MFP during the use of a specific function of the Di3510 Series/Di3510f Series MFP. The specific function is a secure print (Lock Job) function in which a password is set and sent to the MFP by a client PC, and when the password is entered from the operations panel of the MFP body and is matched, then the print data that was sent to the MFP and which is in a print pending condition will be printed, and the user box function controls the access to the user box that is set as the storage area for the scanned data.

The expected general environment for usage is shown in Figure 1-1

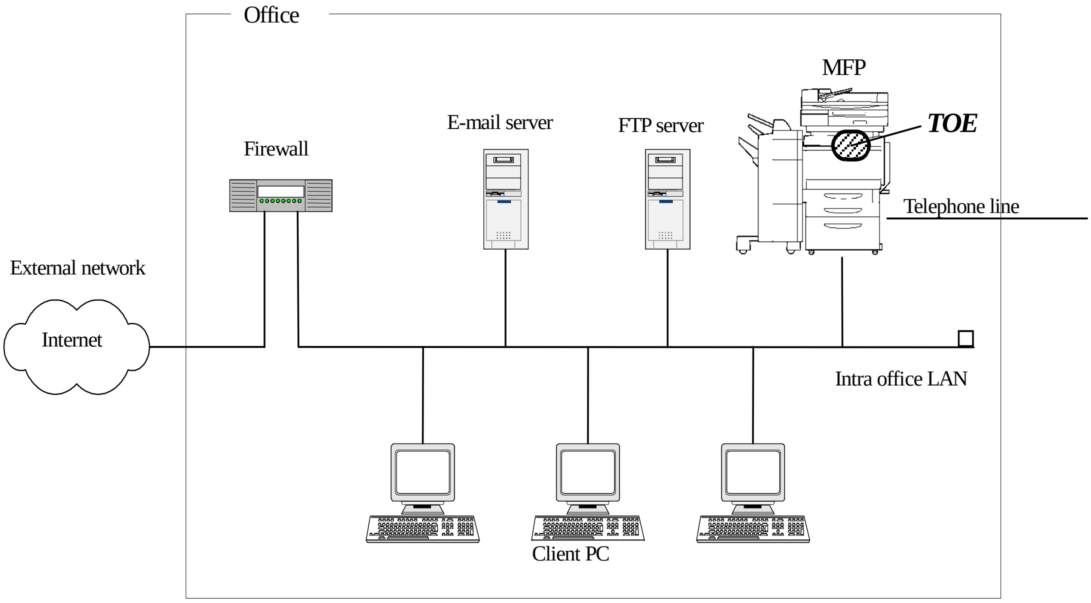

Figure 1-1 An example of the expected environment for usage of the MFP

As described in the above-mentioned figure, the MFP is installed in a general office. The MFP connects to the client PCs via the intra-office LAN, and has mutual data communication. When an e-mail server and FTP server are connected to the intra-office LAN, the MFP can carry out data communication by using these. The MFP is connected to the telephone line for fax transmission/reception and in order to communicate with the support center that carries out the maintenance and management of the MFP.

1.2.3 Scope of TOE and Overview of Operation

The “User Interface” and the “Network Module” that are the TOE operate on the OS (VxWorks) that runs on the MFP controller in the MFP body as object code that is integrated with other MFP control software components. Figure 1-2 shows the structure of these MFP control software components. The physical area of the TOE is indicated in the dark color in the figure.
The outline of the operation carried out by the TOE is described as follows.

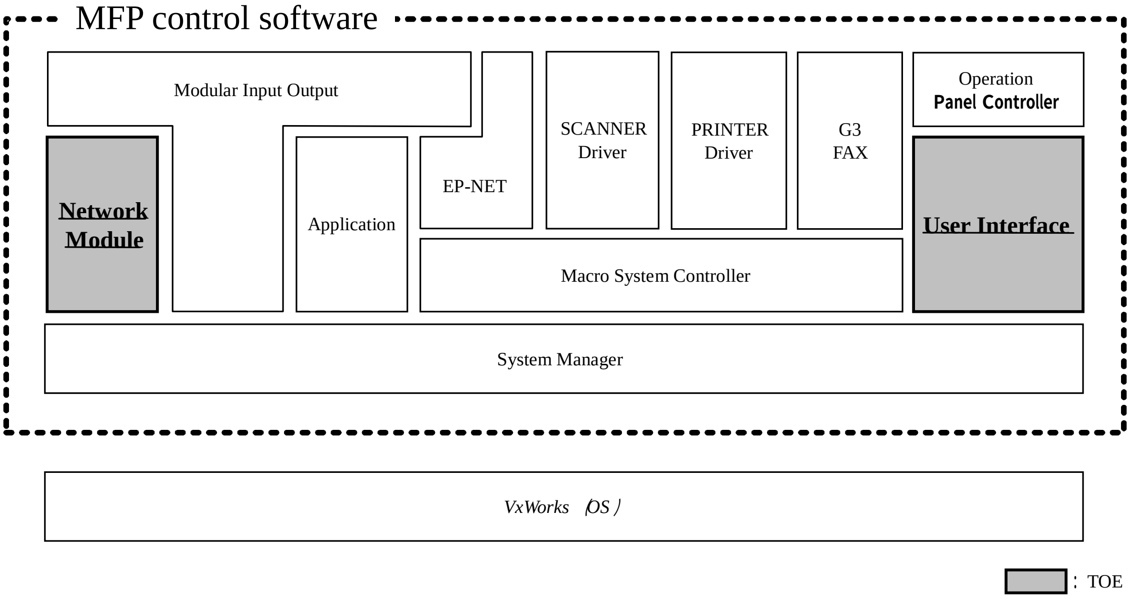

Figure 1-2 Structure of the MFP control software component

- User Interface (commonly known as the UI)

  It processes the information entered from the “Operations Panel Controller” and passes notification to the “System Manager,” the “Macro System Controller,” or the “Network Module” depending on the process. In addition, it processes messages from the “System Manager,” the “Network Module,” and the “Macro System Controller” and passes notification to the “Operations Panel Controller.”

- Network Module (Commonly known as the NM)

  By responding to operation requests from the client PC, it receives the data that the “Modular Input Output” received from the network with a designated protocol (HTTP, IPP, MIB), and processes and controls the data. Depending on the process, it requests processing to “VxWorks,” the “System Manger,” the “Macro System Controller,” or the “User Interface,” and receives the data that is processed by “VxWorks,” the “System Manger,” the “Macro System Controller,” or the “User Interface,” and then requests processing to the “Modular Input Output.”

1.2.4 TOE Functionality

General users and the administrator use a variety of functions of the MFP with the built-in TOE from the client PC and the operations panel of the MFP body. A service engineer can use the functions for service engineers from the operations panel of the MFP body. General User Functions that a general user and administrator operate, a variety of functions in the administrator mode that can be operated only by administrators (Administrator Functions (Panel), Administrator Functions (PC)) and a variety of functions for service engineers (Service Engineer Functions) are described as follows. General user means persons who uses the MFP, and who are allowed to enter the office where the MFP is installed.

1.2.4.1 General user functions

General users can use the copying function, the printing function, the scanning function and the faxing function, which are the main functions of the MFP. The TOE takes a partial role in the controlling processes of these main functions. The processes run by the TOE for each function are described as follows.

(1) Copying function

During this copying function, the reception of the execution, the displaying of an indication of the progress of the process, and the reception of the cancellation process are carried out.

(2) Print function

The print function includes normal printing, reprinting, secure printing, and HDD storage printing. From the above-mentioned multiple print functions, the TOE carries out a display process that shows that the print data is being received, a display process that shows the printing is in progress, and a cancellation process for the print function that is being executed while it is on the display. The secure print receives a password entry and a verification process during the print pending status stage.

- Secure print (Lock Job)

  When a document with high confidentiality is printed, “Lock Job” is selected from the printer driver of the client PC, the password is set and the print data is sent to the MFP. A job ID is given to the print data received by the MFP and registered as secure print job information data. The TOE verifies the password entered from the operations panel of the MFP body with the password of the secure print job information data and when they match, cancellation of print pending for the secure print job identified by the job ID is carried out.

(3) Scanning function

The scanning carries out the reception of execution, displays an indication of what is currently being executed and receives the cancellation of scanning.

(4) Faxing function

The fax function receives an execution for the fax transmission, displays an indication for the transmission process, and executes the cancellation process for the fax transmission.

(5) Internet fax function

During e-mail transmission with an attached file with a standard image compression format as an Internet fax (e-mail with a standard attached image format) which contains image data loaded to the MFP by the scanning function, it receives the transmission execution, displays an indication of the transmission process and executes a cancellation process for the transmission.

(6) User box function

Using the web browser of the client PC, it creates a user box where the scanned image data will be stored (new setting for the name, and password) and provides the following operations for the user box where the image data (hereinafter referred to as the user box data) is stored using the web browser of the client PC.

- Downloading the user box data to the client PC
- Deletion of user box data
- Deletion of user box
- Modifications to the settings for the user box (name change, password change)

1.2.4.2 Administrator functions

The TOE provides management functions (administrator functions) that supervise the general user functions with an administrator mode that is available only for the administrator. The following are descriptions for two categories: the administrator functions (panel) that can be executed from the operations panel of the MFP body, and the administrator functions (PC) that can be executed from a client PC.

(1) Administrator functions (panel)

- Function to change the administrator mode password
- Function for setting the operational status of the access check function
- Penalty reset function (A function that clears the unauthorized access detection count value for secure printing and a user box to zero.)
- A variety of setting functions for the administrator (bulk deletion of secure print jobs, automatic cancellation settings for user box data, a variety of settings for a network, settings for limiting the number of copies, settings for date and time, etc.)

(2) Administrator functions (PC)

- Deletion of user box data
- Deletion of user box
- Change in settings for a user box (name change, password change)
- A variety of setting functions for the administrator (setting of the storage period for user box data, a variety of settings for a network, settings for limiting the number of copies, settings for date and time, etc.)

1.2.4.3 Service engineer functions

The TOE provides management functions (service engineer functions) for general user functions and administrator functions in service mode, maintenance mode and initialization mode that can only be operated by a service engineer from the operations panel of the MFP body. The present functions are described as follows.

(1) Service mode

- ROM version display function
- Initialization function for administrator mode password
- Function to change the service code (service engineer password)
- A variety of setting functions for service engineers (operation setting function for each setting function provided for general users, settings for the counter for the number of pages to be printed, operational checks for each function, a sensor check, settings for an HDD installation, the HDD format, etc.)

(2) Maintenance mode

- A variety of setting functions for a service engineer (display adjustment for the operations panel of the MFP body, etc.)

(3) Initialization mode

- A variety of setting functions for the service engineer (language setting, etc.)

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 “Di3510 Series/Di3510f Series Multi Function Peripheral Security Kit Security Target Version 1.18” 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 “Di3510 Series/Di3510f Series Multi Function Peripheral Security Kit 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 June, 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 EAL3 conformance.

1.5.3 SOF

This ST claims “SOF-basic” as its minimum strength of function.
It is assumed that the present TOE is operated under conditions where adequate physical and personnel security conditions are secured. Therefore, the threat agent can be specified as low level personnel. Therefore, the “SOF-basic,” which is a level that can counteract against a low-level attack potential can fulfill the condition.

1.5.4 Security Functions

Security functions of the TOE are as follow.

(1) Security functions for the general user function

- Identification and authentication that allows access by a general user to a secure print job

  A function that identifies and authenticates that a general user is a valid user for secure print job information data when the secure print job information data is printed. After failing three times at authentication it locks the authentication function for the concerned secure print job information data and access is denied.

- Function to create a user box

  A function by which a general user specifies a name and creates a user box.

- Identification and authentication that allows access to a user box by a general user and an access control function

  A function that identifies and authenticates that a general user is an authenticated user of a user box when accessing the user box. After failing three times, it locks the authentication function for the concerned user box and access is denied.

  When authentication is successful, the downloading of all the user box data in the user box is permitted. (The user box named as “Public” is not subject to the present security function.)

- User box control function for general users whose access is authenticated

  A function by which a general user, who is a valid user of the user box, can change the settings (name, password) of the user box.

(2) Security functions for the administrator function

- <u>Identification and authentication function that allows access to the administrator mode</u>

  A function that identifies and authenticates the administrator when accessing the administrator mode using the operations panel of the MFP body or using a web browser on the client PC. Failing three times locks the authentication function and access is denied.

- <u>Security-related functions for administrator mode</u>

  The following functions allowing operation from the operations panel of the MFP body in administrator mode.

  • Function to change the administrator mode password

  • Function for setting the operation status of the access check function

  • Penalty reset function

  The following functions, which can be operated from the client PC in administrator mode.

  • Functions to change the setting of the user box (name change, password change)

(3) Security functions for the service engineer function

- <u>Identification and authentication function that allows access to the service mode</u>

  A function that identifies and authenticates the service engineer when accessing the service mode. Failing three times locks the authentication function and access is denied.

- <u>Security-related functions for service engineer mode</u>

  The following functions allowing operation in service mode

  • Initialization function for the administrator mode password.

  • Function to change the service code.

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.ACCESS-SECURE-PRINT	Unauthorized operation of the secure print job data: Unauthorized exposure of secure print job information data when a malicious general user accesses the secure print job information data

	from the operations panel of the MFP body and prints the secure print job information data by pretending to be an authorized user.
T.ACCESS-USER-BOX	Unauthorized operation of the user box data: Unauthorized exposure of user box data when a malicious general user accesses the created user box from the client PC and downloads the user box data of a user box by pretending to be an authorized user.

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.BEHAVIOR-ACCESS-CHECK	Operation setting function for the access check function: The access check function can be terminated to maintain compatibility with the existing model for operation purposes under a secure environment.

1.5.7 Configuration Requirements

The present TOE is a software product loaded to the Di3510 series/Di3510f series MFP for monochrome printing, which is provided by Konica Minolta Business Technologies, Inc.

"Di3510 series" indicates the Multi Function Peripheral (MFP) identified by Di1810, Di2010, Di2510, Di3010 and Di3510. In addition, "Di3510f series" indicates the Multi Function Peripheral (MFP) identified by Di1810f, Di2010f, Di2510f, Di3010f and Di3510f. The fax function is an optional product for the "Di3510 Series," whereas the "Di3510f Series" is the MFPs that have a built-in fax function.

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.ACCESS-CHECK	Operation setting conditions for the access check function: The user of the MFP uses the MFP under the condition of a setting in which the access check function always runs.
A.ADMIN	Personnel conditions to be an administrator: The administrator, in the role given to them, shall not carry out a malicious act during the series of

	permitted operations given to them.
A.AUTH	Operation conditions for passwords: Each password used for using the TOE shall be managed so that it will not be divulged by the owner of the password.
A.HDD	Protection conditions for the HDD: The HDD shall not be taken out, unless the administrator permits the service engineer to take it out.
A.NETWORK	Network connection conditions for MFP: • The organization that uses the MFP shall construct a network environment for an intra-office LAN where the MFP will be installed, which will not be intercepted. • When the intra-office LAN where the MFP with the TOE will be installed is connected to an external network, access from the external network to the MFP is not allowed.
A.PHYSICAL	Installation conditions for the MFP: The MFP where the TOE is loaded will be installed in a place where it is physically protected and where only the general users, administrator and service engineer are permitted to enter.
A.SERVICE	Personnel conditions to be a service engineer: The service engineer, in the role given to them, shall not carry out a malicious act during the series of permitted operations during the installation of the TOE and the maintenance of the MFP.
A.SESSION	Session control conditions: • General users shall always terminate the session after using the box function whenever leaving the place. • The administrator shall always terminate the session after using the administrator function. • The service engineer shall always terminate the session after using the service engineer function.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

- Japanese version

  <Document for CE>

  - Service Manual Security Kit Ver. 2.0 2004.04
  - Set-up Instructions Security Kit (ADO_IGS Setup Instructions NDL 1.00-040524 domestic)
  - Installation Check List Security Kit (ADO_IGS_Installation Check List -NDL 1.02-031226 J)
  - Additional Information/Additional Information (Japanese-English Bilingual Test,

ADO_IGS_Additional Information NDL 1.00-031120)

<Documents for Administrators and General Users>

- User Manual Security Kit 2004.04
- User Manual PageScope Light 2004.01

- Overseas version

  <Document for CE>

  - Service Manual Security Kit Ver. 2.0 2004.04
  - Set-up Instructions Security Kit (Japanese-English Bilingual Test for abroad, ADO_IGS Setup Instructions NDL 1.01-031226J/E)
  - Installation Check List Security Kit (ADO_IGS_Installation Check List NDL 1.02-031226 E)
  - Additional Information/Additional Information (Japanese-English Bilingual Test, ADO_IGS_Additional Information NDL 1.00-031120)

  <Documents for Administrators and General Users>

  - User Manual Security Kit 2004.05
  - User Manual PageScope Light 2004.01

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 September, 2003 and concluded by completion the Evaluation Technical Report dated June, 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 December, 2003 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 January, 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

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

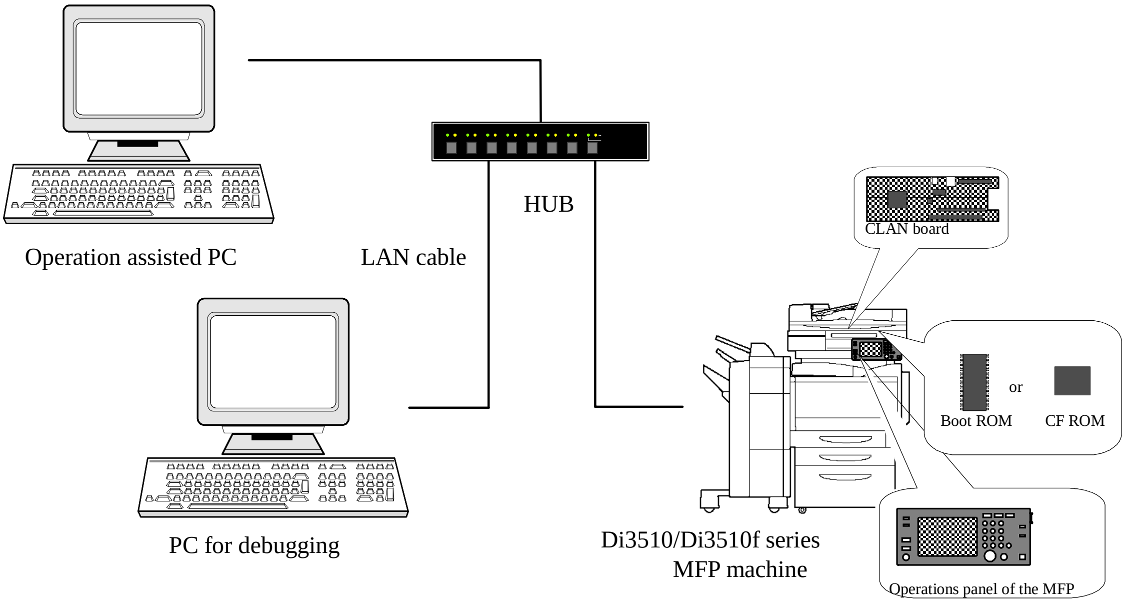

Figure 2-1 Configuration of Developer Testing

2) Outlining of Developer Testing

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

a. Test configuration

Test configuration performed by the developer is showed in the Figure 2-1. Developer testing was performed at the same TOE testing environment with the TOE configuration identified in ST.

b. Testing Approach

For the testing, following approach was used.

(1) Test items were set so that they covered all of the security functions (security functions for administrator mode, security functions for secure printing, security functions for service mode, and security functions for the user box).

(2) Security functions were checked by operation from the operations panel of the MFP body or a web browser screen of the client PC.

(3) If a test result could not be checked by the operations panel or the web browser screen, it was checked by the debugging module.

c. Scope of Testing Performed

Testing is performed about 550 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 same configuration with developer testing.

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

Test configuration performed by the evaluator is showed in the Figure 2-1. Evaluator testing was performed at the same TOE testing environment with the TOE configuration identified in ST.

b. Testing Approach

For the testing, following approach was used.

(1) Test items were set so that they covered all of the security functions.

(2) Security functions were checked by operation from the operations panel of the MFP body or the web browser screen of the client PC.

(3) If a test result could not be checked by the operations panel or a web browser screen, it was checked by the debugging module.

c. Scope of Testing Performed

Total of 232 items of testing; namely 61 items from testing devised by the evaluator and 171 items from testing from sampling of developer testing was conducted. As for selection of the test subset, the following factors are considered.

1. The results of developer testing to doubt that a security function operates as specified.
2. Further significant security function than the other security function.
3. Security function subjected for strength of function.
4. Function used by different interface.

d. Result

All evaluator testing conducted is completes correctly and could confirm the behaviour of the TOE. The evaluator also confirmed that all the test results are consistent with the behaviour.

2.4 Evaluation Result

The evaluator had the conclusion that the TOE satisfies all work units prescribed in CEM Part 2 by submitting the Evaluation Technical Report.

3. Conduct of Certification

The following certification was conducted based on each materials submitted by evaluation facility during evaluation process.

1. Contents pointed out in the Observation Report shall be adequate.
2. Contents pointed out in the Observation Report shall properly be reflected.
3. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.
4. Rationale of evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.
5. The Evaluator’s evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

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

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

4. Conclusion

4.1 Certification Result

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

VxWorks(OS) Basic software component required for the MFP control software to operate. An operating system. It provides services such as network functions, file system functions and multi-processing for the Di3510 series/Di3510f series MFP.

System Manager A software component that registers and starts up jobs, and manages resources.

Operation Panel Cntroller(abbr. OPE) A software component that controls hardware such as LCDs, LEDs and keys on the MFP body operations panel. The information entered from the MFP body operations panel is processed by this software component and is given to the "User Interface." Also, it receives the processing results from the "User Interface" and displays on the panel.

Modular Input Output(abbr. MIO) A software component that converts the data received from a variety of external interfaces (network unit, Centronics I/F) to data that is handled by the "Application," the "Network Module," and the "System Manger." It realizes a WWW server function. In addition, it carries out a variety of network setting processes for the IP address, DNS server, etc.

Macro System Controller(abbr. MSC)

A software component that analyzes scanned image data and registers it as a job. It also controls the job sequence for copying, printing, scanning and faxing.

Application

An application software component that carries out e-mail transmission and reception (Internet fax transmission and reception), an FTP transmission and the receiving of print processing from a PC.

SCANNER Driver

A software component that controls the scanner device that carries out the scanning process during scanning.

PRINTER Driver

A software component that controls the printer device during printing (*It is different from the printer driver of the client PC.)

G3 FAX

A software component for a G3 standard fax transmission and reception.

EP-NET

A software component that receives access to a “remote maintenance function” from telephone lines (public lines) or the “Module Input Output,” and carries out a remote maintenance function. The remote maintenance function is a function that receives a request for access from the support center via a telephone line. The support center collects information such as the number of MFP problems, a value that indicates the wear and tear on the expendable parts, and a printing counter value via a telephone line. In addition, it also has a function such that when a specific malfunction (significant malfunction) is generated in the MFP, it automatically accesses the support center and transmits the malfunction information for the MFP. An e-mail remote maintenance function that realizes the same function using e-mail is also available.

Job

Operational unit for a series of functions in the MFP, such as the copying function, scanning function, printing function, faxing function, etc

Secure Print

A form of printing when printing from a client PC. When a password is set by the printer driver on a client PC, and printing data is transmitted to MFP, the printing is not executed but rather is pending at the MFP. When a set password is entered at the MFP, the pending is cancelled and the printing is executed.

Secure Print Job Information Data

Print data received by the MFP for secure print. This ST handles this as a protective asset.

HDD Store print

A function that stores the print job information data in the HDD of the MFP. Printing can be done by operating the operations panel of the MFP body. There is no particular access limit for the operation of print execution.

User Box

A directory set as a storage area at the MFP for scanned image data when the HDD is loaded. Individual users can set the name and password only from a client PC. The user box indicated as “Public” is shared, so a password cannot be set. A name change cannot be carried out either.

User Box Data

Image data stored in the user box. This ST handles this as a protective asset.

Administrator Mode

Functions that are provided for authenticated administrators only.

Administrator Mode Password

Passwords set for the administrator mode. Eight-digit numbers can be set.

Service Mode

Functions that are provided for authenticated service engineers only.

Service Code

A password that is set for the service mode, maintenance mode and initialization mode. Eight-digit numbers and “*” and “#” can be used.

Access Check Function

A function for which the operation setting is controlled by the administrator. When this function is valid, the user box authentication function operates and a series of unsuccessful authentication attempts is detected for each of the authentication functions for the administrator function, secure print function and user box function, and depending on the number of unsuccessful authentications, it locks each authentication function.

Unauthorized access detection count value for a user box

A value that is counted and stored as the number of unsuccessful trials, when an authentication trial fails for the user box authentication function while the access check function is operating.

Unauthorized access detection count value for secure print	A value that is counted and stored as the number of unsuccessful trials, when an authentication trial fails for the secure print authentication function while the access check function is operating.
Penalty reset function	A function that clears the unauthorized access detection count value for a user box and the unauthorized access detection count value for secure print to zero. When the authentication function for a user box and secure print are locked, execution of this function unlocks them.

6. Bibliography

[1] Di3510 Series/Di3510f Series Multi Function Peripheral Security Kit Security Target Version 1.18 (June 4, 2004) KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

[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] Di3510 Series/Di3510f Series Multi Function Peripheral Security Kit Evaluation Technical Report Version 1.5 June 4, 2004 Japan Electronics and Information Technology Industries Association, Information Technology Security Center