Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2010-2-22 (ITC-0291)
Certification No.	C0261
Sponsor	RICOH COMPANY, Ltd.
Name of TOE	Following MFP with FCU(Fax Option Type 3351) MFP: Ricoh Aficio MP 2851, Ricoh Aficio MP 3351, Savin 9228, Savin 9233, Lanier LD528, Lanier LD533, Lanier MP 2851, Lanier MP 3351, Gestetner MP 2851, Gestetner MP 3351, nashuatec MP 2851, nashuatec MP 3351, Rex-Rotary MP 2851, Rex-Rotary MP 3351, infotec MP 2851, infotec MP 3351 FCU: Fax Option Type 3351
Version of TOE	MFP Software /Hardware Version : Software System/Copy 1.00 Network Support 7.29.3 Scanner 01.12 Printer 1.01 Fax 01.00.00 Web Support 1.01 Web Uapl 1.03 Network Doc Box 1.00 Hardware Ic Key 1100 Ic Hdd 01 FCU Version : GWFCU3-20(WW) 01.00.00
PP Conformance	None
Conformed Claim	EAL3
Developer	RICOH COMPANY, Ltd.
Evaluation Facility	Information Technology Security Center

This is to report that the evaluation result for the above TOE is certified as follows.
2010-6-29

Takumi Yamasato, Technical Manager
Information Security Certification Office
IT Security Center

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following criteria prescribed in the "IT Security Evaluation and Certification Scheme".

- Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 2
- Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 2

Evaluation Result: Pass

"Following MFP with FCU(Fax Option Type 3351) MFP: Ricoh Aficio MP 2851, Ricoh Aficio MP 3351, Savin 9228, Savin 9233, Lanier LD528, Lanier LD533, Lanier MP 2851, Lanier MP 3351, Gestetner MP 2851, Gestetner MP 3351, nashuatec MP 2851, nashuatec MP 3351, Rex-Rotary MP 2851, Rex-Rotary MP 3351, infotec MP 2851, infotec MP 3351 FCU: Fax Option Type 3351" has been evaluated in accordance with the provision of the "IT Security Certification Procedure" 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 "Following MFP with FCU(Fax Option Type 3351) MFP: Ricoh Aficio MP 2851, Ricoh Aficio MP 3351, Savin 9228, Savin 9233, Lanier LD528, Lanier LD533, Lanier MP 2851, Lanier MP 3351, Gestetner MP 2851, Gestetner MP 3351, nashuatec MP 2851, nashuatec MP 3351, Rex-Rotary MP 2851, Rex-Rotary MP 3351, infotec MP 2851, infotec MP 3351 FCU: Fax Option Type 3351" (hereinafter referred to as "the TOE") conducted by Information Technology Security Center (hereinafter referred to as "Evaluation Facility"), and it reports to the sponsor, RICOH COMPANY, Ltd. and provides information to the users and system operators who are interested in this TOE.

The reader of the Certification Report is advised to read the corresponding ST. The operational conditions, details of usage assumptions, corresponding security objectives, security functional and assurance requirements needed for its enforcement, their summary of security specifications and rationale of sufficiency are specifically described in ST.

This certification report assumes "the person who managed this TOE" to be a reader. 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.

1.1.1 EAL

Evaluation Assurance Level of TOE defined by this ST is EAL3 conformance.

1.1.2 PP Conformance

There is no PP to be conformed.

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows;

Name of Product:	Following MFP with FCU(Fax Option Type 3351)		
	MFP:	Ricoh Aficio MP 2851, Ricoh Aficio MP 3351, Savin 9228, Savin 9233, Lanier LD528, Lanier LD533, Lanier MP 2851,Lanier MP 3351, Gestetner MP 2851, Gestetner MP 3351, nashuatec MP 2851, nashuatec MP 3351, Rex-Rotary MP 2851, Rex-Rotary MP 3351, infotec MP 2851, infotec MP 3351	
	FCU:	Fax Option Type 3351	
Version:	MFP	Software/Hardware version:	
		Software	System/Copy 1.00
			Network Support 7.29.3
			Scanner 01.12
			Printer 1.01

Fax 01.00.00
Web Support 1.01
Web Uapl 1.03
Network Doc Box 1.00
Hardware Ic Key 1100
Ic Hdd 01
FCU version: GWFCU3-20(WW) 01.00.00

Developer: RICOH COMPANY, Ltd.

1.2.2 Product Overview

The functions of copier, scanner, printer, and fax are for digitizing paper documents, and managing and printing those digitized documents. The subject device of this certification is a digital MFP (hereafter "MFP") made by RICOH COMPANY, LTD., and which provides these functions. The target of this certification is a device equipped with the optional Fax Function.

This device is an I/O device that incorporates the functions of copier, scanner, printer, and fax. Such a device will normally be connected to an office LAN and used to input, store, and output document data. This device protects internally stored document data from accidental disclosure and operation. It also prevents leakage of document data being sent and received between the device and a client computer.

1.2.3 Scope of TOE and Security Functions

1.2.3.1 Scope of TOE

If the device satisfies all of the following conditions, that device is considered covered by this certification. If the configuration of the device does not satisfy some of the following settings, the device is not the TOE. Once the device's Service Mode Lock is cancelled and its Maintenance Function is used, the possibility exists that the device is no longer the TOE (since there is a possibility that the Maintenance Function changes the device itself).

- Service Mode Lock not set to "Off"
- Uses IPv4 protocol (not IPv6)
- Does not use the IP-Fax or Internet Fax Function
- Uses Basic Authentication as its Identification and Authentication Function (does not use any other method of authentication)

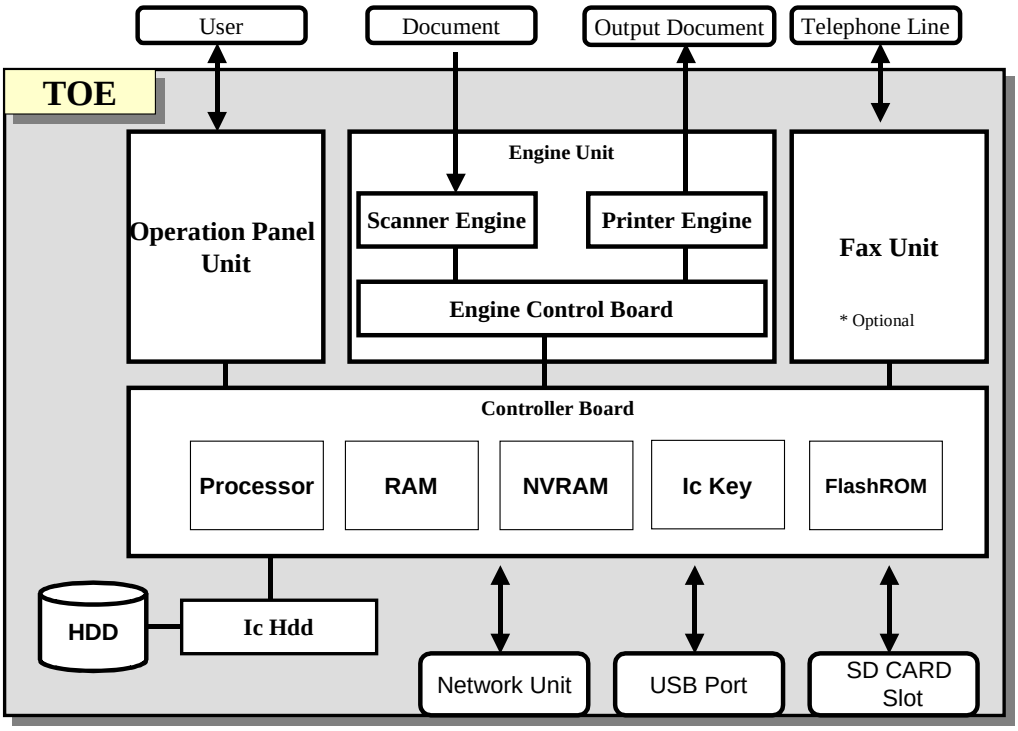

Fig. 1-1 TOE Configuration

Figure 1-1 shows the physical components that constitute the TOE. Following is a brief description of each item:

- Operation Panel Unit (hereafter Operation Panel)
  The Operation Panel is an interface device that is installed on the TOE for use by users. It features key switches, LED indicators, an LCD touch screen, and the Operation Panel Control Board.
- Engine Unit
  The Engine Unit contains a Scanner Engine, Printer Engine and the Engine Control Board. The Scanner Engine is an input device to read the paper documents. The Printer Engine is an output device for printing and outputting of paper documents.
- Fax Unit (Optional)
  The Fax Unit is a device that has a modem function to send and receive fax data when connected to a telephone line.
- Controller Board
  The Controller Board contains Processors, RAM, NVRAM, Ic Key and FlashROM. MFP Control Software is installed in FlashROM that is on this Controller Board. MFP Control Software has the elements that can identify TOE components such as System/Copy, Network Support, Scanner, Printer, Fax, Web Support, Web Uapl and Network Doc Box. The Ic Key is a security chip that generates random numbers and encryption keys, and detects any tampering with the MFP Control Software.
- Ic Hdd
  Ic Hdd is a security chip that encrypts information to be stored on the HDD, and decrypts information to be read from the HDD.
- HDD
  HDD is a hard disk drive, where image data and user information for identification and authentication are stored. The area where image data are stored as document data is called D-BOX.

- Network Unit
  The Network Unit is an interface board for connection to an Ethernet (100BASE-TX/10BASE-T) network.
- USB Port
  The USB Port is used to connect a client computer to the TOE, print or fax from the client computer.
- SD CARD Slot
  The SD CARD Slot is used for setting the Stored Data Protection Function and Maintenance. No maintenance works based on this certification are assumed, so this interface is used only when the TOE is installed.

1.2.3.2 Overview of TOE Operation

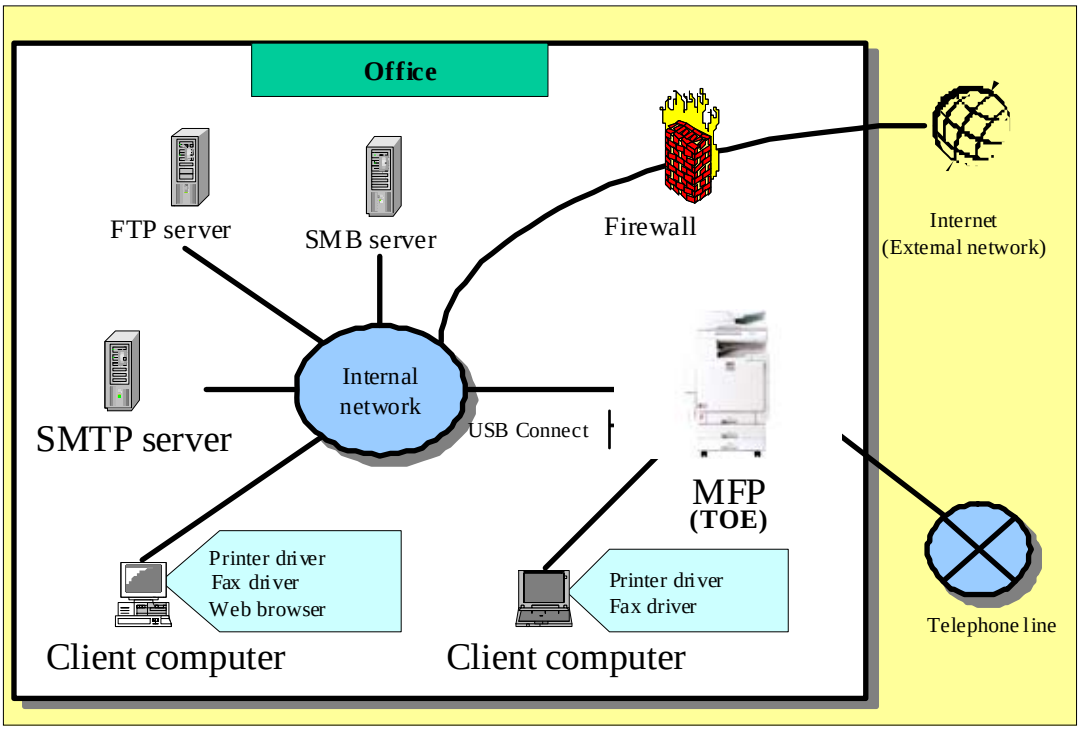

Fig. 1-2 Example of TOE Usage Environment

Figure 1-2 gives an example environment where the TOE is used mainly for inputting, outputting, and storing image data. Following are the methods of inputting and outputting image data. The TOE can simply output the data it receives, or store input data.

- How the TOE receives image data input:
  > By optically scanning an original using the Scanner Engine.
  > By receiving the data from a client computer via the Network Unit or USB Port.
  > By receiving the data from a telephone line via the Fax Unit.
- How the TOE outputs image data:
  > By print using the Printer Engine.
  > By sending to a client computer through the Network Unit.
  > By sending as attachments to e-mail through the Network Unit.
  > By sending either to an FTP server using the FTP protocol, or to an SMB

server using the SMB protocol.
> By sending from the Fax Unit via a telephone line.

1.2.3.3 TOE Functions

The TOE features a Copy Function, Printer Function, Fax Function, Scanner Function, Document Server Function, Management Function, and Web Service Function. Following are descriptions of each function:

1) Copy Function
This function is for scanning originals as image data using the Scanner Engine, and for printing the image data in accordance with the specified Print Settings using the Printer Engine.
Scanned image data can be stored in the D-BOX as document data generated using a non-Scanner Function (hereafter, "document data (non-Scanner Function)").

2) Printer Function
This function is for receiving via the Network Unit or USB Port print data sent from a client computer, and for printing data using the Direct Print Function or the Store and Print Function. The Direct Print Function simply prints out received print data using the Printer Engine. The Store and Print Function stores the print data in the D-BOX as document data (non-Scanner Function). It does not print it immediately. Actual printout is performed using "1.2.3.3 8) Document Server Function (Management)", which is described later.

3) Fax Function (Reception)
This function is for receiving fax data from the Fax Unit and either printing or storing received fax data.
When printing received fax data, this function simply prints it using the Printer Engine.
When storing received fax data, this function converts it to Fax Reception data and then stores it in the D-BOX. It does not print it immediately. Actual printout is performed using "1.2.3.3 8) Document Server Function (Management)", which is described later.
*Note: Fax data received by the TOE is not a target of this certification. (Refer to "5.2.1 Notes Concerning Protected Assets".)

4) Fax Function (Immediate Transmission/Memory Transmission)
This function is for scanning originals as image data using the Scanner Engine and sending the image data from the Fax Unit using the Immediate Transmission or Memory Transmission Function.
The Immediate Transmission Function connects the device to the destination fax, and then sends the image data as it is being scanned.
The Memory Transmission Function first scans the entire original, then connects the device to the destination fax, and then sends the image data.

5) Fax Function (Stored Documents Fax Transmission)
This function is for sending the "specified document data stored in the D-BOX" from the Fax Unit.

6) Fax Function (LAN-Fax Transmission)
This function is for receiving via the Network Unit or USB Port print data from a client computer, and sending it from the Fax Unit.

7) Document Server Function (Scan)
This function is for scanning originals as image data using the Scanner Engine, and for storing the image data as document data (non-Scanner Function) in the D-BOX.

8) Document Server Function (Management)
This function is for performing one of the processes described below on "specified document data (non-Scanner Function) in the D-BOX or on specified fax reception data."
- Print (using the Printer Engine)
- Delete (deletion of data stored in the D-BOX)
- Download (transfer of data to a client computer via the Network Unit)
*Note: Document data (hereafter, "document data (for Scanner Function use only)") that is generated using the "Scanner Function (Scan)" cannot be managed using the "Document Server Function (Management)", but can be managed using the "Scanner Function (Management)".

9) Scanner Function (Scan)
This function is for scanning the original using the Scanner Engine and then sending the image data by e-mail, delivering it to a folder, or storing it.
When e-mail is sent using this function, the image data will be sent as an e-mail attachment via the Network Unit to a specified e-mail address.
When image data is sent using "Deliver to Folder", the image data will be sent by FTP or SMB protocol via the Network Unit to the specified folder.
When image data is stored using this function, the image data will be stored as document data (for Scanner Function use only) in the D-BOX.
*Note: Management of document data (for Scanner Function use only) generated using this function differs from management of document data (for non-Scanner Function) generated using other functions. Document data (for Scanner Function use only) generated using this function is managed using the "Scanner Function (Management)", and document data (for non-Scanner Function) generated using other functions is managed by the "Document Server Function (Management)".

10) Scanner Function (Management)
This function is for performing one of the processes described below on "specified document data (for Scanner Function use only) in the D-BOX".
- Send (by e-mail or Deliver to Folder of the "Scanner Function (Scan)")

- Delete (deletion of document data in the D-BOX)
- Download (transfer of document data to a client computer via the Network Unit)

*Note: This function only manages document data (for Scanner Function use only) stored using the "Scanner Function (Scan)". The "Document Server Function (Management)" manages the document data (for non-Scanner Function) stored using other functions.

11) Management Function
This function is for configuring the following settings: TOE machine settings, network connection settings, authorised user information settings, and settings restricting use of document data information. The user's ability to manage this information is determined in accordance with the user role of the authorised TOE users(general users, administrators, or supervisor).

12) Web Service Function
This function is for remote operation of the TOE by authorised TOE users (general users, administrators, and the supervisor) using a Web browser running on a client computer.
Although this function is available for the functions described in "1) Copy Function" to "11) Management Function", there are some functions that are not available with this function.

1.2.3.4 TOE Security Functions

1) Identification and Authentication Function, Document Data Access Control Function
"1.2.3.3 TOE Functions" includes operations for reading document data (extracting data stored as document data in the TOE by methods such as printing or sending), and the procedure for deleting document data. The TOE has functions for identifying and authenticating its users, and controlling access so that reading and deleting of document data cannot be performed unless the owner of the document intends to perform these operations.

2) Stored Data Protection Function
To prevent information leakage from the HDD after disposal of the TOE, the TOE has a function for encrypting data written to the HDD.

3) Network Communication Data Protection Function
The TOE has a function for encrypting the data it sends and receives over internal networks, which prevents leakage of information due to local eavesdropping.
The objects of encryption are limited to data the TOE communicates via the internal networks. Data the TOE communicates via USB or telephone lines is not included.

4) Telephone Line Intrusion Protection Function

The TOE has a function for accepting only permitted communications from telephone lines, thus preventing unauthorised use of the TOE via telephone line.

5) MFP Control Software Verification Function
The TOE has a function for verifying that the MFP Control Software is properly provided by RICOH COMPANY, LTD.

6) Audit Function
The TOE has a function for recording events as audit logs so that in the event of a security-related occurrence, operation status can be checked and security breaches detected.

7) Security Management Function
The TOE provides a function for configuring information related to the performance of the Security Functions. This information is determined by the role of the authorised TOE user (general user, administrator, or supervisor) so that the security limitations can be maintained.

8) Service Mode Lock Function
This function restricts use of the Maintenance Function unless expressly maintenance operations are allowed by the machine administrator.

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 "IT Security Evaluation and Certification Scheme"[2], "IT Security Certification Procedure"[3] and "Evaluation Facility Approval Procedure"[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 "Aficio MP 2851/3351 series with Fax Option Type 3351 Security Target" as the basis design of Security Functions for the TOE (hereinafter referred to as "the ST")[1], the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex A of CC Part 1 (either of [5] or [8]) and Functional Requirements of CC Part 2 (either of [6] or [9]) 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] or [10]) as its rationale. Such evaluation procedure and its result are presented in "RICOH COMPANY, Ltd. Aficio MP 2851/3351 series with Fax Option Type 3351 Evaluation Technical Report" (hereinafter referred to as "the Evaluation Technical Report") [13]. Further, evaluation methodology shall comply with the CEM (either of [11] or [12]).

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. Evaluation is completed with the Evaluation Technical Report dated 2010-6 submitted by the evaluation facility 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.

2. Summary of TOE

2.1 Security Problem and assumptions

The followings are the problems to be addressed and the assumptions required by the TOE.

2.1.1 Threat

This TOE assumes the threats shown in Table 2-1 and provides the functions that counter these threats.

Table 2-1 Assumed Threats

Identifier	Threat
T.ILLEGAL_USE	Attackers may read or delete document data by gaining unauthorised access to the TOE though the device's interfaces (the Operation Panel, network interface, USB Port, or SD CARD interface).
T.UNAUTH_ACCESS	Authorised TOE users may breach the limits of authorised usage and access document data through the external TOE interfaces (the Operation Panel, Network Interface, or USB Port) that are provided for them.
T.ABUSE_SEC_MNG	Persons not authorised to use Security Management Functions may abuse them.
T.SALVAGE	Attackers may remove the HDD from the TOE and disclose document data.
T.TRANSIT	Attackers may illegally obtain, leak or tamper with document data or print data sent or received by the TOE via the internal network. *Note: The "document and print data sent or received by the TOE" can exist on the USB interface or telephone lines; however, obtaining and tampering with data that is in transit through these media is not considered a threat.
T.FAX_LINE	Attackers may gain access to the TOE through telephone lines.

2.1.2 Organisational Security Policy

Organisational security policy required in use of the TOE is shown in Table 2-2.

Table 2-2 Organisational Security Policy

Identifier	Organisational Security Policy
P.SOFTWARE	Measures are provided for verifying the integrity of MFP Control Software, which is installed in the FlashROM of the TOE.

2.1.3 Assumptions for Operational Environment

Table 2-3 shows the assumptions concerning the environment where the TOE is used. The effective performance of the TOE Security Functions are not assured unless these assumptions are satisfied.

Table 2-3 Assumptions in Use of the TOE

Identifier	Assumptions
A.ADMIN	Administrators shall have sufficient knowledge to operate the TOE securely in the roles assigned to them and will instruct general users to operate the TOE securely also. Additionally, administrators shall not abuse their permissions maliciously. *Note: The "sufficient knowledge to operate the TOE securely" includes the following: - No use of the following function: > Back up/Restore Address Book - Use of the TOE with the following settings maintained: > Service Mode Lock not set to "Off" > Use of the IPv4 protocol (not IPv6) > No use of IP-Fax or Internet Fax Function > Use of Basic Authentication for the Identification and Authentication Function (use of authentication for Basic Authentication only)
A.SUPERVISOR	Supervisor shall have sufficient knowledge to operate the TOE securely in the roles assigned to them, and are shall not abuse their permissions maliciously.
A.NETWORK	When the network that the TOE is connected to (the internal network) is connected to an external network such as the Internet, the internal network shall be protected from the external network.

2.1.4 Documents Attached to Product

Identification of the documents attached to the TOE is listed below. TOE users are required to fully understand and follow the documents shown below in order to satisfy the assumptions.

Table 2-4 [English version - 1]

Name of Guidance Documents
9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351 Operating Instructions About This Machine
9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351 Operating Instructions Troubleshooting
Notes for Users
App2Me Start Guide
Manuals for Users 9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351
Manuals for Administrators 9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351
Manuals for Administrators Security Reference Supplement 9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351
Notes for Administrators: Using this Machine in a CC-Certified Environment
VM Card Manuals

Table 2-5 [English version - 2]

Name of Guidance Documents
Quick Reference Copy Guide
Quick Reference Fax Guide
Quick Reference Printer Guide
Quick Reference Scanner Guide
Manuals for This Machine
Safety Information for Aficio MP 2851/Aficio MP 3351
Notes for Users
App2Me Start Guide
Manuals for Users MP 2851/3351 Aficio MP 2851/3351 A
Manuals for Administrators Security Reference MP 2851/3351 Aficio MP 2851/3351
Manuals for Administrators Security Reference Supplement 9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351
Notes for Administrators: Using this Machine in a CC-Certified Environment
VM Card Manuals

Table 2-6 [English version - 3]

Name of Guidance Documents
Quick Reference Copy Guide

Quick Reference Fax Guide
Quick Reference Printer Guide
Quick Reference Scanner Guide
Manuals for This Machine
Safety Information for MP 2851/MP 3351
Notes for Users
App2Me Start Guide
Manuals for Users MP 2851/3351 Aficio MP 2851/3351 A
Manuals for Administrators Security Reference MP 2851/3351 Aficio MP 2851/3351
Manuals for Administrators Security Reference Supplement 9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351
Notes for Administrators: Using this Machine in a CC-Certified Environment
VM Card Manuals

Table 2-7 [English version - 4]

Name of Guidance Documents
MP 2851/MP 3351 MP 2851/MP 3351 Aficio MP 2851/3351 Operating Instructions About This Machine
MP 2851/MP 3351 MP 2851/MP 3351 Aficio MP 2851/3351 Operating Instructions Troubleshooting
Quick Reference Copy Guide
Quick Reference Fax Guide
Quick Reference Printer Guide
Quick Reference Scanner Guide
Notes for Users
App2Me Start Guide
Manuals for Users MP 2851/3351 Aficio MP 2851/3351
Manuals for Administrators MP 2851/3351 Aficio MP 2851/3351
Manuals for Administrators Security Reference Supplement 9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351
Notes for Administrators: Using this Machine in a CC-Certified Environment
VM Card Manuals

2.1.5 Configuration Requirements

Figure 1-2 shows the connections between the TOE and the external environments. The TOE is not necessarily connected to the external environments specified below. Depending on how the TOE is used, the TOE is connected to the required external environments.

- Client computer connected to the TOE via a USB Port
- Client computer connected to the TOE via Ethernet
- SMTP server connected to the TOE via Ethernet
- FTP server connected to the TOE via Ethernet
  (The FTP server must support IPSec)

- SMB server connected to the TOE via Ethernet
  (The SMB server must support IPSec)
- Public telephone line or equivalent

Drivers are required if the TOE is to be used from client computers. Client drivers are acquired from the Web page specified in the user's guidance. See below for the driver information at the time of this evaluation.

- PCL 6 driver V1.0.0.0
- LAN Fax driver V1.61

If the TOE is to be used from a Web browser running on a client computer (i.e. "client computer connected to the TOE via Ethernet"), Internet Explorer 6.0 or later must be installed on the client computer.

2.2 Security Objectives

TOE counters threats described in 2.1.1 as follows by implemented Security Functions and fulfills the organisational security policy in 2.1.2.

2.2.1 Countermeasures against T.ILLEGAL_USE, T.UNAUTH_ACCESS, T.ABUSE_SEC_MNG

These threats are countered by a sequence of countermeasure, identification and authentication, and access control.
The TOE requires users who attempt to use it to enter their user ID and authentication information (password). The TOE then verifies the authenticity of the entered user ID and authentication information.
The TOE has the following functions to counter impersonation by attempted entry of another user's ID and authentication information:

- Following the Lockout Policy, if the number of consecutive unsuccessful attempts to authenticate meets the specified Number of Attempts before Lockout, the TOE locks out that user ID, denying usage of the TOE by any user entering that ID.
- When users attempt to register or change their authentication information, the TOE only accepts passwords that satisfy the conditions of Minimum Password Length and Password Complexity Setting.

The TOE verifies the user ID and authentication information and either of the following, (1) or (2), happens:

(1) If the TOE does not recognise the user ID and authentication information as valid, the TOE denies usage.
Since only users who are authorised to use the TOE have a valid user ID and authentication information, this restriction (1) prevents unauthorised users having usage of the TOE. This is the countermeasure against T.ILLEGAL_USE.

(2) If the TOE recognises the entered user ID and authentication information as valid, it identifies the user and user role by the user ID. After identifying these, it allows the usage of the TOE functions.

The following are the user roles recognised by the TOE:

- General user
- Administrator

- Supervisor

If the administrator role is assigned, the following roles are also specified. These roles are not exclusively performed, so multiple roles can be assigned to one user ID of the administrator.

- User administration
- Machine administration
- Network administration
- File administration

After the TOE performs (2), the user instructs the TOE to perform the required operation. The instruction can be either an "operation on document data" or a "use of the Management Function". Depending on which instruction is referred to, (3) or (4) below is then performed.

(3) If the instruction refers to an "operation on document data", the TOE determines if the user has permissions for the operation according to the user's ID and role (determined in (2)). The TOE follows the instruction and performs the operation only if the user has permission to perform it. The TOE permits or denies the instructed operation based on the following criteria.

- If the general user role is assigned to the user
  Each document data contains information (the document data ACL) that shows the users permitted to access the document, and the operations permitted to each user (read, change Print Settings, delete, and document data ACL permissions). The TOE determines if the user has permissions for the requested operation, by matching the user's ID (determined in (2)) against the document data ACL.

- If the general user role is not assigned to the user
  If a user who is identified in (2) as an administrator with the role of file administration, the user is allowed to delete arbitrary document data. If not, operations on document data are not allowed.

Since (3) restricts access to operations on document data to authorised TOE users only (based on whether the user is authorised in the ACL as a general user or administrator) the TOE counters the T.UNAUTH_ACCESS.

(4) If the instruction refers to "use of the Management Function", the TOE determines if the user has permissions for the operation, according to the user's ID (determined in (2)) and the operator's role. The TOE follows the instruction and allows the use of the Security Management Function only if the user has permission to perform it.
The Security Management Function controls operations on the following TOE data:

- Document Data ACL
- Registration Information about Users
- Lockout Policy (number of consecutive unsuccessful attempts before Lockout, whether or not to release Lockout based on time elapsed , Lockout Release Timer)
- System Date, Time
- HDD Encryption Key
- Audit Log

- Service Mode Lock Function
- Password Policy (Minimum Password Length, and the minimum combination of characters in the password)

The TOE allows operations on this data provided the user has the role of administrator or supervisor.* However, the TOE also allows general users to perform the document data operations described below provided the security limitations are maintained.

- Document file owner and general users specified in the document data ACL can perform operations on the document data ACL (except for changing the document file owners).
- General users can change their own registration information: "authentication information", "document data default ACL (except for changing the document file owners)" and "S/MIME User Information".

Since (4) limits the use of the Security Management Function to a "person authorised to use the Security Management Function", the TOE counters the T.ABUSE_SEC_MNG.

2.2.2 Countermeasures against T.SALVAGE

The TOE counters T.SALVAGE by preventing understanding of document data unless access to it is through the normal way (using the functions described in "1.2.3.3 TOE Functions" from the Operation Panel or client computer). (Stored Data Protection Function)

This function is enforced by performing encryption of data just before it is written to the HDD, and by decryption of data just after it is read from the HDD. This function uses the following cryptographic algorithm and key size:

- Cryptographic algorithm: AES
- Key size: 256 bits

2.2.3 Countermeasures against T.TRANSIT

To counter T.TRANSIT, the TOE protects document and image data that is sent or received via an internal network from interception and tampering.
Selection of the mechanism (S/MIME, SSL, or IPSec) used by the TOE is determined by the type of data requiring protection. S/MIME is applied by TOE functions; the communication path for SSL is created through cooperation between the TOE and client computer; and the communication path for IPSec is created through cooperation between the TOE and either the SMB or FTP server.
The scope of protection depends on the mechanism used for data protection. The following tables, 2-8 (1), 2-8 (2), and 2-8 (3), show the specific scopes.

* Some operations might not be available to administrators or supervisors. There is a rule that determines which administration operations are allowed to which types of administrator (user administration, machine administration, network administration and file administration) and the supervisor. The details of this rule are outside the scope of this document.

Table 2-8 (1) Specific Data, Mechanism and Scope

Target data
Print data that is sent to the Network Unit from a client computer via an internal network using the "Printer Function" (except for via USB Ports)
Protection mechanism and protected scope
The internal networks between client computer and Network Unit are protected by the SSL mechanism

Table 2-8 (2) Specific Data, Mechanism and Scope

Target data
Print data that is sent to the Network Unit from a client computer via an internal network using the "Fax Function (LAN-Fax)" (except for via USB Ports)
Protection mechanism and protected scope
Internal networks between client computers and the Network Unit are protected by the SSL protocol

Table 2-8 (3) Specific Data, Mechanism and Scope

Target data
Document data that is output from the Network Unit using the "Scanner Function (Scan)" or the "Scanner Function (Management)"
Protection mechanism and protected scope
When delivering to folders: Internal networks between the Network Unit and the "SMB server or FTP server containing the specified folders" are protected by the IPSec mechanism. When sending to an e-mail address: The networks (including internal networks) between the Network Unit and the "e-mail client of the destination address" are protected by the S/MIME mechanism. When downloading: Internal networks between the Network Unit and client computers are protected by the SSL mechanism.

2.2.4 Countermeasures against T.FAX_LINE

The TOE does not have an active mechanism for countering the T.FAX_LINE.
However, since the TOE does not perform any operations via a telephone line except for sending and receiving faxes, T.FAX_LINE is countered.

2.2.5 Enforcement of P.SOFTWARE

In order to enforce P.SOFTWARE, the TOE has a function that checks that the executable code of the MFP Control Software, which is embedded in the FlashROM, is in exactly the same condition as the genuine code provided by RICOH.
Code verification is enforced by confirmation of the electronic signature that is appended to the executable code.
Use of this function and version checking of each element of TOE output confirm that the software was provided by RICOH by the normal method and its version is correct.
Although it is not possible to assume specific threats to the executable code of MFP Control Software based on the description of the ST, this Organisational Security Policy was defined in order to make consumers aware that integrity checking of the MFP Control Software is possible.

2.2.6 Support for Other Security Functions

The TOE has an Audit Function that detects security breaches.
If this function is applied, events that can be used to detect security breaches will be recorded in an audit log whenever such events occur.

3. Conduct and Results of Evaluation by Evaluation Facility

3.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance requirements in CC Part 3. Details for evaluation activities are reported 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.

3.2 Overview of Evaluation Conducted

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

Evaluation has started on 2010-2 and concluded by completion the Evaluation Technical Report dated 2010-6. The evaluation facility received a full set of evaluation deliverables necessary for evaluation provided by the 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 2010-4 and 2010-5 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and development security by investigating records and staff hearing. Further, the evaluation facility executed sampling check of conducted testing by the developer and the evaluator testing by using developer testing environment at developer site on 2010-4. However, a part of procedural status conducted in relation to each work unit for development security was

adopted by the judgment that the result of the survey on 2010-10 and 2010-11 executed for other TOE at the same guarantee level was able to be trusted even now.

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

3.3 Product Testing

The evaluator confirmed the validity of the test that the developer had executed.
The evaluator executed reappearance tests, additional tests and penetration tests based on vulnerability assessments judged to be necessary from the evidence shown by the process of the evaluation and results by the verification of the developer testing.

3.3.1 Developer Testing

The evaluator evaluated the integrity of the developer testing conducted by the developer and the deliverables of actual test results.
The overview of evaluated developer testing is shown as follows;

1) Developer Test Environment

The configuration of the developer testing is shown in Figure 3-1.

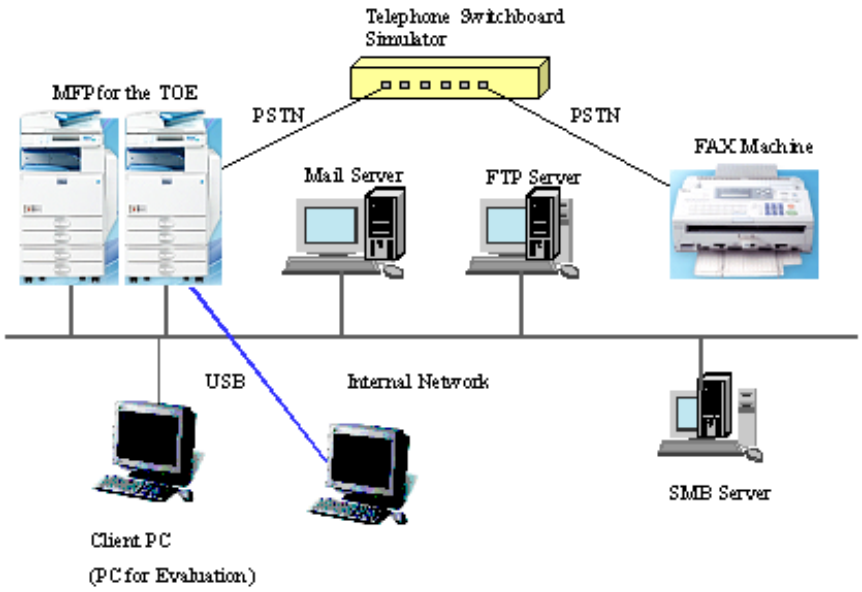

Figure 3-1 Configuration of Developer Testing

Following is an outline of the elements of the test configuration.

- MFP for the TOE
  The following devices were the subjects of the testing:
  Aficio MP 2851
  Aficio MP 3351

- Client computer
  The following Web browsers were used:
  > Internet Explorer 6.0
  > Internet Explorer 7.0
  > Internet Explorer 8.0

  The following drivers were used:
  > PCL 6 Driver V1.0.0.0
  > LAN Fax Driver V1.61

- Mail Server
  Windows Server 2003 SP2 was used as the software with the SMTP server function.

- FTP Server
  Windows Server 2003 SP2 was used as the software with the FTP server function.

- SMB Server
  Windows Server 2003 SP2 was used as the software with the SMB server function.

- Fax machines
  Ricoh Aficio MP 2851 and Ricoh Aficio MP 3351 were used as the Fax Function-equipped devices.

- Telephone Switchboard Simulator
  TLE-101III (manufactured by LSI JAPAN Co., Ltd.) was used as a public line-emulating device.

Models other than Ricoh Aficio MP 2851/3351 ("Savin 9228/9233", "Lanier LD528/533", "Lanier MP2851/3351", "Gestetner MP 2851/3351", "nashuatec MP 2851/3351", "Rex-Rotary MP 2851/3351", and "Infotec MP 2851/3351") are OEM devices, and device names will vary depending on the region. Therefore, "Ricoh Aficio MP 2851/3351" and other models are identical apart from their device names. "Ricoh Aficio MP 2851" and "Ricoh Aficio MP 3351" have the same Security Functions but different print speeds (28 sheets/minute; 33 sheets/minute).

The functionalities of "Ricoh Aficio MP 2851" and "Ricoh Aficio MP 3351", which were the target devices in the developer testing, conform to the ST, and such functionalities are consistent with the TOE structures specified in the ST. Therefore, the developer testing is considered to be conducted in the same TOE test environment as the TOE configuration identified in the ST.

2) Outlining of Developer Testing
Outlining of the testing performed by the developer is as follows;

a. Test outline

The testing procedure solely consisted on stimulation of the external TOE interface by assumed TOE operations (operations of the Operation Panel, the client computer connected via the internal network or USB, and fax machines) and visual observation of the results. When such methods were not suitable, the following methods were used instead:

(1) Capture of data communicated over the internal network and verification of

the communication protocol (SSL and IPSec) using packet capture software.

(2) Checking of output debug information using internal tools that produce debug information for the purpose of observing activity inside the TOE.

(3) Replacement of the MFP Control Software with software that had "compromised validity" for the purpose of verifying the integrity of the MFP Control Software validity checking function, and checking of output debug information using internal tools that produced debug information.

Furthermore, vulnerability testing of the Web interfaces was performed using a diagnostic tool that detects vulnerabilities within Web applications.

b. Scope of Testing Performed

The developer conducted 513 items (1008 cases) of testing.
The coverage analysis was conducted, and it was examined that all of the Security Functions and the external interfaces described in the functional specification were adequately tested. The depth analysis was conducted, and it was examined that all of the subsystems and the subsystem interfaces described in the TOE design were adequately tested.

c. 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.

3.3.2 Evaluator Independent Testing

1) Evaluator Independent Test Environment

The configuration of the tests conducted by the evaluator was the same as the configuration of the developer testing..
Figure 3-1 shows the configuration of the tests conducted by the evaluator.

- MFP for the TOE
  The following devices were the subjects of the testing:
  Aficio MP 2851
  Aficio MP 3351

- Client computers
  The following Web browsers were used:
  > Internet Explorer 6.0
  > Internet Explorer 7.0
  > Internet Explorer 8.0

  The following drivers were used:
  > PCL 6 Driver V1.0.0.0
  > LAN Fax Driver V1.61

- Mail Server

Windows Server 2003 SP2 was used as the software with the SMTP server function.

- FTP Server
  Windows Server 2003 SP2 was used as the software with the FTP server function.

- SMB Server
  Windows Server 2003 SP2 was used as the software with the SMB server function.

- Fax machines
  Ricoh Aficio MP 2851 and Ricoh Aficio MP 3351 were used as the Fax Function-equipped devices.

- Telephone Switchboard Simulator
  TLE-101III (manufactured by LSI JAPAN Co., Ltd.) was used as a public line-emulating device.

The configuration of the TOE used in the evaluator testing was the same as that of the TOE used in the developer testing. For this reason, evaluator testing can be considered performed in the TOE test environment specified in the ST.

2) Outlining of Evaluator Independent Testing

Independent testing performed by the evaluator is as follows;

a. Viewpoints of Evaluator Independent Testing

The evaluator independently devised 40 test items around the following viewpoints:

(Viewpoint 1) To make the tests conducted by the developer more rigorous, conduct additional tests based on new parameters and conditions.

(Viewpoint 2) As for characteristic Security Functions for protecting communication (SSL, IPSec, S/MIME), conduct supplemental tests to ensure these functions always work effectively.

To take these viewpoints into account and to test the Security Functions and interfaces, 192 items were identified for developer testing.

- Testing will be enforced for the following behaviours, which are essential to verify correct operations of the Security Functions.
  - > Every possible combination of Access Control Function related to stored documents.
  - > Every possible combination of authorised user and authorised Security Management Function operation.
  - > Every possible combination of authentication failure conditions.
  - > Performance of all functions related to verification of software validity.
  - > Checking functions for password strength.
  - > The Lockout and Lockout Release functions following password authentication failure.
  - > The encryption functions on stored documents.
  - > The Self-Test function for encryption at TOE initialization.
  - > The Network Communication Protection Function.
- Included in testing was verification of audit log completeness and verification of the audit log records obtained.

- Testing covered all possible TOE interfaces (Operation Panel, Web interfaces, etc.)

b. Outlining of Evaluator Independent Testing

Outlining of evaluator independent testing performed by the evaluator is as follows;

For (Viewpoint 1), testing was performed using the same methods as used in the developer testing. For example:

- Use of different combinations of operating interfaces when developer testing involved testing of competing operations on the same document.
- Use of different combinations of operating interfaces and roles when developer testing involved access control testing.

For (Viewpoint 2), testing was performed using an environment and under settings that made SSL, IPSec, and S/MIME inactive. This ensured the TOE did not perform any communications not encrypted by SSL, IPSec, or S/MIME. For SSL and IPSec, packet capture software was used to check the content of communications. For S/MIME, checks were made to verify that e-mail could not be sent from the client computer.

Testing sampled from the developer testing was performed using the same methods as those used in the developer testing.

c. Result

All of the evaluator independent testing were completed correctly, and the behaviour of the TOE could be confirmed. The evaluator confirmed that all the test results were in conformity with the expected behaviour.

3.3.3 Evaluator Penetration Testing

The evaluator devised and conducted the necessary penetration testing about the possibility of exploitable concern at assumed environment of use and attack level. Outlining of Evaluator penetration testing is as follows;

1) Outlining of Evaluator Penetration Testing

Outlining of penetration testing performed by the evaluator is as follows;

a. Vulnerability of concern

The evaluator searched the deliverables and the public domain information for the potential vulnerabilities, and then identified the following vulnerabilities which require the penetration testing.

Table 3-1 Anticipated Vulnerabilities

No.	Anticipated Vulnerabilities
V1	When access to the TOE through the Web browser is established, the TOE may be accessed through direct call to the CGI, without the user to having to complete the identification and authentication process.

No.	Anticipated Vulnerabilities
V2	If a general user is registered with the same user ID as an administrator, administrator role may be assigned to the general user at login.
V3	Some interfaces may allow access to the TOE's protected assets prior to user identification and authentication through the Operation Panel or Web browser.
V4	General user IDs and administrator IDs may not be distinguished, so a general user can be registered with the same ID as an administrator, resulting in that general user obtaining administrator privileges.
V5	An unauthorised program may be introduced through the TOE's USB Port, resulting in disclosure of protected assets. Unauthorised access to the HDD may also be gained through connection of a computer to the TOE's USB Port.
V6	If an error occurs during the HDD check at start-up and then the HDD initialization process starts, the TOE's security may be weakened.
V7	Users accessing the TOE from the Operation Panel or Web browser at start-up may obtain access before the TOE's Security Functions come into effect.
V8	The TOE may open unnecessary TCP/IP ports, and the ports in use may affect enforcement of SFR.
V9	Vulnerabilities in cross-site scripting and cross-site request forgery.

b. Scope of Test Performed

The evaluator conducted the following penetration testing to determine the exploitable potential vulnerability.

Table 3-2 Overview of Penetration Testing

No.	Overview of Penetration Testing	Anticipated Vulnerability
T1	Checking opened ports: Performed a scan of the LAN port and ensured unnecessary ports were not open or opened.	V8
T2	Penetration testing on open ports: Ensured the TOE's operating system cannot be accessed directly from a remote computer via the LAN port.	V8
T3	Unauthorised access to document files through the Internet: Ensured that unauthorised users do not have access to document files, even if they specify a URL directly using delivered URL link information.	V1
T4	Obtain information using direct URLs: Ensured access via URL is denied, even if URLs for protected assets and TOE resources are derived from URLs used by the TOE.	V1
T5	Verify TOE access that does not require identification and authentication from the Web interface: Ensured no Security Functions are usable through the Web interfaces without prior identification and authentication of the user.	V3

No.	Overview of Penetration Testing	Anticipated Vulnerability
T6	Check whether access through the Operation Panel does not require identification and authentication: Ensured no Security Functions are usable through the Operation Panel without prior identification and authentication of the user.	V3
T7	Check for vulnerabilities in Web applications: Used vulnerability detection tools to check whether or not the various methods of Web access to the TOE present potential security vulnerabilities.	V9
T8	Check for TOE access vulnerabilities at initialisation: Accessed the TOE through the Web interfaces and the Operation Panel during the TOE's initialisation phase, and checked for vulnerabilities, such as the TOE becoming available before its Security Functions are in effect.	V6, V7
T9	Abuse of USB Ports: Ensured that any TOE operations other than printing and faxing are not available from computers connected to the USB Ports.	V5
T10	Operations without authentication by users without permission: Ensured users are forced to complete the identification and authentication process when user switching is attempted through the Web interface.	V2, V3
T11	Misidentification and authentication through the same ID: Ensured that users with the same ID but different roles cannot be registered.	V4

c. Result

In the conducted evaluator penetration testing, the vulnerability that attackers who have the assumed attack potential could exploit was not found.

3.4 Evaluation Result

3.4.1 Evaluation Result

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

3.4.2 Evaluator comments/Recommendations

There is no recommendations to consumers.

4. Conduct of Certification

The certification body conducted the following certification 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.

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

5. Conclusion

5.1 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 determined the TOE is satisfied the assurance requirements of EAL3 prescribed in CC Part 3.

5.2 Recommendations

5.2.1 Notes for Protection Target Assets

The following data are not the target of protection in this certification.

- The received data by the TOE using Fax Function

5.2.2 Notes for Restricted Settings and Functions

A device matches the evaluated target device only if its settings are configured and remain configured in accordance with the specified settings. This means that when a device is not configured as specified, the possibility exists that changes have been made to the device itself, so "the device is not the TOE of this certification". For specific settings and restrictions, refer to "1.2.3.1 Scope of TOE".

The availability of some TOE functions is limited. If TOE administrators cannot use those TOE functions or TOE administrators restrict those TOE functions to users, the TOE can be used securely. Refer to A.ADMIN in "2.1.3 Assumptions for Operational Environment" for details about which functions are restricted.

Before purchasing this device, consumers are required to check whether or not the settings and functions that they expect include such restricted settings and functions.

6. Glossary

The abbreviations relating to CC 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
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Functions

The abbreviations relating to TOE used in this report are listed below.

D-BOX	Name of the storage area for document data on the HDD.
FCU	Fax Controller Unit.
FTP	File Transfer Protocol.
HDD	An abbreviation for Hard Disk Drive. Indicates the HDD installed in the TOE.
Ic Hdd	A hardware device that encrypts the data to be written on HDD and decrypts the data to be read from HDD.
Ic Key	A chip that contains a microprocessor for encryption processing and EEPROM where a private key for secure communication is held. The Ic Key holds the keys for validity authentication and encryption processing, and a random number generator.
IPSec	Security Architecture for Internet Protocol. It is a protocol to provide the functions of data tampering protection and hiding secret data by each IP packet by using cryptographic technology.
MFP	An abbreviation for digital multi function product.
NVRAM	Non-Volatile Random Access Memory, where MFP control data governing MFP operations is stored.
PSTN	An abbreviation for Public Switched Telephone Networks.
RAM	A volatile memory medium used for image processing.
S/MIME	Secure / Multipurpose Internet Mail Extensions It is a standard of an encryption of E-mail by the public key system and the digital signature.
SSL	Secure Socket Layer It is a protocol for secure communications.
USB	It is an abbreviation of Universal Serial Bus, and one of the serial bus standards to connect various peripherals with the computer.

The definition of terms used in this report is listed below.

Address Book	A database containing general user information for each general user.
Administrator	One of the authorised TOE users who manages the TOE. Administrators are given administrator roles and perform administrative operations accordingly. Up to four administrators can be registered, and each administrator is given one or more administrator roles.
Administrator Role	Management Functions given to administrators. There are four types of administrator role: user administration, machine administration, network administration and file administration. Each administrator role is assigned to a registered administrator.
Basic authentication	It is the most basic user authentic method that identifies the user on the Internet and verifies validity. It is defined by the HTTP specification, and a lot of web servers and web browsers can use it. It authorises access by verifying user names and passwords.
Password Complexity Setting	The minimum combination of character types that can be registered in passwords. There are four character types: upper-case letters, lower-case letters, numbers, and symbols. There are Level 1 and Level 2 Password Complexity Setting. Level 1 requires passwords to include a combination of more than two types of character. Level 2 requires passwords to include a combination of more than three types of character.
Deliver to Folder	A function that sends document data from the TOE to folders on an SMB or FTP server via a network.
Direct Print Function	A function that prints print data received by the TOE.
Document Data	Electronic data sent to the MFP by authorised MFP users who perform either of the following operations. 1. Scanning from paper and digitizing. 2. Received as print data and then converted by the MFP into a format that can be processed by the MFP.
Document Data ACL	An access control list of general users that is set for each document data.
Document Data Default ACL	An items of general user information. The default value that is set for the document data ACL of a new document data to be stored.
Ethernet	It is one of the standards of the computer network, and it is most generally used at an office and a home of all over the world.
External Networks	Networks that are not managed by the organization that manages the MFP. Generally, indicates the internet.
LAN-Fax Transmission	A function that faxes document data from a client computer via the TOE when the client computer is connected to the TOE via a network or USB Ports.
File Administration	An administrator role assigning responsibility for management of the D-BOX, where document data is stored on the TOE, and management of the document data ACL, which is the list that controls the access to the document data. The file administrator is a person who has the role of file administration
FTP Server	A server for sending files to a client computer and receiving files from a client computer using File Transfer Protocol.

General User	One of the authorised TOE users who uses the Basic Functions of the TOE.
General User Information	A database containing information about general users as data items that include the general user ID, general user authentication information, document data default ACL, and S/MIME user information.
Immediate Transmission	A function that dials first, then faxes data while scanning the original.
Internal Networks	Networks managed by an organisation that has an MFP. Normally refers to an office LAN environment established as an intranet.
Internet Fax	A function that reads a fax original then converts the scanned image to an e-mail format for sending as data over the Internet to a machine with an e-mail address.
IP-Fax	A function that sends and receives document files between two faxes that are directly connected to a TCP/IP network. It can also send document files to a fax that is connected to a telephone line.
IPv4 Protocol	It is a procedure or a rule provided through the widely-used internet to exchange data between computers now. It uses the 32 bits address notation.
IPv6 Protocol	It is an expansion of the address space of IPv4, and is strengthening of the security of IPv4. It uses the 128 bits address notation.
Lockout	A function that prohibits access to the TOE to the specific user IDs.
Machine Administration	An administrator role that assigns responsibility for machine management and performing audits. The machine administrator is a person who has the machine management role
Memory Transmission	A function that stores scanned data of an original in memory and then dials and faxes that data at a later time.
MFP Control Data	A generic term for a set of parameters that controls the operation of an MFP.
MFP Control Software	Software installed in the TOE that can identify TOE components such as System/Copy, Network Support, Scanner, Printer, Fax, Web Support, Web Uapl and Network Doc Box. Manages the resources for units and devices that comprise the MFP and controls their operation.
Minimum Password Length	The minimum number of digits that can be registered in passwords.
Network Administration	An administrator role assigning responsibility for management of the TOE's network connections. The network administrator is a person with network management responsibility.
Operation Panel	A display-input device that consists of a touch screen LCD, key switches, and LED indicators, and is used for MFP operation by users. Also known as an "Operation Panel Unit".
Packet Capture Software	It is software that can record and inspect contents by intercepting the network communication’s flows.
Print Data	The document files in a client computer that are sent to the TOE from a client computer to be printed or faxed. Drivers must be installed in the client computer in advance: a printer driver for printing and a fax driver for faxing. Print data is received by the TOE through the Network Unit or USB Port.

Print Setting	Print Settings for printed output, including paper size, printing magnification, and custom information (such as duplex or layout settings). Print Settings for stored document data can be updated by the user who prints the document data.
Processor	It is computer's hardware to execute software. It is composed of the computing unit, the peripheral circuitry, and the memory that stores instructions and information.
Responsible Manager for MFP	A person in an organization in which MFPs are placed and who has the authority to assign MFP administrators and a supervisor (or the person who is responsible for the organisation). E.g., MFP purchasers, MFP owners, a manager of the department in which MFPs are placed, a person who is in charge of IT department.
S/MIME User Information	Information about each general user that is required for using S/MIME. Includes E-mail address, user certificates and specified value for S/MIME use.
Sending by E-mail	A function that sends e-mail with the attached document data from the TOE.
SMB Server	A server for sharing files with a client computer using Server Massage Block protocol.
SMB Protocol	It is called Server Message Block Protocol. It is a procedure or a rule provided to exchange data between computers.
SMTP Server	A server for sending E-mail using Simple Mail Transfer Protocol.
Store and Print Function	A function that converts print data received by the TOE into document data and stores it in the D-BOX. The document data stored in D-BOX can be printed at a later time.
Stored Data Protection Function	A function that protects document data stored on the HDD from leakage.
Stored Documents Fax Transmission	A function that faxes document data stored earlier in the D-BOX.
Supervisor	One of the authorised TOE users who manages a password of administrator.
User Administration	An administrator role assigning responsibility for management of general users. The user administrator is a person who has the user management role.

7. Bibliography

[1] Aficio MP 2851/3351 series with Fax Option Type 3351 Security Target Version 1.00 (Jun. 17, 2010) RICOH COMPANY, Ltd.

[2] IT Security Evaluation and Certification Scheme, May 2007, Information-technology Promotion Agency, Japan CCS-01

[3] IT Security Certification Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-02

[4] Evaluation Facility Approval Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 3.1 Revision 1, September 2006, CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components Version 3.1 Revision 2, September 2007, CCMB-2007-09-002

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components Version 3.1 Revision 2, September 2007, CCMB-2007-09-003

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 3.1 Revision 1, September 2006, CCMB-2006-09-001 (Japanese Version 1.2, March 2007)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components Version 3.1 Revision 2, September 2007, CCMB-2007-09-002 (Japanese Version 2.0, March 2008)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components Version 3.1 Revision 2, September 2007, CCMB-2007-09-003 (Japanese Version 2.0, March 2008)

[11] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 3.1 Revision 2, September 2007, CCMB-2007-09-004

[12] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 3.1 Revision 2, September 2007, CCMB-2007-09-004 (Japanese Version 2.0, March 2008)

[13] RICOH COMPANY, Ltd. Aficio MP 2851/3351 series with Fax Option Type 3351 Evaluation Technical Report Version 1.6, June 18, 2010, Information Technology Security Center