Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2009-06-08 (ITC-9256)
Certification No.	C0244
Sponsor	RICOH COMPANY, LTD.
Name of TOE	Japan: Ricoh imagio MP 2550/3350 series Overseas: Ricoh Aficio MP 2550/3350 series Savin 9025/9033 series Lanier LD425/LD433 series Lanier MP 2550/3350 series Gestetner MP 2550/3350 series nashuatec MP 2550/3350 series RexRotary MP 2550/3350 series infotec MP 2550/3350 series
Version of TOE	Following software and hardware

System/Copy:	1.14	Web Support:	1.52
Network Support:	7.23	Web Uapl:	1.10
Scanner:	1.11	Network Doc Box:	1.10C
Printer:	1.05	Ic Key:	1100
Fax:	05.00.00	Ic Hdd:	01

PP Conformance	None
Conformed Claim	EAL3
Developer	RICOH COMPANY, LTD.
Evaluation Facility	Information Technology Security Center Evaluation Department

This is to report that the evaluation result for the above TOE is certified as follows.
2010-02-25

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

"Japan: Ricoh imagio MP 2550/3350 series, Overseas: Ricoh Aficio MP 2550/3350 series, Savin 9025/9033 series, Lanier LD425/LD433 series, Lanier MP 2550/3350 series, Gestetner MP 2550/3350 series, nashuatec MP 2550/3350 series, RexRotary MP 2550/3350 series, infotec MP 2550/3350 series Version System/Copy 1.14, Network Support 7.23, Scanner 1.11, Printer 1.05, Fax 05.00.00, Web Support 1.52, Web Uapl 1.10, Network Doc Box 1.10C, Ic Key 1100, Ic Hdd 01" 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 "Japan: Ricoh imagio MP 2550/3350 series, Overseas: Ricoh Aficio MP 2550/3350 series, Savin 9025/9033 series, Lanier LD425/LD433 series, Lanier MP 2550/3350 series, Gestetner MP 2550/3350 series, nashuatec MP 2550/3350 series, RexRotary MP 2550/3350 series, infotec MP 2550/3350 series Version System/Copy 1.14, Network Support 7.23, Scanner 1.11, Printer 1.05, Fax 05.00.00, Web Support 1.52, Web Uapl 1.10, Network Doc Box 1.10C, Ic Key 1100, Ic Hdd 01" (hereinafter referred to as "the TOE") conducted by Information Technology Security Center Evaluation Department (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 "persons who are responsible for management of the TOE in the organisation that uses the 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:	Japan:	Ricoh imagio MP 2550/3350 series
	Overseas:	Ricoh Aficio MP 2550/3350 series
		Savin 9025/9033 series
		Lanier LD425/LD433 series
		Lanier MP 2550/3350 series
		Gestetner MP 2550/3350 series
		nashuatec MP 2550/3350 series
		RexRotary MP 2550/3350 series
		infotec MP 2550/3350 series
Version:		System/Copy 1.14
		Network Support 7.23
		Scanner 1.11
		Printer 1.05
		Fax 05.00.00
		Web Support 1.52
		Web Uapl 1.10
		Network Doc Box 1.10C
		Ic Key 1100
		Ic Hdd 01
Developer:		RICOH COMPANY, LTD.

The "~ series" in the product names indicates it is the generic name for multiple products. The following are the specific product names indicated by "~ series". These products are divided into two: products with Fax Function, and products without Fax Function. When an "F" is suffixed to the product name, it indicates the product has the Fax Function, and when an "F" is not suffixed, the product does not have the Fax Function.

Japan:	Ricoh imagio MP 2550SP
	Ricoh imagio MP 2550SPF
	Ricoh imagio MP 3350SP
	Ricoh imagio MP 3350SPF
Overseas:	Ricoh Aficio MP 2550
	Ricoh Aficio MP 2550SP
	Ricoh Aficio MP 2550SPF
	Ricoh Aficio MP 3350
	Ricoh Aficio MP 3350SP
	Ricoh Aficio MP 3350SPF
	Savin 9025
	Savin 9025SP
	Savin 9025SPF
	Savin 9033
	Savin 9033SP
	Savin 9033SPF
	Lanier LD425
	Lanier LD425SP
	Lanier LD425SPF
	Lanier LD433

Lanier LD433SP
Lanier LD433SPF
Lanier MP 2550
Lanier MP 3350
Gestetner MP 2550
Gestetner MP 2550SP
Gestetner MP 2550SPF
Gestetner MP 3350
Gestetner MP 3350SP
Gestetner MP 3350SPF
nashuatec MP 2550
nashuatec MP 2550SP
nashuatec MP 3350
nashuatec MP 3350SP
RexRotary MP 2550
RexRotary MP 2550SP
RexRotary MP 3350
RexRotary MP 3350SP
infotec MP 2550
infotec MP 2550SP
infotec MP 3350
infotec MP 3350SP

1.2.2 Product Overview

The target product in this certification is a digital MFP (hereafter MFP), made by RICOH COMPANY, LTD., that provides the functions of copier, scanner, printer and fax (optional). Those functions are for digitising the paper document files, managing the document files and printing the document files.

This product is an I/O device that incorporates the functionality of copier, scanner, fax and printer. In general, this product is connected to an office LAN and is used to input, store and output the Document Data. This product protects the internally stored Document Data from the unintentional disclosure and operation, and prevents Document Data, which are sent and received between the MFP and a client, from leakage.

1.2.3 Scope of TOE and Security Functions

1.2.3.1 Scope of TOE

The TOE is the target in this certification, and it is configured as it satisfies all of the following. If the configuration of the product does not satisfy any of the following, it means that the product is not the TOE. Once its Service Mode Lock is cancelled and its Maintenance Function is used, it leaves the possibility that the product is no longer the TOE (since there might be a possibility that the Maintenance Function changes the product itself).

- Do not set Service Mode Lock to "Off".
- Use IPv4 protocol. (Do not use IPv6 protocol.)
- Do not use IP-Fax and Internet Fax Function.
- Use Basic Authentication for Identification and Authentication Function. (Do not use the authentication except for Basic Authentication.)

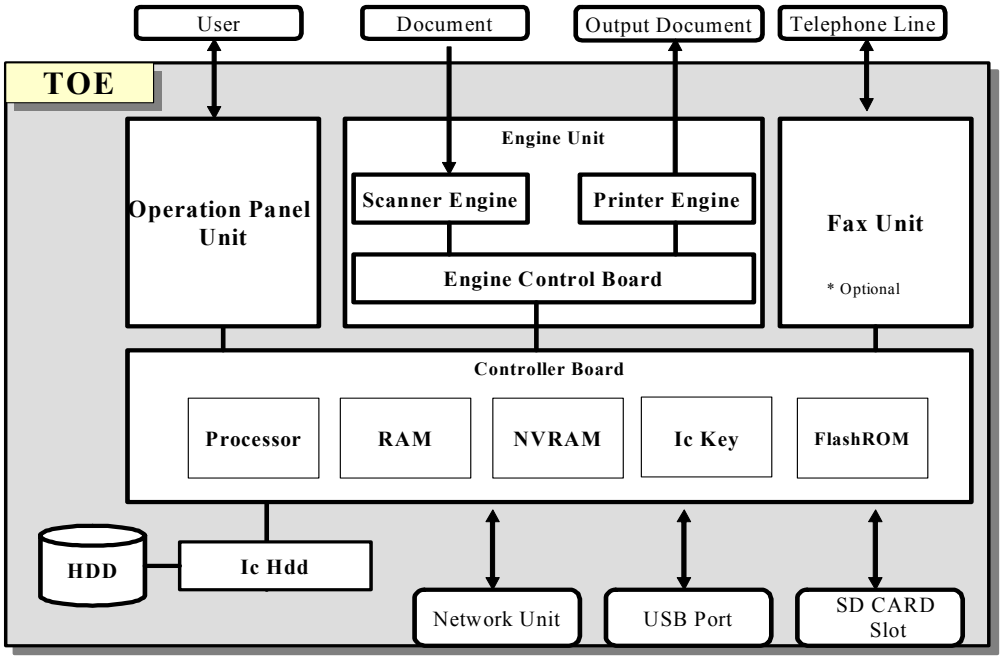

Fig.1-1 TOE Configuration

Figure 1-1 shows the physical items that constitute the TOE. The brief description of each item is as follows:

- Operation Panel Unit (hereafter Operation Panel)
  The Operation Panel is an interface device that is equipped on the TOE and is used by TOE users for TOE operation. It is configured with key switches, LED, touch screen LCD, and the Operation Panel Control Board.

- Engine Unit
  The Engine Unit consists of a Scanner Engine, Printer Engine and Engine Control Board. The Scanner Engine is an input device to read the paper documents. The Printer Engine is an output device to print and output the paper documents.

- Fax Unit (Optional)
  The Fax Unit is a device that has a modem function and sends and receives fax data when connected to a telephone line.

- Controller Board
  The Controller Board contains Processors, RAM, NVRAM, Ic Key and FlashROM. The brief description of each item is as follows:
  [Processor] A processor that carries out the processing such as arithmetic processing according to software.
  [RAM] A volatile memory that is used for an image processing memory.
  [NVRAM] A non-volatile memory in which MFP Control Data to configure the MFP operation is stored.
  [Ic Key] A security chip that has the functions of random number generation and encryption key generation, and is used to detect the tampering of MFP Control Software.
  [FlashROM] A memory in which MFP Control Software is installed. MFP Control Software has the elements that identify the TOE such as System/Copy, Network Support, Scanner, Printer, Fax, WebSupport, Web Uapl and Network Doc Box.

- Ic Hdd
  Ic Hdd is a security chip that has the functions to encrypt the information to be stored on HDD, and to decrypt the information to be read from HDD.

- HDD
  HDD is a hard disk drive in which the image data, and user information used for identification and authentication are written. The area where image data are stored as Document Data is called D-BOX.

- Network Unit
  The Network Unit is an interface board for Ethernet (100BASE-TX/10BASE-T) networks.

- USB Port
  The USB Port is used to connect a client PC to the TOE with USB, and is used for printing or faxing from that client PC.

- SD CARD Slot
  SD CARD Slot is an interface that is used to enable the Stored Data Protection Function when installing the TOE, and is used for the maintenance work. However, since the maintenance work is not assumed in this certification, this is used only when installing the TOE.

1.2.3.2 Operation Overview of TOE

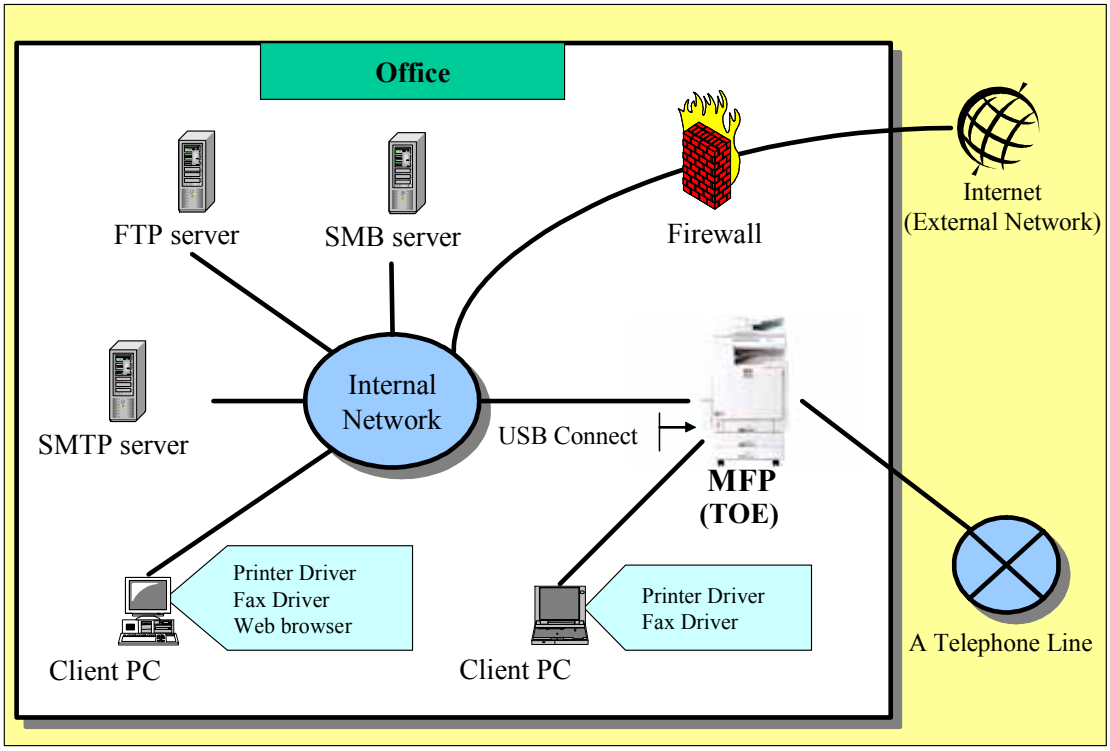

Fig. 1-2 Example of Usage Environment of TOE

The TOE, for example, is used in the environment as Figure 1-2, and its main purpose is to input, output, and store image data. The following are the methods to input and output image data. The TOE can simply output the data that were put into the TOE, and can also keep the data.

- How to input image data to the TOE
  > Scan the original optically using Scanner Engine.
  > Receive the data from the client PC via Network Unit or USB Port.
  > Receive the data from a telephone line via Fax Unit.

- How to output image data from the TOE
  > Print image data using Printer Engine.
  > Transfer image data to client PC from Network Unit.
  > Send image data attached to e-mail from Network Unit.
  > Send image data either to an FTP Server using FTP protocol, or to an SMB Server using SMB protocol.
  > Fax image data from Fax Unit via a telephone line.

1.2.3.3 TOE Function

The TOE has Copy Function, Printer Function, Fax Function, Scanner Function, Document Server Function, Management Function and Web Service Function. The following are the descriptions of each function:

1) Copy Function
   The Copy Function is used to scan the original as image data using Scanner Engine and to print out the image data in accordance with the specified Print Settings using Printer Engine.
   The scanned image data can be stored in D-BOX as Document Data (except for the Scanner Function).

2) Printer Function
   The Printer Function is used to receive the Print Data sent from a client PC via Network Unit or USB Port, and to print out the data using Direct Print Function or Store and Print Function.
   Direct Print Function simply prints out the received Print Data using Printer Engine.
   Store and Print Function stores (does not print out immediately) the Print Data in D-BOX as Document Data (except for the Scanner Function). The actual printout is performed using "8) Document Server Function (Management)", which is described later.

3) Fax Function (Reception)
   The Fax Function (Reception) is used to receive fax data from Fax Unit and either to print out or store the fax data.
   When printing the fax data, it simply prints out the received fax data using Printer Engine.
   When storing the fax data, it converts the received fax data into the Fax Reception Data and then stores it in D-BOX (does not print out immediately). The actual printout is performed using "8) Document Server Function (Management)", which is described later.

   *Note: The received fax data by the TOE is not the protected target in this certification. (Refer to "5.2.1 Notes for Protection Target Assets")

4) Fax Function (Immediate Transmission/Memory Transmission)
   The Fax Function (Immediate Transmission/Memory Transmission) is used to scan the original as image data using Scanner Engine and to send the image data from Fax Unit using Immediate Transmission or Memory Transmission.
   Immediate Transmission sends the generated image data to the destination fax sequentially while scanning the original, after connecting to the destination fax.
   Memory Transmission completes scanning the original before connecting to the destination fax. Then, after scanning the original, it connects to the destination fax and sends the image data.

5) Fax Function (Stored Documents Fax Transmission)
The Fax Function (Stored Documents Fax Transmission) is used to send the "specified Document Data stored in D-BOX" from Fax Unit.

6) Fax Function (Fax Transmission from PC)
The Fax Function (Fax Transmission from PC) is used to receive Print Data from the client PC via Network Unit or USB Port, and to send the Print Data from Fax Unit.

7) Document Server Function (Scan)
The Document Server Function (Scan) is used to scan the original using Scanner Engine as image data, and to store the scanned data as Document Data in D-BOX (except for the Scanner Function).

8) Document Server Function (Management)
The Document Server Function (Management) is used to perform the specified process (described below) to one of the "specified stored Document Data in D-BOX (except for the Scanner Function) or the Fax Reception Data".

- Print (Printing using Printer Engine)
- Delete (Deleting the stored data in D-BOX)
- Download (Transferring data to client PC via Network Unit)

*Note: The Document Data (for Scanner Function use only) generated using the "Scanner Function (Scan)" cannot be stored using "Document Server Function (Management)", but can be stored using "Scanner Function (Management)".

9) Scanner Function (Scan)
The Scanner Function (Scan) is used to scan the original as image data using Scanner Engine, and then to send it by e-mail, deliver to folder or store.
For sending by e-mail, this function sends the image data attached to e-mail to the specified e-mail address from Network Unit.
For Deliver to Folder, this function transfers the image data to the specified folder using the FTP protocol or SMB protocol from Network Unit.
For storing, this function stores image data as Document Data (for Scanner Function use only) in D-BOX.

*Note: The management of the Document Data generated using this function differs from the management of the Document Data generated using other functions. The Document Data generated using this function is managed using the "Scanner Function (Management)", and the Document Data generated using other functions are managed using the "Document Server Function (Management)".

10) Scanner Function (Management)
The Scanner Function (Management) is used to perform the specified process (described below) to the "specified Document Data (for Scanner Function use only) in D-BOX".

- Send (Sending by e-mail or Deliver to Folder of the "Scanner Function (Scan)")
- Delete (Deleting Document Data in D-BOX)
- Download (Transferring Document Data to client PC via Network Unit)

*Note: This function only manages the Document Data stored using the "Scanner Function (Scan)". The "Document Server Function (Management)" manages the Document Data stored using other functions.

11) Management Function
The Management Function is used to configure the following settings: the TOE machine settings, settings for network connection, settings for authorised user information, and settings for the information to restrict the use of the Document Data. A user's ability to manage this information is determined in accordance with that user's authorised role (General User, Administrator, or Supervisor).

12) Web Service Function
The Web Service Function is used to operate the TOE remotely from the web browser of a client PC by authorised TOE users (General Users, Administrators or Supervisor).
Although the Web Service Function is available for the functions described above in "1) Copy Function" ~ "11) Management Function", there are some functions that are not available using this Web Service Function.

1.2.3.4 TOE Security Function

1) Identification and Authentication Function, Document Data Access Control Function
"1.2.3.3 TOE Function" includes the operation to read the Document Data (to take out the data, which are stored as Document Data in the TOE, in some ways such as printing or sending), and the operation to delete the Document Data. The TOE has the functions to identify and authenticate the TOE operators, and control the access so that these operations on Document Data are not performed despite the owner's intention.

2) Stored Data Protection Function
The TOE has the function to encrypt the data that are written onto HDD in order to prevent the information leakage from HDD after discarding the TOE, etc.

3) Network Communication Data Protection Function
The TOE has the function to encrypt the data the TOE communicates via the Internal Networks in order to prevent the information leakage by eavesdropping on the Internal Networks.
The object is limited to the data the TOE communicates via the Internal Networks, and the data the TOE communicates via USB or telephone lines are not included.

4) Telephone Line Intrusion Protection Function
The TOE has the function to accept only permitted communication from telephone lines in order to prevent the TOE from being abused via telephone lines.

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

6) Audit Function
The TOE has the function to record the events as audit logs in the case of the event occurrence that is usable for detecting the security intrusion.

7) Security Management Function
The TOE provides the function to configure the information related to the performance of security functions. The configurable information is respectively determined according to the role of the authorised TOE users (General User, Administrator, and Supervisor) so that the security is maintained without any interference.

8) Service Mode Lock Function
This is a function to prohibit the operation of Maintenance Function unless the Machine Administrator explicitly allows to do so.

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 "imagio MP 2550/3350 series, Aficio MP 2550/3350 series 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. imagio MP 2550/3350 series, Aficio MP 2550/3350 series 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. Certification review is also prepared for those concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report dated 2010-02 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.

2. Summary of TOE

2.1 Security Problem and assumptions

Problems should be solved by TOE and necessary assumptions are as follows;

2.1.1 Threat

This TOE assumes such threats presented in Table 2-1 and provides functions for countermeasure to them.

Table 2-1 Assumed Threats

Identifier	Threat
T.ILLEGAL_USE	Attackers may read or delete the Document Data by gaining unauthorised access to the TOE from the TOE external interfaces (Operation Panel, Network Interface, USB Interface or SD CARD Interface).
T.UNAUTH_ACCESS	Authorised TOE users may go beyond the bounds of the authorised usage and access to Document Data from the TOE external interfaces (Operation Panel, Network Interface or USB Interface) that are provided to the authorised TOE users.
T.ABUSE_SEC_MNG	Persons who are not authorised to use Security Management Function may abuse the Security Management Function.
T.SALVAGE	Attackers may take HDD out of the TOE and disclose Document Data.
T.TRANSIT	Attackers may illegally obtain, leak or tamper Document Data and Print Data that are sent or received by the TOE via the Internal Networks. *Note: The "Document Data and Print Data that are sent or received by the TOE" can exist on the USB interfaces and telephone lines, however, obtaining and tampering the data on these are not considered as threats.
T.FAX_LINE	Attackers may gain unauthorised access to the TOE from telephone lines.

2.1.2 Organisational Security Policy

Organisational security policy required in use of the TOE is presented 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 FlashROM in the TOE.

2.1.3 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 2-3.
The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

Table 2-3 Assumptions in Use of the TOE

Identifier	Assumptions
A.ADMIN	Administrators will have adequate knowledge to operate the TOE securely in the roles assigned to them, and guide General Users operate the TOE securely. Additionally, Administrators will not carry out any malicious acts using Administrator permissions. *Note: The "adequate knowledge to operate the TOE securely" includes the following: - Do not use the following function. > Back up/Restore Address Book - Use the TOE with the following settings maintained. > Do not set Service Mode Lock to "Off" > Use the IPv4 protocol. (Do not use the IPv6 protocol.) > Do not use IP-Fax and Internet Fax > Use Basic Authentication for Identification and Authentication Function. (Do not use the authentication except for Basic Authentication.)
A.SUPERVISOR	Supervisor will have adequate knowledge to operate the TOE securely in the role assigned to him/her, and will not carry out any malicious acts using Supervisor permissions.
A.NETWORK	The Internal Networks will be protected from the External Networks when the TOE-connected networks are connected to the External Networks such as the Internet.

2.1.4 Documents Attached to Product

The identification of documents attached to the TOE is listed below. TOE users are required full understanding of following documents and compliance with descriptions.

For Japan (Japanese version)

- Printed documents

> imagio MP 3350/2550 series Operating Instructions <Security Reference> (written in Japanese) (D019-7950)

> Notes for Users (written in Japanese) (D015-7103)

> For imagio MP 3350/2550 series Users (written in Japanese) (D019-7630)

> imagio MP 3350/2550 series Manuals for This Machine (written in Japanese) (D019-7501)

> imagio MP 3350/2550 series Quick Guide (written in Japanese) (D019-7654)

> imagio MP 3350/2550 series Operating Instructions <About This Machine> (written in Japanese)
(D019-7750)

> imagio MP 3350/2550 series Operating Instructions <Troubleshooting> (written in Japanese)
(D019-7800)

> Notes for Security Functions (written in Japanese)
(D011-7750A)

> Notes for Administrators: Using this Machine in a CC-Certified Environment (written in Japanese)
(D019-7954)

- Documents in CD-ROM

> Operating Instructions, Drivers & Utilities imagio MP 3350/2550 (written in Japanese)
(D017-7500A)

For North America (English version)

- Printed documents

> 9025/9025b/9033/9033b
MP 2550/MP 2550B/MP 3350/MP 3350B
LD425/LD425B/LD433/LD433B
Aficio MP 2550/2550B/3350/3350B
Operating Instructions About This Machine
(D019-7753)

> 9025/9025b/9033/9033b
MP 2550/MP 2550B/MP 3350/MP 3350B
LD425/LD425B/LD433/LD433B
Aficio MP 2550/2550B/3350/3350B
Operating Instructions
Troubleshooting
(D019-7803)

> Notes for Users Back Up/Restore Address Book
(D015-7107)

> Notes for Administrators: Using this Machine in a CC-Certified Environment
(D019-7955)

- Documents in CD-ROM

> Manuals
9025/9025b/9033/9033b
MP 2550/3350/2550B/3350B
LD425/LD425B/LD433/LD433B
Aficio MP 2550/3350/2550B/3350B
(D017-7502A)

> Manuals for Administrators
Security Reference
9025/9025b/9033/9033b
MP 2550/3350/2550B/3350B
LD425/LD425B/LD433/LD433B
Aficio MP 2550/3350/2550B/3350B
(D017-7504A)

> Manuals for Administrators
Security Reference Supplement
9025/9025b/9033/9033b
MP 2550/2550B/3350/3350B
LD425/LD425B/LD433/LD433B
Aficio MP 2550/2550B/3350/3350B
Notes for Security Functions
(D017-7522)

For Europe (English version)

- Printed documents

> Manuals for This Machine
(D019-7506)

> Notes for Users Back Up/Restore Address Book
(D015-7109)

> Notes for Administrators: Using this Machine in a CC-Certified Environment
(D019-7956)

- Documents in CD-ROM

> Manuals General Setting Manuals
MP 2550/3350/2550B/3350B
Aficio MP 2550/3350/2550B/3350B
(D017-7510)

> Manuals Functions and Network Manuals
MP 2550/3350/2550B/3350B
Aficio MP 2550/3350/2550B/3350B
(D017-7514A)

> Manuals for Administrators Security Reference
MP 2550/3350/2550B/3350B
Aficio MP 2550/3350/2550B/3350B
(D017-7512)

> Manuals for Administrators
Security Reference Supplement
9025/9025b/9033/9033b
MP 2550/2550B/3350/3350B
LD425/LD425B/LD433/LD433B
Aficio MP 2550/2550B/3350/3350B
Notes for Security Functions
(D017-7522)

For Asia (English version)

- Printed documents

> MP 2550/MP 2550B/MP 3350/MP 3350B
MP 2550/MP 2550B/MP 3350/MP 3350B
Aficio MP 2550/2550B/3350/3350B
MP 2550/MP 2550B/MP 3350/MP 3350B
Operating Instructions
About This Machine
(D019-7755)

> MP 2550/MP 2550B/MP 3350/MP 3350B
MP 2550/MP 2550B/MP 3350/MP 3350B
Aficio MP 2550/2550B/3350/3350B
MP 2550/MP 2550B/MP 3350/MP 3350B
Operating Instructions
Troubleshooting
(D019-7805)

> Notes for Users Back Up/Restore Address Book
(D015-7107)

> Notes for Administrators: Using this Machine in a CC-Certified Environment
(D019-7955)

- Documents in CD-ROM

> Manuals
MP 2550/3350/2550B/3350B
Aficio MP 2550/3350/2550B/3350B
(D017-7506A)

> Manuals for Administrators Security Reference
MP 2550/3350/2550B/3350B
Aficio MP 2550/3350/2550B/3350B
(D017-7508A)

> Manuals for Administrators
Security Reference Supplement
9025/9025b/9033/9033b
MP 2550/2550B/3350/3350B
LD425/LD425B/LD433/LD433B
Aficio MP 2550/2550B/3350/3350B
Notes for Security Functions
(D017-7522)

2.1.5 Configuration Requirements

The TOE is connected to the following external environment as Figure 1-2 shows. The entire following external environment is not required but it depends how the TOE is used.

- Client PC connected to the TOE via a USB Port
- Client PC connected to the TOE via Ethernet
- SMTP Server connected to the TOE via Ethernet
- FTP Server connected to the TOE via Ethernet
  (An FTP Server has to support the IPSec communication)
- SMB Server connected to the TOE via Ethernet
  (An SMB Server has to support the IPSec communication)
- Public telephone line or equivalent line

When using the TOE from client PCs via drivers, the drivers, which are acquired from the Web page specified in the documents identified in "2.1.4 Documents Attached to Product", are required. The information about the drivers at the time of this evaluation is as follows:

- RPCS Driver V7.66 for domestic machines
- RPCS Driver V7.67 for overseas machines

- PC Fax Driver V1.59 for domestic machines
- LAN Fax Driver V1.60 for overseas machines

Internet Explorer 6.0 or later is required for the "client PCs connected to the TOE via Ethernet" when using the TOE from the browser.

2.2 Security Objectives

The TOE counters the threats in 2.1.1, and satisfies the organisational security policy in 2.1.2 with its security functions as described below.

2.2.1 Countermeasure to T.ILLEGAL_USE, T.UNAUTH_ACCESS, T.ABUSE_SEC_MNG

These threats are countered with a sequence of countermeasure, identification and authentication, and access control.
For the persons (operators) who attempt to use the TOE, the TOE requires them to enter their user IDs and the authentication information (passwords). Then it verifies the integrity of the entered user ID and authentication information.
The TOE has the following functions to counter the impersonation by the attempt of entering the user ID and authentication information.

- According to the Lockout Policy, if the number of consecutive unsuccessful attempts to identify and authenticate a particular user ID meets the Number of Attempts before Lockout, the TOE lockouts this user ID (prevents the TOE from being used with the ID).

- When accepting users to register or change their authentication information, the TOE only accepts the passwords, which satisfy the conditions of Minimum Password Length and Complexity Setting for Password, as the authentication information.

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

(1) If the user ID and authentication information cannot be verified, the TOE does not allow the operator to use the TOE functions.

    Since the users who are not allowed to use the TOE do not have the valid user ID and authentication information, (1) indicates the unauthorised TOE users cannot use the TOE functions. This is the countermeasure to T.ILLEGAL_USE.

(2) If the user ID and authentication information are verified, the TOE identifies the operator by the user ID, and then identifies the user's User Role by the user ID. After the TOE identifies these, the TOE allows the user to use the TOE functions. The following are the roles that are identified by the TOE.
    - General User
    - Administrator
    - Supervisor

    For Administrators, the user can also be identified by the any of the following roles. The following roles are not exclusive, and more than one role can be assigned to one Administrator user ID.
    - User Administration
    - Machine Administration
    - Network Administration
    - File Administration

After the TOE performs (2), the operator gives the instruction to the TOE of what he/she wants to operate. The instruction may include the "operation on Document Data" or "use of the Management Function". Either (3) or (4) is processed depending on the instruction.

(3) For the instruction including the "operation on Document Data", the TOE determines if the instructed operation is authorised for the user or not, based on the user ID and operator's role, authenticated in (2). The TOE follows the instruction and performs the operation only if it is authorised. The TOE determines the instructed operation based on the following criteria.
- When the operator's role is the General User
  Each Document Data has the information (Document Data ACL) that determines who to allow the operation and what kind of operation to allow (there are some phases, such as to allow only to read, to change Print Setting, to delete, and to operate on the Document Data ACL). The TOE determines if the instructed operation is authorized or not, based on the user ID that is authenticated in (2) and the Document Data ACL.
- When the operator's role is not the General User
  If the operator's role identified in (2) is the Administrator, and has also the role of File Administrator, it is allowed for the operator to delete the arbitrary data. If not, no operations on Document Data are allowed.

Since (3) limits the operation on Document Data by the authorised TOE user according to the access control (if the user is the General User who are authorised with the Document Data ACL or not, OR if the user is authorised Administrator or not), the TOE counters T.UNAUTH_ACCESS.

(4) For the instruction including the "use of the Management Function", the TOE applies to the "Security Management Function", based on the user ID and the operator's role authenticated in (2).
The Security Management Function is the operations on the following data the TOE has.
- Document Data ACL
- Registration Information about Users
- Lockout Policy (Number of consecutive unsuccessful attempts before Lockout, whether or not to release Lockout based on the elapsed time, Lockout Release Timer)
- System date, time
- HDD Encryption Key
- Audit Log
- Service Mode Lock Function
- Password Policy (Minimum Password Length, and the minimum of combination of character types for password)

The TOE allows the operations on these data provided that the operator's role is the Administrator or Supervisor[*1]. However, the TOE also allows General Users to perform the operations on Document Data provided that the operator can leaves the security maintained as described below.
- It is allowed for the document file owners, and the General Users who are set for each Document Data to perform the operations on Document Data ACL (except for changing the document file owners).
- It is allowed for the General Users to change their own "authentication information", "Document Data Default ACL (for other persons' Document Data)" and "S/MIME User Information".

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

[*1] Some operations may not be allowed for the Administrators or Supervisor. There is a rule that determines which operation is allowed for the detailed Administrator (User Administration, Machine Administration, Network Administration and File Administration) and Supervisor. The detail of this rule is beyond the scope of this document.

2.2.2 Countermeasure to T.SALVAGE

The TOE protects Document Data from leakage by making it difficult to understand unless the Document Data is accessed in the normal way (using the function described in "1.2.3.3 TOE Function" from the Operation Panel or Client PC) to counter T.SALVAGE. (Stored Data Protection Function)
This function is accomplished by encrypting the data just before writing it on HDD with the following cryptographic algorithm and cryptographic key size, and by decrypting the data just after reading it from HDD.

- Cryptographic algorithm: AES
- Key size: 256 bits

2.2.3 Countermeasure to T.TRANSIT

The TOE protects the Document Data and image data that are sent or received by the TOE via the Internal Networks from interceptions and tampering to counter T.TRANSIT.
The used mechanism, SSL, IPSec or S/MIME, varies depending on the type of protected data. Although S/MIME is accomplished by the TOE functions, the communication path for SSL is established by the cooperation of the TOE and client PCs, and the communication path for IPSec is established by the cooperation of TOE and either SMB Server or FTP Server.
The protected scope depends on the mechanism used for the data protection. The following Tables, 1-1 (1) - (3), show the specific scopes.

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

Target data
Print Data that are sent to Network Unit from client PC via Internal Networks using the "Printer Function" (except for via USB Ports)
Protection mechanism and protected scope
The Internal Networks between client PC and Network Unit are protected by SSL mechanism

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

Target data
Print Data that are sent to Network Unit from client PC via Internal Networks using the "Fax Function (Fax Transmission from PC)" (except for via USB Ports)
Protection mechanism and protected scope
The Internal Networks between client PC and Network Unit are protected by SSL mechanism

Table 1-1 (3) Specific Data, Mechanism and Scope

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

2.2.4 Countermeasure to T.FAX_LINE

The TOE does not have the active mechanism to counter T.FAX_LINE.
Since the TOE does not perform any operations via a telephone line except for sending and receiving faxes, the TOE counters T.FAX_LINE.

2.2.5 Realisation of P.SOFTWARE

The TOE has the function that checks the executable code of MFP Control Software, which is installed in FlashROM, is in the same condition as the ones that are provided by RICOH in order to accomplish P.SOFTWARE.
This function is accomplished by checking the electronic signature added to the executable code.
Along with this function and checking of the version for each element that the TOE outputs, the "correct version for the software is provided by Ricoh with the regular method".
Although it is not possible to specifically assume the threats to the executable code of MFP Control Software by the description in the ST, it is defined in Organisational Security Policy in order to specify the consumers that it is possible to check the integrity of MFP Control Software.

2.2.6 Support for Other Security Functions

The TOE has the Audit Function that is used to detect the security invasion, and this function does not directly counter to the threats.
This function records the audit logs when the events that are used to detect the security invasion 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 2009-06 and concluded by completion the Evaluation Technical Report dated 2010-02. 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 2009-08 and 2009-10 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 developer and evaluator testing by

using developer testing environment at developer site on 2009-10 and 2009-11.
About some portions of procedural status conducted in relation to work unit for development security, the evaluation facility determined that the result that was examined on 2008-10, 2008-12 and 2009-01 as evaluation of another TOE (that assurance level is same as the TOE) was now also acceptable, and accepted the result as evaluation of the TOE.

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

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

3.3 Product Testing

The evaluator validated the tests performed by the developer, and verified the evidence, which were provided during the evaluation process, and the developer's tests. Then judging by the results, the evaluator performed the required reproduction and additional tests, and penetration tests based on the vulnerability assessment.

3.3.1 Developer Testing

The evaluator evaluated the integrity of the developer testing performed by the developer, and the documentation of the actual test results. The following are the overview of the evaluated developer testing.

1) Developer Testing Environment

The test configuration that the developers performed is shown in Figure 3-1 Configuration of Developer Testing.

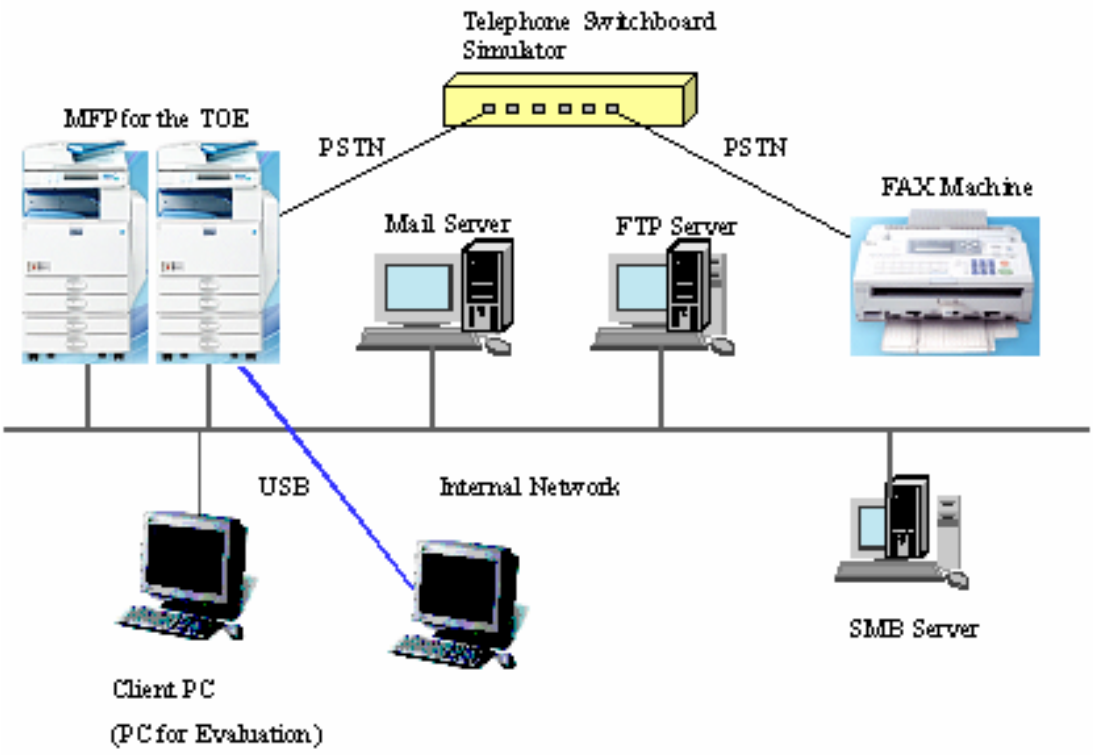

Fig. 3-1 Configuration of Developer Testing

The following outlines show the elements of the test configuration.

- MFP for the TOE
  The targets of testing were as follows:
  Japan: Ricoh imagio MP 2550SP
  Ricoh imagio MP 2550SPF
  Ricoh imagio MP 3350SPF
  Overseas: Ricoh Aficio MP 2550SP
  Ricoh Aficio MP 2550SPF

- Client PC
  The following were used as Web browser:
  > Internet Explorer 6.0
  > Internet Explorer 7.0
  > Internet Explorer 8.0
  The following drivers were used:
  > RPCS Driver V7.66 for domestic machines
  > RPCS Driver V7.67 for overseas machines
  > PC Fax Driver V1.59 for domestic machines
  > LAN Fax Driver V1.60 for overseas machines

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

- FTP Server
  Windows Server 2003 Pro was used as Software with FTP server function.

- SMB Server
  Windows Server 2003 Pro was used as Software with SMB server function.

- Fax machines
  Ricoh imagio MP2550SPF, Ricoh AficioMP 2550SPF were used as machines with Fax function.

- Telephone Switchboard Simulator
  TLE-101Ⅲ (manufactured by LSI JAPAN CO., LTD.) was used as machines to be considered equivalent to public lines.

The configuration of the developer testing covers the TOE configuration that is identified in this ST except for MFP as the TOE. Since the configuration of the developer testing also covers the properties (print speed, domestic or overseas machines, with/without Fax Function) of each MFP identified in this ST, it is considered as covering each MFP for the TOE identified in ST.

2) Overview of Developer Testing

The overview of testing that the developers performed is as follows:

a. Test Overview

Testing, mainly from assumed usage of the TOE (operate the Operation Panel, internal network or client PC which is connected with USB, operate Fax machines), stimulated an external interface to the TOE and performed in a way to eye-check and observe the results. Sometimes it is inappropriate to use such ways. In that case, the following approach was used:

(1) To ensure that the communication over the Internal Network is SSL, IPSec protocol, capture the communication over the Internal Network using WireShark, and then check it.

(2) To ensure the operation that is inside of the TOE, replace MFP control software with the embedded code to output the debug information and then check the output debug information.

(3) To ensure the function of checking the integrity for MFP Control Software, replace the MFP Control Software with the code, "which is embedded to output the debug information and in which the integrity is damaged", and then check the output debug information.

Furthermore, the vulnerability diagnosis for Web interfaces was also performed using the vulnerability diagnostic tool to detect any vulnerabilities of Web application.

b. Test Scope

647 items of testing are performed by the developers.
It was verified that the coverage analysis was performed, and all of the security functions and external interfaces described in the function specifications were completely tested. Also, it was verified that the depth analysis was performed, and all of the subsystems and subsystem interfaces described in TOE design were fully 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

The evaluators performed the independent testing using the evidence, which were provided during the evaluation process, in order to revalidate the security functions of the product are securely performed. The following are the overview of the independent testing that the evaluators performed.

1) Evaluator Independent Testing Environment

The configuration of testing that the evaluators performed is the same as the one as the developer testing.
Figure 3-1 shows the configuration of testing performed by the evaluators.

- MFP for the TOE
  The targets of testing were as follows:
  Japan: Ricoh imagio MP 3350SP
  Ricoh imagio MP 2550SPF
  Overseas: Ricoh Aficio MP 2550SPF

- Client PC
  The following were used as Web browser:
  > Internet Explorer 6.0
  > Internet Explorer 7.0
  > Internet Explorer 8.0
  The following drivers were used:
  > RPCS Driver V7.66 for domestic machines
  > RPCS Driver V7.67 for overseas machines
  > PC Fax Driver V1.59 for domestic machines
  > LAN Fax Driver V1.60 for overseas machines

- Mail Server
  Windows Server 2003 Pro was used as Software with SMTP server function.

- FTP Server
  Windows Server 2003 Pro was used as Software with FTP server function.

- SMB Server
  Windows Server 2003 Pro was used as Software with SMB server function.

- Fax machines
  Ricoh imagio MP2550 was used as a machine with Fax function.

- Telephone Switchboard Simulator
  TLE-101Ⅲ (manufactured by LSI JAPAN CO., LTD.) was used as a machine to be considered equivalent to public lines.

The configuration of the evaluator testing covers the TOE configuration that is identified in this ST except for MFP as the TOE and drivers. Since the configuration of the developer testing also covers the properties (print speed,

domestic or overseas machines, with/without Fax Function) of each MFP identified in this ST, it is considered as covering each MFP for the TOE identified in ST. For drivers, it is considered as covering each driver identified in ST because it was performed by identifying the equality of the different version.

2) Overview of Evaluator Independent Testing

The following are the performed independent testing:

a. Perspective of Independent Testing

40 items of testing were independently devised by evaluators in the following perspectives:

(Perspective 1) To increase the rigour of testing, change the parameters and conditions and perform the testing that the developers performed.

(Perspective 2) Consider SSL, IPSec, S/MIME, which are the functions to protect the communications, as the characteristic security functions, and complement the testing that ensures there are no conditions to disable these functions.

Covering the security functions and interfaces for testing, and considering the following perspectives, 192 items of developer testing sampling were selected.

- Regarding the following as the important behaviours to ensure that security functions correctly operate, the following must be selected clearly:
  > Combination of each condition in the Access Control Function to stored documents.
  > Combination of the authorised operator and the authorised operation in the Security Management Function.
  > Combination of each condition in the actions for authentication failure.
  > Checking the performance of function to verify software validity.
  > Function to check the password strength.
  > Encryption function for stored documents.
  > Self-Test function for encrypting at the TOE initialisation.
  > Network Communication Protection Function.

- It is ensured to include the testing of the completeness of auditable log events and the testing to check the contents of the obtained audit log records.

- It is ensured to include all types of the interface (classification of the Operation Panel, Web interface, etc.).

b. Test Overview

The overview of independent testing performed by the evaluators is as follows:

From (Perspective 1), testing was performed in the same approach as the developer testing. For example:
- Different combination of operating interfaces for the developer testing in which there are competing operations on the same document.
- Different combination of the roles and operating interfaces for the developer testing of access control.

From (Perspective 2), testing in which operating the TOE communication in the settings or environment that might cause the concern that the communication

is performed with SSL, IPSec, and S/MIME deactivated was performed, and the testing validated that the communication was not performed with SSL, IPSec, and S/MIME deactivated. For SSL and IPSec, the communication was captured using WireShark in order to check the detail of the communication. For S/MIME, it was validated from client PC that sending e-mail cannot be performed. The sampled testing from developer testing was performed in the same approach as the developer testing.

c. Result

All of the evaluator independent testing was correctly completed, and the performance of the TOE was checked. The evaluator validated that all testing results matched the expected behaviour.

3.3.3 Evaluator Penetration Testing

The evaluator devised and performed the penetration testing required for the vulnerability possibility in the assumed usage environment and by the assumed attack level using the evidence, which were provided during the evaluation process. The following are the overview of the evaluator penetration testing:

1) Evaluator Penetration Testing Overview

The following are the penetration testing performed by the evaluator.

a. Concerned Vulnerability

The evaluator searched the potential vulnerabilities using the provided evidence and information in the public domain, and identified the following vulnerabilities that required the penetration testing.

(1) There may be unenforced network port interfaces and the TOE may be accessed from these.
(2) Identification and Authentication Function and Access Control Function may be bypassed by specifying the direct URL and accessing from the Web interfaces.
(3) There may be the methods on Operation Panel and Web interfaces that can operate the TOE by bypassing the Identification and Authentication Function.
(4) There may be the vulnerabilities, which were not discovered by the vulnerability diagnostic tool used for developer testing to discover the vulnerability of Web application, on the Web interfaces.
(5) It is not determined that the operation that breaks the security cannot be performed before the TOE initialisation completes.
(6) There are operations that might result in the concern of bypassing the TOE Identification and Authentication Function.

b. Test Scope

The evaluator performed the following penetration testing in order to determine whether or not there was the potential exploitable vulnerability.

(1) Investigate the available network ports of the TOE by using the tools for port scan and the command (Rlogin, Telnet, SSH, Rsh, and FTP) to access the network ports.

(2) Investigate the URLs that possibly bypass the Identification and Authentication Function and Access Control Function, and then attempt to enter the applicable URLs into the browser and access.
(3) Attempt to perform every possible operation, except for the login, from the Operation Panel and Web interfaces.
(4) Use the vulnerability diagnostic tool that is different from the one used for the developer testing, and diagnose the vulnerability of Web interfaces.
(5) Attempt the operation on the TOE before the TOE initialisation completes.
(6) Attempt the operations that might cause the bypassing of the TOE Identification and Authentication Function.

c. Result

In the penetration testing performed by the evaluator, the exploitable vulnerability by the attackers with the assumed attack potential 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

None.

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.

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

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

For some setting items of the product, some product, of which the settings are not as specified, are not considered as the evaluated target unless the product is set as specified. This means it is not considered as the "TOE in this certification" unless the product is set as specified. Refer to "1.2.3.1 Scope of TOE" for the specific setting items and restrictions.
For some functions of the TOE, some functions are limited their availability. This means the TOE is not securely used unless the TOE Administrator let or does not let the users use such functions. Refer to A.ADMIN in "2.1.3 Assumptions for Operational Environment" for the specific functions that are restricted.
If the users do not expect these "restricted settings and functions" for the product, it is not an issue. However, if the users expect these settings and functions, attention is required when determining whether the product is suitable to their own environment.

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
SOF:	Strength of Function
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Functions

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

Address Book	A database containing General User Information for each General User.
Administrator	An authorized TOE user 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 Roles: User Administration, Machine Administration, Network Administration and File Administration. Each Administrator Role is assigned to at least one of the registered Administrators.
Complexity Setting for Password	The minimum combination of character types that can be registered for passwords. There are four character types: upper-case letters, lower-case letters, numbers, and symbols. There are two complexity setting levels for Complexity Setting for Password, Level 1 and Level 2. Level 1 requires passwords with a combination of more than two character types. Level 2 requires passwords with a combination of more than three character types.
D-BOX	A storage area for Document Data on the HDD.
Deliver to Folder	A function that sends the Document Data to folders in SMB Server or FTP Server from the TOE via networks.
Direct Print Function	A function that prints out the received Print Data by the TOE.

Document Data	Electronic data that are loaded into MFP by authorized MFP users using either of the following operations. 1. Electronic data that are scanned from paper-based original and digitised by authorized MFP users' operation. 2. Electronic data that are sent to the MFP by authorized MFP users and converted by the MFP from received Print Data 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	One of the data items of General User Information. The default value that is set for the Document Data ACL of a new Document Data to be stored.
External Networks	Networks that are not managed by the organization that manages the MFP. Generally, indicates the Internet.
Fax Transmission from PC	A function that faxes Document Data from a client PC via the TOE when connecting client PC to networks or with USB Ports.
File Administration	The Administrator Role that manages the D-BOX, which stores the Document Data stored in the TOE, and manages the Document Data ACL, which 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 client PC and receiving files from client PC using File Transfer Protocol.
General User	An authorized TOE user who uses the basic functions of the TOE.
General User Information	A record containing information about a General User. Data items include the General User IDs, General User authentication information, Document Data Default ACL, and S/MIME User Information.
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 that stores a private encryption key for secure communication. It keeps the keys for validity authentication and encryption processing and the random number generator.
Immediate Transmission	A function that dials first, then faxes data while scanning the original.
Internal Networks	Networks managed by an organization that has MFP. Normally indicates the office LAN environment established as the intranet.
Internet Fax	A function that converts scanned document images to e-mail format and transit the data over the Internet, and a machine that has an e-mail address can receive the e-mail sent using this function.

IP-Fax	A function that sends and receives document files between two faxes directly via a TCP/IP network. It is also possible to send document files to a fax that is connected to a telephone line using this function.
Lockout	A function that prohibits the access for the specific user IDs to the TOE.
Machine Administration	The Administrator Role that manages machines and plays the role of performing the audit. The Machine Administrator is a person who has the machine management role.
Memory Transmission	A function that stores the scanned data of the original in memory, and then dials and faxes the data.
MFP	An abbreviation for digital multi function product.
MFP Control Data	A generic term for a set of parameters that control the operation of MFP.
MFP Control Software	Software installed in the TOE and has the elements that identify the TOE such as System/Copy, Network Support, Scanner, Printer, Fax, Web Support, Web Uapl and Network Doc Box. It 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 for passwords.
Network Administration	One of the Administrator Roles that manages the TOE network connections. The Network Administrator is a person who has the network management role.
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. Operation Panel Unit.
Print Data	The document files in client PC that are sent to the TOE from a client PC to be printed or faxed. It is necessary to install drivers into client PC in advance - printer driver for printing and fax driver for faxing. Print Data is taken into the TOE from Network Units or USB Ports.
Print Setting	Print Settings for printed output, including paper size, printing magnification and customised information (such as duplex and layout).
PSTN	An abbreviation for Public Switched Telephone Networks.
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.

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 client PC using Server Message Block protocol.
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.
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 D-BOX. Document Data stored in D-BOX can be printed out according to users' instruction.
Stored Data Protection Function	A function that protects the Document Data stored on HDD from leakage.
Stored Documents Fax Transmission	A function that faxes Document Data previously stored in D-BOX.
Supervisor	The authorized TOE user who manages the passwords of Administrators.
User Administration	The Administrator Role that manages General Users. The User Administrator is a person who has the user management role.

7. Bibliography

[1] imagio MP 2550/3350 series, Aficio MP 2550/3350 series Security Target Version 1.05 (February 8, 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. imagio MP 2550/3350 series, Aficio MP 2550/3350 series Evaluation Technical Report Version 1.7, February 17, 2010, Information Technology Security Center Evaluation Department