Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2010-06-14 (ITC-0299)
Certification No.	C0285
Sponsor	RICOH COMPANY, LTD.
Name of TOE	Following MFP with FCU, DataOverwriteSecurity Unit and HDD Encryption Unit MFP: Ricoh Aficio MP 4001, Ricoh Aficio MP 4001G, Ricoh Aficio MP 5001, Ricoh Aficio MP 5001G, Savin 9240, Savin 9240G, Savin 9250, Savin 9250G, Lanier LD140, Lanier LD140G, Lanier LD150, Lanier LD150G, Lanier MP 4001, Lanier MP 5001, Gestetner MP 4001, Gestetner MP 4001G, Gestetner MP 5001, Gestetner MP 5001G, nashuatec MP 4001, nashuatec MP 5001, Rex-Rotary MP 4001, Rex-Rotary MP 5001, infotec MP 4001, infotec MP 5001 FCU: Fax Option Type 5001 DataOverwriteSecurity Unit: DataOverwriteSecurity Unit Type I HDD Encryption Unit: HDD Encryption Unit Type A
Version of TOE	- Software System/Copy 1.02 Network Support 7.34 Scanner 01.24 Printer 1.01 Fax 02.00.00 RemoteFax 02.00.00 Web Support 1.04 Web Uapl 1.02 Network DocBox 1.00 animation 1.3 Option PCL 1.03 OptionPCLFont 1.01 Engine 1.00:01 OpePanel 1.08 LANG0 1.07 LANG1 1.07 - Hardware Ic Key 1100 Ic Hdd 01 - Options Data Erase Opt 1.01m GWFCU3-19(WW) 02.00.00
PP Conformance	IEEE Std 2600.1-2009

Assurance Package	EAL3 Augmented with ALC_FLR.2
Developer	RICOH COMPANY, LTD.
Evaluation Facility	Electronic Commerce Security Technology Laboratory Inc. Evaluation Center

This is to report that the evaluation result for the above TOE is certified as follows.
2011-03-29

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 Release 3
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 3

Evaluation Result: Pass

"Following MFP with FCU, DataOverwriteSecurity Unit and HDD Encryption Unit
MFP: Ricoh Aficio MP 4001, Ricoh Aficio MP 4001G, Ricoh Aficio MP 5001, Ricoh Aficio MP 5001G, Savin 9240, Savin 9240G, Savin 9250, Savin 9250G, Lanier LD140, Lanier LD140G, Lanier LD150, Lanier LD150G, Lanier MP 4001, Lanier MP 5001, Gestetner MP 4001, Gestetner MP 4001G, Gestetner MP 5001, Gestetner MP 5001G, nashuatec MP 4001, nashuatec MP 5001, Rex-Rotary MP 4001, Rex-Rotary MP 5001, infotec MP 4001, infotec MP 5001
FCU:Fax Option Type 5001
DataOverwriteSecurity Unit:DataOverwriteSecurity Unit Type I
HDD Encryption Unit:HDD Encryption Unit Type A" 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 5
1.1 Product Overview 5
1.1.1 Assurance Package 5
1.1.2 TOE and Security Functionality 5
1.1.2.1 Threats and Security Objectives 6
1.1.2.2 Configuration and Assumptions 6
1.1.3 Disclaimers 6
1.2 Conduct of Evaluation 6
1.3 Certification 7
2. Identification 8
3. Security Policy 9
3.1 Security Function Policies 10
3.1.1 Threats and Security Function Policies 10
3.1.1.1 Threats 10
3.1.1.2 Security Function Policies against Threats 11
3.1.2 Organisational Security Policies and Security Function Policies 12
3.1.2.1 Organisational Security Policies 12
3.1.2.2 Security Function Policies to Organisational Security Policies 13
4. Assumptions and Clarification of Scope 15
4.1 Usage Assumptions 15
4.2 Environment Assumptions 15
4.3 Clarification of scope 17
5. Architectural Information 18
5.1 TOE boundary and component 18
5.2 IT Environment 19
6. Documentation 20
7. Evaluation conducted by Evaluation Facility and results 24
7.1 Evaluation Approach 24
7.2 Overview of Evaluation Activity 24
7.3 IT Product Testing 25
7.3.1 Developer Testing 25
7.3.2 Evaluator Independent Testing 27
7.3.3 Evaluator Penetration Testing 29
7.4 Evaluated Configuration 31
7.5 Evaluation Results 31
7.6 Evaluator Comments/Recommendations 32
8. Certification 33
8.1 Certification Result 33

8.2 Recommendations 33
9. Annexes 34
10. Security Target 34
11. Glossary 35
12. Bibliography 38

1. Executive Summary

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "Following MFP with FCU, DataOverwriteSecurity Unit and HDD Encryption Unit
MFP: Ricoh Aficio MP 4001, Ricoh Aficio MP 4001G, Ricoh Aficio MP 5001, Ricoh Aficio MP 5001G, Savin 9240, Savin 9240G, Savin 9250, Savin 9250G, Lanier LD140, Lanier LD140G, Lanier LD150, Lanier LD150G, Lanier MP 4001, Lanier MP 5001, Gestetner MP 4001, Gestetner MP 4001G, Gestetner MP 5001, Gestetner MP 5001G, nashuatec MP 4001, nashuatec MP 5001, Rex-Rotary MP 4001, Rex-Rotary MP 5001, infotec MP 4001, infotec MP 5001
FCU:Fax Option Type 5001
DataOverwriteSecurity Unit:DataOverwriteSecurity Unit Type I
HDD Encryption Unit:HDD Encryption Unit Type A" (hereinafter referred to as "the TOE") developed by RICOH COMPANY, LTD., and evaluation of the TOE was finished on 2011-03 by Electronic Commerce Security Technology Laboratory Inc. Evaluation Center (hereinafter referred to as "Evaluation Facility"). 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 Security Target (hereinafter referred to as "the ST") that is the appendix of this report together. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in ST.

This certification report assumes "the general consumers who purchase this TOE" to be a reader. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee individual IT product itself.

1.1 Product Overview

Overview of the TOE functions and operational conditions is as follows. Refer to and after Chapter 2 for details.

1.1.1 Assurance Package

Assurance Package of the TOE is EAL3 augmented with ALC_FLR.2.

1.1.2 TOE and Security Functionality

The TOE is a digital MFP (hereafter "MFP") made by RICOH COMPANY, LTD., and which provides the functions of copy, scanner, printer, and fax (option) for digitising paper-based documents, document management, and printing.

This MFP is an IT product which incorporates each function of scanner, printer, and fax with Copy Function, and which is generally connected to an office LAN and used for inputting, storing, and outputting document data.

This TOE provides Security Functions required for IEEE Std 2600.1-2009 [14], which is a Protection Profile (hereafter, "conformance PP") for digital MFPs, and also provides the

Security Functions to accomplish the necessary security policy for an organisation which manages the TOE.

For these security functionalities, the evaluation for the validity of the design policy and the correctness of the implementation is conducted in the scope of the assurance package. The next clause describes the assumed threats and assumptions in this TOE.

1.1.2.1 Threats and Security Objectives

This TOE assumes the following threats and provides the Security Functions to counter them.
For protected assets such as the document data that the TOE handles and the setting information relevant to the Security Functions, there are threats of disclosure and tampering caused by unauthorised access to both the TOE and the communication data on the network. This TOE provides the Security Functions to protect those protected assets from unauthorised disclosure and tampering.

1.1.2.2 Configuration and Assumptions

The evaluated product is assumed to be operated under the following configuration and assumptions.

This TOE is equipped with Fax Controller Unit (hereafter, "FCU") to provide Fax Function for the MFP, and equipped with Security Card that is an optional device used to overwrite residual data, and also with HDD Encryption Unit to provide the function to encrypt the storage.

It is assumed that this TOE is located in an environment where physical components and interfaces of the TOE are protected from the unauthorised access. And for the operation, the TOE shall be properly configured, maintained, and managed according to the guidance documents.

1.1.3 Disclaimers

This TOE is assumed to be operated while the following functions are deactivated. The security is not assured if the TOE is operated after changing this setting:

- Maintenance Function
- IP-Fax and Internet Fax Function
- Authentication methods except for Basic Authentication

1.2 Conduct of Evaluation

Evaluation Facility conducted IT security evaluation, and completed on 2011-03 based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme"[1], "IT Security Certification Procedure"[2], "Evaluation Facility Approval Procedure"[3] provided by Certification Body.

1.3 Certification

The Certification Body verifies the Evaluation Technical Report prepared by Evaluation Facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. The Certification Body confirmed that the TOE evaluation is appropriately conducted in accordance with CC ([4][5][6] or [7][8][9]) and CEM (either of [10][11]).The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by Evaluation Facility and concluded fully certification activities.

2. Identification

The TOE is identified as follows:

Name of TOE	Following MFP with FCU, DataOverwriteSecurity Unit and HDD Encryption Unit MFP: Ricoh Aficio MP 4001, Ricoh Aficio MP 4001G, Ricoh Aficio MP 5001, Ricoh Aficio MP 5001G, Savin 9240, Savin 9240G, Savin 9250, Savin 9250G, Lanier LD140, Lanier LD140G, Lanier LD150, Lanier LD150G, Lanier MP 4001, Lanier MP 5001, Gestetner MP 4001, Gestetner MP 4001G, Gestetner MP 5001, Gestetner MP 5001G, nashuatec MP 4001, nashuatec MP 5001, Rex-Rotary MP 4001, Rex-Rotary MP 5001, infotec MP 4001, infotec MP 5001 FCU: Fax Option Type 5001 DataOverwriteSecurity Unit: DataOverwriteSecurity Unit Type I HDD Encryption Unit: HDD Encryption Unit Type A
Version of TOE	- Software System/Copy 1.02 Network Support 7.34 Scanner 01.24 Printer 1.01 Fax 02.00.00 RemoteFax 02.00.00 Web Support 1.04 Web Uapl 1.02 Network DocBox 1.00 animation 1.3 Option PCL 1.03 OptionPCLFont 1.01 Engine 1.00:01 OpePanel 1.08 LANG0 1.07 LANG1 1.07 - Hardware Ic Key 1100 Ic Hdd 01 - Options Data Erase Opt 1.01m GWFCU3-19(WW) 02.00.00
Developer	RICOH COMPANY, LTD.

The user can verify that a product is the TOE, which is evaluated and certified, by the following means.

According to the procedures described in the guidance documents, the user can confirm that the installed product is this evaluated TOE by comparing the names that are displayed on the MFP exterior and the versions on the Operation Panel of the TOE with the applicable descriptions in the list of the TOE configuration items.

3. Security Policy

This chapter describes security function policies and organisational security policies.

The TOE provides the Security Functions to counter the unauthorised access to the stored document data in the MFP, and to protect the communication data on the network.

For meeting the organisational security policies, the TOE provides the functions to overwrite the internal stored data, to encrypt the stored data in an HDD, and to prevent the unauthorised access through telephone lines via fax I/F.

And for each setting that is relevant to the above mentioned Security Functions, only administrators are permitted to set configurations in order to prevent the deactivation and unauthorised use of the Security Functions.

Tables 3-1 and 3-2 show the protected assets for the Security Functions of this TOE.

Table 3-1: TOE protected assets (user data)

Type	Asset
Document information	Digitised user documents, deleted documents, temporary documents and their fragments under the TOE control. (Hereafter, referred to as "document".)
Function information	Active Job executed by users. (Hereafter, referred to as "user job".)

Table 3-2: TOE protected assets (TSF data)

Type	Asset
Protected data	The information that shall be protected from changes by users without edit permission. Includes Login user name, Number of Attempts before Lockout, year-month-day setting, time setting, Minimum Password Length, etc. (Hereafter, referred to as "TSF protected data".)
Confidential data	The information that shall be protected from changes by users without edit permission, and also shall be protected from reading by users without viewing permission. Includes Login password, audit log, and HDD cryptographic key. (Hereafter, referred to as "TSF confidential data".)

3.1 Security Function Policies

The TOE possesses the security functions to counter the threats shown in Chapter 3.1.1 and to meet the organisational security policies shown in Chapter 3.1.2.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The TOE assumes the threats shown in Table 3-3 and provides the functions as countermeasures against them. These threats are translated from English PP into Japanese and the evaluation process confirmed the equivalence of both threats.

Table 3-3 Assumed Threats

Identifier	Threat
T.DOC.DIS (Document disclosure)	Documents under the TOE management may be disclosed to persons without a login user name, or to persons with a login user name but without an access permission to the document.
T.DOC.ALT (Document alteration)	Documents under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the document.
T.FUNC.ALT (User job alteration)	User jobs under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the user job.
T.PROT.ALT (Alteration of TSF protected data)	TSF Protected Data under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the TSF Protected Data.
T.CONF.DIS (Disclosure of TSF confidential data)	TSF Confidential Data under the TOE management may be disclosed to persons without a login user name, or to persons with a login user name but without an access permission to the TSF Confidential Data.
T.CONF.ALT (Alteration of TSF confidential data)	TSF Confidential Data under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the TSF Confidential Data.

* "Persons with a login user name" mean persons who are permitted to use the TOE.

3.1.1.2 Security Function Policies against Threats

All threats shown in Table 3-3 describe breaches (viewing or alteration) of user data and TSF data caused by persons who are not permitted users for the TOE, or by persons who do not have any valid authorities.
These threats are countered by the following Security Functions:

(1) User identification and authentication
The TOE requires persons who attempt to use the TOE to input the login user names and login passwords, and the TOE confirms that the input is identical to the user data managed internally by the TOE. The entry means are the input from Operation Panel of the TOE itself, the input on a Web browser of client computers, and the input via drivers when using Printer Function and LAN-Fax Transmission.

As a means to ensure the necessary functional strength, the following functions are provided:

- If users fail to be authenticated consecutively until reaching the specified number of times set by the MFP administrator, the user accounts are forced to be locked out. (The user accounts cannot be used until the lockout time (60 minutes) elapses or the lockout is released).
- The login passwords are required, when they are set, to be composed of more than the level of quality that has been established in terms of the length (number of characters) and the character types.

If confirmed that the login user names and passwords are valid, the user is allowed to use the TOE with TOE user permissions that are pre-assigned to each user role.
The user roles specified by the TOE are as follows:

- Normal user
- MFP administrator
- Supervisor

Also, as a means to support the Identification and Authentication Function, the following functions are provided:

- Display dummy characters in place of the entered login password on the input screen.
- After once logged in, if at any time the TOE is not operated by the user or anyone in a certain period of time, the user account will be automatically logged out.

(2) Access control (Access control against the user data)
For processing request by the users, access control to the document information and the user jobs is performed, based on the login user names and permissions of each user role of the users.
User documents are associated with specific information (a document user list) that stipulates which user is allowed to perform the operation (deletion, printing, and downloading). Access control to allow or deny the operation request by normal user is performed, according to the login user names and the information in the document user

list. The MFP administrator is permitted to delete any user's documents, but is not permitted to perform any other operation on user documents.
User jobs are associated with the login user names of the users that create the jobs, and the normal user who is associated with the login user name is allowed to delete the applicable job. The MFP administrator is allowed to delete all the user jobs. The supervisor is forbidden to perform any operations on the user data.

(3) Overwrite residual data
In order to protect from unauthorised access to user documents that have been deleted but remain residually stored in the HDD, temporary documents and their fragments in the HDD, the residual data shall be overwritten by specified data when deleting the document data.

(4) Network protection
In order to prevent information leakage by being monitored via communication paths, SSL encrypted communication is used between the TOE and client computers for the operations via a Web browser, communications using Printer Function, and LAN-Fax communication. Also, IPsec communication and S/MIME communication are used for the communications between the TOE and the clients.

(5) Security management
In order to protect the TSF data from unauthorised access beyond the user permissions, access control is performed on actions, such as viewing or altering TOE setting information, and newly creating or altering user data in accordance with the TOE user roles. As a permission policy of information alteration (modification), normal users are only authorised to alter their login passwords and supervisor is only authorised to alter the login passwords of the supervisor and the MFP administrators. Only MFP administrators are allowed to alter the TSF data, except for the above mentioned permissions.

3.1.2 Organisational Security Policies and Security Function Policies

3.1.2.1 Organisational Security Policies

Organisational security policies required in use of the TOE are shown in Table 3-4. The evaluation process has confirmed that the security policies except for P.STORAGE.ENCRYPTION are identical to the security policies in the conformance PP. P.STORAGE.ENCRYPTION is the security policy that assumes writing data into the HDD not in a directly readably format.

Table 3-4 Organisational Security Policies

Identifier	Organisational Security Policy
P.USER.AUTHORIZATION (User identification and authentication)	Only users with a login user name shall be authorised to use the TOE.
P.SOFTWARE.VERIFICATION (Software verification)	Procedures shall exist to self-verify executable code in the TSF.
P.AUDIT.LOGGING	The TOE shall create and maintain a log of TOE use

(Management of audit log records)	and security-relevant events. The audit log shall be protected from unauthorised disclosure or alteration, and shall be reviewed by authorised persons.
P.INTERFACE.MANAGEMENT (Management of external interfaces)	To prevent unauthorised use of the external interfaces of the TOE (Operation Panel, LAN, USB and telephone lines), operation of those interfaces shall be controlled by the TOE and its IT environment.
P.STORAGE.ENCRYPTION (Encryption of storage devices)	The TOE shall encrypt the stored data on the HDD inside the TOE.

3.1.2.2 Security Function Policies to Organisational Security Policies

The TOE provides the security functions to meet the Organisational Security Policies shown in Table 3-4.

(1) Means to support Organisational Security Policy, "P.USER.AUTHORIZATION".
This security policy requires that the officially registered TOE users be allowed only to use the TOE.
The TOE implements this policy by the following Security Functions:

(a) User identification and authentication
According to the method of the Identification and Authentication (hereafter, I&A) described in 3.1.1.2, the TOE requires persons who attempt to use the TOE to input the login user names and login passwords. And then, the TOE confirms that the persons are the authorised users who are registered in the TOE, and associates the login user names of the persons with the roles that correspond to them.
The TOE allows only a validated user to use the functions provided by the TOE.

(b) Security management
In order to protect the TSF data from unauthorised access beyond the user permissions, the access control is performed on actions of viewing or altering the TOE setting information, in accordance with the TOE user roles.
Only MFP administrators are allowed to alter the available functions list.

(2) Means to support Organisational Security Policy, "P.SOFTWARE.VERIFICATION".
This security policy requires the validity of the TOE executable code to be self-verified.
The TOE implements this policy by the following Security Functions:

(a) Self test
The TOE (component items except for FCU) runs a self test during the initialisation start-up after turning on the power, and it checks the integrity and the validity of executable code in the MFP control software. The self test verifies the hash values of firmware and confirms the completeness of the executable code. The test verifies each application on the basis of a signature key and confirms the validity of the executable code.

If something abnormal is recognised during the self test, an error message is displayed on the Operation Panel and the TOE stops the operations so normal users cannot use the TOE. If no abnormal operations are recognised, the TOE continues the start-up

processing and makes itself usable for the users.

As for the FCU, the TOE provides the verification information that allows the users to confirm for the integrity. To use the TOE, the users need to verify the FCU based on this information.

(3) Means to support Organisational Security Policy, "P.AUDIT.LOGGING".
This security policy requires audit logs for the security events of the TOE to be acquired, and the audit logs to be appropriately managed.
The TOE implements this policy by the following Security Functions:

(a) Security audit
When auditable security events occur, the TOE generates the audit logs that consist of such items as event type, user identification, occurrence date and time, and outcome, etc. to add and save to the audit logging file. Only successfully authenticated MFP administrators are allowed to read and delete the generated audit logging file. Reading the audit logging file is executed by text format through a Web browser of client computers.
Also, in order to record the occurrence date and time of the audit event log, the date and time information are acquired from the system clock of the TOE.

(4) Means to support Organisational Security Policy, "P.INTERFACE.MANAGEMENT".
This security policy requires that external interfaces (Operation Panel, LAN interface, USB interface, and telephone lines) of the TOE be appropriately managed without being used by unauthorised persons.
The TOE implements this policy by the following Security Functions:

(a) User identification and authentication
By the I&A described in 3.1.1.2, the TOE requires persons who attempt to use the TOE to input the login user names and login passwords, and the TOE confirms that the persons are the authorised users who are registered in the TOE, and it allows the users to use the TOE.

(b) Restricted forwarding of data to external interfaces
This function is not implementation for active mechanism, but is addressed as architectural design of external interfaces. By its architecture, any information received from an external interface is processed by the TSF, and any information sent to an external interface is controlled by the TSF. Thus, unauthorised forwarding of data between the different external interfaces is prevented.
As for USB interfaces, unauthorised forwarding of data by using this interface is prevented by deactivating the use of USB interfaces.

(5) Means to support Organisational Security Policy, "P.STORAGE.ENCRYPTION".
This security policy requires that the TOE encrypt the stored contents on the HDD inside the TOE.
The TOE implements this policy by the following Security Functions:

(a) Stored data protection function
The encryption and decryption by AES are performed for all data written into or reading out to the HDD. When encrypting and decrypting the data, the key of 256-bits length is used. The key is created from the administrator setting an initial value and stored in the TOE.

4. Assumptions and Clarification of Scope

In this chapter, it describes the assumptions and the operational environment to operate the TOE as useful information for the assumed readers to judge the use of the TOE.

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE. Although assumptions are expressed differently from the PP, the evaluation process confirmed the equivalence of both assumptions.

The effective performance of the TOE security functions are not assured unless these assumptions are upheld.

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumptions
A.ACCESS.MANAGED (Access management)	According to the guidance document, the TOE is placed in a restricted or monitored area that provides protection from physical access by unauthorised persons.
A.USER.TRAINING (User training)	The responsible manager of MFP trains users according to the guidance document and users are aware of the security policies and procedures of their organisation and are competent to follow those policies and procedures.
A.ADMIN.TRAINING (Administrator training)	Administrators are aware of the security policies and procedures of their organisation, are competent to correctly configure and operate the TOE in accordance with the guidance document following those policies and procedures.
A.ADMIN.TRUST (Trusted administrator)	The responsible manager of MFP selects administrators who do not use their privileged access rights for malicious purposes according to the guidance document.

4.2 Environment Assumptions

This TOE is installed in general offices and connected to the local area networks, and it is used by client computers connected to the Operation Panel of the TOE itself as well as the local area networks.
Figure 4-1 shows the general operational environment as assumptions of the TOE.

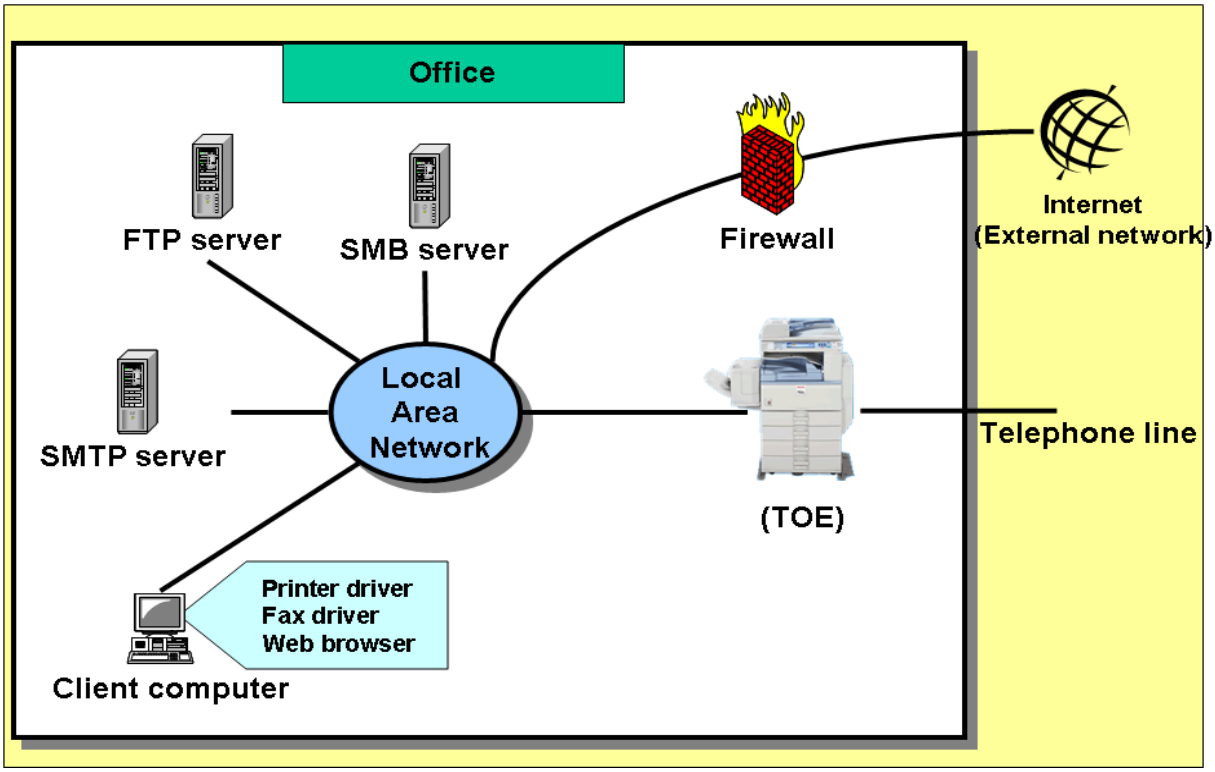

Figure 4-1 Operational Environment and Configuration

Figure 4-1 gives an example environment to handle office documents in general offices where the TOE is assumed to be used. The TOE is connected to the local area network and telephone lines.

When the TOE is connected to the local area network that is connected to an external network such as the Internet, firewalls are installed at the boundaries between the external network and the local area network to protect the local area network and the TOE from attacks that originate from the external network. The local area network is connected to server computers such as an FTP server, an SMB server, and an SMTP server, and is connected to client computers. The local area network performs the communication of the document data with the TOE.

The operation of the TOE includes cases both of using the Operation Panel of the TOE and client computers. Installing printer drivers or fax drivers in client computers enables to process printing via the local area network from the client computers.
Although the reliability of hardware and software shown in this configuration is outside the scope of this evaluation, it is assumed to be trustworthy.

Also, Table 4-2 shows the associated users to use of the TOE in this environment.

Table 4-2: TOE users

User Definition		Explanation
Normal user		A user who is allowed to use the TOE. A normal user is granted a login user name and can use normal functions of MFP.
Administrator	Supervisor	Authorised to delete and newly register a login password of MFP administrators.
	MFP administrator	A user who is allowed to manage the TOE and performs the management operations such as user data management of normal user, device management, file management, and network management.

As shown in Table 4-2, the TOE users are classified into normal user and administrator. According to the roles, administrators shall be identified as supervisor and MFP administrator. The users shown in Table 4-2 are direct users of the TOE. There is also a responsible manager of the MFP who, as an indirect TOE user, is authorised to select the MFP administrators and supervisor. The responsible manager of MFP is assumed to be an organisational manager in the operational environment.

4.3 Clarification of scope

The scope of this TOE covers the entire products as sold to users that are equipped with FCU that provides Fax Function to MFP, Security Card that is a residual data overwrite option, and HDD Encryption Unit that provides the function to encrypt the storage. Developers install options in MFP itself on the user site and deliver the TOE to the users after checking the operations.
Also, although this TOE supports S/MIME as the Communication Data Protection Function, for the e-mail transmission, the administrators need to be responsible for managing the availability and validity of the certificate of the S/MIME recipient.

5. Architectural Information

This chapter explains scope of the TOE and the main components (subsystems).

5.1 TOE boundary and component

Figure 5-1 shows the composition of TOE. The TOE is the entire MFP product equipped with options.

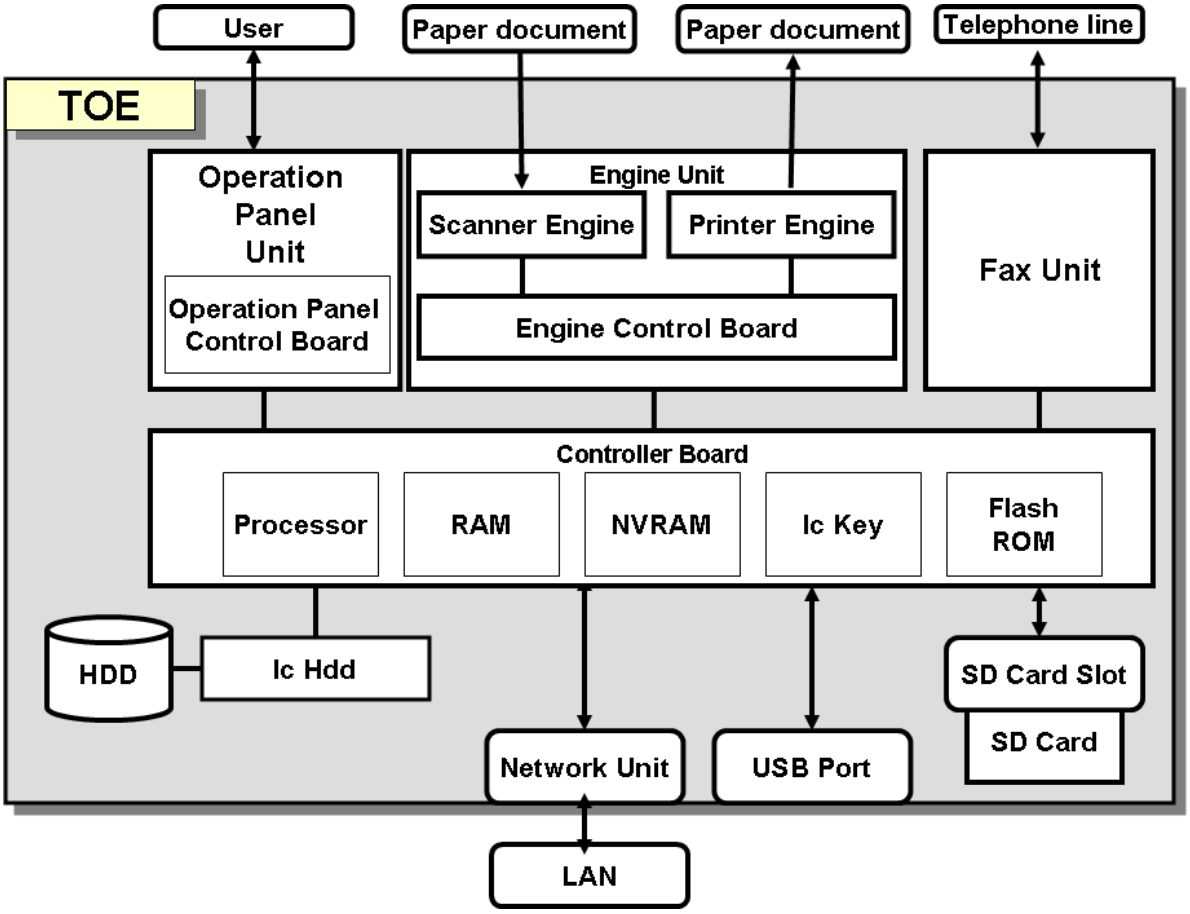

Figure 5-1 TOE boundary

As shown in Figure 5-1, the TOE consists of the following hardware: Operation Panel Unit, Engine Unit, Fax Unit, Controller Board, HDD, Ic Hdd, Network Unit, USB Port, and SD Card Slot/SD Card. The general description of each configuration item is described as follows:

[Operation Panel Unit (hereafter, referred to as "Operation Panel")]
The Operation Panel is an interface device that the TOE users use for the TOE operation. It features the following devices: key switches, LED indicators, an LCD touch screen, and Operation Control Board.

[Engine Unit]
The Engine Unit contains a Scanner Engine that is an input device to read the paper

documents, Printer Engine that is an output device to print and eject the paper documents, and Engine Control Board that controls each engine.

[Fax Unit]
The Fax Unit is a unit that has a modem function and sends or receives fax data to and from other fax devices with G3 standard when connected to a telephone line. FCU is the identifier of the Fax Unit among the components that constitute the TOE.

[Controller Board]
The Controller Board is a device that contains Processors, RAM, NVRAM, Ic Key and FlashROM. The following describes the components of the Controller Board:

- Processor
  A semiconductor chip which carries out the basic arithmetic processing of MFP operations.
- RAM
  A volatile memory medium which is used as the image data.
- NVRAM
  A non-volatile memory medium which stores the MFP control data to configure the MFP operation.
- Ic Key
  A security chip which has the function of a random number generation and encryption key generation. It is used to detect alteration of the MFP Control Software.
- FlashROM
  A non-volatile memory medium in which the MFP Control Software is installed. The following software, which is part of the TOE, includes: System/Copy, Network Support, Scanner, Printer, Fax, RemoteFax, Web Support, Web Uapl, Network DocBox, animation, Option PCL, OptionPCLFont, LANG0, and LANG1.

[HDD]
The HDD is a hard disk drive which image data and user data to be used for identification and authentication are written into.

[Ic Hdd]
The Ic Hdd is a security chip that has the functions to encrypt the information stored into the HDD, and decrypt the information read from the HDD.

[Network Unit]
The Network Unit is an external interface to an Ethernet (100BASE-TX/10BASE-T) LAN.

[USB Port]
The USB Port is an external interface to connect a client computer to the TOE for printing directly from client computers. This interface is disabled at the time of installation.

[SD Card/SD Card Slot]
The SD Card Slot is used for inserting an SD Card. The SD Card is a memory medium which holds the Residual Data Overwrite Function software (Data Erase Opt). The SD Card Slot is inside the MFP, and the SD Card is not usually operated at the maintenance.

5.2 IT Environment

The TOE is connected to the LAN. And the TOE communicates with server computers such as an FTP server, an SMB server, and an SMTP server and communicates with client computers. The TOE communicates with fax devices via the telephone line.

The client computer belonging to LAN uses the TOE through the printer driver, the fax driver, and the web browser.

The client computer performs not only communication of document data to the TOE, but also operation of some management functions and status checking of the TOE via the web browser.

6. Documentation

The identification of documents attached to the TOE is listed below. There are five sets of guidance documents of the TOE. Each of them is used in accordance with the sales area and/or sales company in which the TOE is sold. There are differences between the document sets in English, organisation of the documents, and regulation depending on a country or area. However, the equivalency of the security-relevant contents between them is confirmed by the evaluation process.

TOE users are required to fully understand and comply with the following documents in order to uphold the assumptions.

[English version-1] (Product attached documents for North America)

Document Name	Version
9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001 Operating Instructions About This Machine	D092-7753
9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001 Operating Instructions Troubleshooting	D092-7803
Notes for Users	D092-7727
App2Me Start Guide	D085-7906B
Manuals for Users 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001	D092-7502
Manuals for Administrators 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001	D092-7504
Manuals for Administrators Security Reference Supplement 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001	D092-7790
Notes for Users	D060-7781
Notes for Users	G189-6775
Notes for Users	D092-7905
To Users of This Machine	D029-7904
Operating Instructions Notes On Security Functions	D0857810
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std.2600.1-2009	D3817501
VM Card Manuals	D377-7500
Help(83NHAQENZ)	Ver1.20

Manuals DataOverwriteSecurity Unit Type H/I	D377-7900A
Notes for Users	D377-7250

[English version-2] (Product attached documents for The U.S. government)

Document Name	Version
9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001 Operating Instructions About This Machine	D092-7757
9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001 Operating Instructions Troubleshooting	D092-7807
Notes for Users	D092-7729
App2Me Start Guide	D085-7905B
Manuals for Users 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001	D092-7502
Manuals for Administrators 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001	D092-7504
Manuals for Administrators Security Reference Supplement 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001	D092-7790
Notes for Users	D060-7782
Notes for Users	G189-6776
Notes for Users	D092-7905
To Users of This Machine	D029-7903
Operating Instructions Notes On Security Functions	D3817503
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std.2600.1-2009	D3817502
VM Card Manuals	D377-7500
Help(83NHAQENZ)	Ver1.20
Manuals DataOverwriteSecurity Unit Type H/I	D377-7900A
Notes for Users	D377-7250

[English version-3] (Product attached documents for Europe)

Document Name	Version
Quick Reference Copy Guide	D092-7714
Quick Reference Fax Guide	D509-8534
Quick Reference Printer Guide	D381-7303
Quick Reference Scanner Guide	D381-7309
Manuals for This Machine	D092-7704
Safety Information for Aficio MP 4001/Aficio MP 5001	D092-7700

Notes for Users	D092-7726A
App2Me Start Guide	D085-7904B
Manuals for Users MP 4001/5001 Aficio MP 4001/5001 A	D092-7510
Manuals for Administrators Security Reference MP 4001/5001 Aficio MP 4001/5001	D092-7512
Manuals for Administrators Security Reference Supplement 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001	D092-7790
Notes for Users	D060-7781
Notes for Users	G189-6785
Notes for Users	D092-7907
To Users of This Machine	D029-7907
Operating Instructions Notes On Security Functions	D0857809
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std.2600.1-2009	D3817500
VM Card Manuals	D377-7500
Help(83NHAQENZ)	Ver.1.20
Manuals DataOverwriteSecurity Unit Type H/I	D377-7900A
Notes for Users	D377-7250

[English version-4] (OEM Product attached documents for Europe)

Document Name	Version
Quick Reference Copy Guide	D092-7714
Quick Reference Fax Guide	D509-8534
Quick Reference Printer Guide	D381-7303
Quick Reference Scanner Guide	D381-7309
Manuals for This Machine	D092-7704
Safety Information for MP 4001/MP 5001	D092-7701
Notes for Users	D092-7726A
App2Me Start Guide	D085-7904B
Manuals for Users MP 4001/5001 Aficio MP 4001/5001 A	D092-7510
Manuals for Administrators Security Reference MP 4001/5001 Aficio MP 4001/5001	D092-7512
Manuals for Administrators Security Reference Supplement 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001	D092-7790
Notes for Users	D060-7781
Notes for Users	G189-6785
Notes for Users	D092-7907
To Users of This Machine	D029-7907

Operating Instructions Notes On Security Functions	D0857809
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std.2600.1TM-2009	D3817500
VM card Manuals	D377-7500
Help(83NHAQENZ)	Ver.1.20
Manuals DataOverwriteSecurity Unit Type H/I	D377-7900A
Notes for Users	D377-7250

[English version-5] (Product attached documents for Asian Pacific)

Document Name	Version
MP 4001/MP 5001 MP 4001/MP 5001 Aficio MP 4001/5001 Operating Instructions About This Machine	D092-7755
MP 4001/MP 5001 MP 4001/MP 5001 Aficio MP 4001/5001 Operating Instructions Troubleshooting	D092-7805
Quick Reference Copy Guide	D092-7715
Quick Reference Printer Guide	D381-7307
Quick Reference Scanner Guide	D381-7407
Notes for Users	D092-7730
App2Me Start Guide	D085-7906B
Manuals for Users MP 4001/5001 Aficio MP 4001/5001	D092-7506
Manuals for Administrators MP 4001/5001 Aficio MP 4001/5001	D092-7508
Manuals for Administrators Security Reference Supplement 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001	D092-7790
Notes for Users	D060-7781
Notes for Users	G189-6775
Notes for Users	D092-7905
To Users of This Machine	D029-7904
Operating Instructions Notes On Security Functions	D0857810
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std.2600.1TM-2009	D3817501
VM Card Manuals	D377-7500
Help(83NHAQENZ)	Ver1.20
Quick Reference FAX Guide	D509-8535
Manuals DataOverwriteSecurity Unit Type H/I	D377-7900A
Notes for Users	D377-7250

7. Evaluation conducted by Evaluation Facility and results

7.1 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance components in CC Part 3. Details for evaluation activities are reported in the Evaluation Technical Report. In the Evaluation Technical Report, it explains the summary of the TOE, the content of evaluation and verdict of each work unit.

7.2 Overview of Evaluation Activity

The history of evaluation conducted was presented in the Evaluation Technical Report as follows.

Evaluation has started on 2010-06 and concluded by completion of the Evaluation Technical Report dated 2011-03.The evaluator 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 evaluator directly visited the development and manufacturing sites on 2010-07, 2010-08, 2010-09, 2010-10 and 2010-11, and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff interview.

Because the same level of security has been verified by the evaluation process of the alternative evidence, the site visit of a part of development sites hasn't been done.

Further, the evaluator executed the sampling check of the developer testing and the evaluator testing by using developer testing environment at developer site on 2010-12.

7.3 IT Product Testing

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

7.3.1 Developer Testing

The evaluator evaluated the integrity of the developer testing that the developer executed and the testing documentation of actual testing results. It explains the content of the developer testing evaluated by the evaluator as follows.

(1) Developer Testing Environment

Figure 7-1 shows the testing configuration used by the developer and Table 7-1 shows the main configurations.

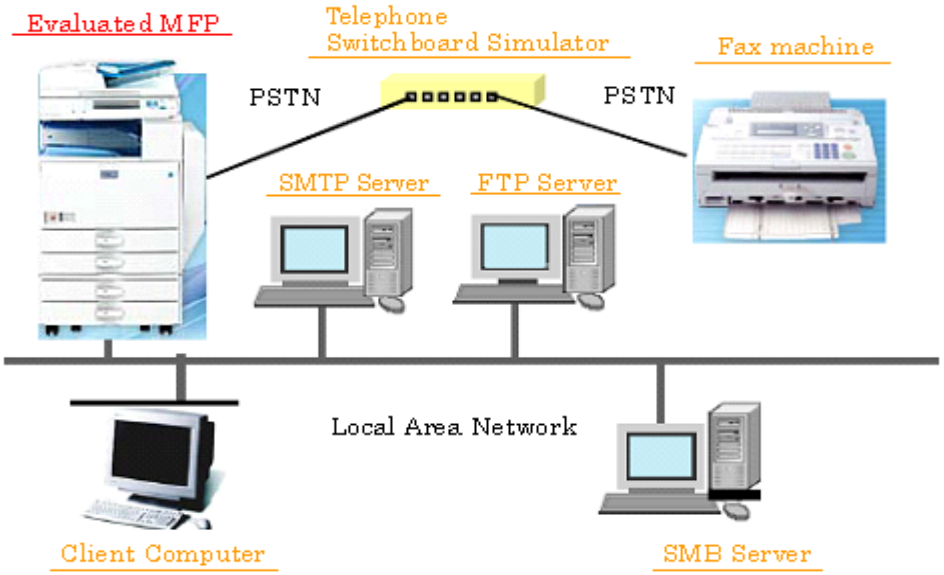

Figure 7-1 Configuration of the Developer Testing

Table 7-1: Test Configurations

Configuration Item	Detail
TOE	- Ricoh Aficio MP 4001 - Ricoh Aficio MP 5001 Version - Software System/Copy 1.02 Network Support 7.34 Scanner 01.24 Printer 1.01 Fax 02.00.00 RemoteFax 02.00.00 Web Support 1.04 Web Uapl 1.02 Network DocBox 1.00 animation 1.3 Option PCL 1.03 OptionPCLFont 1.01 Engine 1.00:01 OpePanel 1.08 LANG0 1.07 LANG1 1.07 - Hardware Ic Key 1100 Ic Hdd 01 - Options Data Erase Opt 1.01m GWFCU3-19(WW) 02.00.00
Client Computer	OS: Windows XP Pro SP3/Windows Vista Business SP1 Web browser: Internet Explorer 6.0/7.0/8.0 Printer driver: PCL6 Driver Ver. 1.0.0.0 PC Fax driver: LAN FAX Driver Ver.1.6.2
SMTP Server	SMTP Server Function of Windows Server 2003 SP2
FTP Server	FTP Server Function of Windows Server 2003 SP2
SMB Server	SMB Server Function of Windows Server 2003 SP2
Fax Machine	Aficio C3501 (MFP provided by RICOH with Fax Function was used.)
Telephone Switchboard Simulator	TLE-101III (AVM GmbH)

Although TOEs (2 models of MFPs) used in the developer testing are some models of several MFPs that are identified in the ST, the other models are OEM products of MFP used in the testing. They are the same models but have different product names. There is some difference of the print speeds between the two models that were tested; however, their Security Functions are identical.

As mentioned above, the two models of "Ricoh Aficio MP 4001" and "Ricoh Aficio MP 5001" selected as the targets for the developer testing are consistent with the descriptions in the ST and cover the TOE configurations identified in the ST. Therefore, the developer testing is executed in a TOE testing environment with the same TOE configuration as that identified in this ST.

(2) Summary of Developer Testing

Summary of the developer testing is as follows.

(a) Developer Testing Outline

Outline of the developer testing is as follows.

<Developer Testing Approach>

The testing approaches consisted of stimulating the assumed external interfaces (Operation Panel, Web browser, and etc.) in normal use of the TOE, and visually observing the results. The other approaches consisted of analysing the generated audit log and the logging data for debug, and checking the communication protocols between client computers/each server and the TOE with packet capture. And, tests such as the following were also executed: a test simulating abnormal events, such as an invalid TSF implementation.

<Content of execution of the developer testing>

The expected values of testing results described in testing specifications which are provided in advance by the developer were compared to the values of the actual developer testing results described in the testing result reports which are also provided by the developer. As a result, it was found that the values of the actual testing results are in conformity to those of the expected testing results.

(b) Scope of Execution of the Developer Testing

The developer testing is executed about 645 items by the developer.

By the coverage analysis, it was verified that all security functions and external interfaces described in the functional specification had been tested.

By the depth analysis, it was verified that all the subsystems and subsystem interfaces described in the TOE design had been sufficiently tested.

(c) Result

The evaluator confirmed an approach of the executing developer testing and legitimacy of tested items, and confirmed consistencies between testing approach described in the testing plan and actual testing approach.

The evaluator confirmed consistencies between the testing results expected by the developer and the actual testing results executed by the developer.

7.3.2 Evaluator Independent Testing

The evaluator executed the sample testing to reconfirm the execution of the security function by testing items extracted from the developer tests, and the evaluator executed evaluator independent testing (hereinafter referred to as "the Independent Testing") to gain further assurance that security functions are certainly implemented, based on the evidence shown by the process of the evaluation.

The independent testing executed by the evaluator is explained below.

(1) Independent Testing Environment

The configuration of the testing executed by the evaluator was the same as the configuration of the developer testing as shown in Figure 7-1.

(2) Summary of Independent Testing

Summary of the Independent testing is as follows.

(a) Independent Testing Points of View

The points of view for the independent testing that the evaluator designed from the developer testing and the provided evaluation evidence materials are shown below.

<Independent Testing Viewpoints>

1. For TSFI that has many types of input parameters and to which the developer testing is insufficient from viewpoints of completeness, the testing items such as parameter scheme, boundary values, and abnormal values are added.
2. For execution timing of several TSFs and combination of execution, the testing items to which conditions are added are executed.
3. The testing items to which the different variation from the developer testing is added are executed in procedures of exception and cancellation.
4. The testing items are selected in the sampling testing from the following viewpoints:

   - The testing items are selected to include all of TSFs and TSFIs to meet the completeness.
   - The testing items are selected to cover the different testing approaches and testing environments.
   - From the point of view to make the test go efficiently, the testing items involving TSFI that meet many of the SFRs are mainly selected.
   - Considering the functionality difference from the similar products that have been CC-certified, the testing items for TSFs which are newly added in this TOE are preferably selected.

(b) Independent Testing Outline

Outline of the independent testing that the evaluator executed is as follows.

<Independent Testing Approach>

In setting the different initialisation and the different parameters from the developer testing, the independent testing approach consisted of stimulating the assumed external interfaces (Operation Panel, Web browser, and etc.) in normal use of the TOE, and visually observing the results. The other approaches consisted of analysing the generated audit log, and checking the communication protocols between client computers by packet capture, or between each server and the TOE.

<Content of Execution of the Independent Testing >

Based on the viewpoints of the independent testing, 14 items for the independent testing and 26 items for the sampling testing are executed.

The outline of the main executed independent testing and corresponding viewpoints are shown in Table 7-2.

Table 7-2: Points of view for the Independent Testing

Points of view for the independent testing	Outline of the independent testing
1	- By changing the access timing, confirmed that the behaviours of the Identification and Authentication Function were as specified when accessed from several interfaces.

2	- Confirmed that the lockout process of accounts was performed as specified while normal users and administrators simultaneously log on. - Confirmed that the Security Functions were performed as specified even if performing parallel several normal functions.
3	- Confirmed that the behaviours were performed as specified when accessing the TOE in the unexpected setting from drivers of client computers. - Confirmed that the behaviours were performed as specified when turning on the power with ejection of the SD Card which was installed in the TOE. - Confirmed that the S/MIME procedure was performed as specified when using the expired certificates.

(c) Result

All the executed independent testing was correctly completed, and the evaluator confirmed the behavior of TOE.

The evaluator confirmed consistencies between the expected behavior and all the testing results.

7.3.3 Evaluator Penetration Testing

The evaluator devised and executed the necessary evaluator penetration testing (hereinafter referred to as "the penetration testing") to test items with the possibility of exploitable vulnerabilities in the assumed environment of use and attack level, based on the evidence shown by the process of the evaluation.

Penetration testing executed by the evaluator is explained below.

(1) Summary of the Penetration Testing

Summary of the penetration testing executed by the evaluator is as follows.

(a) Vulnerability of concern

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

1. Unauthorised access to the TOE may be caused by unintentional network port interfaces.
2. Security Functions may be bypassed if entering data which has the unintentional values and formats of the TOE for interfaces.
3. There are some vulnerabilities when implementing secure channels, resulting in the Security Functions of the TOE may be bypassed.
4. Security Functions may be bypassed by maintaining the TOE overloaded.
5. Security Functions may be bypassed due to the occurrence timing of unexpected

user operations and exceptional events.

6. Security Functions may be bypassed due to the physical operations to the internal board.

(b) Penetration Testing Outline

The evaluators executed the following penetration testing to identify possibly exploitable vulnerabilities.

< Penetration Testing Environment>

The penetration testing configuration is identical with those of the developer testing shown in Figure 7-1.

Table 7-3 shows tools used by the penetration testing.

Table 7-3: Penetration Testing Tools

Name(Version)	Outline
Paros (3.2.13)	Inspection tool of Web vulnerabilities with Proxy traffic.
Nmap Zenmap (5.00)	Port Scan Tool
Wireshark (0.99.8)	Packet Capture Tool

<List of Executed Penetration Testing>

Table 7-4 shows vulnerabilities concerned and the content of related penetration testing. The evaluator executed 11 test cases in the following penetration testing to identify possibly exploitable vulnerabilities:

Table 7-4: Outline of Executed Penetration Testing

Points of view for the penetration testing	Outline of the penetration testing
1	Confirmed that the unnecessary network ports were not opened using the port scan tool. And checked no vulnerabilities to unauthorised inputs for available ports.
2	Checked no publicly-known vulnerabilities on Web interfaces to access the TOE. Confirmed that the Security Functions may not be bypassed by the specified URL at the time of connecting to the TOE via a Web browser.
3	Checked no implementation-specific vulnerabilities regarding the encryption communication with SSL and IPsec.
4	Confirmed that the TOE was not unsecured due to the overloaded CPU and insufficient resources.
5	Confirmed that the Security Functions may not be bypassed even if executing the exception procedures for

	hardware such as misfeed, or forcibly disconnecting telephone lines.
6	Confirmed that the Security Functions may not be bypassed even if, in both cases, one FCU that has the different version, and the other FCU that has part of alteration are installed in the TOE.

(c) Result

In the penetration testing conducted by the evaluator, the evaluator could not find the exploitable vulnerability that attackers could exploit who have the assumed attack potential.

7.4 Evaluated Configuration

In this evaluation, the configurations shown in Figure 7-1 were evaluated. IPv4 is used in the network. This TOE will not be used in the configuration which is significantly different from the above configuration components. Therefore, the evaluator determined the configuration of the above evaluation is appropriate.

7.5 Evaluation Results

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

In the evaluation, the following were confirmed.

- PP Conformance:

  2600.1, Protection Profile for Hardcopy Devices,
  Operational Environment A(IEEE Std 2600.1-2009)

  And the TOE conforms to following SFR packages defined in above PP.

  - 2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A
  - 2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A
  - 2600.1-CPY, SFR Package for Hardcopy Device Fax Functions, Operational Environment A
  - 2600.1-FAX, SFR Package for Hardcopy Device Copy Functions, Operational Environment A
  - 2600.1-DSR, SFR Package for Hardcopy Document Storage and Retrieval Functions, Operational Environment A
  - 2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A

- Security functional requirements: Common Criteria Part 2 extended

- Security assurance requirements: Common Criteria Part 3 Conformant

As a result of the evaluation, the verdict "PASS" was confirmed for the following assurance components.

- All assurance components of EAL3 package

- Additional assurance component ALC_FLR.2

The result of the evaluation is applied to the composed by corresponding TOE to the identification described in the Chapter 2.

7.6 Evaluator Comments/Recommendations

The evaluator recommendations for users are mentioned in the following functions:

- The following functions described in the guidance of this TOE are outside the scope of this evaluation:
    - Unauthorised Copy Guard Function
    - Confidential Print
    - Access Control for each administrative role.
      (Device administrator, user administrator, network administrator, file administrator)
    - IP-Fax, and Internet Fax
    - App2Me

Moreover, the following functions related to the maintenance functions that are deactivated in this TOE will be deactivated by the procedure of installation according to the guidance in the TOE.

- @Remote
- RFU (Remote Firmware Update)

8. Certification

The certification body conducted the following certification based on each materials submitted by Evaluation Facility during evaluation process.

1. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.

2. Rationale of evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.

3. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

8.1 Certification Result

As a result of verification of submitted Evaluation Technical Report and related evaluation deliverables, Certification Body determined that the TOE satisfies all components of the EAL3 and components ALC_FLR.2 in the CC part 3.

8.2 Recommendations

As shown in 1.1.3, it is assumed that the use of Maintenance Functions is deactivated as the evaluation environment of this TOE. If the Maintenance Functions are activated and used, the MFPs may not be the TOEs.

Also, the TOE users need to see the descriptions of 4.3 Clarification of Scope and 7.6 Evaluator Comments/Recommendations, and they need to know whether or not the evaluated scope of this TOE and the operational requirement items can be handled in the actual operating environment of the TOE.

9. Annexes

There is no annex.

10. Security Target

Security Target[12] of the TOE is provided within a separate document of this certification report.

Aficio MP 4001/5001 series with DataOverwriteSecurity Unit Type I Security Target
Version 1.00 (March 10, 2011)　RICOH COMPANY, LTD.

11. 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 Functionality

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

HDD	An abbreviation of Hard Disk Drive. In this document, it indicates the HDD installed in the TOE if simply described as "HDD".
IPsec	Secure Architecture for Internet Protocol. A protocol that provides the functions of data tampering prevention and data confidentiality with IP packets traffic using cryptographic technology.
MFP	An abbreviation of a digital multifunctional product.
PSTN	An abbreviation of Public Switched Telephone Networks.
RFU	An abbreviation of Remote Firmware Update. A function to remotely connect to the TOE and update firmware. (This function is not the evaluation assurance.)
S/MIME	Secure / Multipurpose Internet Mail Extensions. A standard for e-mail encryption and digital signatures with a public key system.

The definitions of terms used in this report are listed below.

App2Me	An application for client computers in order to support the MFP operations and settings.
Internet Fax	A function to perform the fax communications with the system of sending or receiving e-mails. It also uses the Internet lines.
IP-Fax	A generic term of Realtime-Internet Fax of RICOH conformant with the International Standard ITU-T T.38. Assigns IP address to a fax that is connected to a telephone line.

LAN-Fax Transmission	One of Fax Functions. A function that transmits fax data and stores the documents using the fax driver on client computers.
@Remote	A function to remotely operate the TOE via the Internet. The purpose of the remote operation is remote failure diagnosis, counter information collection, and toner information collection.(This function is not the evaluation assurance.)
Confidential Print	A function that requires the password entry set in advance when printing the stored documents. (This function is not the evaluation assurance.)
Administrative role	Pre-defined roles that enable administrators to be given. Although the following four types of administrative roles are defined and can be assigned to each of administrator, respectively, this TOE assumes the MFP administrator who is assigned to all the roles. (The access control for each subcategorised administrative role is not the evaluation assurance.) - Device administrator (executes device administration and audit) - User administrator (executes the management of normal user) - Network administrator (executes the network connection management of the TOE) - File administrator (executes the management of user documents and document user list)
Documents	Information for digital image data under the TOE control which is generated by using the functions of Copier, Printer, Scanner, Fax, and Document Server Function. The stored documents in the HDD of the TOE explicitly referred to as "user documents" in this ST. If simply described as "documents", it includes deleted documents, temporary documents and their fragments when copying and printing.
Unauthorised Copy Guard Function	A function to protect the information data from document copy by executing the process that corresponds to detection of peculiar markings printed in the background of the documents. (This function is not the evaluation assurance.)
Maintenance Function	A function to perform maintenance service for machine malfunctions. In this TOE operation, the Service Mode Lock Function is set to "ON" for deactivating this function.
User job	A work where users require the operations for the TOE. The continuous work from beginning to end is regarded as one job. The operations are storing user documents, printing, downloading, and deleting.
Login password	A password corresponding to each login user name.
Number of Attempts before Lockout	The number of failed consecutive attempts to identify and authenticate users that is allowable until locking out the

	users. The MFP administrator can assign 1 to 5 as a setting value at the initialisation of the TOE, which shall not be changed after setting the value.
Login user name	An identifier assigned to each user. The TOE identifies users by this identifier.
Lockout	The state of making the user accounts unavailable.
Lockout time	The time from being locked out to automatically releasing the user accounts. This TOE is set to 60 minutes and maintained by the MFP administrator.

12. Bibliography

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

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

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

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001, (Japanese Version 1.0, December 2009)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002, (Japanese Version 1.0, December 2009)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003, (Japanese Version 1.0, December 2009)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004, (Japanese Version 1.0, December 2009)

[12] Aficio MP 4001/5001 series with DataOverwriteSecurity Unit Type I Security Target, Version 1.00, (March 10, 2011), RICOH COMPANY, LTD.

[13] Aficio MP 4001/5001 series with DataOverwriteSecurity Unit Type I Evaluation Technical Report, Version 2.0, March 11, 2011, Electronic Commerce Security Technology Laboratory Inc. Evaluation Center

[14] IEEE Std 2600.1-2009, IEEE Standard for a Protection Profile in Operational Environment A, Version 1.0, June 2009