Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2010-2-22 (ITC-0292)
Certification No.	C0274
Sponsor	RICOH COMPANY, Ltd.
Name of TOE	Following MFP with Fax Option Japan: MFP: imagio MP 6001 SP, imagio MP 7501 SP Fax Option: imagio FAX Unit Type 18 Overseas: MFP: Ricoh Aficio MP 6001 SP, Ricoh Aficio MP 7001 SP, Ricoh Aficio MP 8001 SP, Ricoh Aficio MP 9001 SP, Savin 9060sp, Savin 9070sp, Savin 9080sp, Savin 9090sp, Lanier LD360sp, Lanier LD370sp, Lanier LD380sp, Lanier LD390sp, Lanier MP 6001 SP, Lanier MP 7001 SP, Lanier MP 8001 SP, Lanier MP 9001 SP, Gestetner MP 6001 SP, Gestetner MP 7001 SP, Gestetner MP 8001 SP, Gestetner MP 9001 SP, nashuatec MP 6001 SP, nashuatec MP 7001 SP, nashuatec MP 8001 SP, nashuatec MP 9001 SP, Rex-Rotary MP 6001 SP, Rex-Rotary MP 7001 SP, Rex-Rotary MP 8001 SP, Rex-Rotary MP 9001 SP, infotec MP 6001 SP, infotec MP 7001 SP, infotec MP 8001 SP, infotec MP 9001 SP Fax Option: Fax Option Type 9001
Version of TOE	MFP Software /Hardware Version : Software System/Copy 1.15 Network Support 8.65 Scanner 01.19 Printer 1.15 Fax 02.00.00 Web Support 1.09 Web Uapl 1.05 Network Doc Box 1.04 Hardware Ic Key 1100 Ic Ctlr 03 FCU Version : GWFCU3-16(WW) 02.00.00
PP Conformance	None
Assurance Package	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.
2010-9-28

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 2
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 2

Evaluation Result: Pass
"Following MFP with Fax Option Japan: MFP: imagio MP 6001 SP, imagio MP 7501 SP Fax Option: imagio FAX Unit Type 18 Overseas: MFP: Ricoh Aficio MP 6001 SP, Ricoh Aficio MP 7001 SP, Ricoh Aficio MP 8001 SP, Ricoh Aficio MP 9001 SP, Savin 9060sp, Savin 9070sp, Savin 9080sp, Savin 9090sp, Lanier LD360sp, Lanier LD370sp, Lanier LD380sp, Lanier LD390sp, Lanier MP 6001 SP, Lanier MP 7001 SP, Lanier MP 8001 SP, Lanier MP 9001 SP, Gestetner MP 6001 SP, Gestetner MP 7001 SP, Gestetner MP 8001 SP, Gestetner MP 9001 SP, nashuatec MP 6001 SP, nashuatec MP 7001 SP, nashuatec MP 8001 SP, nashuatec MP 9001 SP, Rex-Rotary MP 6001 SP, Rex-Rotary MP 7001 SP, Rex-Rotary MP 8001 SP, Rex-Rotary MP 9001 SP, infotec MP 6001 SP, infotec MP 7001 SP, infotec MP 8001 SP, infotec MP 9001 SP Fax Option: Fax Option Type 9001" 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

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "Following MFP with Fax Option Japan: MFP: imagio MP 6001 SP, imagio MP 7501 SP Fax Option: imagio FAX Unit Type 18 Overseas: MFP: Ricoh Aficio MP 6001 SP, Ricoh Aficio MP 7001 SP, Ricoh Aficio MP 8001 SP, Ricoh Aficio MP 9001 SP, Savin 9060sp, Savin 9070sp, Savin 9080sp, Savin 9090sp, Lanier LD360sp, Lanier LD370sp, Lanier LD380sp, Lanier LD390sp, Lanier MP 6001 SP, Lanier MP 7001 SP, Lanier MP 8001 SP, Lanier MP 9001 SP, Gestetner MP 6001 SP, Gestetner MP 7001 SP, Gestetner MP 8001 SP, Gestetner MP 9001 SP, nashuatec MP 6001 SP, nashuatec MP 7001 SP, nashuatec MP 8001 SP, nashuatec MP 9001 SP, Rex-Rotary MP 6001 SP, Rex-Rotary MP 7001 SP, Rex-Rotary MP 8001 SP, Rex-Rotary MP 9001 SP, infotec MP 6001 SP, infotec MP 7001 SP, infotec MP 8001 SP, infotec MP 9001 SP Fax Option: Fax Option Type 9001 MFP Software /Hardware Version : Software System/Copy 1.15, Network Support 8.65, Scanner 01.19, Printer 1.15, Fax 02.00.00, Web Support 1.09, Web Uapl 1.05, Network Doc Box 1.04, Hardware Ic Key 1100, Ic Ctlr 03, FCU Version : GWFCU3-16(WW) 02.00.00" (hereinafter referred to as "the TOE") developed by RICOH COMPANY, Ltd., and evaluation of the TOE was finished on 2010-9-14 by Information Technology Security Center Evaluation Department (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, the assurance requirements for TOE and rationale for sufficiency of those requirements of the TOE are described in ST.

This certification report assumes "the person who managed this TOE" to be a reader. Note that the Certification Report presents the certification result based on assurance requirements 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 are as follows. Refer to Chapter 2 and below for details.

1.1.1 Assurance Package

Assurance package of the TOE requires EAL3.

1.1.2 TOE and Security Functionality

The subject device of this certification is a digital MFP (hereafter "MFP") made by RICOH COMPANY, LTD., and which provides the functions of copier, scanner, printer, and fax (option). However, the target of this certification is a device equipped with the optional Fax Function. This product is used for inputting, storing and outputting document data in the environments which handle office documents in general offices.

This TOE contains the functions to encrypt the document data when storing into the TOE, and the communicating document data when sending out of the TOE, in order to protect the document data from accidental disclosure. Also, in order to allow only the specified users to operate the document data stored in the TOE, the device prevents performing the function to handle the document data and reading and writing the document data. It provides storing, printing, and sending the document data from the trusted TOE.

For managing these Security Functions, this TOE enforces the identification and authentication to prevent TOE users (general user, administrator, and supervisor) from the unauthorised operation of the Security Management Functions and it protects the Security Functions from unauthorised persons by limiting the usage of the Security Management Functions.

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 counters threats with the following Security Functions:

In order to protect the document data as protected assets from viewing and tampering by a third party who is not permitted to use the TOE, the TOE performs user identification and authentication for the TOE users and the TOE also restricts access to the document data and available functions according to user roles. This function enables only users who have been identified, authenticated, and permitted to access the functions of the TOE and the stored document data in the TOE.

When permitted users store document data via internal networks into the TOE, in order to ensure the confidentiality and completeness of the document data during data communications, the device contains functions to encrypt the data between the connected computers and the TOE, and to decrypt the data on client computers and the TOE for communication on the internal network. This enables protection of document data from leakage and tampering by eavesdropping on the internal network from a third party.

As for setting of the Security Functions mentioned above, in order to prevent users without permission to set the functions from changing and stopping the functions, the TOE confirms the user identification of supervisor and administrators and limits to the minimum necessary the Security Functions that can be operated by the supervisor and administrators to avoid the risk of stopping the Security Functions by misuse of privileges.

1.1.2.2 Configuration and Assumptions

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

This TOE is assumed to be used in the environments which handle the office documents in general offices. Also, the TOE is used through operation panel of the TOE, and through printer drivers and Web browsers of client computers which are connected via internal networks and telephone lines, and USB.

Internal networks use IPv4. Server computers such as FTP server, SMB server, and SMTP server and client computers are connected to the internal networks. If connecting the TOE to the internal networks which are connected to the external networks such as Internet, not to attack in the TOE from the external networks through network, install firewalls in the boundaries of the external networks and internal networks and protect the internal networks and the TOE.

Administrators of this TOE have sufficient knowledge to securely operate the TOE and they securely keep the TOE and the operational environment for the TOE. The administrators shall not perform the illegal acts to abuse their own privileges, leak or tamper the document data as protected assets, and to deactivate the Security Functions of the TOE. Also, for general users who use the MFP, provide the necessary advice and attentions to securely operate the TOE.

Supervisor and Customer Engineers have sufficient knowledge to securely operate the TOE. They shall not perform the illegal acts to abuse their own privileges, leak or tamper the document data as protected assets, and to deactivate the Security Functions of the TOE.

1.1.3 Disclaimers

This TOE cannot assure security in the following cases:

- If the settings in the Service Mode Lock Function are disabled, the TOE after that will not be CC-certified.
- In the same way, if the TOE is configured with the following settings, the TOE will not be CC-certified.
  > Use IPv6 protocol
  > Use IP-Fax and Internet Fax Function
  > Use an authentication method other than Basic Authentication
- Fax data that the TOE receives is not a target of this evaluation so it will not be CC-certified.
- Address book data that was stored to SD card as a backup and was restored from a backup are not the target of this evaluation so it will not be CC-certified.
- Although there are "document data and print data sent or received by the TOE" via USB interfaces or telephone lines, leakage or tampering of document data and print data via USB interfaces or telephone lines are not the target of this evaluation. Protection of such data will not be CC-certified.

1.2 Conduct of Evaluation

Evaluation Facility conducted IT security evaluation, and completed on 2010-9 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[13] and Observation Report prepared by the Evaluation Facility and evaluation evidentiary materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure.

Those concerns pointed out by the Certification Body are fully resolved, and 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 the Evaluation Facility and concluded fully certification activities.

2. Identification of TOE

The TOE is identified as follows.

Name of TOE

Following MFP with Fax Option

Japan:
MFP:
imagio MP 6001 SP, imagio MP 7501 SP
Fax Option:
imagio FAX Unit Type 18

Overseas:
MFP:
Ricoh Aficio MP 6001 SP, Ricoh Aficio MP 7001 SP,
Ricoh Aficio MP 8001 SP, Ricoh Aficio MP 9001 SP,
Savin 9060sp, Savin 9070sp, Savin 9080sp, Savin 9090sp,
Lanier LD360sp, Lanier LD370sp, Lanier LD380sp,
Lanier LD390sp, Lanier MP 6001 SP, Lanier MP 7001 SP,
Lanier MP 8001 SP, Lanier MP 9001 SP,
Gestetner MP 6001 SP, Gestetner MP 7001 SP,
Gestetner MP 8001 SP, Gestetner MP 9001 SP,
nashuatec MP 6001 SP, nashuatec MP 7001 SP,
nashuatec MP 8001 SP, nashuatec MP 9001 SP,
Rex-Rotary MP 6001 SP, Rex-Rotary MP 7001 SP,
Rex-Rotary MP 8001 SP, Rex-Rotary MP 9001 SP,
infotec MP 6001 SP, infotec MP 7001 SP,
infotec MP 8001 SP, infotec MP 9001 SP
Fax Option: Fax Option Type 9001

Version of TOE	MFP	Software /Hardware Version :		
		Software	System/Copy	1.15
			Network Support	8.65
			Scanner	01.19
			Printer	1.15
			Fax	02.00.00
			Web Support	1.09
			Web Uapl	1.05
			Network Doc Box	1.04
		Hardware	Ic Key	1100
			Ic Ctlr	03
	FCU Version :		GWFCU3-16(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.

The user can confirm that the installed product is this evaluated TOE by comparing the names and the versions of hardware and firmware that are displayed on the operation panel of the TOE in MFP itself and in Fax Controller Unit, 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 imports the paper documents of users, receives the document data from client computers which are connected via Network, stores the confidential document data into HDD of the TOE, and performs outputting by print and delivery. Therefore, the TOE is a digital MFP with security function regarding receiving, storing, and outputting the document data.

The Security Functions of the TOE protect the stored document data and setting data in the TOE from tampering and leakage by a third party with the user identification and authentication, the access control, and the encryption, and it protects the communication data on the internal network with the communication encryption.

And the Security Functions of the TOE have the functions to confirm that MFP control software is software officially provided by RICOH COMPANY, LTD. and to record as audit logs the events when checking the operation status of the entire TOE, or in the occurrence of security breaches such as consecutive failures of the password entry.

Furthermore, the Security Functions of the TOE have the functions to manage the settings related to the Security Functions, and to record the processing of the Security Functions. Preventing and detecting against the breaches of the usage of the assumed TOE Security Functions protect these implemented Security Functions.

3.1 Security Function Policies

The TOE possesses the Security Functions to counter the threats shown in Subsection 3.1.1 and to meet the organisational security policy shown in Subsection 3.1.2.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The TOE assumes the threats shown in Table 3-1 and provides the functions for countermeasure against them.

Table 3-1 Assumed Threats

Identifier	Threat
T.ILLEGAL_USE	Attackers may read or delete document data by gaining unauthorised access to the TOE though the external TOE interfaces (the operation panel, network interface, USB interface, or SD card interface).
T.UNAUTH_ACCESS	Authorised TOE users may breach the limits of authorised usage and access document data through the external TOE interfaces (the operation panel, network interface, or USB interface).
T.ABUSE_SEC_MNG	Persons not authorised to use Security Management Functions may abuse them.
T.SALVAGE	Attackers may remove the HDD from the TOE and disclose document data.

Identifier	Threat
T.TRANSIT	Attackers may illegally obtain, leak or tamper with document data or print data sent or received by the TOE via the internal network. *Note: The "document and print data sent or received by the TOE" can exist on the USB interface or telephone lines; however, obtaining and tampering with data that is in transit through these media is not considered a threat.
T.FAX_LINE	Attackers may illegally gain access to the TOE through telephone lines.

3.1.1.2 Security Function Policies against Threats

The TOE counters the threats shown in Table 3-1 by the following security function policies.

(1) Countermeasures against the threat T.ILLEGAL_USE

T.ILLEGAL_USE in which attackers may read or delete document data by gaining unauthorised access to the TOE is countered by the user identification and authentication and the audit as follows:

The TOE requires those who attempt to use the functions (hereafter, operators) to enter their user IDs and authentication information (hereafter, password). The TOE then verifies the authenticity of the entered user ID and password. After the TOE verifies the user ID and password, either 1) or 2) happens:

1) If the TOE does not recognise the user ID and password as valid, the TOE prevents the operator from using TOE functions. Operator who is authorised to use the TOE has valid user ID and password, while operator who is unauthorised to use the TOE does not have any valid user ID and password. Therefore, unauthorised operator is regarded as unpermitted user for the TOE and they cannot use the TOE functions.
2) If the TOE recognises the entered user ID and password as valid, it identifies the operator and furthermore, operator role by the user ID. The TOE, in accordance with the operator (hereafter, user) role that is permitted for the TOE usage, allows the usage of the TOE functions.

In order to counter spoofing by entering the user ID and password, the TOE has the following functions:

1) If with the same user ID, the number of consecutive unsuccessful attempts to authenticate reaches the specified Number of Attempts before Lockout, the TOE locks out that user ID (will not authenticate users with that user ID).
2) When requiring registering or changing their passwords, the TOE only accepts passwords that satisfy the conditions of minimum password length and complexity setting for password.
3) Recording the entry of the user ID and password in the audit logs enables to re-detect spoofing by users attempting to enter a user ID and password.

As mentioned above, T.ILLEGAL_USE in which attackers illegally access the TOE and operate the document data is countered by the user identification and authentication and the audit because the unpermitted TOE users cannot use the TOE functions.

(2) Countermeasures against the threat T.UNAUTH_ACCESS

T.UNAUTH_ACCESS, by which authorised TOE users may breach the limits of authorised usage and access document data, is countered by the user identification and authentication and the access control of protected assets.

The TOE, if users request the usage of the TOE functions, in accordance with user roles, checks whether or not the users are authorised to use TOE functions, and grants the permission for using the functions. The available roles for the TOE are as follows:

- General User
- Supervisor
- Administrator

  The administrator has the following roles. These roles are not performed exclusively, so multiple roles can be assigned to one administrator user ID.

  > User Administrator
  > Machine Administrator
  > Network Administrator
  > File Administrator

The following shows the relation between the user roles and the TOE functions and the authorities to access the document data.

1) General User

The general user is permitted to actively use the following MFP Basic Functions and part of the Security Functions:

Basic Functions:

> Copy Function
> Printer Function
> Fax Function
> Scanner Function
> Document Server Function
> Web Service Function
> Management Function

Security Functions:

> Security Management Functions

(Management functions of document data ACL, management functions of general user information, etc.)

The document data is added to the document data ACL. The document data ACL states the general users who can use the document data, and the operational authorities for the document data. The general user who can manage the document is allowed to read, delete the document data, change print settings, and manage the document data ACL depending on whether or not the user is authorised to access the document data shown in Table 3-2. Also, the general user can modify only the document data ACL of the document data only if the user is the document file owner. The general user cannot change the general user ID by using the management functions of the general user. Therefore, the general user cannot manage the document data by modifying the document data ACL of the document data if the other general user is the document file owner.

Table 3-2 Relation between Operational Authorities for the Document Data and the Operation Permission (Document File Owner)

Authorised Operations	Operational Authorities for the Document Data			
	View	Edit	Edit/Delete	Full Control
Read Document Data	X	X	X	X
Delete Document Data	-	-	X	X
Change Print Settings	-	X	X	X
Modify Document Data ACL - Newly create document file users - Delete document file users - Change operational authorities	-	-	-	X

As mentioned above, although a general user is allowed to use the Basic Functions to manage the document data, the scope of operation on document data is restricted by the document data ACL. T.UNAUTH_ACCESS, by which authorised TOE users may breach the limits of authorised usage and access document data, is countered by the user identification and authentication and the access control of protected assets.

2) Supervisor

The supervisor is permitted to actively use the following Basic Functions and Security Functions:

Basic Functions:

> Web Service Function
> Management Function

Security Functions:

> Security Management Functions
(The parts of the Security Management Functions that are permitted for supervisor such as management of administrator information, management of supervisor information, etc.)

The supervisor is a user who can manage the information of the administrator and supervisor. Such information includes the administrator password, supervisor ID and the password.

3) Administrator (File Administrator)

The file administrator is permitted to use the following Basic Functions and Security Functions:

Basic Functions:

> Document Server Function (for deletion only)

> Web Service Function

> Management Function

Security Functions:

> Security Management Function
(The parts of the Security Management Functions that are permitted for administrators (file administrators) such as management of the document data ACL, management of administrator information, etc.)

Whatever the contents of the document data ACL are, the administrator (file administrator) is allowed to delete all the document data and modify all document data ACL (newly create the document file users, delete the document file users, change the operational authorities and document file owners).

As mentioned above, the administrator (file administrator) is allowed to delete the document data of the document server function for all the document data. However, the administrator (file administrator), according to the assumption "A.ADMIN (Conditions of Administrators)", must not illegally exploit their privileges for malicious purposes in the administrator's work. Therefore, in this case, T.UNAUTH_ACCESS, by which authorised TOE users may breach the limits of authorised usage and access document data, is an exception.

4) Administrator (User Administrator, Machine Administrator, and Network Administrator)

The administrator (User Administrator, Machine Administrator, and Network Administrator) is permitted to use the following Basic Functions and the Security Functions:

Basic Functions:

> Web Service Function

> Management Function

Security Functions:

> Security Management Functions
(The parts of the Security Management Functions that are permitted for administrators (user administrators, machine administrators, and network administrators) such as management of administrator information, management of general user information, management of machine control data, etc.)

The administrator (User Administrator, Machine Administrator, and Network Administrator) is a user who manages general user information, audit logs, and network connections.

As mentioned above, T.UNAUTH_ACCESS, by which authorised TOE users may breach the limits of authorised usage and access document data, may be possible for general users. Although all general users are identified and authenticated by the user's ID and password and the scope of operations on the document data are restricted by the document data ACL. Therefore, T.UNAUTH_ACCESS is countered by the user identification and authentication and the access control of protected assets.

(3) Countermeasures against the threat T.ABUSE_SEC_MNG

T.ABUSE_SEC_MNG, in which users not authorised for Security Management Functions may abuse, is countered by the user identification and authentication, the security management, and the audit as follows:

For the identification and authentication of the MFP users, "(1) Countermeasures against the threat T.ILLEGAL_USE", and "(2) Countermeasures against the threat T.UNAUTH_ACCESS" are as described.

According to the roles, users are allowed for the Security Management Function. Users, their roles, and the Security Management Functions permitted for the usage in accordance with the roles are as follows:

1) Management Functions of the Document data ACL

> General User (Document File Owner and Document File User who have the role to authorise the full control)
+ Query Document data ACL
+ Newly create and delete the document file users for the Document data ACL
+ Change the operational authority on the document data of the Document data ACL

> Administrator (File Administrator)
+ Query Document data ACL
+ Newly create and delete the document file users for the Document data ACL
+ Change the operational authority on the document data of the Document data ACL
+ Change the document file owners

2) Management Functions of Administrator Information

> Supervisor
+ Query all administrators' IDs
+ Change all administrators' passwords

> Administrator
+ Query, change, and delete the applicable administrator's ID
+ Newly create the other administrators' IDs
+ Change the applicable administrator's password
+ Query the role of the applicable administrator
+ Delete the role of the applicable administrator (in case of the other administrator who has the administrator role of the applicable administrator)
+ Add the administrator role to the other administrator (only possible for the administrator role assigned to the applicable administrator)

3) Management Function of General User Information

> User Administrator
+ Query, newly create, and delete general user's ID
+ Query, newly create, change, and delete general user's password
+ Query, newly create, delete, and change S/MIME User Information
+ Query and modify the Document data default ACL

> General User
+ Query general user's ID
+ Query and change the applicable general user's password
+ Query, newly create, delete, and change S/MIME User Information of the applicable general user
+ Query and modify the Document data default ACL for the applicable general user

4) Management Functions of Supervisor Information

> Supervisor

- + Query and change supervisor's ID
- + Change supervisor's password

5) Management Function of Machine Control Data

> Administrator (File Administrator)
- + Query the date and time of system clock
- + Query Service Mode Lock Function

> Administrator (Machine Administrator)
- + Query and modify Number of Attempts before Lockout
- + Query and modify Settings for Lockout Release Timer
- + Query and modify Lockout Time
- + Query and modify the date and time of system clock
- + Query and modify Lockout Flag of supervisor
- + Query and newly create HDD Encryption Keys
- + Query audit logs and delete all logs
- + Query and modify Service Mode Lock Function

> Administrator (User Administrator)
- + Query and specify Minimum Password Length
- + Query and specify Password Complexity
- + Query the date and time of system clock
- + Query Service Mode Lock Function
- + Query and modify Lockout Flags for general users
- + Query Destination Information for Deliver to Folder

> Administrator (Network Administrator)
- + Query the date and time of system clock
- + Query Service Mode Lock Function

> Supervisor
- + Query the date and time of system clock
- + Query Service Mode Lock Function
- + Query and modify Lockout Flags for administrators

> General User
- + Query the date and time of system clock
- + Query Service Mode Lock Function
- + Query Destination Information for Deliver to Folder

As mentioned above, all the Security Management Functions 1) to 5) properly permit the available functions according to the user role.

Recording implemented actions of the Security Management Functions in audit logs enables re-detection of security breaches for the Security Management Functions as auditable events.

Therefore, T.ABUSE_SEC_MNG, in which users not authorised for Security Management Functions may abuse, is countered by the user identification and authentication, the security management, and the audit.

(4) Countermeasures against the threat T.SALVAGE

T.SALVAGE, by which attackers may remove the HDD from the TOE and disclose document data, is countered by the prevention of disclosing the memory storage data and the audit.

The TOE generates a 256 bit encryption key by using a generation algorithm for the encryption key which conforms to BSI-AIS 31. The TOE uses the generated encryption key and cryptographic algorithm AES that matches and FIPS PUB 197, encrypts the document data, and stores it on the HDD. The TOE decrypts this when loading the document data from the HDD. Furthermore, the TOE checks the validity for the encryption key and performance of the hardware "Ic Ctlr" to process the encryption and decryption at start-up. Finally, the TOE confirms that the processing of the encryption is performed correctly.

Also, recording the results of the encryption key generation and encryption processing in audit logs enables re-detection of security breaches if the encryption key generation and the encryption processing are not correctly performed.

Therefore, T.SALVAGE, by which attackers may remove the HDD from the TOE and disclose document data, is countered by the prevention of disclosing the memory storage data and the audit.

(5) Countermeasures against the threat T.TRANSIT

T.TRANSIT, by which attackers may illegally obtain, leak, or tamper with document data or print data sent or received by the TOE via the internal network, is countered by the protection of the network communication data and the audit.

The TOE uses IPSec Protocol for data communications and encrypts the document data that is delivered to folders between the TOE and FTP server and between the TOE and SMB server.

The TOE uses S/MIME and sends the encrypted document data sent by e-mail from the TOE to client computers.

The SSL protocol is used for communication between the TOE and a client computer when connecting via an internal network and accessing the Web service of the TOE. The SSL protocol is also used when sending and printing print data from a client computer to the TOE via an internal network and also when sending document data by fax from a client computer via an internal network. The TOE encrypts the communication including the document data or the print data.

As mentioned above, communication for the Web service, document data, and print data are encrypted in order to prevent leakage and tampering. However, the document data and the print data sent or received via a USB interface or telephone line by the TOE are not regarded as a threat of leakage and tampering.

Also, recording implemented action of the above-encrypted communication in audit logs enables re-detection of security breaches if the encryption communication is not correctly performed.

Therefore, T.TRANSIT, by which attackers may illegally obtain, leak or tamper with document data or print data sent or received by the TOE via the internal network, is countered by the protection of the network communication data and the audit.

(6) Countermeasures against the threat T.FAX_LINE

T.FAX_LINE, by which attackers may illegally gain access to the TOE through the telephone line, is countered by the intrusion prevention via telephone lines and the audit.

The TOE, only if the type of data received from the telephone line connected to a fax device is fax data, transfers the received data from fax process of the fax unit to fax reception process of the controller board.
Also, recording implemented actions of intrusion prevention via telephone lines in audit logs enables re-detection of security breaches if the intrusion prevention via telephone lines is not correctly performed.

Therefore, T.FAX_LINE, by which attackers may illegally gain access to the TOE through telephone lines, is countered by the intrusion prevention via telephone lines and the audit.

3.1.2 Organisational Security Policy and Security Function Policies

3.1.2.1 Organisational Security Policy

Organisational security policy required in use of the TOE is shown in Table 3-3.

Table 3-3 Organisational Security Policy

Identifier	Organisational Security Policy
P.SOFTWARE	In order to prove the trusted MFP Control Software for consumers, measures are provided for verifying the integrity of MFP Control Software in the TOE.

3.1.2.2 Security Function Policies to Organisational Security Policy

The TOE provides the Security Functions to meet the Organisational Security Policy shown in Table 3-3.

(1) Countermeasures against Organisational Security Policy, "P.SOFTWARE".

By verifying the e-signature added to the executable codes of the MFP control software in the TOE can confirm that these executable codes are manufacturer-genuine and officially supplied by RICOH COMPANY, LTD.

Considering the function of verifying the integrity of this software, and checking the version information outputted from the TOE, it is confirmed that the software is a correct version and officially supplied by RICOH COMPANY, LTD.

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 judgment before the assumed reader uses the TOE.

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE.

The effective performance of the TOE Security Functions are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumptions
A.ADMIN	Administrators of this TOE shall have sufficient knowledge to securely operate the TOE, and shall securely keep the TOE and the operational environment for the TOE. Administrators shall not abuse their permission maliciously, and they also shall not illegally act such as leakage or tampering of the document data as protected assets, and deactivating the Security Functions of the TOE. And provide the necessary advice and attentions for general users who use MFP in order to securely operate the TOE. The sufficient knowledge to securely operate the TOE includes the following: No use of the following functions and the settings: - Backup/Restore Address Book - Service Mode Lock set to "Off" - Use of the IPv6 protocol - Use of IP-Fax or Internet Fax Function - Use of Authentication method except for Basic Authentication
A.SUPERVISOR	Supervisor shall have sufficient knowledge to securely operate the TOE, and shall not abuse their permission maliciously. Also, they shall not illegally act such as leakage or tampering of the document data as protected assets, and deactivating the Security Functions of the TOE.
A.NETWORK	When the TOE is connected to the internal network connected to an external network such as the Internet, not for attacking in the TOE by the communication via the external network, install firewalls in the boundaries of the external network and the internal network to protect the internal network and the TOE.

4.2 Environment Assumptions

This TOE is installed in general offices and connected to the internal networks, and it is used by client computers connected to the internal networks likewise.

Figure 4-1 shows the general operational environment as assumptions of this TOE.

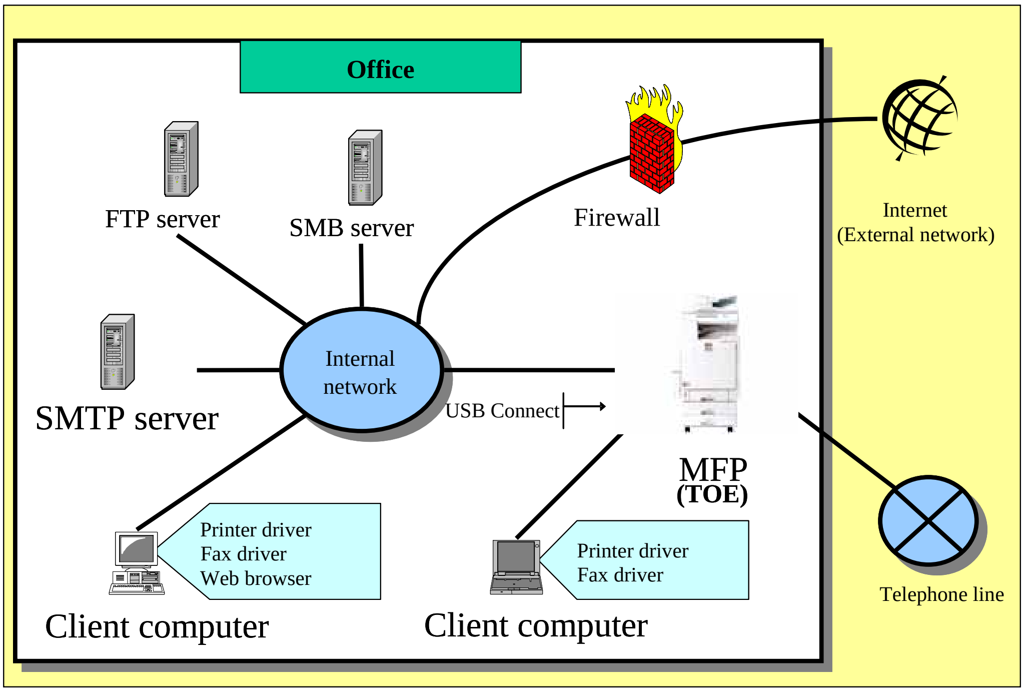

Figure 4-1 Operational Environment and Configuration

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 internal network, telephone lines, and USB.

When the TOE is connected to the internal network connected to an external network such as the Internet, through the network, not for attacking in the TOE by the communication via the external network, install firewalls in the boundaries of the external network and the internal network to protect the internal network and the TOE. The internal network uses IPv4. The internal network is connected to server computers and client computers such as FTP server, SMB server, and SMTP server and it performs the communication of the TOE and the document data.

The operation of the TOE includes both cases of using the operation panel of the TOE and client computers. Installing printer drivers in client computers enables to send the print data into the TOE and process printing via the internal network or USB from client computers. And it enables to send the document data into the TOE via the internal network from client computers and the TOE can send by fax. The Web browser can operate the TOE on client computers.

Also, the TOE can send the document data to client computers by e-mail via SMTP server and can deliver to folders the document data between the TOE and FTP server, and between the TOE and SMB server.

However, the reliability of hardware shown in this configuration and the working software is outside the scope of this evaluation but it is considered of being fully reliable.

4.3 Clarification of scope

Table 4-2 shows the relation of the Basic Functions of the TOE (Copy Function, Pinter Function, Fax Function, Scanner Function, Document Server Function, Management Function, and Web Service Function) and the information of protected assets used by the Basic Functions, and the protection by the Security Functions.

Table 4-2 Information Relation which Basic Functions and Security Functions Regard as Protected Assets

Basic Function	Explanation	Protected Assets	Protection
Copy Function	Scan paper documents using the scanner engine, and print the documents in accordance with the specified print settings using the printer engine. Scanned image data can be stored in the D-BOX as document data (hereafter, "document data (non-Scanner Function)").	Document data (non-Scanner Function)	x
Print Function	Receive print data via the internal network from a client computer, immediately print, or print the data once stored on the HDD. Especially when printing the stored data on the HDD, the received print data is stored as document data (non-Scanner Function) after encrypted in the D-BOX, and the data is printed out after decrypted.	Print data	x
	If receiving the print data via USB from a client computer, it is outside the scope of this evaluation.	Document data (non-Scanner Function)	- (*)
Fax Function (Reception)	Receive fax data from the connected telephone lines, print or store the received fax data on the HDD. Especially when storing on the HDD, this function stores the fax data and converts it to Fax Reception Data and then (after encrypted) stores it in the D-BOX. However, the Fax Reception Data is outside the scope of this evaluation.	Fax Reception Data	- (*)

* Refer to "1.1.3 Disclaimer" and "8.2 Recommendations".

Basic Function	Explanation	Protected Assets	Protection
Fax Function (Immediate Transmission / Memory Transmission)	Scan paper documents using the scanner engine and immediately send by fax via the telephone line, or send by fax via the telephone line once stored in the memory medium. If immediately sending (hereafter, "Immediate Transmission"), after connecting the telephone line to the fax device of the destination fax, perform the sequential transmission of the generated image data to the fax device of the destination fax as it is being scanned. If sending after stored in the memory (hereafter, "Memory Transmission"), connect the fax device of the destination fax to the telephone line and send the image data after scanning originals and being stored in the memory medium.	N/A	X
Fax Function (Stored Documents Fax Transmission)	Decrypt and send the document data (non-Scanner Function) stored in the D-BOX into the fax device of the destination fax via the telephone line. However, after the document data (non-Scanner Function) is sent to the telephone line, it is outside the scope of this evaluation.	Document data (non-Scanner Function)	- (*)
Fax Function (Fax Transmission from Computer)	Receive a print data from a client computer via the internal network, and send the data by fax via the telephone line.	Print data	x
	The case of receiving via USB print data from a client computer is outside the scope of this evaluation.	Print data	- (*)

* Refer to "1.1.3 Disclaimer" and "8.2 Recommendations".

Basic Function	Explanation	Protected Assets	Protection
Fax Function (IP-Fax)	Fax Function (IP-Fax) is outside the scope of this evaluation. Do not use this function.	- (*)	- (*)
Fax Function (Internet Fax Function)	Fax Function (Internet Fax Function) is outside the scope of this evaluation. Do not use this function.	- (*)	- (*)
Scanner Function (Scan)	Scan paper documents using the scanner engine and then send the scanned data by e-mail. The scanned image data is encrypted and will be sent as an e-mail attachment to a specified e-mail address.	E-mail	X
	Scan paper documents using the scanner engine and then send the scanned data to the specified folder of the FTP server or SMB server by using the encrypted FTP or SMB protocol.	FTP or SMB communication	X
	Scan paper documents using the scanner engine and then convert the scanned data to document data (only for the Scanner Function). The document data will be encrypted and stored in the D-BOX.	Document data (Only for Scanner Function)	X
Scanner Function (Administration)	After decrypting the document data (only for the Scanner Function) stored in the D-BOX, the decrypted data is encrypted and will be sent as an e-mail attachment to a specified e-mail address.	E-mail	X
	After decrypting the document data (only for the Scanner Function) stored in the D-BOX, the decrypted data will be sent to the specified folder of FTP or SMB server by using the encrypted FTP or SMB protocol.	FTP or SMB communication	x

* Refer to "1.1.3 Disclaimer" and "8.2 Recommendations".

Basic Function	Explanation	Protected Assets	Protection
	After decrypting the document data (only for the Scanner Function) stored in the D-BOX, the Web browser of a client computer will download the data by the encrypted communication via the internal network.	Web communication	x
Document Server Function (Scan)	Scan paper documents using the scanner engine, encrypt and store the documents as document data (non-Scanner Function) in the D-BOX. Cannot use "document data (only for Scanner Function)" which is encrypted and stored in the D-BOX by "Scanner Function (Scan)".	Document data (non-Scanner Function)	x
Document Server Function (Management)	Decrypt and print the document data (non-Scanner Function) stored in the D-BOX.	Document data (non-Scanner Function)	x
	After decrypting the document data (non-Scanner Function) stored in the D-BOX, the Web browser of a client computer will download the data by the encrypted communication via the internal network.	Web communication	x
	Encrypt and print the fax reception data stored in the D-BOX. However, the Fax Reception Data is outside the scope of this evaluation.	Fax Reception Data	- (*)
Management Function	Configure the following settings: TOE machine settings, network connection settings, authorised user information settings, and settings for information to restrict the usage of document data. The user's ability to manage this information is determined in accordance with the user role of the authorised TOE user (general user, administrator, or supervisor).	Setting information	x

* Refer to "1.1.3 Disclaimer" and "8.2 Recommendations".

Basic Function	Explanation	Protected Assets	Protection
Web Service Function	Remotely operate the TOE by authorised TOE users (general users, administrators, and the supervisor) using a Web browser running on a client computer. However, this function can only operate the function described in this table from "Copy function" to "Management function". There are some functions that are not available with this function.	Web communication (Command, Document data, etc.)	x

5. Architectural Information

This chapter explains the purpose and the relation on a scope of the TOE and the main component.

5.1 TOE boundary and component

The TOE consists of configuration items shown in Figure 5-1. The TOE is equipped with Fax Unit (FCU) which is an optional product to MFP.

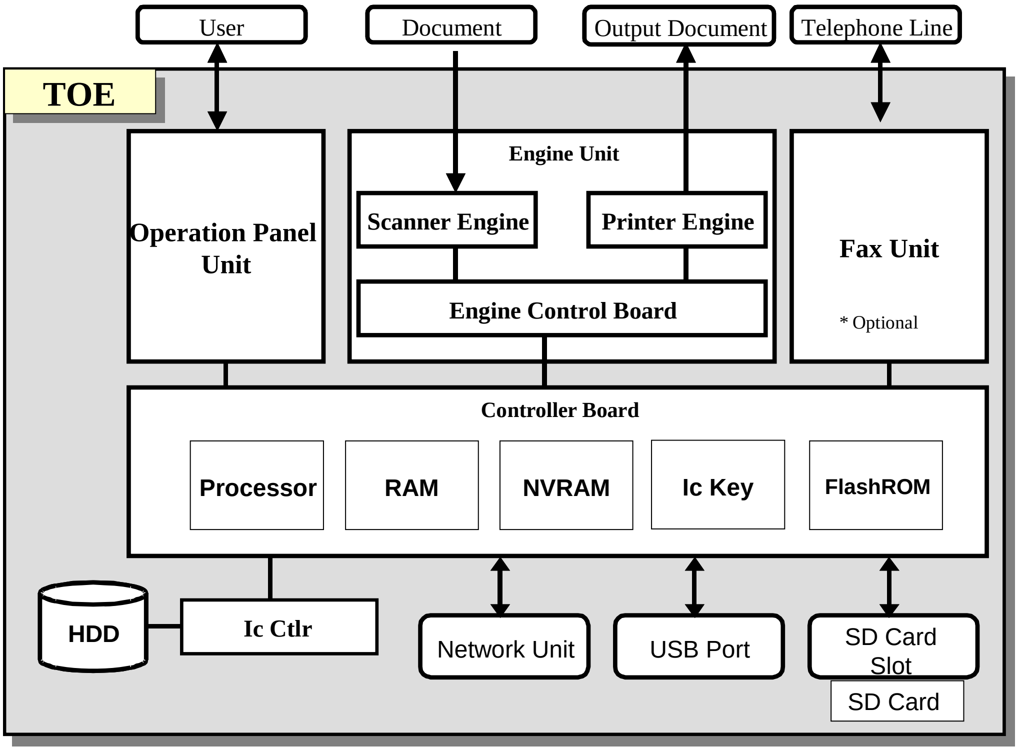

Figure 5.1 TOE boundary

The physical components that constitute the TOE of Operation Panel Unit, Engine Unit, Fax Unit (option), Network Unit, Controller Board, Ic Ctlr, USB port, and SD card slot / SD card are described.

(1) Operation Panel Unit

The Operation Panel Unit (hereafter Operation Panel) is a physical interface device that is installed on the TOE when the TOE users directly operate the TOE. It features key switches, LED indicators, an LCD touch screen, and the Operation Panel Control Board.

(2) Engine Unit

The Engine Unit contains a scanner engine, printer engine and the engine control board. The scanner engine is an input device for reading paper documents. The printer engine is an output device for printing and outputting paper documents.

(3) Fax Unit (optional)

The Fax Unit is a device that has a modem function to send and receive fax data when connected to a telephone line. This TOE is a product equipped with Fax Function (optional).

(4) Network Unit

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

(5) Controller Board

The controller board contains processors, RAM, NVRAM, Ic Key and FlashROM. The Ic Key is a security chip that generates random numbers and encryption keys, and detects any tampering with the MFP control software.

MFP control software is installed in the FlashROM that is on this Controller Board. MFP control software consists of the following software such as System/Copy, Network Support, Fax, Web Support, Web Uapl, and Network Doc Box.

(6) Ic Ctlr

Ic Ctlr is a security chip that encrypts information to be stored on the HDD, and decrypts information to be read from the HDD.

(7) HDD

HDD is a hard disk drive where document data (non-Scanner Function), document data (only for the Scanner Function), print data, fax reception data, user information for identification and authentication, and audit logs are recorded. The area that stores document data (non-Scanner Function), document data (only for Scanner Function), print data, and fax reception data is called D-BOX.

(8) USB Port

The USB port is used to connect a client computer to the TOE, print or fax from the client computer.

(9) SD Card Slot / SD Card

SD card slot is a slot for inserting an SD card installed the MFP Control Software "Scanner" and "Printer". The MFP Control Software works as TOE being read to the MFP. And also Customer engineers use SD card slot for maintenance with SD card. SD card slot is on the side of the TOE and is usually covered by a cover with a screw. The customer engineers remove this cover and insert the SD card for maintenance. The slot is used for the activation of the Stored Data Protection Function and the initial settings to encrypt the HDD when the TOE is installed. No maintenance based on this certification is assumed, so this interface is used only for the installation of the TOE.

5.2 IT Environment

The TOE is connected to the internal network and performs communication with server computers such as FTP server, SMB server, SMTP server, and client computers. Then the TOE performs the communication with client computers connected by USB and the fax device of the destination fax connected via telephone lines.

The TOE performs the document data transmission into server computers such as FTP server, SMB server, and SMTP server that are connected via the internal network.

Client computers that are connected to the TOE via the internal network or USB use the TOE through the printer driver and Web browser. The client computers send and receive document data, They also operate some Management Functions and check the TOE performance through the Web browser.

However, the TOE must not modify the following environments and settings:

- Store and restore an address book data to the SD card.
- Use of IPv6 protocol
- Use of IP-Fax or Internet Fax Function

6. Documentations

The identification of documents attached to the TOE is listed below.

The document attached to this TOE has the following three sets by the difference between the selling area and sales companies. The English version's documents has two kinds from the difference of the region. It explains the difference of those sets as follows. It is the same content except the explained difference.

- Difference in British English and United States English (center : centre, enquirely : inquirely, color : colour)
- Difference of specification method for the paper size
  - > Names of Standard specification, such as A4 and B5 (for Asia for Europe)
  - > Specification by inch (for North America)
- Difference of sample screen (for date or content) illustrated in document
- Difference of description of regulation by country (Describe it dividing the regulation in each region and the country into North America and Europe.)
- Difference number of part and document name

TOE users are required fully understanding and complying with the following documents in order to satisfy the assumptions.

Table 6-1 [Japanese version] Product attachment document for Japan

Document Name	Number of part
imagio MP 9001/7501/6001 series Operating Instructions <About This Machine>	D062-7103
imagio MP 9001/7501/6001 series Operating Instructions <Troubleshooting>	D062-7140A
imagio MP 9001/7501/6001 series Operating Instructions <Copy & Document Server Reference>	D062-7120
imagio MP 9001/7501/6001 series Operating Instructions <Facsimile Reference>	D418-7100
imagio MP 9001/7501/6001 series Operating Instructions <Security Reference>	D062-7150
Operating Instructions Drivers & Utilities imagio MP 9001/9001T/7501/6001	D066-8750A
imagio MP 9001/7501/6001 series Operating Instructions <Notes for Security Functions>	D062-7157
Notes for Administrators: Using this Machine in a CC-Certified Environment	D062-7107

Table 6-2 [English version-1] Product attachment document For North America

Document Name	Number of part
9060/9070/9080/9090 MP 6001/MP 7001/MP 8001/MP 9001 LD360/LD370/LD380/LD390 Aficio MP 6001/7001/8001/9001 Operating Instructions About This Machine	D062-7133
9060/9070/9080/9090 MP 6001/MP 7001/MP 8001/MP 9001 LD360/LD370/LD380/LD390 Aficio MP 6001/7001/8001/9001 Operating Instructions Troubleshooting	D062-7143
9060/9070/9080/9090 MP 6001/MP 7001/MP 8001/MP 9001 LD360/LD370/LD380/LD390 Aficio MP 6001/7001/8001/9001 Operating Instructions Copy and Document Server Reference	D062-7114
Quick Reference Copy Guide	D062-7116
Quick Reference Fax Guide	D418-7105
Quick Reference Printer Guide	D462-7104
Quick Reference Scanner Guide	D462-7124
Manuals for Users 9060/9060sp/9070/9070sp/9080/9080sp/9090/9090sp MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP LD360/LD360 sp/LD370/LD370 sp/LD380/LD380 sp/LD390/ LD390 sp Aficio MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/ MP 8001 SP/MP 9001/MP 9001 SP	D066-7317
Manuals for Administrators 9060/9060sp/9070/9070sp/9080/9080sp/9090/9090sp MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP LD360/LD360sp/LD370/LD370 sp/LD380/LD380 sp/LD390/ LD390 sp Aficio MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/ MP 8001 SP/MP 9001/MP 9001 SP	D066-7318
Notes for Security Functions	D062-7156
Notes for Administrators: Using this Machine in a CC-Certified Environment	D062-7108

Table 6-3 [English version- 2] Product attachment document for Europe

Document Name	Number of part
Manuals for This Machine	D062-7102
Quick Reference Copy Guide	D062-7113
Quick Reference Fax Guide	D418-7103
Quick Reference Printer Guide	D462-7102
Quick Reference Scanner Guide	D462-7122
Manuals for Users MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP Aficio MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/ MP 8001 SP/MP 9001/MP 9001 SP A	D062-7000
Manuals for Administrators Security Reference MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP Aficio MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/ MP 8001 SP/MP 9001/MP 9001 SP	D062-7002
Notes for Security Functions	D062-7156
Notes for Administrators: Using this Machine in a CC-Certified Environment	D062-7109

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 the evaluation and verdict of each work unit.

7.2 Overview of Evaluation Activity

The history of evaluation conducted was present in the Evaluation Technical Report as follows. Evaluation has started on 2010-2 and concluded by completion the Evaluation Technical Report dated 2010-9. 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 Evaluation Facility directly visited the development and manufacturing sites on 2010-4, 2010-5 and 2010-6, 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 TOE is product intended for the United States, Europe and Asia, TOE is manufactured and distributed from Japan and two or more overseas branches. The evaluator went to branch factories in Japan, the United States, Europe and Asia where the investigation was necessary, and conducted the investigation to note manufacturing and the assembly process of TOE across two or more branches.

Further, the evaluator executed the sampling check of the developer testing and the evaluator testing by using developer testing environment at developer site on 2010-6.

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

7.3 IT Product Testing

The evaluator confirmed the validity of the developer testing. By the evidence in the evaluation process and that 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. The following explains the content of the developer testing evaluated by the evaluator.

1) Developer Testing Environment

Figure 7-1 shows the testing configuration executed by the developer.

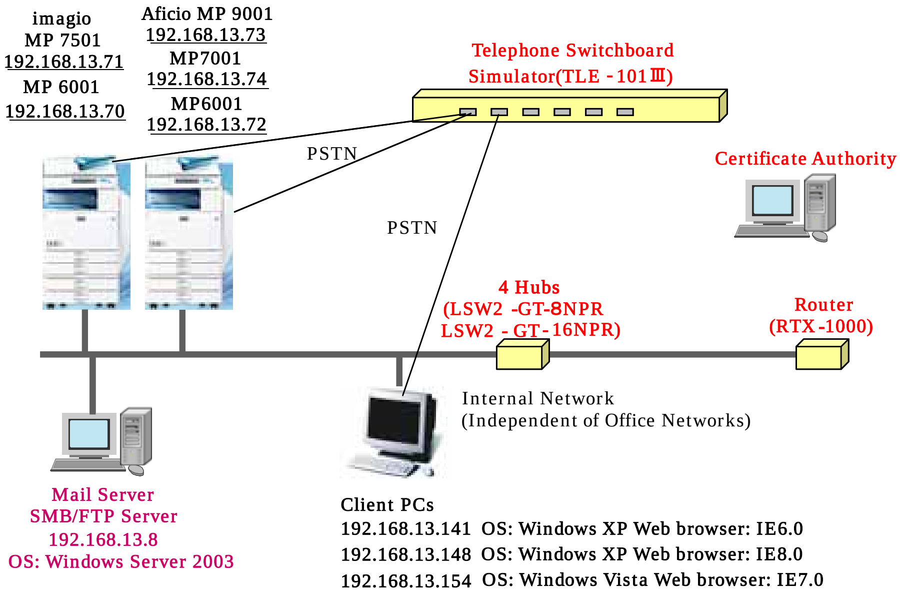

Figure 7-1 Developer Testing Configurations

The TOEs for the evaluation are machines for domestic (imagio MP 7501 SP, imagio MP 6001 SP) machines for oversea(Aficio MP 9001 SP, Aficio MP 7001 SP, Aficio MP 6001 SP).
The TOE targets include the following 34 machines: imagio MP 6001 SP, imagio MP 7501 SP, Ricoh Aficio MP 6001 SP, Ricoh Aficio MP 7001 SP, Ricoh Aficio MP 8001 SP, Ricoh Aficio MP 9001 SP, Savin 9060sp, Savin 9070sp, Savin 9080sp, Savin 9090sp, Lanier LD360sp, Lanier LD370sp, Lanier LD380sp, Lanier LD390sp, Lanier MP 6001 SP, Lanier MP 7001 SP, Lanier MP 8001 SP, Lanier MP 9001 SP, Gestetner MP 6001 SP, Gestetner MP 7001 SP, Gestetner MP 8001 SP, Gestetner MP 9001 SP, nashuatec MP 6001 SP, nashuatec MP 7001 SP, nashuatec MP 8001 SP, nashuatec MP 9001 SP, Rex-Rotary MP 6001 SP, Rex-Rotary MP 7001 SP, Rex-Rotary MP 8001 SP, Rex-Rotary MP 9001 SP, infotec MP 6001 SP, infotec MP 7001 SP, infotec MP 8001 SP, infotec MP 9001 SP. See below for different names assigned to these models:

- Because of different sales areas or companies, these models have different names, but the TOE configurations and Security Functions are identical. (imagio MP, Ricoh Aficio MP, Savin, Lanier LD, Lanier MP, Gestetner MP, nashuatec MP, Rex-Rotary MP, infotec MP)
- The figures in the TOE names indicate print speeds only ("9001/8001/7501/7001/6001": "9001" means 90 sheets per minute, "8001" means 80 sheets per minute, "7501" means 75 sheets per minute, "7001" means 70 sheets per minute, and "6001" means 60 sheets per minute. "9090/9080/9070/9060": "9090" means 90 sheets per minute, "9080" means 80 sheets per minute, "9070" means 70 sheets per minute, and "9060" means 60 sheets per minute. "360/370/380/390": "360" means 60 sheets per minute, "370" means 70 sheets per minute, "380" means 80 sheets per minute, and "390" means 90 sheets per minute.). The TOE configurations and Security Functions of machine models with different TOE names are identical.

As targets of the testing, the TOE of domestic models (imagio MP 7501 SP, imagio MP 6001 SP) and of overseas models (Aficio MP 9001 SP, Aficio MP 7001 SP, Aficio MP 6001 SP) are selected. The developer is afraid of some differences of testing results by the different print speeds selected the above models. Because the difference other than that is only the naming. Depending on this combination, all 34 machine models can be regarded as the same case of conducting the testing which considered the difference.

Table 7-1 explains non-TOE configuration items in the developer testing.

Table 7-1 Developer Testing Configuration Items

Configuration Item	Detail
Client Computer (3 machines)	Web browser - Internet Explorer 6.0 (IE6) - Internet Explorer 7.0 (IE7) - Internet Explorer 8.0 (IE8) Driver - For domestic models: RPCS driver V8.02 PC Fax driver V1.61 - For oversea models: PCL 6 driver V1.1.0.0 or V1.0.0.0 LAN Fax driver V1.61
Mail Server	SMTP Server Function of Windows Server 2003 SP2
FTP Server	FTP Server Function of Windows Server Function 2003 SP2
SMB Server	SMB Server Function of Windows Server Function 2003 SP2
Fax Device	Ricoh imagio MP 6001 SP, Ricoh Aficio MP 9001 SP
Telephone Switchboard Simulator	TLE-101 III (manufactured by LSI JAPAN Co., Ltd.)
Certification Authority Server	Linux (Fedora 8)

The developer testing is executed in the same TOE testing environment as TOE configuration identified in 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 procedure consisted of stimulation of the external TOE interface by the assumed TOE operations (operations of the operation panel, the client computer connected via the internal network or USB, and fax machines) and visual observation of the results. And the vulnerability in the Web interface of TOE was investigated with a vulnerability detection tool of the Web application. However, if not visually observing the testing results, the following approaches were used instead:

- The communication over the internal network captures data and it verifies the communication protocol (SSL and IPSec) using packet capture software.

- Use internal tools that produce debug information and check the activity inside the TOE from output debug information.
- Replace the MFP Control Software with software that had "compromised validity", use internal tools that produced debug information, and verify the integrity of the MFP Control Software Validity Checking Function from the outputted debug information.

<Tools for The Developer Testing>
Table 7-2 shows the tools used in the developer testing. "Debugging console to monitor the TOE internal operation" and "SD card for changing or overwriting the internal configuration items of the TOE" are developed by the developer and are used after confirming that they are normally operated.

Table 7-2 Tools for the Developer Testing

Name of tool	Outline and purpose of use
WireShark 1.0.2	Tool to obtain or monitor packets over LAN (software)
Zenmap 4.68	Tool to investigate the status of using the communication port of computer connected to network (software)
Debugging console to monitor the TOE internal operation	A debugging console to monitor the TOE internal operation is software installed in the computer. This tool was developed by RICOH COMPANY, LTD. for testing and is not publically available. The computer with the installed debugging console and the controller board for the TOE were connected by special serial connectors and a special debugging serial cable. This tool was used to specify necessary testing items to check TOE internal operations.
SD card for changing or overwriting the internal configuration items of the TOE	The SD card stores programs and data for testing that performs changing and overwriting the internal configuration items of the TOE, which were developed in accordance with the testing items. This tool was used to specify necessary testing items to check TOE internal operations.

<Content of execution of the developer testing>
The values of testing plans expected in advance that is described in the expected testing results of individual testing specifications which are evidentiary materials provided by the developer was compared with the values of the developer testing results described in the notes of the individual testing items (judgments) of the individual testing result reports which are evidentiary materials provided by the developer as well. As a result, it was found that the expected results are consistent with the actual testing results of testing evidentiary materials.

b. Scope of Execution of the Developer Testing
The developer testing is executed about 516 items (1011 cases) 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 subsystems and subsystem interfaces indicated in the TOE design had been tested enough.

c. Result

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

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.

7.3.2 Evaluator Independent Testing

The evaluator executed the evaluator independent testing to reconfirm that Security Functions are certainly implemented from the evidence shown by the process of the evaluation. The following explains the evaluator independent testing executed by the evaluator.

1) Evaluator Independent Testing Environment

Figure 7-2 shows the evaluator independent testing configuration executed by the evaluator.

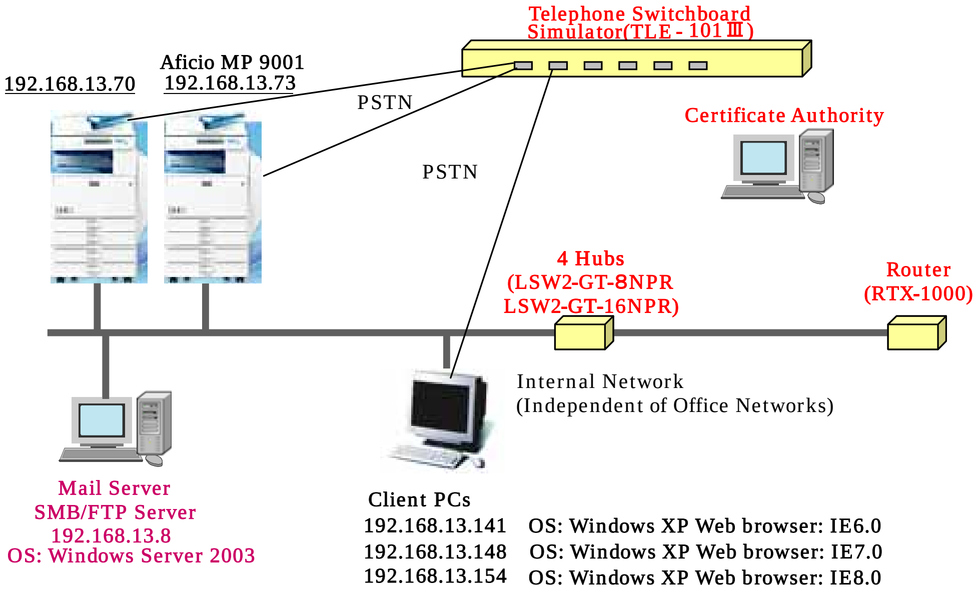

Figure 7-2 Evaluator Independent Testing Configurations

The testing models included in the TOE are imagio MP 6001 SP and Aficio MP 9001 SP. Because in this evaluator independent testing, depending on the different print speeds, there are no concerns in which the difference occurs as the result of the evaluator independent testing. The above configuration is determined. The non-TOE configuration items in the configuration of the evaluator independent testing are identical to the configuration of the developer testing except for client computers equipped with Internet Explorer 7.0 (IE7). However, it was found that the operation of Internet Explorer 7.0 (IE7) has no difference by the difference of OS equipped with client computers. Therefore, the configuration of the evaluator independent testing is regarded as the one of the developer testing.

The evaluator independent testing is executed in a TOE testing environment with the same TOE configuration as that identified in this ST.

2) Summary of Independent Testing

Summary of the Evaluator Independent testing is as follow.

a. Independent Testing Viewpoints

<Independent Testing>
The evaluator independently devised 40 testing items in the following viewpoints by the developer testing and the evidentiary materials provided:

- (Viewpoint 1) To make the testing conducted by the developer more rigorous, execute additional tests based on new parameters and conditions
- (Viewpoint 2) As for characteristic Security Functions for protecting communication (SSL, IPSec, S/MIME), execute supplemental tests to ensure these functions always work effectively.

<Sampling Testing>
To take these viewpoints into account and to test the Security Functions and interfaces, 195 items were identified for sampling testing of the developer testing.

- Testing will be enforced for the following behaviours, which are essential to verify correct operations of the Security Functions.
  > Every possible combination of Access Control Function related to stored documents.
  > Every possible combination of authorised users and authorised Security Management Function operations.
  > Every possible combination of authentication failure conditions.
  > Performance of all functions related to verification of software validity.
  > Checking functions for password strength.
  > The Lockout and Lockout Release functions following password authentication failure.
  > The encryption functions on stored documents.
  > The Self-Test Function for encryption at TOE initialisation.
  >The Network Communication Protection Function.

- Testing covered the verification of audit log completeness and verification of the audit log records obtained.
- Testing covered all possible TOE interfaces (operation panel, Web interfaces, etc.)

b. Independent Testing Outline
Outline of the independent testing that the evaluator executed is as follow.

< Independent testing approach>

For (Viewpoint 1) of the independent testing, testing was executed using the same approaches as used in the developer testing. For example:

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

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

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

<Tools for the independent testing>
The independent testing used the tools of Table 7-2 in the developer testing.

<Content of execution of the independent testing >
For evaluator independent testing, 40 items for independent testing and 195 items for sampling testing are specified in Table 7-3 and 7-4.

Table 7-3 Executed Independent Testing

Number	Category name of testing item	Number of testing item
1	Access control (Stored document)	2
2	User authentication	4
3	Lockout	4
4	Password policy	7
5	Password entry	7
6	TSF administration / TSF data administration (via Panel)	3
7	TSF administration / TSF data administration (via WIM)	2
8	IPSec	2
9	SSL / TLS	1
10	S/MIME	4
11	Simultaneous access	4
Total		40

Table 7-4 Executed Sampling Testing

Number	Category name of testing item	Number of testing item
1	Access control (Stored document)	52
2	User authentication	9
3	Lockout	7
4	Password policy	8
5	TSF administration / TSF data administration (via Panel)	32
6	TSF administration / TSF data administration (via WIM)	44
7	IPSec	2
8	SSL/TLS	3
9	S/MIME	3
10	Fax lines intrusion	2

Number	Category name of testing item	Number of testing item
11	Version display	1
12	Logging document data	5
13	Log overflow	2
14	Document operation log	3
15	Stored document deletion	4
16	Password entry	9
17	Confirming the firm validity	3
18	Encryption of HDD data	1
19	Generation of encryption key and update processing	2
20	Firmware configuration mode lock	3
Total		195

c. Result
All the executed evaluator 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 conducted the necessary evaluator penetration testing about the possibility of exploitable concern at assumed environment of use and attack level. The following explains the evaluator penetration testing executed by the evaluator.

1) Summary of the Evaluator 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 evaluator potential vulnerabilities, and then identified the following vulnerabilities which require the penetration testing.

Table 7-5 Anticipated Vulnerabilities

No.	Anticipated Vulnerabilities
V1	When access to the TOE through the Web browser is established, the TOE may be accessed through direct call to the CGI without the procedures of the user identification and authentication.
V2	If a general user is registered with the same user ID as an administrator, administrator roles may be assigned to the general user at login.
V3	Some interfaces may allow access to the TOE's protected assets prior to user identification and authentication through the operation panel or Web browser.
V4	If general user ID and administrator ID cannot be distinguished, and general user can register with the same ID as an administrator, then general user may obtain an administrator privilege.

No.	Anticipated Vulnerabilities
V5	The TOE's USB port may run an unauthorised program that causes disclosure of protected assets. And unauthorised access to the HDD may also be gained through connection of a computer to the TOE's USB port.
V6	If an error occurs during the HDD check at start-up and then the HDD initialisation process starts, the TOE's security may be weakened.
V7	Users accessing the TOE from the operation panel or Web browser at start-up may obtain access before the TOE's Security Functions come into effect.
V8	The TOE may open unnecessary TCP/IP ports, and the ports in use may affect enforcement of SFR.
V9	Vulnerabilities in cross-site scripting and cross-site request forgery.
V10	The TOE may be altered and cause malfunction by removing an SD card where MFP Control Software is stored, and inserting another SD card where the illegal MFP Control Software is stored.

b. Evaluator Penetration testing Outline

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

<Evaluator Penetration Testing Environment>

The testing environment is the same as the environment of the evaluator independent testing. The configuration figure is also the same as the one in Figure 7-2. This environment is assumed that the TOE is securely installed and operated according to "Security Objectives for the TOE" and "Security Objectives for Operational Environment" in this ST. For instance, the attack via networks from the external network such as the Internet is the exception because the unnecessary ports are closed in the boundaries of the external network and the internal network. Under the above conditions, it is assumed that attacks occur using public interfaces and usual available tools by general users and attackers except for administrators.

Table 7-6 shows the difference between the developer testing and evaluator independent testing for evaluator penetration testing. It also shows the tools used.

Table 7-6 Configuration Items for the Evaluator Penetration Testing

Component Item	Details
Computer for Penetration Testing	Hardware: Toshiba dynabook SS RX1
	OS: Windows XP Pro SP3
	Browser: Internet Explorer 8.0 (IE8)
	Software for Port Scan: Zenmap 4.76
	Software for line trace: Wireshark V1.0.6
	Unix Access Tool: Cygwin V2.573.23
	Vulnerability Detection Tool: Paros V3.2.13

<Execution of Penetration testing>

For anticipated vulnerabilities identified in Table 7-5 to search for potential vulnerabilities, Table 7-7 shows the penetration testing that corresponds to this. The evaluator executed the following penetration testing to identify possibly exploitable vulnerabilities.

Table 7-7 Overview of Evaluator Penetration Testing

No.	Overview of Penetration Testing	Anticipated Vulnerability
T1	Checked opened ports.	V8
T2	Executed a scan of the LAN ports and ensured unnecessary ports were not open or opened.	V8
T3	Penetration testing on open ports.	V1
T4	Ensured that unauthorised users cannot access to the OS of the TOE directly via LAN ports from the remote client computer.	V1
T5	Unauthorised access to document files through the Internet.	V3
T6	Ensured that unauthorised users cannot access to document files, even if they specify a URL directly using delivered URL link information.	V3
T7	Obtained information using direct URLs.	V9
T8	Ensured access via URL is denied, even if URLs for protected assets and TOE resources are derived from URLs used by the TOE.	V6, V7
T9	Ensured no access measures to the TOE are usable through the Web interfaces without prior identification and authentication of the user.	V5
T10	Ensured no Security Functions are usable through the Web interfaces without prior identification and authentication of the user.	V2, V3
T11	Ensured no access measures to the TOE are usable through the operation panel without prior identification and authentication of the user.	V4
T12	Checked to stop operating, to display alerts and to request login of machine administrators if a SD card is removed during the MFP start-up and the operation.	V10

c. Result

The executed evaluator penetration testing did not find any vulnerability exploitable by attackers with the assumed attack potential.

7.4 Evaluated Configuration

In this evaluation, the configurations outlined in "7.3.2 Evaluator Independent Testing" and Figure 7-2 were evaluated. The TOE will not be used in the configuration which is significantly different from 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: none
- Security functional requirements: Common Criteria Part 2 Conformant
- 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

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 not mentioned.

8. Certification

The certification body conducted the following certification based on each materials submitted by the 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.

8.1 Certification Result

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

8.2 Recommendations

For TOE operations, the guidelines require that the Service Mode Lock Function is always enabled. If the TOE is operated in the assumed operating environment, it should not be placed in maintenance mode. When administrators release the settings of the Service Mode Lock Function and the TOE operation mode is changed to the maintenance mode, after that, you must note that the TOE become outside the scope of CC-certification.

There are some cases where the TOE is not able to counter threats and it was outside the CC-certified scope for this TOE as described in "1.1.3 Disclaimers". Before purchasing this product, consumers need to be especially cautious and check the expected settings and functions for the product in the operational environment are not duplicated by the settings and functions, which are restricted to the previously-described environment.

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.

imagio MP 7501/6001 series, Aficio MP 9001/8001/7001/6001 series Security Target Version 1.00 (August 31, 2010) 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.

AES	Advanced Encryption Standard (AES Encryption)
BSI-AIS 31	Standard for the hardware random number generation issued by Bundesamt fur Sicherheit in der Informationstechnik (BSI)
D-BOX	Name of the storage area for document data on the HDD.
FCU	Fax Controller Unit
FIPS PUB 197	Federal Information Processing Standards Publication 197
FTP	File Transfer Protocol
HDD	An abbreviation of "Hard Disk Drive". Refers to the HDD installed in the TOE.
Ic Ctlr	A hardware device that encrypts the data to be written on the HDD and decrypts the data to be read from the HDD.
Ic Key	A chip that contains a microprocessor for encryption processing and EEPROM where a private key for secure communication is held. The Ic Key holds the keys for validity authentication and encryption processing, and a random number generator.
IPSec	Secure Architecture for Internet Protocol. A protocol that provides the functions of data tampering protection and data confidentiality of IP packets using cryptographic technology.
MFP	An abbreviation for digital "multi function product".
NVRAM	Non-Volatile Random Access Memory, where MFP Control Data governing MFP operations is stored.
PSTN	Public Switched Telephone Networks
RAM	A volatile memory medium used for image processing.
S/MIME	Secure/Multipurpose Internet Mail Extensions. A standard for e-mail encryption that uses digital signatures and a public key system.
SSL	Secure Sockets Layer. A protocol for secure communication.
USB	An abbreviation of Universal Serial Bus. A serial bus standard for connecting peripherals to computers.

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

Address Book	A database containing general user information for each general user.
Administrator	One of the authorised TOE users who manages the TOE. Administrators are given administrator roles and perform administrative operations accordingly. Up to four administrators can be registered, and each administrator is given one or more administrator roles.

Administrator role
Management Functions given to administrators. There are four types of administrator role: user administration, machine administration, network administration and file administration. Each administrator role is assigned to a registered administrator.

Basic Authentication
The most basic authentication method, it identifies and verifies users accessing through the Internet. It is supported by HTTP as standard, and by many Web servers and browsers. It authorises access by verifying user names and passwords.

Deliver to Folder
A function that sends document data from the TOE to folders on an SMB or FTP server via a network.

Document data
Electronic data sent to the MFP by authorised MFP users who perform either of the following operations.
1. Scanning from paper and digitizing.
2. Received as print data and then converted by the MFP into a format that can be processed by the MFP.

Document data ACL
An "access control list" of general users that is set for each document data.

Document data default ACL
An item of general user information.
The default value that is set for the document data ACL of a new document data to be stored.

Ethernet
A computer network standard. The most common technical standard used in communication networks in offices and homes around the world. There are other Ethernet standards, such as 100BASE-TX or 10BASE-T.

External Networks
Networks that are not managed by the organisation that manages the MFP. Generally indicates the Internet.

File administration
An administrator role assigning responsibility for management of the D-BOX, where document data is stored on the TOE, and management of the document data ACL, which is the list that controls the access to the document data. The file administrator is a person who has the role of file administration.

FTP Server
A server for sending files to a client computer and receiving files from a client computer using File Transfer Protocol.

General user
One of the authorised TOE users who uses the Basic Functions of the TOE.

General user information
A database containing information about general users as data items that include the general user ID, general user authentication information, document data default ACL, and S/MIME user information.

Internal networks
Networks managed by an organisation that has an MFP. Normally refers to an office LAN environment established as the intranet.

Internet Fax
A function that reads a fax original then converts the scanned image to an e-mail format for sending as data over the Internet to a machine with an e-mail address.

IP-Fax
A function that sends and receives document files between two faxes that are directly connected to a TCP/IP network. It can also send document files to a fax that is connected to a telephone line.

IPv4 Protocol
A widely used, standard protocol governing communication of data between computers over the Internet. It employs 32-bit addressing.

IPv6 Protocol
A widely used, standard protocol created to provide increased address space and improved security compared to IPv4. It employs 128-bit addressing.

LAN-Fax Transmission
A function that faxes document data from a client computer via the TOE when the client computer is connected to the TOE via a network or USB Ports.

Lockout
A function that prohibits access to the TOE to the specific user IDs.

Machine administration
An administrator role that assigns responsibility for machine management and performing audits. The machine administrator is a person who has the machine management role.

Memory Transmission
A function that stores scanned data of an original in memory and then dials and faxes that data at a later time.

MFP Control Software
Software installed in the TOE that can identify TOE components such as System/Copy, Network Support, Scanner, Printer, Fax, Web Support, Web Uapl, and Network Doc Box.
Manages the resources for units and devices that comprise the MFP and controls their operation.

Minimum Password Length
The minimum number of digits that can be registered in passwords.

Network administration
An administrator role assigning responsibility for management of the TOE's network connections. The network administrator is a person with network management responsibility.

Operation Panel
A display-input device that consists of a touch screen LCD, key switches, and LED indicators, and is used for MFP operation by users. Also known as an "Operation Panel Unit".

Packet Capture Software
Software that intercepts communications on networks, records them, and reviews the content of communications.

Password Complexity Setting
The minimum combination of character types that can be registered in passwords.
There are four character types: upper-case letters, lower-case letters, numbers, and symbols.
There are Level 1 and Level 2 Password Complexity Setting. Level 1 requires passwords to include a combination of more than two types of character. Level 2 requires passwords to include a combination of more than three types of character.

Print data
The document files in the client computer that are sent to the TOE from a client computer to be printed or faxed. Drivers must be installed in the client computer in advance: a printer driver for printing and a fax driver for faxing.
Print data is received by the TOE through the Network Unit or USB Port.

Print Settings
Print Settings for printed output, including paper size, printing magnification, and custom information (such as duplex or layout settings).

Processor
Hardware that processes the instructions of software in the computer. It has an arithmetic logic unit, a peripheral circuit, and memory units that store instructions or data.

S/MIME User Information
Information about each general user that is required for using S/MIME.
Includes e-mail address, user certificates, and a specified value for S/MIME use.

Sending by E-mail	A function that sends e-mail with attached document data from the TOE.
SMB Protocol	Server Message Block protocol. A standard protocol governing communication of data between computers.
SMB Server	A server for sharing files with a client computer using Server Massage Block Protocol.
SMTP server	A server for sending e-mail using Simple Mail Transfer Protocol.
Stored Data Protection Function	A function that protects document data stored on the HDD from leakage.
Stored Documents Fax Transmission	A function that faxes document data stored earlier in the D-BOX.
Supervisor	One of the authorised TOE users who manages a password of administrator.
User administration	An administrator role assigning responsibility for management of general users. The user administrator is a person who has the user management role.

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 1, September 2006, CCMB-2006-09-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 2, September 2007, CCMB-2007-09-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 2, September 2007, CCMB-2007-09-003

[7] 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)

[8] 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)

[9] 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)

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

[11] 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)

[12] imagio MP 7501/6001 series, Aficio MP 9001/8001/7001/6001 series Security Target Version 1.00 (August 31, 2010) RICOH COMPANY, Ltd.

[13] RICOH COMPANY, Ltd. imagio MP 7501/6001 series Aficio MP 9001/8001/7001/6001 series Evaluation Technical Report Version 1.3, September 14, 2010, Information Technology Security Center Evaluation Department